République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Batna 2
Faculté de mathématiques et d'informatique
Département d'informatique

Thèse

En vue de l'obtention du diplôme de

Doctorat en Informatique

Proposition d'une nouvelle approche sur les méthodes d'authentification

Présentée Par

Noui Oussama

Soutenue le: 18 / 04 / 2016

Membres du jury :

Président:	Bilami Azeddine	Professeur	Université de Batna
Rapporteur:	Noui Lemnouar	Professeur	Université de Batna
Examinateurs:	Ali pacha Adda	Professeur	Université USTO Oran
	Seghir Rachid	MCA	Université de Batna
	Guenda Kenza	MCA	Université USTHB Alger

Algerian People's Democratic Republic
Ministry of Higher Education and Scientific Research

University of Batna 2

Faculty of mathematics and computer science
Computer science department

Thesis

For obtaining the diploma of
Doctorate in Computer Science

Proposition of a new approach to authentication methods

Presented by:

Noui Oussama

Thesis defended on 18 April 2016

Members of the jury:

Président:	Bilami Azeddine	Professeur	Université de Batna
Rapporteur:	Noui Lemnouar	Professeur	Université de Batna
Examinateurs:	Ali pacha Adda	Professeur	Université USTO Oran
	Seghir Rachid	MCA	Université de Batna
	Guenda Kenza	MCA	Université USTHB Alger

Acknowledgements

First, I would love to thank my supervisor, Prof. Noui Lemnouar, Professor at the Mathematics Department of the University of Batna for giving me the honor to be supervised by him during the realization of this thesis. I am grateful for the time he gave me, his educational and scientific qualities, his frankness and sympathy, his ideas and advices. I learned a lot with him and I should send him my gratitude for all that.

I also show all my appreciation to Prof. Bilami Azeddine, Professor at the Computer Science Department of the University of Batna for the honor that he makes to preside this jury.

I sincerely thank Prof. Ali pacha Adda, Professor at the University of Oran, for accepting to judge this work and to be part of my thesis jury.

I sincerely thank Dr. Seghir Rachid MCA at the Computer Science Department of the University of Batna, for the excellent courses that he provided in the master cycle and for accepting to judge this work and to be part of my thesis jury.

I also show all my appreciation and gratitude to Dr. Guenda Kenza, MCA at the University of USTHB for accepting to judge this work and to be part of my thesis jury.

I thank my parents and all my family members who have given me the support and comfort that accompanied me during this path.

This work could not achieve its goals without the contribution of many people whom I extend my deepest thanks.

Abstract

With the development of the usage of Internet, and the revolution of the information and communication technology, our society is becoming more electronically connected, many enterprises and government departments open their information system to their partners or to their suppliers, it is therefore essential to assure security of their information system and to master the control access to resources and the authentication of the users and the transmitted documents in the system.

In this thesis we present a study about the state of the art methods to achieve both content authentication and user authentication, and we present four novel contributions relative to image encryption, digital watermarking for content authentications.

The first contribution consists in developing a secure image encryption scheme based on polar decomposition and chaotic map, which offer good confusion and diffusion qualities, and a large key space to ensure popular security factor and to overcome the weaknesses of the state of the art encryption schemes.

The second contribution is a novel blind robust watermarking scheme which exploits the positive circulant matrices in frequency domain which is the SVD, different applications such as copyright protection, control and illicit distributions have been given. Furthermore the third contribution is a solution for image authentication, it is a blind fragile watermarking algorithm based on polar decomposition and QR code.

Thus the proposed fragile watermarking scheme can be applied as a solution to authenticate medical images, because medical tradition is very strict with the quality of medical images, and it requires a strict authentication solution. Finally we present a solution for ownership protection and deadlock problem using a novel robust watermarking scheme in frequency domain.

Keywords

Cryptography, content authentication, user authentication, digital watermarking.

Résumé

Avec le développement de l'utilisation d'internet et la révolution de la technologie de l'information et de la communication, notre société est de plus en plus électroniquement connectée, de nombreuses entreprises et ministères ouvrent leur système d'information à leurs partenaires ou à leurs fournisseurs, il est donc essentiel d'assurer la sécurité de leur système d'information et de maîtriser le contrôle d'accès aux ressources et de l'authentification des utilisateurs et les documents transmis dans le système.

Dans cette thèse, nous présentons une étude des méthodes d'authentification de contenu et de l'utilisateur, et nous proposons quatre contributions relatives au chiffrement d'image et le tatouage numérique pour l’authentification de contenu. la première contribution consiste à développer un système de cryptage d'image sécurisé basé sur la décomposition polaire et la carte chaotique, qui offrent de bonnes confusion et diffusion, et un grand espace de clé pour assurer la sécurité et surmonter les faiblesses d’autres systèmes de cryptage. La deuxième contribution est un nouveau schéma de tatouage robuste aveugle qui exploite les matrices circulantes positives dans le domaine fréquentiel et la décomposition SVD, différentes applications telles que la protection du droit d'auteur, le contrôle et les distributions illicites ont été donnés, la troisième contribution est une solution pour l'authentification d'images, il s’agit d’un algorithme de tatouage fragile aveugle basé sur la décomposition polaire et le code QR, ainsi le schéma de tatouage fragile proposé peut être appliqué comme une solution pour authentifier les images médicales, parce que la tradition médicale est très stricte sur la qualité des images médicales, et il nécessite une solution d'authentification stricte. Enfin, nous présentons une solution pour la protection de la propriété et pour résoudre le problème de « deadlock » en utilisant un nouveau schéma de tatouage robuste dans le domaine fréquentiel.

Mots clés

La cryptographie, l’authentification de contenu, l’authentification de l'utilisateur, le tatouage numérique.

ملخص البحث

مع تطور استخدام الإنترنت، وثورة تكنولوجيا المعلومات والاتصال، أصبحت مجتمعاتنا أكثر اتصالا الكترونيا ، العديد من المؤسسات والدوائر الحكومية تفتح نظام معلوماتها لشركائها أو لمورديها ، ولذلك فمن الضروري ضمان أمن نظام المعلومات الخاص بها و التحكم في الوصول إلى الموارد والمصادقة على المستخدمين والمستندات التي أحيلت في النظام.

في هذه الأطروحة نقدم دراسة عن الطرق لتحقيق كلا من المصادقة على المحتوى ومصادقة المستخدم، و نقدم أربع مساهمات جديدة في مجال تشفير الصور، والوشم الرقمي لمصادقة المحتوى.

تتمثل أول مساهمة في تصميم نظام آمن لتشفير الصور الإلكترونية على أساس التحليل القطبي وخريطة الفوضى، والتي تقدم بلبلة جيدة وخاصية نشر جيدة ، ومساحة كبيرة لمفتاح التشفير لضمان عوامل الأمن العامة والتغلب على نقاط الضعف التي توجد في مخططات التشفير الأخرى.

المساهمة الثانية هي مخطط جديد أعمى للوشم الرقمي يستغل المصفوفات الدائرية الإيجابية في مجال التردد الذي هوSVD ، قدمت فيه تطبيقات مختلفة مثل حماية حق المؤلف والرقابة والتوزيع الغير مشروع .والمساهمة الثالثة هي حل للمصادقة على الصور، هي خوارزمية للوشم الرقمي عمياء تعتمد على خصائص التحليل القطبي ورمز الاستجابة السريعة، كما يمكن تطبيق مخطط الوشم الرقمي المقترح كحل للمصادقة على الصور الطبية، لأن المجال الطبي حريص على جودة الصور الطبية، ويتطلب حل صارم للمصادقة. وأخيرا فإننا نقدم حلا لحماية الملكية ومشكلة الجمود باستخدام نظام الوشم الرقمي القوي في مجال التردد.

كلمات مفتاحيه

التشفير, المصادقة على المحتوى, مصادقة المستخدم, الوشم الرقمي.

Publications

- Noui Oussama, Beloucif assia, Noui Lemnouar (2015), “Secure image encryption scheme based on polar decomposition and chaotic map”, Int. J. Information and Communication Technology, Vol. X, No. Y, 2015(in press). Inderscience, http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijict

- Oussama Noui and Lemnouar Noui , (2014), “a robust blind and secure watermarking scheme using positive semi definite Matrices”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No 5, October 2014, pp 97-110

- Oussama Noui and Lemnouar Noui,’ A Blind Robust Watermarking Scheme Based On SVD And Circulant Matrices’ Second International Conference on Computational Science & Engineering (CSE - 2014), pp. 65–77, 2014. CS & IT-CSCP 2014

- Oussama, Noui, and Noui Lemnouar. "A Robust Watermarking Scheme for Ownership Protection and Deadlock Prevention." Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication. ACM, 2015.

- Oussama Noui and Lemnouar Noui, ’Blind Watermarking Scheme for Image Authentication’ ,3ème édition de la conférence JEESI’14. Ecole superieur d’informatique ESI (2014).

- Oussama Noui and Lemnouar Noui, « novel digital signature based on matrix reordering problem. », Journées doctorales sur les technologies de l’information et de la communicaion (JDTIC’14) (2014)

Abbreviations and Acronyms

SVD	Singular values decomposition
RFID	Radio frequency identification
MITM	Attack Man in the Middle
OTP	One time password
DSS	Digital Signature Standard
MD	Message digest
SHA	Secure Hash Algorithm
DFT	Discrete Fourier transform
DCT	Discrete cosine transform
DWT	Discrete wavelet transform
dB	decibel
DVD	Digital versatile disk
HVS	Human visual system
JPEG	Joint photographic experts group
LF	low frequency
LSB	Least significant bit
MSE	mean square error
NPCR	number of pixel change rate
PSNR	Peak signal noise ratio
RGB	Red, Green, Blue
UACI	unified average changing intensity
ACM	Association for Computing Machinery
GIF	Graphical Interchange Format
PNG	Portable Network Graphics
TIFF	Tagged Image File Format
BMP	Bitmap
AI	adobe illustrator
PS/EPS	Postscript / Encapsulated Postscript
SVG	Scalable Vector Graphics
PDF	Portable Document Format
PCR	Polymerase Chain Reaction

Table of contents

Part one

Background and tools

<u>Part two</u>

Contributions

List of figures

List of tables

General Introduction

Due the digital revolution in the 20th century, the usages of digital documents have seen a huge increase in all axes, personal, business and in industry. However this development led to new security challenges and requirements, such as copyright protection, digital document authentication, and access control.

Many techniques and solutions have been proposed in the several last years, such as digital watermarking schemes, encryption schemes and authentication protocols in order to achieve the information security.

Information security is mainly divided into four aspects:

· Authentication.

· Integrity.

· Confidentiality.

· Non-repudiation.

Authentication provides assurance of the identity of an object (a person, a server, application).

Integrity service guarantees that an object has not been modified since its creation by someone other than its author (owner). Confidentiality ensures that a document will not be read by a third party who doesn't own the key. Finally, the purpose of non-repudiation is that the sender of a message cannot deny having sent it and the receiver cannot deny receiving it.

These needs were already existed at the distribution of hard copies documents. But the technology is changing fast, and new patterns have been emerged. The documents currently transmitted are mainly electronic and they circulate on the computer networks. It was therefore necessary to create a set of mechanisms to provide various security services for the digital documents and their transfer.

In this thesis we focus on the authentication aspect, which can be categorized into user authentication and content authentication, for user authentication there are three types of methods.

The most used methods are based on what the person knows, as a password, or what he has like a badge or ID card. A third type of methods, more original and based on what he is (fingerprints or the shape of the hand) or what he can do (the handwritten signature or dynamics of keystrokes). This third approach is based on the characteristics of the individual himself, it is called biometrics.

The term "strong authentication" is used when two or more types of methods are combined to perform authentication. For example, access to payment terminals is allowed only on presentation of the card (what we have) and the indication of PIN associated (what we know), recorded on the chip of the card itself.

Nowadays the authentication is a major enabler of electronic commerce over the web. That's because the Internet is an open public network, which anybody, anywhere, can connect to. All they need is a computer and a connection through an Internet service provider.
In any transaction between two persons, if there's anything of significant value being exchanged, each party wants to be aware *who* they're dealing with. If they can't be sure about that, they won't move forward with the transaction.
In the physical world when individuals are in person face to face, that issue is solved with IDs.

On the Internet, the parties doing the transaction can't see each other, and exchanging paper or plastic ID cards isn't an alternative. The person on the other end of a website, email, or IM message could virtually be anybody.

For financial institutions authentication, deciding whether someone who is who they claim they are when entering into a system, is absolutely important since the people logging on are dealing with other people’s money and very sensitive and confidential personal information. Authentication is a key way in which financial institutions maintain security, which is a top priority as breaches are very costly. A recent survey by PwC (PricewaterhouseCoopers, LLP (accounting/consulting firm) found that 45% of financial services organizations had been struck by cyber-attacks, in comparison to 17% of other types of organizations and institutions. For that reason despite being at the brunt of attacks, financial institutions need to do all they can to ensure breaches do not occur, in order to maintain the trust of their customers.

There is a variety of authentication methods available today, with regards to the level of security and accountability for different situations.

This thesis presents four main contributions related to digital watermarking and encryption schemes to achieve the authentication of the digital documents.

Our thesis is divided into two parts, the first part presents the state of the art of authentication methods, and the second part shows our major contributions.

The first part contains three chapters, the first chapter provides related knowledge to the study, such as general overviews on digital images, hash functions and mathematical backgrounds related to image processing and matrix decompositions.

Then in the second chapter we present different methods for content authentication, starting with the handwritten signature, digital signature then digital watermarking.

The third chapter concentrates on user authentication methods: password, Biometric, RFID and zero knowledge.

The second part of this thesis explains our contributions, the first contribution was presented in chapter four, and it is about a novel secure image encryption scheme based on polar decomposition and chaotic map, in the same chapter we have presented a novel effective algorithm for producing an orthogonal matrix from a random vector which has many applications in cryptography.

The fifth chapter presents the second contribution, we introduce a novel blind robust watermarking scheme which exploits the positive circulant matrices in frequency domain which is the SVD, different applications such as copyright protection, control and illicit distributions have been given.

The sixth chapter concerns a strict authentication solution, we proposed a fragile watermarking method for image authentication based on polar decomposition and QR code. Finally in the seventh chapter we present a solution for ownership protection and deadlock problem using a novel robust watermarking scheme in frequency domain.

Part one

Background and tools

Chapter 1 Related knowledge

Introduction

In this chapter we will provide the important related knowledge for our study, we'll start with a general overviews on digital images then explaining the most used hash functions and mathematical backgrounds related to image processing and matrix decompositions.

1. General overview on digital images

1.1 Introduction

"A picture is worth a thousand words.", is a well-known saying which means that the images tend to have more impact than the text because it is easier to ignore the content of the text information than to question the origin and authenticity of a photo.

Since many years, with the explosion of the Internet and also the large-scale development of digital photography, the field of digital image has become a growing field. This chapter provides an introduction to digital images. In this chapter we will talk about some concepts about the image and its different types, a better understanding of the digital image concept helps to better study the image watermarking which is our purpose.

1.2 Image definition

In Latin "the imago" which means "representation, carried, appearance", it is a structured set of information which, after posting on the screen, has a meaning for the human eye. The image is the representation of a being or thing by the graphic or plastic art produced by human hands (drawing, painting, sculpture) or mediation of a device (photography, computer graphics) [1]. An image is a representation of a scene acquired using image production systems (camera, X-rays, CT). The form may be analogic (photography, video) or digital (scanned images according to various formats, compressed images or not).

1.2.1 Digital image

The term digital image means, in its most general sense, any image that has been acquired, processed and stored is coded by digital values. The digital image is composed of a set of discrete points. Each of these points is seen assigned an intensity to define its color.

The scan operation (or digitalization); is an operation that converts an analog image (analog or continuous signal) to a digital or discrete image.

Mathematically: Let Ω be an open bounded of R^2 (we consider the case where Ω is an open rectangle) .We consider an image as a function U: Ω -----> R.

The function U is defined on R^2 but in image processing, we only have access to the discrete values (U (xi, yi)) of this function U [2].

Remark When it comes to digital image, one speaks about pixels (Figure 1.1)

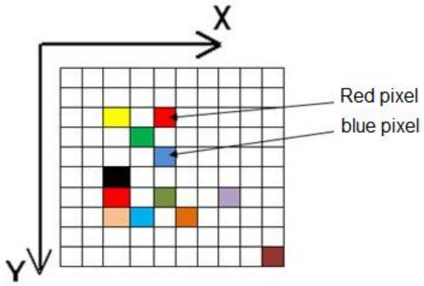


Figure 1-1 Representation of digital image.

A digital image is a collection of pixels each representing a point of the image, coded by numerical values, these values can be scalar (grayscale images) or vectorial (color images).

1.3 Type of images

1.3.1 Bitmap image

The bitmap image is represented by a screen of points which one calls pixels. These are not mathematical formulas which define the forms, but a set of pixels that act like a pointillist painting. [3] It is composed as its name indicates, a matrix (table) of points on several dimensions, each representing a spatial dimension (height, width), or other (resolution level). In the case of two-dimensional images, the dots are called pixels.

Example: A small bitmap image, when we resize it to a ten times bigger image, this can lead to a loss in color quality or sharpness. Then the image becomes distorted (Figure 1.2) [4]

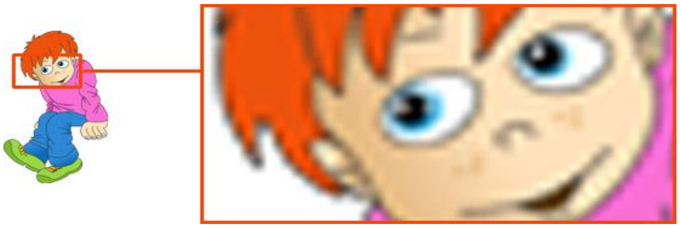


Figure 1-2 Example of bitmap image

1.3.1.1 The characteristics of a bitmap image

The image is a structured set of information characterized by these parameters:

-**The Color coding**

An image is represented by a two-dimensional array in which each cell is a pixel. To represent an image by means of computer, it is sufficient to create an array of pixels in which each cell contains a value. The value stored in a cell is coded on a certain number of bits determining the color or intensity of the pixel, it is called bit depth (sometimes color depth). There are several coding depth standards:

• **Black and white bitmap**: by storing one bit in each cell, it is possible to define two colors (black or white).

• **16 color bitmap or 16 levels of gray**: by storing 4 bits in each cell, it is possible to define 2^4 possibilities of intensities for each pixel, which means 16 gray scales from black to white or 16 different colors.

Bitmap 256 colors or 256 levels of gray: by storing a byte in each box, it is possible to define 2^8 intensities of pixels, 256 gray scales from black to white or 256 different colors.

• **color palette (colormap):** with this method it is possible to define a pallet, or color table containing all the colors that can be contained in the image, each is associated with an index. The number of bits reserved for the coding of each index of the palette determines the number of colors that can be used. Thus by coding the indexes on 8 bits it is possible to define 256 usable colors, which means each case of two-dimensional array representing the image will contain a number indicating an index of the used color. They are called “indexed color image”, whose colors are coded according to this technique.

True color or "real colors": this representation allows to represent an image by defining each component (RGB, for red, green and blue). Each pixel is represented by an integer having the three components, each encoded on a byte, which means a total of 24 bits (16 million colors). It is possible to add a fourth component to add information of transparency or texture, each pixel is then coded on 32 bits.

We can see in the figure below that a color image is actually a combination of three levels of grayscale, each is a base color.

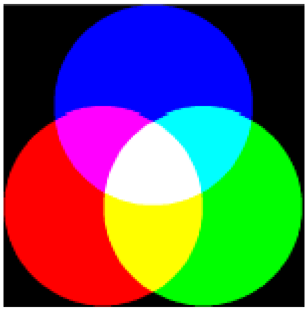


Figure 1-3 Additive synthesis of the colors

Histogram: A histogram is a statistical graph to represent the distribution of the intensities of the pixels of an image, in other words the number of pixels for each luminous intensity (Figure 1.4). [5][6] By convention, a histogram represents the level of intensity in X-coordinate while going from darkest (on the left) to most clearly (on the right). To decrease the error of quantification, to compare two images obtained under different lightings, or to measure certain properties on an image, the corresponding histogram is often modified [7] [8].

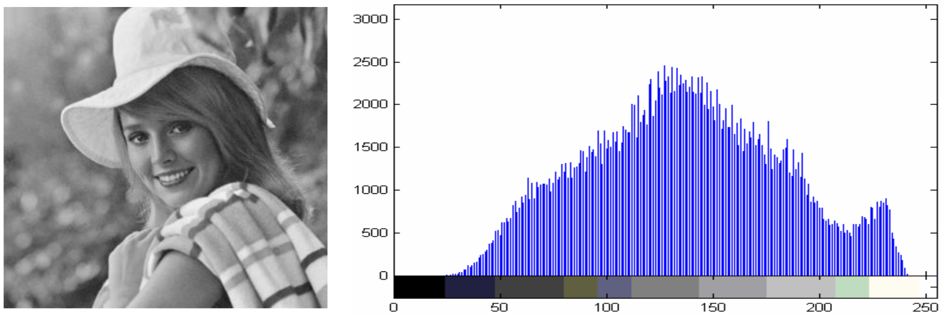


Figure 1-4 Image and the corresponding histogram.

1.3.1.2 The usage of bitmap images

Bitmap images are used for most graphic illustrations with a large number of colors, such as those presented on the web pages, scanned photographs, ... etc.

1.3.1.3 Bitmap formats

The images take a lot of space in memory, if the hard drives and RAM memories of today’s computers are quite capable of managing them, otherwise uploading images over the Internet can be a problem ... Two file formats are used particularly on the net: GIF and JPEG and other.

Table 1.1 The different formats of bitmap

Format	Advantages	Drawbacks	Note
JPEG JPEG 2000 Joint photographic experts group	- excellent compression - doesn't affect on the quality of the image	- destructive compression (lossy)	Specially designed for photographs, however, it is used with delicacy because its compression can blur the image. The JPEG2000 format evolution of the original format, it can be adjusted to compress without loss.
GIF (Graphical Interchange Format)	- Possibility of animation and transparency. - efficient compression	- Limited to 256 colors.	Very common on the Web despite its weaknesses, and a legal problem on its compression format. Not recommended for photos.
PNG (Portable Network Graphics)	- Excellent lossless compression. Possibility of transparency. So perennial Standard,	Not very efficient for large photographs	Format was designed to replace GIF and its limitations. It can replace JPEG and GIF (except with animation feature).
TIFF (Tagged Image File Format)	- Efficient lossless compression, - Transparent layer.	Heaviness of uncompressed files. Proprietary format.	Storage format widely used. Not recommended for the Web
BMP (Bitmap)	Windows default Format	Available only on Microsoft platform	Usually uncompressed and therefore very heavy files

1.3.2 Vector image

The vectorial image is a conceptual representation of form calculated by mathematical formulas, (example, a circle is not determined by pixels but by a mathematical formula that determines its shape, its size and its site) [9], it is composed of different objects marked by their coordinates and including different attributes (border, background, shape, coordinates). Their advantage it is that they can be easily resized. Their coding depends directly on the software that permitted to create them, the most used formats are (SVG "Scalable Vector Graphics" SWF "Flash" PSD "Adobe Photoshop" PDF "Portable Document Forming"). Example: figure 1.5 shows an image of small size that we enlarges it ten times, the result picture is enlarged but it is not distorted because the precision of the image doesn't depend on the enlarging factor (contrary to the bitmap).

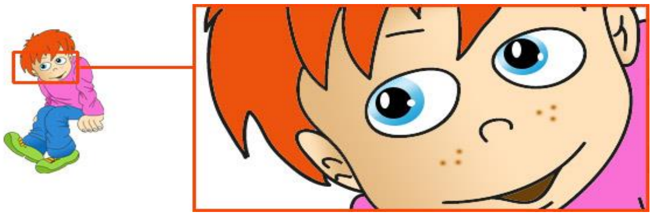


Figure 1-5 Example of vector image.

1.3.2.1 Use of the vector images

These pictures are used to make diagrams, technical drawings or plans.

1.3.2.2 The vector formats

One summarizes the set of vector formats in this (table 1.2)

Table 1.2 The different vector format

Format	Advantages	Drawbacks	Notes
AI (adobe illustrator)	Recognized by all graphics software.	Proprietary format.	Standard format of Adobe Illustrator, one of the most used due to the popularity of the software.
PS/EPS (Postscript / Encapsulated Postscript)	Very well recognized on all systems.	Only useful in printing. File very heavy	Hybrid format bitmap / vector, reserved for printing. EPS is a PostScript file which contains some additional restrictions.
SVG (Scalable Vector Graphics)	XML format So extensible. Highly compressible because it is a text format. Standard so perennial. Allows animations and transparency. Can display bitmap mages.	Yet little known, because few tools available and lack of implementation in browsers (need a plugin).	Promised a good future despite a slow start, this format is often cited as capable of competing with the first versions of Flash.
FLA/ SWF (Flash)	Very versatile. can use MP3, JPEG, videos ... Very widespread on the Web.	Proprietary format and closed.	It is the standard to make vector animations on the Web.
PDF (Portable Document Format)	Very common in the web.	Prohibitive size. Can be read only with the Acrobat software or equivalent software.	Simplified version of PostScript, it was designed to display documents in the same way regardless of the

			system.
PICT (Picture)	Default Mac OS format	Available only on the Apple platform	Has not big interest compared to other existing formats.

1.4 aspects of the image processing

The processing that generally applied to the pictures are:

1.4.1 Improvement or alteration of the image

The image processing corresponds to all possibilities of image editing, alterations or modifications that one can achieve with a computer on an image when it is displayed to the screen.

The software of image processing in pixels permit to achieve some modifications on these pictures to get precise effects:

- To realign a picture

- Modify the size (to the screen or to the impression)

- Retouch some colors

- To integrate a text

- To change a background

- To erase a part of the picture...

1.4.2 Protection by digital watermarking

This technique consists in hiding the watermark in data of the picture. This approach has the advantage not to bother the reading of the picture by the simple spectator while permitting an easy identification. The author pulls an auxiliary advantage of it: the possible inattentive pirate won't be tempted to withdraw or to amend the signature; the more voluntary pirate will see his returned illegal activity a few more difficult or easily provable (by the only presence of the watermark).

1.5 Conclusion

The objective of this section was to present some notions on the domain of numeric picture in a general manner, this domain is classified in two types, matrix and vector. Indeed we presented the different types of codification of color as well as different formats of storages. Then we were concerned with some aspects of the image processing as the alterations, the compression and the watermarking, and this last will be presented and detailed later in (chapter 2, section 3).

2. General overview on Hash functions

2.1 Introduction

Hash functions are used to obtain a limited size output data from a variable sized data, the hashing functions are one way because it is impossible to calculate the original source data from the hashed data. (Figure 1.6)

The hash functions also applied for many cryptographic protocols such as the digital signatures.

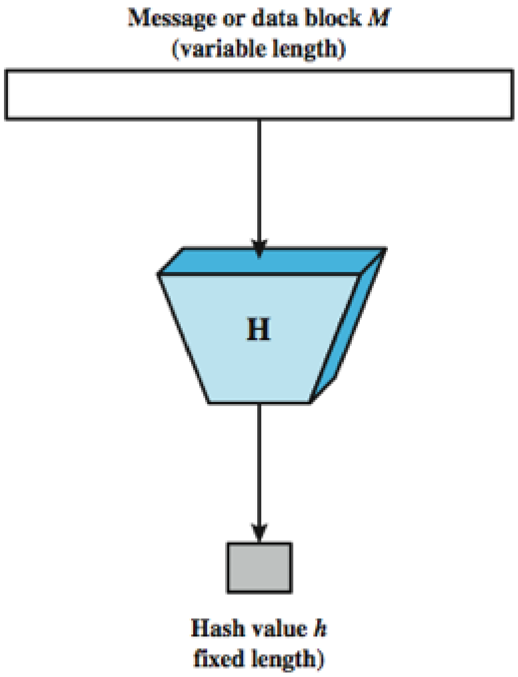


Figure 1-6 hash functions mechanism

These functions are perfectly deterministic, they don't require the use of any key due to their employment contexts, and some security properties must be satisfied:

Collision resistance: it must be computationally difficult to find two different messages leading to the same hash output.

Preimages resistance: when given a value h from the hash space, it must be hard to find M such that $H(M) = h$.

Resistance to second preimages: Given a message M, it must be hard to find a message M ' different from M such that $H(M) = H(M')$.

2.2 Hash functions applications

1- Password storage: instead of storing a clear password in a machine or a database it's more preferred to store its hash, it is the case in /etc/password of UNIX.
2- File integrity: to confirm that no modifications was done to a file, we calculate it's hashed.
3- Communication integrity: we can also use hash functions to assure that the messages during the transmission was not edited.
4- Digital signature: for security raisons it is always advised to sign a hashed message instead of a clear message.

2.3 Common hash functions

MD4 and MD5 (Message Digest) both were developed by Ron Rivest in 1991 [10]. MD5 produces a hashed of 128 bits from blocks of 512 bits.

Using MD5 in digital signatures may cause many attacks scenarios and it is not considered as a secure hash function to be used nowadays.

SHA-1 (secure hash algorithm 1) is based on MD4, it produces a hash of 160 bits from a block of 512 bits and it requires more resources than MD5. [11]

SHA-2 (secure hash algorithm 2) was designed to replace SHA-1, its main differences are in the size of the hashes 256, 384 or 512 bits.

RIPEMD-160 (Ripe Message Digest) [12] is a new version of RIPEMD algorithm, the previous version produces hashed of size 128 bits, but it suffers from security vulnerabilities.

The actual version stays secure, it produces as it is mentioned in its name a hash of size 160 bits it requires more resources than SHA-1 its concurrent.

HAVAL is a hash function that produces hashes of variable sizes. [13]

Whirlpool: is a hash function that was developed by Vincent Rijmen and Paulo Barreto, it produces hashes of size 512 bits. [14]

2.3.1 MD5: (Message Digest)

Developed by Rivest in 1991, MD5 creates a digital hash of length 128 bits from a text of arbitrary length, treated as blocks of 512 bits, it is famous that some downloaded files from the internet are attached with a MD5 file, the raison for this is to verify the integrity of this last file, to happen according to the following way: MD5 manipulates blocks of 512 bits, and it completes the length of a message in input in order that the length will congruent to 448 modulo 512, by adding 1 followed by as many 0 as needed in the end of the message, the padding operation always takes place even if the length of the message is already a multiple of 448, then the initial length before the padding of the message is added to 448 bits, as forms of 64 bits, which leads to a size multiple of 512 bits. Every bloc of 512 bits is decomposed into 16 blocks of 32 bits and the result is represented by a set of 4 letters A, B, C and D.

Notation:

[<<<]s is a rotation of ‘s’ bits to the left, ‘s’ vary for each operation.

[+] represents the addition operation modulo 2^{32}

$\oplus$, $\wedge$, $\vee$, $\neg$ Represents respectively the Boolean operations XOR, AND, OR and Not

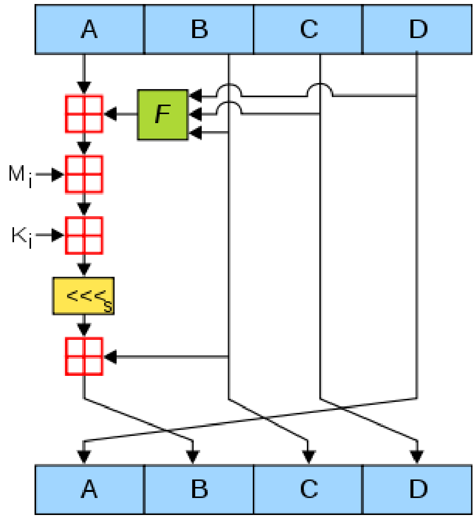


Figure 1-7 The structure of MD5 algorithm.

2.3.2 SHA (Secure Hash Algorithm)

2.3.2.1 SHA-1

SHA-1 is a cryptographic hash function that was developed by the national security agency of the United States (NSA), and published by the government of USA as a federal standard for information processing.

The SHA-1 takes in entry a message of maximum size of 264 bits, it is similar in the function to MD4 and MD5 of Ronald Rivest. Four Boolean operations are defined it takes three words of 32 bits as an entry and calculate a word of 32 bits. a specific function of rotation is available, it allows to move the bits to the left (the movement is circulant and the bits are back to right), one of these rotations was not presented in the recent version of SHA, it allows to break some linear characteristic in the structure, also it allows to avoid the attacks on the neutral bits written by Eli Biham, technique to calculate the collision on SHA-0 (Antoine joux et al.).

The SHA-1 algorithm starts by adding at the end of the message a bit 1 followed by a series of bits 0 then the length of the initial message coded in 64 bits. The series of zeros has a length such that the extended sequence has a length multiple of 512 bits. Then the algorithm works successively on blocks of 512 bits.

For each bloc the algorithm calculates 80 rounds successively and apply a series of transformations on the entry. The first step consists of calculating 80 values on 32 bit. The first 16 values are obtained directly from the bloc "message" in entry. The 64 others are calculated successively, the SHA-1 obtains them due to a rotation that doesn't exist in SHA-0 that be applied on the result of XOR function, it uses for this 4 words that were obtained in the previous iterations. Then we define 5 variables that were initialized with constants (specified with the standard), the SHA-1 uses also four other constants in the calculation process. If a bloc of 512 bits was already calculated before, the variables are initialized with the values obtained at the end of the calculation process on the previous bloc. Then it follows with 80 rounds that alter rotations, adding between variables and constants, Based on the number of rounds, the SHA-1 use one of the four Boolean operations, one of these functions will be applied on 3 of 5 available variables, the variables are updated for the next round due to permutations and a rotation. As a conclusion the SHA-1 changes its calculation method all the 20 rounds and uses the output of the previous rounds. In the end of the 80 round it adds the result with the initial vector, such all the blocs were processed, the five variables merged ($5 \times 32 = 160$ bits) represent the signature.

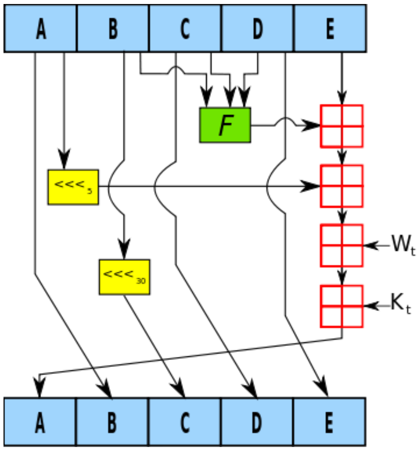


Figure 1-8 The SHA-1 structure

2.3.2.2 SHA-2

As all the hash functions, SHA-2 takes as an entry a message of arbitrary size and produces a hash of fixed size. The size of the hash is indicated by the hash function name suffix: 224 bits for SHA-224, 256 bits for SHA-256, 338 bits for SHA-338 and 512 bits for SHA-512.

The algorithms of SHA-2 family are very similar, there are mainly two deferent functions, SHA-256 and SHA-512, they have the same structure but deferent in the size of the words and blocs used.

This structure is also close to the SHA-1 structure but more complex and robust against known weakness, and it is belong generally to a hash function family inspired from MD4 and MD5 of Ron Rivest. It can found as primitive the addition for integers of fixed size n be an addition modulo 2n, operation non linear …..

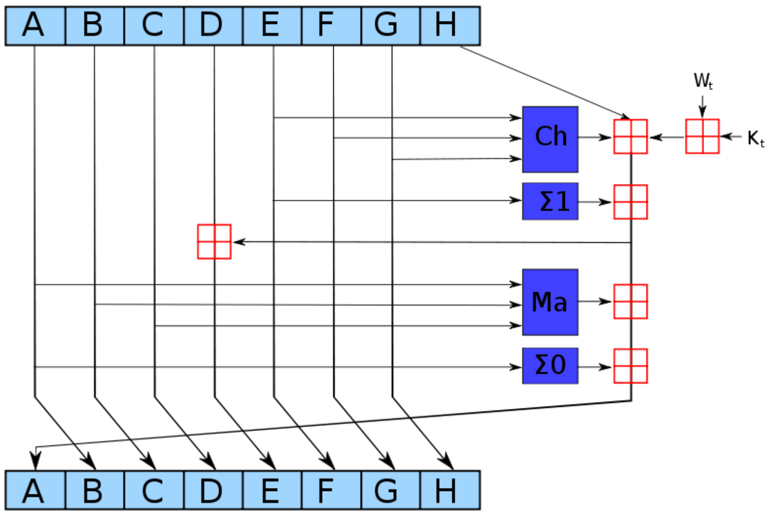


Figure 1-9 Structure of SHA-2 algorithm

Table 1.3 SHA-2 notations

Notations	Definition
Ch, Ma	Non linear operations that calculate bit to bit
W_t	Word 32 or 64 bits that depends on the number of round t
K_t	A Key
$\sum 0, \sum 1$	Circulant shift
A, B, C, D, E, F, G and H	Words of 32 or 64 bits

2.4 Conclusion

In this section we presented a general overview on hash functions, and we presented the famous hash functions such as MD5 and SHA, recently the SHA-2 is widely used in many schemes because it offers a good security and a good hash size, the properties of hash functions allow them to be useful in many applications in cryptography and authentication protocols.

3. Mathematical background

3.1. Positive semi definite matrix

A symmetric $n \times n$ real matrix A is called positive semi definite if $x^t Ax \geq 0$ for all $x \in R^n$, where x^t denotes the transpose of x, and A is called positive definite if $x^t Ax > 0$ for all non-zero $x \in R^n$. It is easy to verify that the following statements are equivalent [18]:

The symmetric matrix A is positive semi definite.

All eigenvalues of A are non-negative.

Example

Given a set E of m vectors $v_1, .., v_m$ in R^n, the $m \times m$ gram matrix $G = (a)_{ij}$ is defined by $a_{ij} = v_i \, v_j^t$

G can be also defined by $V^t V$ where V is a matrix whose columns are the vectors $v_1, .., v_m$.

The matrix of gram is positive semi definite, it is positive definite if and only the vectors $v_1, .., v_m$ are linearly independent.

3.2 Polar decomposition and Singular values decomposition

Every non zero complex z can be written in the polar form

$$z = r\, e^{i\theta} \tag{1}$$

where r is the absolute value of z and

$$e^{i\theta} = \cos\theta + i \sin\theta \tag{2}$$

is called the complex sign of z , we have a similar factorization for matrices:

3.2.1 Polar decomposition

Theorem [15]:

Any matrix $A \in \mathbb{C}^{n\times n}$ has a left polar decomposition namely

$$A = P\,U \tag{3}$$

Where $P \in \mathbb{C}^{n\times n}$is a unique positive semidefinite matrix and U is an unitary matrix.

If A is invertible then P is positive definite and U is also unique.

If $A \in \mathbb{R}^{n\times n}$, the left polar decomposition of A is $A = P\,Q$ where Q is orthogonal($QQ^t = I_n$) and P is symmetric matrix with non negative eigenvalues. In view of the wide range of applications, many aspects of the polar decomposition have been studied in [16].

3.2.2 Singular values decomposition (SVD)

A notion closely related to the polar form is the singular values decomposition (SVD), it is well known that:

Theorem (SVD) [17]

For every real $n \times n$ matrix A of rank r, there are two orthogonal matrices U and V and a diagonal matrix $S = diag(\partial_1, \partial_2 \cdot\cdot, \partial_r)$ such that

$$A = U \times S \times V^t \tag{4}$$

and $(\partial_1, \partial_2 \cdot\cdot, \partial_r)$ are the singular values of A , i.e. the positive square roots of the non zero eigenvalues of $A \times A^t$ and $A^t \times A$ and $\partial_{r+1} = \ldots = \partial_n = 0$

The columns of U are eigenvectors of $A \times A^t$ and the columns of V are eigenvectors of $A^t \times A$.

This theorem can be extended to rectangular $m \times n$ matrices, in applications it is faster and economical for storage to use a reduced versions of the SVD (Thin SVD, compact SVD, truncated SVD,…), for example in the compact SVD $A = U \times S_r \times V^t$ only the non-zero-singular values are used.

It is easy to go from the SVD decomposition to the polar form and conversely, given an SVD decomposition $A = U \times S \times V^t$, let $P = U\,S\,U^t$ and $Q = U\,V^t$

It is clear that Q is orthogonal and that P is positive semi definte symmetric, and

$$A = (U\,S\,U^t)(U\,V^t) = P\,Q \tag{5}$$

Conversely let $A = P\,Q$ be a polar decomposition, then the positive semi definite symmetric matrix P is orthogonally diagonalizable, that is, it can be written in the form $P = Q_1\,D\,Q_1^t$ with Q_1 is orthogonal and D is diagonal.

So $A = Q_1\,D\,Q_1^t\,Q = Q_1\,D\,(Q^t Q_1)^t = U\,S\,V^t$ where $U = Q_1$, $S = D$ and $V = Q^t Q_1$

One can also decompose A in the form

$$A = U\,S\,V^t = (U\,V^t)\,(V\,S\,V^t) = Q'P' \tag{6}$$

This is known as the right polar decomposition.

Note that the SVD of a matrix *A* is not unique, even if *A* is invertible but the polar decomposition is unique if the matrix *A* is invertible.

3.3 Circulant matrices

A $n \times n$ circulant matrix is formed from any n vector $c = (c_1,..,c_n)$ by cyclically permuting the entries, for example if $c = (c_1, c_2, c_3, c_4)$, the 4×4 circulant matrix $C = cir(c)$ is given by

$$\begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ c_4 & c_1 & c_2 & c_3 \\ c_3 & c_4 & c_1 & c_2 \\ c_2 & c_3 & c_4 & c_1 \end{pmatrix} \tag{7}$$

Chapter 2 Content Authentication methods

Introduction

Multimedia authentication is the process of proving the identity and the truth of the content of multimedia, recent reports indicate that the cases of illegal modification and manipulation of multimedia and plagiarism in the internet have been increased.

The development in the editing software and the popularization of the internet made the reproducing and falsifying of the multimedia very easy, for this concern multimedia authentication became essential.

Multimedia authentication handles the following issues:

Is the source of the multimedia data rightful?

Did any change happen to the original multimedia?

If change occurred to multimedia then what's the location and the level of the modification.

Basically there are many strategies that can response to these concerns.

In the following sections of this chapter we'll present those methods, starting with handwritten signature and digital signature then the digital watermarking.

1. Handwritten signature

The signature is a method that has been used long time ago, the ancestor used the seal, to authenticate documents in order to give a sense of responsibility to the individuals towards commitments, contracts... etc [19]. The signature was recognized as a mode of validation associated with the identity of a person, in this section we focus on the recognition of handwritten signature, we'll start by defining the handwritten signature and its classification. Thereafter we will describe the two types of recognition of handwritten signature by putting the point on the offline recognition. The next point will detail the performance measures of a handwritten signature recognition system followed by a conclusion on the importance of recognizing signature.[20] The handwritten signature has been for several centuries the most widespread used technique to express its own will. It is today, and will undoubtedly remain it in the future. The use of the handwritten signature is based on the assumption that in the signature procedure it is more instinctive movements than conscious acts that are involved in the implementation of the signature. This assumption implies that some features of the signature are so stable constant for a signatory. The signature is a mark to identify the author of a document of a work or the cause of a phenomenon: an author signs his writings (Figure 2.1).

Figure 2-1. Handwritten signature.

The handwritten signature of an individual represents a good compromise: while being relatively reliable, it is easy to acquire and it is socially well accepted like mode of identification. The study of the handwritten signature is a special case of the expertise of handwritten documents. Indeed, the information available to analyze a signature is relatively small, compared to the handwritten texts. In addition, a signature more than any other form of writing is the result of a spontaneous gesture and almost automatic [22], [23].

1.2 Types of forgeries

According to the type of searched forgery, the expert uses specific treatments, such as the proportions of the signature, the number of parts of the signatures and projections.

The following types of forgeries are found:

Forgeries by disguise: they are particular because they correspond to signatures made by the supposed signatory (origin) but deliberately disguised in order to deny them later. These signatures are generally resembling in spite of a loss of harmony in the layout and the shifting of speed. A detailed study made by researchers makes it possible to detect them [22] [23] [27].

Forgeries by servile imitation signature: in the case of a false by slavish imitation, the forger must have a copy of the authentic signature. This false although resembling the original but has differences in the spacing and in the inclinations. Also the plot is slow and hesitant where visible changes of the pressure [22].

Forgeries by free imitation: for this forgery the forger studies the authenticate signature carefully and involves himself to reproduce it from memory until being satisfied with the result. It is, in the opinion of the experts, the forgeries most difficult to detect because they are very resembling and the layout is spontaneous. They differ from the originals by the proportions.

Forgeries by Layer: accurately reproduce the image of an authentic signature on a document by using a technique of copying for example: a copy by transparency, with carbon, by photocopy. This forgery is obviously very difficult to detect even for the experts [22].

Coarse forgeries: in the case of a coarse forgery, the forger does not try to make a forgery resembling to the original. This forgery is frequent and it is easiest to detect [23].

Simple forgeries: the forger creates a signature starting from the name of the signatory without imitating an original. This forgery is generally little resembling especially for the signatures of the European type of graphic nature; it is however more difficult to detect than the coarse forgeries. This kind of forgery is interesting from a technical point of view (validation) for the systems treating the signatures of the American type of cursive nature because it makes it possible to test the systems of authentication with forgeries more resembling than the coarse forgeries [22] [23].

1.3 Handwritten signature recognition

Signature recognition systems are responsible of treating the manuscript, they are divided into two categories "online systems” and “offline systems ".

1.3.1 Online recognition

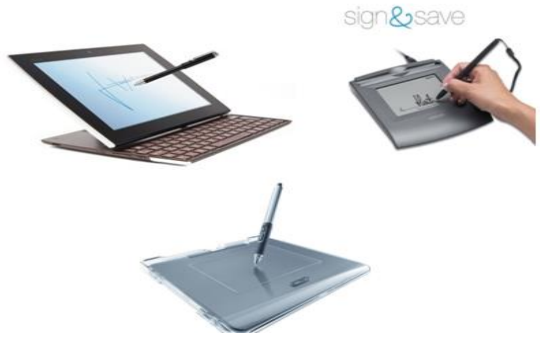


Figure 2-2 Acquisition devices for online handwritten signatures.

In the case of an online system, the signature is performed on a graphics tablet or other support provided with an electronic pen. [21] Figure 2.2 shows examples of online signature acquisition tools.

The online signature is digitized directly by a device which makes it possible to sample the signals at a fixed frequency, at the time when one signs, the acquisition of an online signature requires a specific sensor. A digitizing tablet or a touch screen of a PDA is enough for this task.

In general, the signature is sampled at 100 Hz. At each sampling point, the system can record the coordinates, pressure and the angles of inclination of the pen.

If a touch screen is used for the acquisition, only the pen coordinates are recorded. Some tablets digitizers also allow you to record other information such as the time of torque, rotation of the pen around its axis, etc.

This method allows the use of dynamic information such as speed, pressure and / or inclination of the pen. These systems are primarily used to control access to protected areas or to verify the identity during an online transaction. These systems cannot be used to verify signatures already affixed to documents (bank checks, for example) [22].

There are quite benefits of online handwritten signature recognition, compared to the offline system [24]. For example, the act of signing is different for each person. It is also difficult to falsify because it is not possible to recover the dynamic information of the gesture from the image of a single signature. With this information in addition to the image of the signature, the signature verification becomes a more effective for identity verification.

1.3.2 Offline Recognition

In the applications of the offline handwritten recognition of signature, the signature is carried out on a paper support then scanned (figure 2.3).

The signature is treated as a grayscale image. This is the case especially for bank checks verification systems [21].

The entry of such systems is an image. So the problem becomes more difficult, for example, how to remove noise such as background image items, how to treat the lack of features, etc. Furthermore, there is no additional information as in the first case. Moreover, to apply these systems widely, they must achieve high recognition rate. Typical applications include automatic classification letters, signing bank checks, etc. [24].

This type of recognition systems is more applicable and easier to use compared to the online system.

Figure 2-3 Supports of offline handwritten signatures

In the following point, we will describe the stages to be followed to carry out an offline handwritten signature recognition.

1.3.3 System of recognition of handwritten signature Offline

Generally offline signature recognition system is divided into four main processes: acquisition, preprocessing, feature extraction and recognition. Figure 2.4 shows the general structure of this type of system.

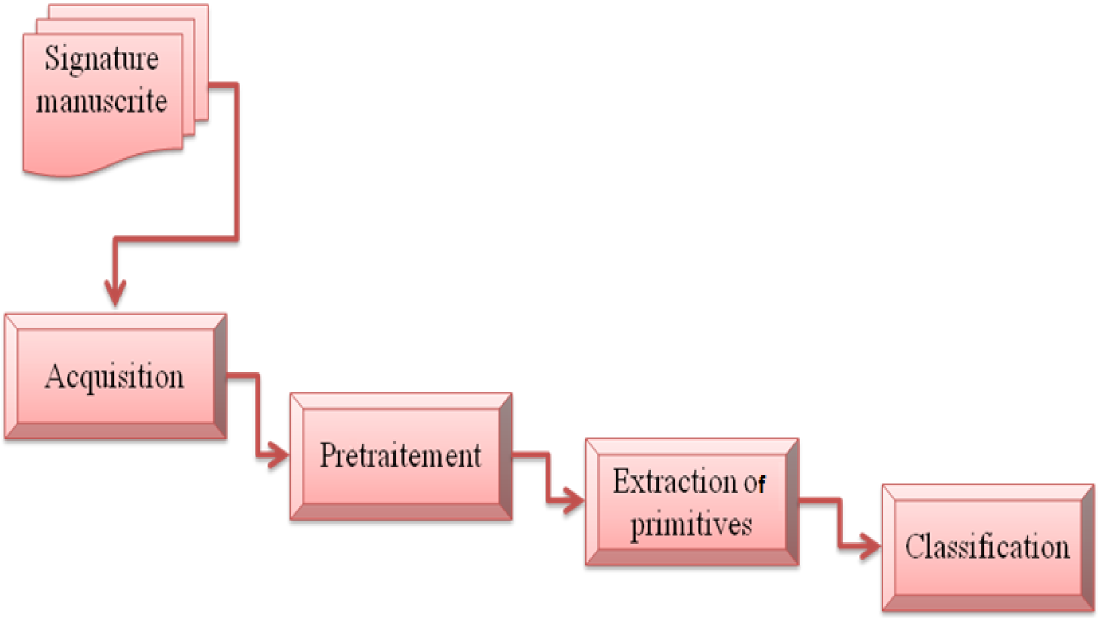


Figure 2-4 Architecture of a handwritten signature recognition offline system.

Starting with the acquisition phase that converts the image of the signature to a digital image, then we go to the pre-treatment phase, this step prepares the input image for the extraction of features. The extraction phase used to represent the signature acquired by a set of values representing the calculated characteristics extracted from the signature. Finally, the recognition phase where the signature will be compared to reference signatures, thereafter, the principle will be explained as well as the techniques used in each phase.

1.3.3.1 Acquisition

The signature is digitized by a scanner, and transformed into an image. This is the input of the system. This step is quite simple but very important because it seriously affects the following steps. Acquisition tools are shown in Figure 2.5.

Figure 2-5 Acquisition tools for offline handwritten signatures.

This is important in pattern recognition and therefore at the signature authentication process. It involves preparing data to be supplied to the authentication module. The quality of these data strongly influences the final results [25].

Pretreatment includes a set of operations such as filtering, normalization, Binarization, Skeletonization, etc [28].

1.3.3.2 Extraction of primitive

The common objective of all primitives (features) is to characterize to better the signatures forms in order to be able to distinguish if two pictures belong to the same class or to different classes.

The primitive are classified in two categories: the structural primitive (or local primitive) and the statistics primitive (or global primitive) [29].

1.3.3.3. Classification

This is the main stage and it represents the development of a decision rule which transforms the attributes characterizing the signatures into class membership (passage of the space of coding towards the space of decision) [30].

Before a decision model is integrated in a signature recognition system, it is necessary to have proceeded before the two stages: the learning step and the classification step.

The Learning stage: the learning step is to characterize the classes of signatures in order to distinguish the homogeneous families' signatures. This is a key step in the recognition system. There are two types of learning: supervised learning and unsupervised learning [31].

Supervised learning: in this case, a representative sample of all signatures to be recognized is provided in the learning module.
Each signature is labeled by an operator called teacher, this label is used to indicate the learning to the module of learning, the class in which the teacher wishes that the signature be arranged [32].

This learning phase consists in analyzing the similarities between elements of the same class and the dissimilarities between elements of different classes in order to deduce the best partition of the space of representations. The parameters describing this partition are stored in a learning table where the decision module will then refer to classify the submitted signatures [32].

The Unsupervised learning: in this case, one provides to the recognition system a large number of not labelled signatures. The stage of Classification will be given the responsibility to identify the signatures automatically belonging to the same class.

- **The stage of testing**: It assesses the performance of the classifier for a given learning. This is an important step because it can involve the choice of primitives or the choice of the learning method. Indeed, it is difficult to find the relevant primitives and the most adapted learning method to the posed problem [32].

To define a classifier, let the representation of any object by a vector of characteristics: $X = [x_1 x_2 ... x_d]^T$

All the vectors that represent the set of objects can be positioned in the Euclidean space R^d where they each correspond to a point. These can then be grouped into clusters, each cluster is associated with a particular class. An example for a two-class problem is shown in Figure 2.6.

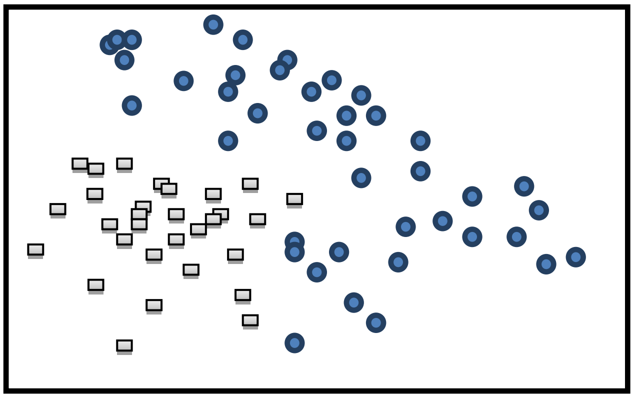


Figure 2-6 Representation of objects belonging to two distinct classes, in a two-dimensional space.

The role of a classifier is to determine, among a finite set of classes, to which belongs a given object.
A classifier must be able to model the boundaries which separate the classes from/to each other. This modelization uses the concept of discriminant function, which allows to express the classification criteria as follows:

Assign the class **ωi** with the object represented by vector X if, and only if, the value of the discriminating function of the class **ωi** is higher than that of the discriminating function of any other class **ωj**".

Or, in mathematical form:

$$X \in W_i \Leftrightarrow \phi_i(X) \geq \phi_j(X) \qquad \forall j = 1, 2, .., C; \;\; j \neq i$$

Where $\phi_i(X)$ is called the discriminant function of the class W_i, and C is the total number of classes.

The process of recognition can be always summarized with a decision of classification. To build a classifier, there exist several approaches: structural, statistical and networks of neurons [32].

Structural approach: it is an approach that is based on the extraction of primitives taking into account the structural information. This approach seeks to structure information describing the topological organization (structure) of the form from the most basic components. It requires a measurement of the similarity between two structural representations. There are several techniques such as graph structures and syntactic structures [33].

Statistical approach: this approach consists in determining characteristics extracted from a form to characterize them in a statistical way. It needs a high number of examples in order to carry out a correct learning of the probability distributions of different classes [34].

Approach based on neural networks: it is an implementation derived from the statistical approach and structural approach. [32] This approach is used widely in recognition systems. The Power, the ease of use, the learning and generalization capabilities are the main reasons to use this approach [26].

1.4 Evaluation of a signature recognition system

To evaluate the performance of a recognition system, two parameters are usually used: False Rejection Rate (FRR) also known as type 1 and False Acceptance Rate (FAR) or type 2 [35].

One can consider the problem of authentication of signatures as a partitioning problem into two classes. For a given signer, first class is formed by the signatures of the signatory and the other class by all other signatures available. Ideally, these two classes are separated by a hyper surface within the space of representations of the signatures [22].

The problem of the recognition is primarily summarized to find the form and the position of this hyper surface in adequate space. Generally, recognition systems use a parameter, called decision threshold, which adjusts the hyper surface. Thus, if the two classes are separable, there exists a decision threshold value that cancels both FRR and FAR error rate (Figure 2.7) [22]

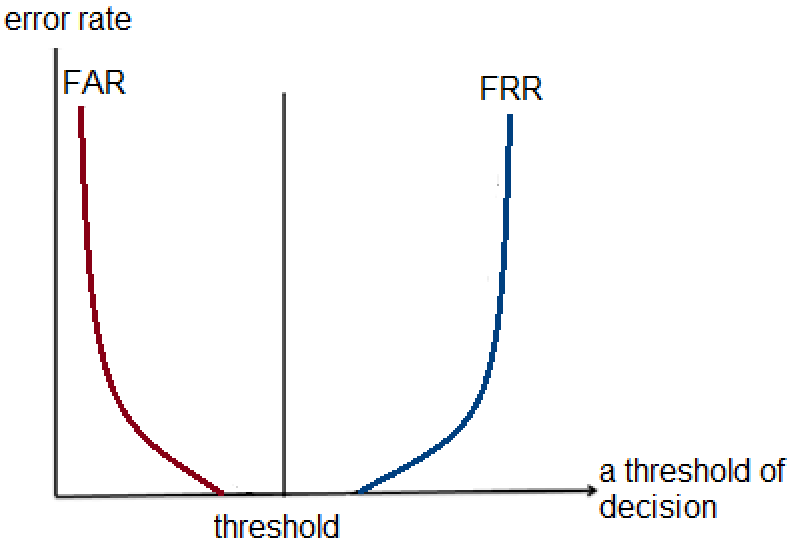


Figure 2-7 Choice of a threshold of decision which cancels the error rates.

In practice, most used signatures of references do not allow the separation in two disjoined classes (figure 2.8).

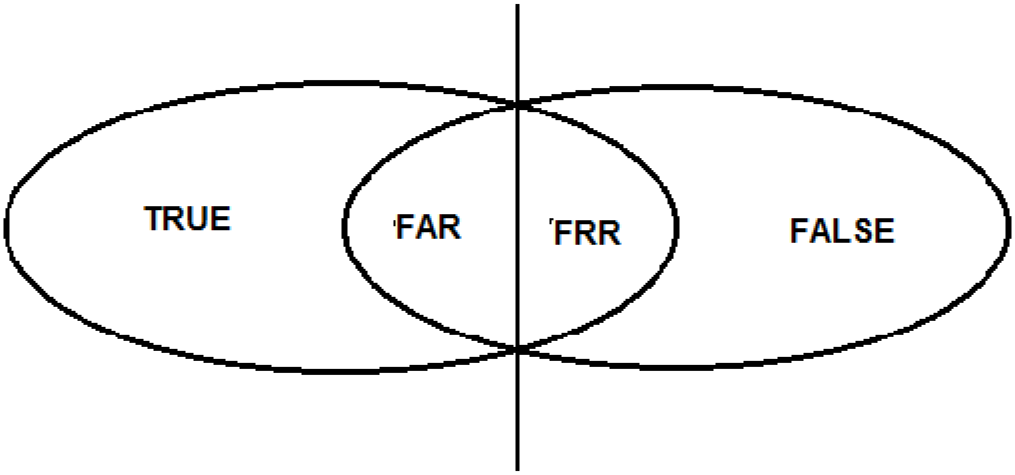


Figure 2-8 Non separable classes

The choice of the decision threshold is constructed from one of the following criteria shown in Figure 2.9 and which are:

– Minimize averages of FRR and FAR rates.

– Ensure that one of the two levels below a desired threshold (eg, less than 1%) [22].

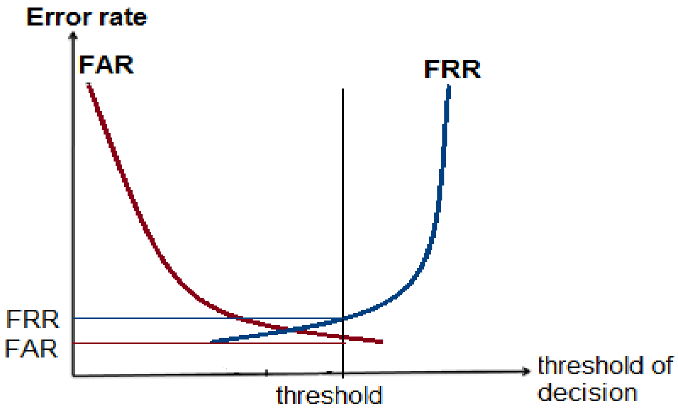


Figure 2-9 Choice of a threshold of decision according to a criterion.

Table 2.1 presents some handwritten signature recognition systems offline. For each system, we introduced the type of classifier and the primitives extraction techniques used. The performance of these systems is indicated by the verification rate [25].

Table 2.1 comparison of different handwritten signature offline recognition systems

Method	The used classifier	The used Primitives	Error rate (FAR)
Piyush and Rajagopalan [36]	Matching Model	(DTW) Dynamic Time Wrapping	2.1%
Justino et al [37]	Hidden Markov model (HMM)	Grides segmentation	4.7%
Jose et al [38]	Network of neurons	Mesures de compression	4.20%
Debnath et al [39]	Statistical approach	Coefficient of correlation	7.9%
Samaneh and Moghaddam [40]		The Wavelets	3.45%
Ramachandra et al [41]	Structural approach	The matching of graphs	3.7%
Emre and Karshgil [42]	Machine with vectors of support (SVM)		9.5%

1.5 Conclusion

Despite all the development in technologies the manuscript signatures remains the most used technique for authenticating a document, validate a contract or financial transaction. The signature can also be used as a password to access confidential documents, or to access to an office. It is as reliable as voice or retinal identification.

We have presented in this section recognition of handwritten signature. We began by defining the handwritten signature and giving its classification. Thereafter, we described the two types of recognition of handwritten signature; online and offline. A general description of a handwritten signature recognition system offline was also discussed; then the details of each steps for constituting an offline signature recognition system was presented, acquisition, pre-processing, feature extraction and classification. We conclude this section with a table describing some relevant work in this area.

2. Digital signature

A digital signature is an information that can be attached to a transmitted message in order to identify the sender and detects unauthorized modification to data. A digital signature scheme consists of three algorithms as follows: key generation algorithm, signing algorithm and verification algorithm.

Users create digital signature to act like physical signature does on a written document, to prove the document source and validate the integrity of transmitted message.

Digital signatures have many applications in information security, including authentication, data integrity and non-repudiation.

2.1 Digital signature properties

A digital signature must be:

Authentic: it convince the recipient that the signer deliberately signed the document.

Unfalsifiable: the digital signature must resist to any falsification.

Non-reusable: the signature attached to a document couldn't be used to sign another document.

Unalterable: any modification to the signed document must be detected.

Non repudiation: the signer cannot deny the authenticity of their signature on a document

2.2 Digital signature classes

As encryption schemes digital signatures can be divided into two classes:

Symmetric signatures: those based on symmetric cryptosystem that use private key.

Asymmetric signatures: which based on an asymmetric schemes using public key, in this case we use the private key in the signature procedure and the public key for the verification process.

Figure 2.10 shows the scheme of a digital signature using public key. In the signing procedure, a hash function was applied to data and signature was done on the hashed data.

When the data size is big, it is more practical to sign the hashed data because the output data of the hash function has a small limited size, and it is faster to sign the hash instead of signing the data.

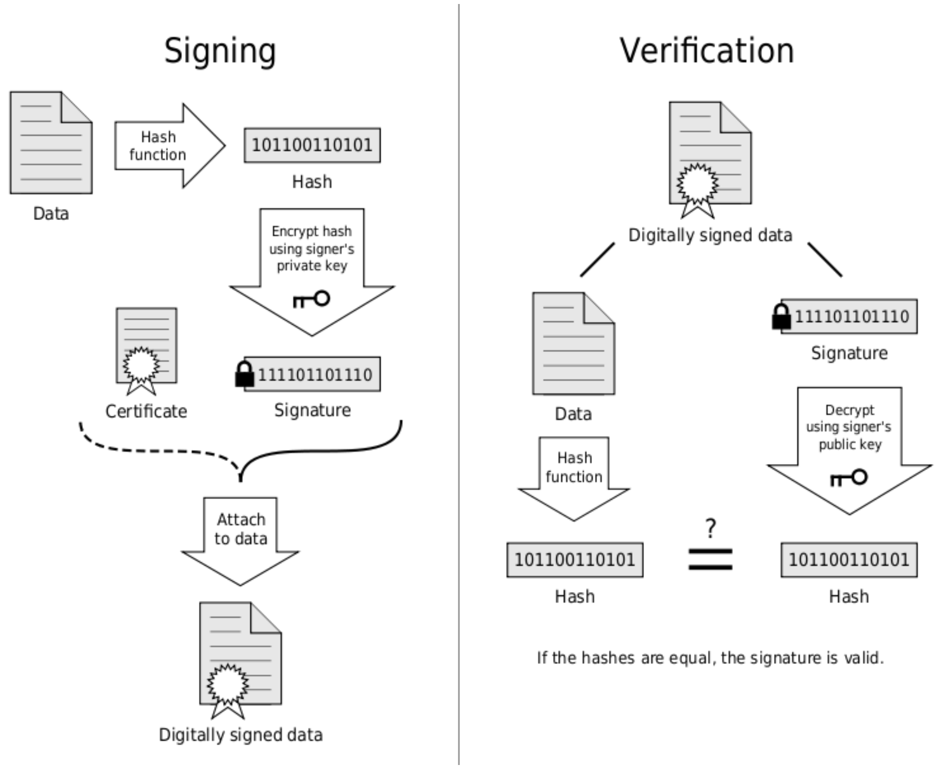


Figure 2-10 An asymmetric digital signature scheme

2.3 Common digital signature algorithms

2.3.1 RSA Signature

'RSA' is the acronym of the names of researchers who proposed this cryptosystem, Ron Rivest, Adi Shamir and Leonard Adleman, RSA is the first asymmetric encryption scheme, it is based on the theory of prime numbers, its security is obtained from the difficulty of factorization of an integer into prime numbers.

RSA signature scheme is as follows:

Key generation:

- We choose two prime numbers “p” and “q” and we calculate: phi (N) = (p -1) (q -1)

- Then put “e” and “d” while: pgcd (e , phi(N)) = 1 and e * d = 1 mod (phi (N))

- The public key is (N , e), and the private key is (d)

Signature process: the signer A calculates the signature “S” of the message “M”:

$S \equiv M^{d} \bmod (N)$ Then he sends (S, M) to the person B.

Verification process: the receiver B verifies the signature by verifying the following equation:

$S^{e} \equiv M \bmod (N)$

2.3.2 Digital Signature Standard (DSS)

In 1991 the National Institute of Standards and Technology (NIST) proposed a novel digital signature algorithm (DSA) as a standard of Federal information processing for use in their Digital signature (DSS). Digital Signature Standard - DSS - is a variant of ElGamal digital signature scheme while the length of the signature is reduced. The main difference between DSA and ElGamal digital signature is that DSA generates a digital signature of length 320 bits on a message of 160 bits, using Z_P where “p” has 512 bits, offering operations in a field with 2^{160} elements.

Digital signature algorithm

The parameters (p, q, g) are public.

“p” is a prime number of 521 bits

“q” is a prime factor of 160 bits for p-1

$g \in Z_p^*$

We define the following sets:

$$P = Z_p^* \;;$$
$$A = Z_q \;\; X \;\; Z_q$$
$$K = \left\{ \left(p, q, g, X_A, Y_A \right) \middle| X_A is\ in\ Z_q^*\ and\ Y_A \equiv g^{x} \bmod p \right\}$$

Alice’s pair of secret and public key is (X_A, Y_A).

For $k = \left(p, q, g, X_A, Y_A\right)$ and for a randomly chosen secret number $x \in Z_q^*$ the pair (r, s) represents the signature of Alice on the message “m”.

$$r = g^x \bmod p \bmod q$$
$$s = \frac{x + r \cdot X_A}{x} \bmod q$$

Verification for DSA

$$Ver(m, (r, s)) = T \Leftrightarrow g^{(m \cdot s^{-1}) \bmod q} \cdot Y_A^{(r \cdot s^{-1}) \bmod q} (\bmod p)\,(\bmod q) = r$$

2.3.3 Elgamel Signature [43]

Key generation: We’ll use the following notation:

“P” is big prime number

“g” is a generator

“x" is an integer between 0 and (p-1) and $Y \equiv g^x \bmod P$

the public key is the triple (p, g, Y) and the private key is “x”

signature procedure: for k is between 0 and (p-2), the signature function can be defined as:

$$sig(M) = (k, S) = \begin{Bmatrix} K \equiv g^k \bmod p \\ S \equiv (M - xk)k^{-1} \bmod (p-1) \end{Bmatrix}$$

Verification procedure:

$$ver(M, k, S) = true \text{ if } Y^k k^S \equiv g^M \bmod p$$

2.4 Digital signatures based on RSA, Elgamel and DSA

Based on these schemes many other digital signature procedures have been proposed in the past years by many researchers for diverse applications.

Dimitrios Poulakis and Robert Rolland [44] proposed a digital signature scheme based on two intractable problems, namely the integer factorization of RSA problem and the discrete logarithm problem for elliptic curves. It is suitable for applications requiring long-term security and provides smaller signatures than the existing schemes based on the integer factorization and integer discrete logarithm problems.

Haipeng Chen el al. [45] designed a new digital signature algorithm similar to ELGamal(H-S DSA). And this signature algorithm is based on transformation of hash round function and self-certified public key system.

Neetesh Saxena and Narendra Chaudhari [46] proposed a variant of digital signature based on DSA algorithm for Short Message Service (SMS) authentication on mobile devices;

Chou chen yang et al. [47] have presented a new group signature scheme based on RSA assumption and they reduced the amount of computing time compared to other methods.

2.5 Conclusion

In this section we have presented a general overview on digital signature, we introduced the digital signature properties and its two main classes, then we provided the common digital signature schemes which are the RSA, Elgamel and DSA, based on these schemes many other digital signature procedures have been proposed in the past years by many researchers for diverse applications and they achieved good security and performance results.

3. Digital watermarking

Introduction

The digital watermarking is a recent science emerged in the early of the years 90s, it aims to ensure copyright, integrity and authentication. In this section, we present the principle of digital watermarking for images and we explain its applications in some areas.

We start this section by providing a historical overview of this technique, then we will describe some representations of the image in spatial and frequency domain, and then we will present briefly the evaluation of digital watermarking schemes in terms of imperceptibility and robustness.

3.1 History of digital watermarking

Information is an essential element in all areas. Throughout history, mankind has always tried to exchange information in a secure way. For this reason, the data hiding and watermarking were strategies used for military to exchange secret information.

We distinguish mainly two major categories: steganography and watermarking.

The conventional use of steganography took place for more than two thousand years ago. Herodotus, the Greek historian, tells that Xerxes the king of Persia, decided to invade

Greece, then when the offensive was launched, the Greeks have known his intentions, because a warning was sent to them and it was writing on the wooden backing of a wax tablet before applying its beeswax surface [49].

Another example of information hiding is when Histie encourages his son Aristagoras, governor of Milet, to revolt against his king, Darius. To transfer his message Histie shaved off the head of a slave and tattooed his message on the skull and waited until the hair grows back then sent the slave to Milet [49].

In the 80s, Margaret Thatcher, British Prime Minister suspected certain of her ministers to transmit information to the press. So in order to identify the guilty, she demanded that all documents of his cabinet have spacing in specific words for each ministry to identify the source of the leak of information.

However, the art of tattooing was invented in China for over a thousand years, for tattoing paper (papermarking), but the oldest watermarked archived paper was dated in 1292 and its origin is the Fabriano city in Italy. The main purpose of the first watermarking are uncertain, but they were used for practical functionalities such as the identification of the origin of the paper and the manufacturer identification.

In the 18th century, watermarking was used in Europe and America, initially to identify a manufacturer or a paper mill. And later was used to indicate the format and quality of the paper, and also for authentication purpose and an anti-counterfeiting measure for money and other documents.

The watermarking term have been derivative from the german word “wassermarke”.

But it is difficult to determine when the digital watermarking was introduced for the first time, but the first article that used the term Digital Watermark was Komatsu Tominaga [48] in 1988.

Since 1996 the researches on this technique have seen large increase, as it is shown in Figure 2.11 that shows the number of publications with the keyword "watermarking" on the bibliographic database ACM and Science direct.

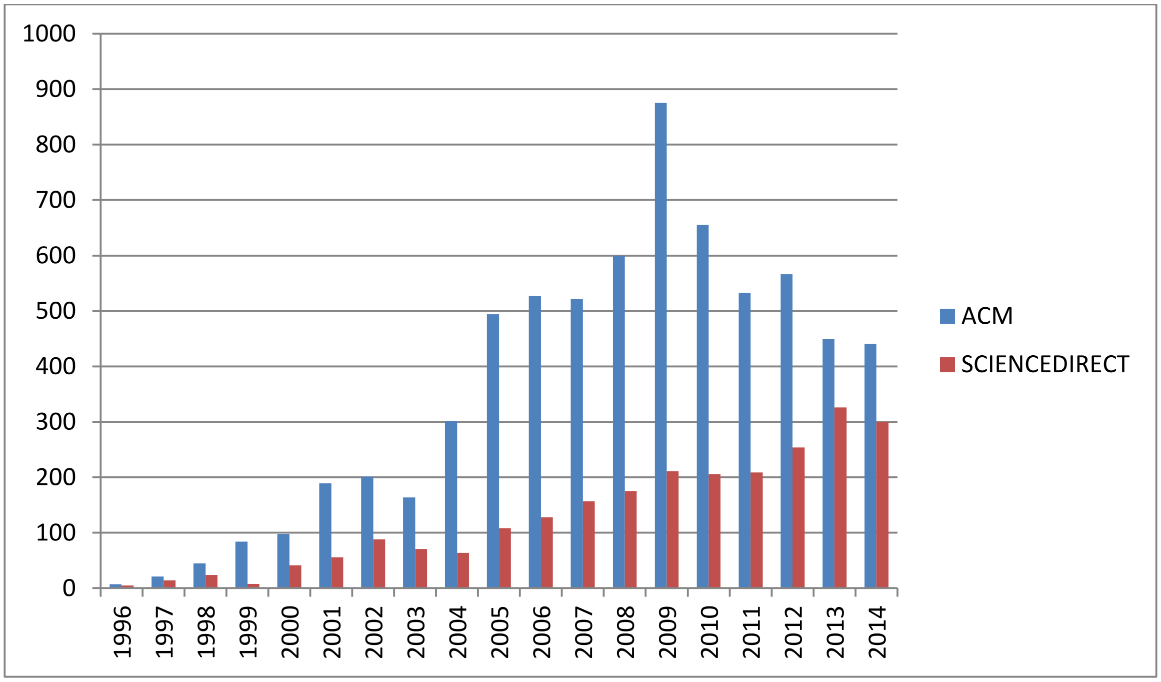


Figure 2-11 Number of publications on digital watermarking (ACM, Science direct)

In addition, in these years several organizations have begun to consider the digital watermarking and include it in their standards. The Copy Protection Technical Working Group has tested the digital watermarking systems for the protection of the video in DVD discs. Two projects (Viva and Talisman) were sponsored by the Union European in order to test the digital watermarking for broadcasting control. In the end of the 90s, several companies were established to launch digital watermarking products on the market. In the field of image processing, the Adobe Company made a collaboration with the Digimarc

Company to use this technique in its software Adobe Photoshop. Since then, the digital watermarking was used in various applications as the broadcast monitoring, Copyright identification, transaction tracking, content authentication, copy control and device control [49].

3.2 Principle of digital watermarking

The principle of digital watermarking is to insert an invisible mark or sometimes visible into an image or document for several purposes such as the protection against fraud, and copyright protection.

The inserted mark is usually a random sequence, a binary logo or an image and it must be known only by the owner or the broadcaster. The insertion of the mark is performed generally in the spatial or frequency domain. However the inserted mark must respect two major constraints: imperceptibility and indelibility. Imperceptibility means that the deformation of the image must be low enough that the user can't distinguish between tattooed image and the original image. And indelibility means that the inserted mark should not be erased after various benevolent or malicious attacks. This second constraint implies the appearance of robustness, which is with the capacity and imperceptibility, are important constraint to design an efficient digital watermarking algorithm. (Figure 2.12)

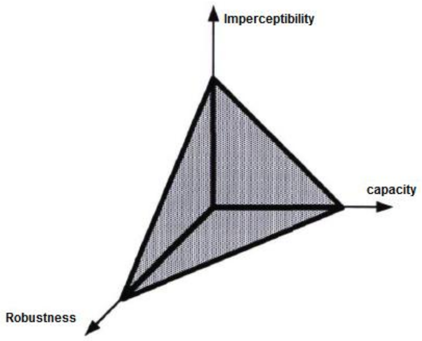


Figure 2-12 the problematic of digital watermarking.

It is clear that these three criteria are contradictory, in other words it is unrealistic to design a watermarking system that inserts a large amount of information (high capacity) and be also very robust. This means that if you want a more robust watermarking, it will take in consideration the effect of making it also more visible. Similarly, if we want to increase the amount of information inserted, it will in return cause a decreasing in strength and imperceptibility. It is therefore necessary to find the best possible compromise between these three parameters depending on the required application [49].

Capacity: is the amount of information that you want to insert into the image, this amount varies depending on the application. In general, few bits are sufficient to protect the author's copyrights with an identifier, but not enough to insert a company logo.

However, it is necessary to hide several bits of information to allow images authentication.

Imperceptibility: the digital watermarking process will certainly distort the watermarked image. This constraint requires that such distortions must be as low as possible so that the visually watermarked image remains very similar to the original image. To do this, the characteristics of the human visual system (HVS) can be used to make the watermark less noticeable. The quality of the watermarked image compared to the original image can be evaluated using mathematical tools such as the peak signal to noise (PSNR), structural similarity (SSIM), etc. The imperceptibility criterion is a property only related to the invisible watermarking.

Robustness: is the ability to recover the inserted watermark even if the watermarked image has been manipulated by image processing attacks. It is necessary to distinguish between several types of attacks depending on whether they are considered Benevolent or malicious. Benevolent attacks are the operations performed by a user in good faith. Included in this category: JPEG compression, some geometric transformations, the spatial and frequency filtering, noise addition, printing and scanning, gamma correction and histogram equalization.

In addition to the above constraints, other criteria must also be considered:

- **False alarm**: which is the detection of a watermark in an image while the image was not even watermarked or it was tattooed with another watermark. This constraint is measured by the probability of false alarm. The threshold of this probability depends on the wanted application: for copyright protection, it is typically of the order 10^{-6}. Otherwise in a copy control application, thousands watermark detectors are running on thousands of images. If a non-watermarked image consistently generates false alarms, this could cause serious problems. So for copy control application, the probability of false alarm must be very low.
- **Algorithmic Cost**: Some applications, such as broadcast control must use fast digital watermarking algorithms which are inexpensive in computing time, in order to support real-time implementation.

- **Encryption and watermarking key**: the security of a watermarking algorithm cannot be based on the fact that its insertion and extraction algorithm is not public. For this, many digital watermarking algorithms are designed to use a cryptographic key. In such a system, the watermark embedding procedure depends on this key. Also a key can be used to detect the watermark if it is existed in the image.

3.3 General scheme of digital watermarking for images

The general scheme of an image watermarking system can be described mainly by two fundamental phases: the insertion and extraction of the watermark. However, a third step may be considered: the transmission.

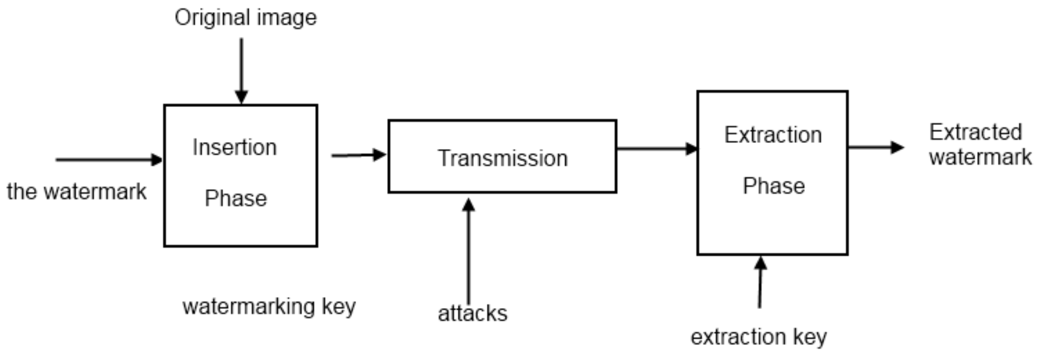


Figure 2-13 General scheme of digital watermarking for images

3.3.1 The watermark insertion procedure

The insertion procedure consist of inserting the watermark M on the original image I_0 and obtain a watermarked image I_W and a third optional parameter can be added which is the secret key of the watermarking C_m which ensures a certain level of security for the watermarking process.

The key generation process can be included in the insertion procedure.

Key generation

The watermark generally is generated from a sequence $m = \{ m_1, m_2, .., m_{N_1} \} \in \mathrm{M}^{N_1}$ and a secret key $c_W \in C_W$. The inserted watermark $w = \{ w_1, w_2, .., w_{N_2} \} \in W^{N_2}$ will be generated using the watermark generation function F_M, most of the times it is a cryptographic function. The binary alphabets $M = \{ 0, 1 \}$ and bipolar $M = \{ -1, +1 \}$ are often used.

The generation of the watermark is mathematically generated as follows:

$$\begin{aligned} &M^{N_1} \times C_w \to W^{N_2} \\ &F_M : (m, c_w) \to w \end{aligned} \tag{1}$$

Insertion of the watermark

In the insertion procedure we generate the watermarked image I_w from the mark w and the original image I_0 using the insertion function F_I.

Lets note $s = \{ s_1, s_2, .., s_N \} \in S^N$ is the sequence of the original image I_0 elements

$$I_w = F_I(s, w) \tag{2}$$

for example if the original image I_0 is an gray scale image of size 512×512 pixels, then each element s_i may correspond to the luminosity of n^{th} pixel, with N= 262144 and $S = \{ 0, 1, .., 255 \}$

the insertion of the watermark can be done mainly according to rules: by multiplication or by substitution.

Insertion using multiplicative rule can be defined mathematically by the following equations:

$$\begin{aligned} I_{w_i} &= s_i + \alpha \cdot w_i \\ I_{w_i} &= s_i (1 + \alpha \cdot w_i) \\ I_{w_i} &= s_i + e^{\alpha \cdot w_i} \end{aligned} \tag{3}$$

Where α is the positive scaling factor which controls the intensity strength of the watermark in order to have the best combination between imperceptibility and robustness. And with the insertion using the substitution the inserted watermark will not be added but substituted with the components of the original image I_0. The addition of the mark by substitution can be done using various methods such as substitution of the least significant bits (LSB) [50], the histogram substitution, substitution of geometric and quantification substitution.

The insertion according to the multiplicative rule is very robust against attacks, but its insertion capacity is very limited. Otherwise the insertion using substitution provides a great capacity, but a limited robustness, to achieve a better robustness it is necessary to make an intelligent selection of coefficients in addition to integrate techniques such as error correction codes.

3.3.2 The watermark extraction phase

Depending on the design of the extraction algorithm, the watermarking scheme can be categorized into three types: blind, semi blind and non blind scheme.

A non blind watermarking scheme is when the original image is required for the extraction of the watermark, semi blind is when a part of an image is required and a blind scheme is when we don’t need the original image or a part of it to recover the watermark only a key can be required in some cases.

3.4 The different representations of the image

Image watermarking algorithms are based on the representation of the image. For the image, there are two types of representation, spatial representation and a frequency representation.

3.4.1 Spatial representation

An image I_0 is an application of the space of a spatial coordinates towards a set of quantized values, each pixel (i, j) of this image is associated with a value $I_0(i, j)$, this value can be expressed in different ways. A pixel in a gray scale image can be represented by its luminance, while the pixels of a color image are generally represented by three components.

There are several color spaces for the images, among them we can mention the fields: (R, G, B) and (Y, U, V) , these spaces have been used in many watermarking algorithms for images [51] [52] [53].

The space (R, G, B) is the best known color space, in this space, the component R represent the red quantity, G the green and the blue component is B. This space is based on an additive color mixing. Which means any color perceived by the human visual system is considered as a linear combination of the three primary colors. The mixture of these components (R, G, B) with different proportions allows to reproduce a significant number of colors. For example, if each component is coded in 256 levels, this allows to have more than 16 million colors $(256 \times 256 \times 256 = 16\ 777\ 216)$.

The human visual system is more sensitive to the components G (green) and R (red) than the component B (blue). For this reason, most of the color image watermarking algorithms insert the watermark using the component B in order to ensure better imperceptibility [54].

The space (Y, U, V) can be described as a mathematical transformation of the space (R, G, B). In this space Y represents the luminance of the pixel and U and V represent the chrominance parameters. The linear relationship between the (R, G, B) space and (Y, U, V) is given by:

$$\begin{pmatrix} Y \\ U \\ V \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ -0.147 & -0.289 & 0.436 \\ 0.615 & -0.515 & -0.100 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} \tag{4}$$

The human visual system is less sensitive to the luminance Y than the chrominance

(U and V).

Since the grayscale image is represented only by its luminance Y, we only consider the grayscale images in this thesis.

The spatial representation of the image does not give a good perceptual analysis, it is difficult to predict the impact of image processing attacks on watermarked images. For example, JPEG compression primarily reduces the high frequencies, that is, the less sensitive to the human eye components. However, in the case of a digital watermarking images in the spatial domain, it is difficult to isolate these high frequencies, which will be potentially attacked and therefore require special handling during insertion and extraction phases.

3.4.2 Frequency representation of the image

The frequency domain allows to further analyze the image and provide a more adequate representation for watermarking.

3.4.2.1 Discrete Fourier transform

This last has been widely applied for watermarking schemes because it offers the possibility of controlling the frequency of the signal. This allows to choose properly the parts of the image that will be watermarked in order to obtain a good balance between visibility and robustness. This transformation is used to merge the signature with the medium in the modulation phase, but also used to divide the image into perceptual bands. Fourier theory allows to decompose an image into a series of sinusoids at different frequencies. Equation (5) gives the decomposition of an image I_0 of size $N_1 \times N_2$ using the Fourier transform:

$$\mathrm{T}_{DFT}\ [I_0] = \Gamma_0(e, f) = \frac{1}{N_1 N_2} \sum_{n_1=1}^{N_1} \sum_{n_2=1}^{N_{21}} I_0(n_1, n_2) \cdot \exp\left\{ -2\pi i \left(\frac{en_1}{N_1} + \frac{fn_2}{N_2} \right) \right\} \tag{5}$$

With $i = \sqrt{-1}, \quad e = 1,2,.., N_1, \quad f = 1,2,.., N_2$

The decomposition of the inverse Fourier transform is given by:

$$\mathrm{T}_{DFT}^{-1}[\Gamma_0] = I_0(n_1, n_2) = \frac{1}{N_1 N_2} \sum_{e=1}^{N_1} \sum_{f=1}^{N_{21}} \Gamma_0(e, f) \cdot \exp\left\{ 2\pi i \left(\frac{en_1}{N_1} + \frac{fn_2}{N_2} \right) \right\} \qquad (6)$$

Equation (6) may also be represented in the form:

$$\Gamma_0(e, f) = \left| \Gamma_0(e, f) \right| \exp\{ i \cdot \phi(e, f) \} \qquad (7)$$

where the function $\left|\Gamma_0\right|$ represents the spectrum of the Fourier transform of I_0 while ϕ is its phase. And $\left|\Gamma_0\right|^2$ is the power spectrum of I_0.

Figure 2.14 shows the Cameraman image and the spectrum of its Fourier transform.

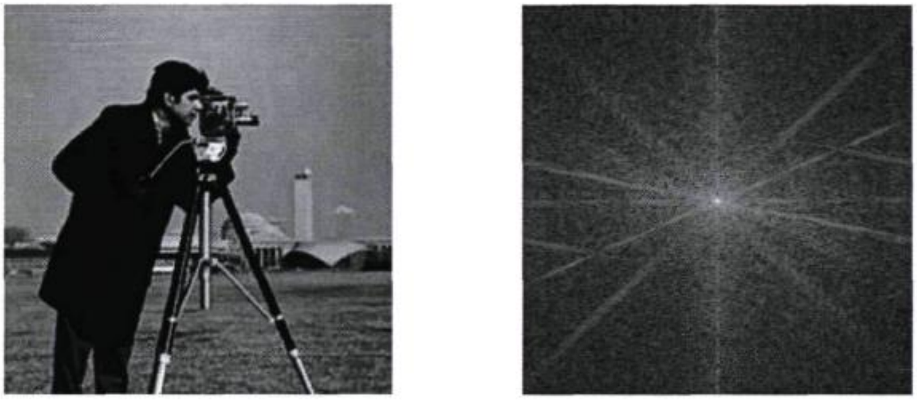


Figure 2-14 Cameraman test image and the spectrum of its Fourier transform.

3.4.2.2 Discrete cosine transform

The watermarking schemes implemented in the DCT domain are often more robust to JPEG and MPEG compression. The creator of watermark can prevent such attacks more easily. Furthermore, the studies concerning the visual distortions on the watermarked image, contribute to a better prediction of the visual impact of a watermark on the medium. Also, the insertion of the watermark in the compressed domain reduces computation time.

The discrete cosine transform of an image I_0 of size $N_1 \times N_2$, noted by $\Gamma_{DCT}[I_0]$ is determined by:

$$\Gamma_{DCT}[I_0] = \Gamma_0(e, f) = \frac{2\Lambda(e)\Lambda(f)}{\sqrt{N_1 N_2}} \sum_{n1=1}^{N_1} \sum_{n2=1}^{N_2} I_0(n_1, n_2) \cdot \cos\left[\frac{\pi(2n_1 + 1)e}{2N_1} \right] \cdot \cos\left[\frac{\pi(2n_2 + 1) f}{2N_2} \right]$$

With :

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & if \quad \xi = 0 \\ 1 & else. \end{cases}$$

And the inverse discrete cosine transform, is noted by Γ_{DCT}^{-1} and is given by:

$$I_0(n_1, n_2) == \frac{2}{\sqrt{N_1 N_2}} \sum_{e=1}^{N_1} \sum_{f=1}^{N_2} \Gamma_0(e, f)\Lambda(e)\Lambda(f) \cdot \cos\left[\frac{\pi(2n_1+1)e}{2N_1}\right] \cdot \cos\left[\frac{\pi(2n_2+1)f}{2N_2}\right]$$

3.4.2.3 Discrete wavelet transform

The Fourier transform is a widely used tool for many scientific purposes, but does not determine the different frequency components of a given signal. For this reason, Morlet [55] introduced a new method called wavelet transform for determining the different frequency components of a given signal, as well as their spatial or temporal localization. By definition, wavelets are functions managed from a mother wavelet ψ by expansions and translations. Thus, the wavelet decomposition involves two parameters which are the scale factor a and a translation factor b .

The scale parameter a provides compressed wavelet (reduced support) and dilated wavelet (extended support) from a mother wavelet.

Compressed wavelets are used to determine the high frequency components while dilated wavelet for determining the low-frequency components. The parameter b, meanwhile, allows analysis by successive translations signal until it is completely covered. The continuous wavelet transform is defined by [55]:

$$\Gamma_{DWT}[\ f(t)\ ] = F(\ a, b) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} f(t)\psi^*\left(\frac{t-b}{a}\right) dt$$

where ψ^* is the complex conjugate of the mother wavelet.

3.5 Applications of digital watermarking images

Digital watermarking applications are numerous among them we mention the following:

3.5.1 Copyright Protection

The copyright protection was one of the first applications of digital watermarking. In legal cases, the owner of an image is able to prove that he is the owner even if attacks have been affected to the image, such application should ensure robustness against attacks, avoid ambiguity of the evidence and minimize distortion related to the insertion of the watermark.

3.5.2 Authentication of image contents

The basic idea of this application is to insert a fragile watermark into the image in order to detect any possible modification of the image by an unauthorized person and locate precisely the manipulated regions. This application is typically used in the legal and medical field.

3.5.3 Control the number of copies

Digital data can be duplicated without reducing the quality, in this context, it is easy for any person who has a digital document, to illegally produce an unlimited number of copies of this document with equal quality to the original document. Digital watermarking can handle this situation. An information about the number of authorized copies are encrypted in the watermark. This principle has been used in videos where the watermark indicates whether the video can be copied or not.

• **Other applications**: there are other applications such as indexing and access control, etc.

watermarking applications can be categorized into local and network architecture, depending on the watermarking application area, in the local architecture we find copyright protection, copy control and indexation applications otherwise diffusion control, transaction management and copyright communication are categorized in the network architecture, while both architectures contains common applications such authentication and electronic commerce, (see figure 2.15).

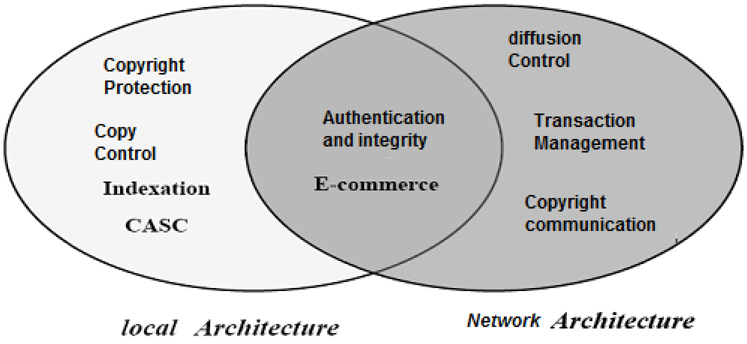


Figure 2-15 The categories of watermarking applications

3.6 Image processing attacks

We can regroup the attacks in the following categories according to the attacker's objective:

3.6.1 Geometric attack

Aiming to reform the watermarked document sufficiently and prevent the detection of the watermark, the most used are:

3.6.1.1 Flipping: Several images can be returned without losing their values. Well the resistance to this type of attack is generally simple to put in work but few systems that prevent this type of transformation.

3.6.1.2 Rotation: a small angles of rotation doesn't really change the value of the image, but can make the watermark non detectable.

3.6.1.3 Scaling (modification of the dimension): this type of operation is used when a picture is scanned or when a digital picture of high resolution is used for digital applications such as the publication in the Web.

3.6.1.4 The Cropping: To suppress or to cut a part of a picture.

3.6.2 Attacks of clair

Aiming to suppress the watermark from the watermarked document, the most developed attacks of clear are:

3.6.2.1 Noises effects: The objective of this manipulation is to approach to better the waveform of the watermark to be able to remove it. The watermark can be estimated by using filtering of Wiener. This evaluation is subtracted then from the original picture to obtain a copy of the message.

3.6.2.2 JPEG compression: The JPEG compression is a technique of compression with losses which suppresses the redundant information of the pictures in order to decrease the size of the image file. As the watermark is invisible, it can be considered as no meaningful and therefore be deleted.

3.6.2.3 Volumetric modifications: it exists a category of processing ('display of histogram, compensation of histogram, or Gamma transformation) that doesn't take into account just the brightness to improve the image. As the alteration is made on the brightness, the watermarked information on the chrominance can be desynchronized.

3.6.2.4 Addition of an additive or multiplicative noise.

Filtering: the filters the most used are: median filter, gausian filter, laplacien filter and average filter.

3.6.2.5 Enhancement and antialiasing: The enhancement corresponds the increase of the components of high frequencies of the image. The picture becomes then more contrasted. The antialiasing is the contrary operation of the enhancement, it reduces the high frequency components of the image which becomes then blurred. These operations can also change the high components frequency of the message and make them lose their particularities.

3.6.3 Cryptography Attacks

Aiming to decrypt the secret key, by using cryptanalyst attacks.

3.6.4 Attacks of protocols

Aiming to find vulnerability in the protocol of management of the copyrights.

The first two types of attacks can be considered as attacks on the robustness, whereas the cryptographic and attacks on protocols are on the security.

3.7 Watermarking scheme based on error correcting codes

Error correcting codes have been considered as one of the good choices to correct errors when extracting the watermark, the errors may occurs during the transmission or when we apply an image processing attacks on the watermarked image.

The encoding of the signature can be performed by using error correcting codes. The work presented in articles [56] [57] [58] [59] are references to a potential use of these error correcting codes to improve the robustness of watermarking algorithms.

The use of such codes appears natural effect if the problem of the robustness of the tattoo is taken communication point of view of a signal over a noisy channel. The use of correction codes in the tattoo remains an open topic, requiring the design of compact codes capable of taking into account the diversity of attacks. Several categories of these correction codes used in the formatting process of signing, are presented in [60] a few of which are listed below:

Linear block codes (n, k) are composed of $M = 2^K$ binary sequences of length n. Any linear combination of code words also form a word code.

Linear cyclic codes: are the most important class of codes in linear blocks. Any circular left permutation of j bits of a code word gives a code word. For these codes, it is generally used polynomial representation of code words rather than vector representation.

Codes (BCH) and the Reed-Solomon codes are examples of these cyclic linear codes.

Convolutional codes are a second family of correcting codes errors at least as important as block codes. To be generated, they use memory registers. A code generated by a symbol also depends on the value of the previous symbol. The Viterbi coding [61] and the Fano [62] are most known convolutional codes.

Turbo codes are another way to construct codes with a minimum distance starting from simple codes and less performance. More specifically, in their basic form, the turbo codes are built by parallel concatenation of two (or more) convolutional codes. The main Turbo Code advantage is the possibility of iteratively decoding a cost calculation that is approximately the same as the cost of decoding the constituent codes [63].

Repeat Codes This is an intuitive way to protect a message, since it consists in repeating n times each of its bits. Each bit of the message is assigned with a code word of size n. Decoding can simply be done by averaging and thresholding the received words. This coding principle is very simple to implement and is often effective when the channel is disrupted (low capacity) [63].

3.8 Conclusion

In this section we have presented an overview of digital watermarking technique, we presented the global classification of digital watermarking schemes for images, and the principle of watermarking in spatial and frequency domains, furthermore we provided the most common applications of digital watermarking such as copyright protection, authentication of digital images, and the control of the number of copies. Then we presented the image processing attacks targeting the watermarked image.

The digital watermarking is considered a very active research area for content authentication in the last decade.

Chapter 3 User Authentication methods

1. Passwords state of the art

1.1. Definition

When a user wants access to a system it must initially perform an identification and authentication procedure. In the identification phase of establishing the identity of the user, it allows him to answer the question: "Who are you?”. The user uses a username (email, etc.) that identifies and assigned to him individually, this identifier is unique.

Then there is the phase of authentication which is a phase that allows the user to prove his identity. It comes after the identification phase. It answers the question: "Are you really that person?” The user uses an authenticator or "secret code" that only he knows.

The secret code of a user is a personal information that should not in any case be disclosed, it is also commonly named "password". The password does not provide a right of access, it only helps to ensure accountability in the use of these access rights.

1.2 Attacks on Passwords

We can identify various attacks used by hackers to find a password [64]:

1.2.1 Brute Force Attack

There are two types of attacks using dictionaries, the direct attack when the attacker has no way to access the password hash.
Thus, it will launch a program that will test all combinations until it finds the right one. There are different types of software to brute-force attack, from simple tester numbers, uppercase and lowercase letters, special characters, through testing those passwords with a dictionary of words to some much more advanced that test passwords shape. Because in some cases (companies) positions administrator passwords are composed of different variables that change in each case but have a similar structure.

If a password is: 22-NOV 4-OSSOS
The hacker will test: [0-9] [-] [AAA-ZZZ] [0-9] [-] [AAAAA-ZZZZZ]

This thus reducing several orders of magnitude the number of attempts. A second type of attack by brute-force can be produced from the "hashes" of passwords. Generally, passwords in a database are "hashed", so when the hacker has a view of the database, he cannot see passwords in clear.
The hacker, who obtained a hashed password will try again to break the brute force, but not as before trying all combinations of letters and numbers etc. It will pass by "Rainbow Tables" [65] allowing it to attack by comparative brute force to find the right password.

This vulnerability became harder to exploit when an administrator will add "Salts”.

The "salts" are simply an added string to the password before being hashed and compared in the database.

For example:

Salt= Ly25_13C_

Password=test
Salt+password= Ly25_13C_test

By using the hash function MD5 we obtain:

Hash(Salt+password) = a6e013de18c29203281220fa638d1a02

Thus, an attack by "Rainbow Tables" will find no correspondence and will be doomed to failure, except of course if the attacker has access to the source code of the application and knew how the Salt is being generated before comparing or registering our password in the database. So the salts also can be vulnerable, and may fail to protect the password, because the hacker can create his own Rainbow-tables based on the known salt.

In the process of creating the salt rainbow tables the hackers use the zombie computers or cloud computing in order to make the procedure faster. An administrator can also combine Salts with an iteration number for the encryption algorithm. Which means after concatenated values Salts and password, it is possible to iteratively apply the same (or more) encryption algorithm on a result of the hash. In terms of performance, the cost of this technique is negligible for the final user but becomes a real handicap for the pirate.

Other attacks may be committed in order to find passwords or simply bypass; we will mention a few and some ways to counter them.

1.2.2 Attack Man in the Middle (MITM)

This attack is one of the most known attacks, it consists to sniff data that passing through a computer network in order to recover the flow of information contained primarily in the application layer of the ISO model. Thus, all of the passwords in plain passing over the network can be recovered. The only protection for this is the use of secure protocols [66] SFTP, SSL, etc. Although there are some cases of attacks against the most secure protocols.

1.2.3 Replay attack

A replay is a form of network attack in which a transmission is maliciously or fraudulently repeated by a third party intercepting packets on the line.

1.2.4 Injection Attack

This attack targets more the applications which have a connection to a database. They allow the injection of false requests to the database in order to modify, to read or to insert data (run server commands in some cases). We can note such attacks: SQL injection attacks, the blind SQL injection often made in an intranet.

These types of attacks can be resisted by appropriate configuration of server applications or by inserting function doing work in the source code. Beware though, some of these functions are fake and do not provide any protection against injection attacks.

1.2.5 The session hijacking

There are different types of session hijacking, client side the famous "XSS", server side or network side (MITM attack). The hackers hijack a session without having the password to login.

To counter this kind of attacks, we can apply certain protections:
- Restriction by IP address thus allowing to counter the session hijacking via the Web (because IP is unique for each user), but not if it takes place in the same network.
- Restriction by environment is for example, the identification of User Agent of the visitor (Navigator) having the open session. If the pirate does not have the same one, its session will be finished [67].

1.3 Classic Authentication by Passwords

A pair (login and password) are the key to gain access to the system, the pair is recorded in a database of identities, the system generally saves the password in the database in the hashed form.

Most users just use a password easy to remember [70].

The following Table represents a row in the user table of a website using an authentication system by conventional password.

ID	Email	Name	Hased(Password)	Salt (random value)
1	User1@mail.com	User1	a3241b42d2e….	Ly_14_A
…	…	…	…	…

IT systems use hash function to secure password, when the password is hashed, it is still useful. The hash function is deterministic, so we can still rehashing a putative password and see if the result is equal to a given hash value. Thus, an encrypted password is sufficient to check whether a given password is correct or not.

1.4 Improve the password hash with bits of "Salt"

See the following scenario: You have a Web site, users can connect by entering their names and passwords. Once connected, users earn "additional privileges" such as data reading and writing.

The server must stock "something" that can be used to verify the passwords of the users. The more elementary "thing" is the password itself. We can assume that the passwords are stocked in a database, probably at the same time data are used by the application. The bad thing about this "in plain" storage of passwords, which leads to a vulnerability in the case when an attack model where the attacker can get an access in reading-only to the server's data. If these data contains user passwords, then the attacker could use these passwords to connect as user and has the corresponding privileges.

Storing hashed passwords only solves these problems. It is unavoidable that the complete extraction of the server data provides enough information to "try" passwords (using "offline dictionary" or "brute force"), because the discharge allows the attacker to "simulate" the complete server on its own machines, and try passwords during the simulation procedure. A hash function is the right tool for this and the hashing process should include the "Salts" to improve the security in the server.

1.5. Authentication by single password OTP

A single password or OTP (One-Time Password) is a dynamic password that is valid for a session or a transaction. OTP allow to fill the gaps of traditional static passwords, such as vulnerability to replay Attack]. This means that if a potential intruder (MITM) managed to record an OTP which was already used to connect to a service or to perform an operation, it will not be able to use it because it will no longer be valid. However, the OTP cannot be memorized by the people, therefore they require additional technologies to use them.

1.5.1 Generation of OTP

OTP generation algorithms typically use the random to become complex and concrete, such algorithms have different approaches to achieve this, they either:

- based on time synchronization between the authentication server and the client who supplies the password (OTP is only valid for a short period of time).
- Uses a mathematical algorithm to generate a new password based on the previous password (OTP is actually a suite and must be used in a predefined order).

1.5.2. Token of OTP authentication

There are different manners to integrate the user in the next OTP to be used. Some systems use electronic tokens of authentication (Figure 3.1) which generates some OTP and that allows to be gotten while using a small screen. Yet, other systems permit to generate OTP in the server's side and to send it to the user while using a channel of telecommunication as the SMS messaging but it poses a problem if one pirates the server. Finally, in some systems, the OTP are printed on the paper that the user is held to keep with him. The token can be used by a person in the case of theft [68].

Figure 3-1 electronic token of OTP authentication

1.6. Authentication by the Open-ID

The problematic of the unique authentication lands for a long time in the information technology domain. It was question especially within the enterprises, where the user access regularly to a crowd of applications in his daily job (work station, messaging, time management tool, distant server, etc.). Also a user access to a lot of applications for a personal usage. With the explosion of the accesses to Internet, the multiplication of the blogs, wikis, forums and other commercial sites, the question to simplify the management of these multiple accounts arises again [69].

In this case can the Open-ID intervene?

After a short recall on what is the unique authentication, we will detail Open-ID, then we will see the different possibilities of setting up a solution based on Open-ID. The principle of the Open-ID is to allow the user to authenticate itself once for all of his session, and to manage the access to some of his personal data (name, first name, email, etc.) He authenticates himself by the server of authentication (ID / password), All demand of authentication of any application is rerouted toward the server of authentication, which authenticates the user by this application. No intervention is necessary on behalf of the user. The application can get by the server of authentication some personal data on the user of whom will have allowed the diffusion. When the user leaves his session, his authentication is dismissed [67].

1.6.1 The Open-ID Protocol

Open-ID is a free and decentralized solution of unique authentication, it permits to get a numeric identity quickly, to change or to dismiss this identity is also quickly. The architecture being decentralized, and it only depends on one supplier of service, we can change regularly and easily or to host ourselves our numeric identity (Figures 3.2.).

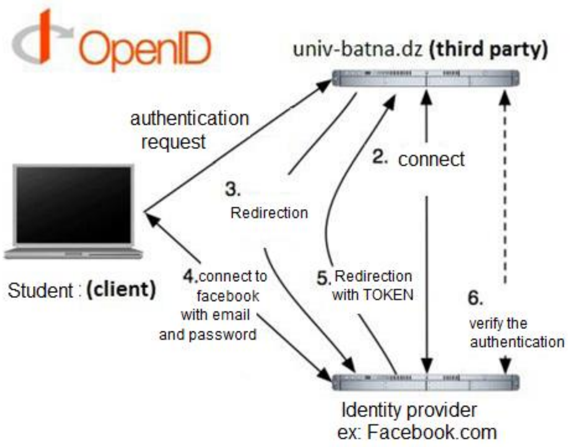

OpenID
univ-batna.dz (third party)
authentication request
2. connect
3. Redirection
Student : (client)
4.connect to facebook with email and password
5. Redirection with TOKEN
6. verify the authentication
Identity provider
ex: Facebook.com

Figure 3-2 the function of the Open-ID Protocol

Thanks to the identity numeric Open-ID, it will able us to:

- To connect only one time and provide us the access to all our favorite websites without carrying all couples (username / Password).
- To centralize the modifications of our information (example: alteration of address email, the name, etc.)
- To manage the access authorizations to our information of every visited site.

1.7. Authentication by the dynamics passwords based on the time

Therefore, the researchers decided to create the new model of authentication on the basis of the dynamic passwords [71], [72]. A model must not contain any complication and can be put merely in work, with the full security and without slowing down the functional system.

There are dynamic passwords schemes that are based on the time but they hash the password that is under mailing toward the server, in order to avoid the Man in the Middle (MITM) attack.

1.8 Conclusion

In this section we presented an overview on the most used method for user authentication, which is the password, many attacks have been given such as brute force attack, man in the middle attack, replay attack and session hijacking, the classic authentication using password can be vulnerable to these attacks, for this concern the password schemes have been improved by including hash functions, adding salts, and recently the OTP and the dynamic password schemes are considered more interesting, because they offer a better security and they resist most password attacks.

2. State of the art Biometric

Introduction

A wide variety of systems require reliable personal identification arrangements which determine the identity of an individual requesting their services. The purpose of such arrangements is to ensure that the services are accessed only by a legitimate user, and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, and mobile phones. In the absence of strong personal identification arrangements, these systems are vulnerable to impostors.

Biometric identification or simply biometrics refers to the automatic identification of individuals based on their physiological features and / or behavioral. By using biometrics it is possible to confirm or establish the identity of an individual based on "who you are", rather than "what you have" (identification card) or "what you remember "(password). Biometric technology has already found its place in various fields; the visual surveillance to access control, the technology in growing root in areas demanding advanced security. If this is impressive, the future is shown to be even more fascinating [73] [74].

In this section we will present the biometric science and the most used techniques in user authentication field.

2.1 Biometric Identification System

Biometrics as a science has in fact quickly turned into a tool used primarily for the creation of security and automatic access control systems such as safety deposit boxes, residences called high security, and of course ATMs. For this purpose a biometric identification system is very effective against any attempted fraud or hacking of secret codes. A biometric identification system must first store the biometric data of authorized users, and when someone tries to access to the protected data (or local), its biometric characteristics are then compared to the one already stored in the identification system. If a certain degree of similarity is registered, the person may have access to the protected information (or local). A good biometric identification system will only consider unique and permanent characteristics of a person. These permanent characteristics change very slowly over time. For example, the hand of an adult should basically keep the same characteristics over a period of five years, except in a case of an accident or surgery for example [75] [76].

2.2 Interest of a biometric identification system

Today, fraud is increasing in our society. Some users called impostors are able to forge their identity with remarkable ease. This is due to the fact that the most widely used authentication systems on the market are based on the conventional solution using an access with a username and a password, often associated with a smart card containing information about identity of its owner. However, users are not completely satisfied with these cards for the following reasons:

- Cards based on passwords are not reliable.
- The cards can be lost, forgotten or misplaced.
- Password may be forgotten or compromised.

We note that a robust authentication system can be constructed by simultaneously combining multiple biometric authentication methods (multimodal system) [78].

Table 3.1 shows a comparison between the biometric authentication and traditional password authentication.

Table 3.1 comparison of biometric authentication and password [79].

Biometric Authentication	Authentication using password
- based on morphological measurements, behavioral or biological. - Authenticate the individual - Information is closely related to the user. - Uses a probabilistic-list comparison. - The biometric information can be modified and / or altered with time, it is uncertain. - Problem of respect of private life - difficult to revoke Information	- Based on what we known or what we have - can be more complicated (complex password) - Authenticates the key. - It can be lost, stolen or forgotten. - The information does not vary, it is certain. - less impact on privacy - Easy to change

2.3 Qualified biological measures of biometric

The physiological characteristic and / or human behavior can be used as a biometric characteristic as long as it meets the following requirements:

Universal: exist in all individuals.
Unique: can differentiate one individual from another.
Permanent: allow evolution over time.
Recordable: characteristics of an individual are collected with his consent.

Measurable: allow future comparison.
Execution: pertaining to the accuracy of identification and achievable speed, the resources required to achieve the desired accuracy and speed of identification, as well as operational and environmental factors that affect the accuracy and the speed.

Acceptability: indicates the point at which people are willing to accept the use of a particular biometric mark (characteristic) in their daily lives, the system must meet certain criteria (ease of acquisition, speed, etc.) in order to be employed [79].

2.4 Biometric Techniques

There are three categories of biometrics technologies, the first is the biological analysis as tests on blood, DNA, urine etc. The second is the behavioral analysis, it treats the dynamics of signature, how to use a keyboard or how to walk. Finally there is the morphological analysis is the most widespread and that processes fingerprints, hand geometry, voice, drawing venous network of the eye, etc. (Figure.3.3)

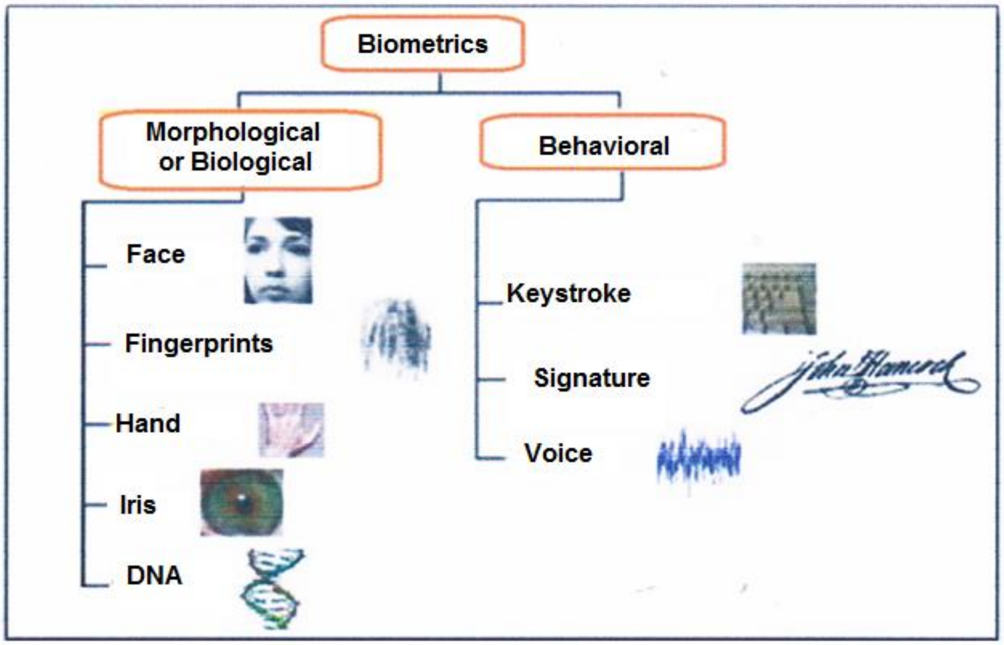


Figure 3-3 biometric techniques [80].

2.4.1 Biological Analysis

The DNA analysis is a method of identifying individuals extremely accurate, it is derived directly from the evolution of molecular biology. The concept of DNA was introduced by an English biologist, Alec Jeffreys in 1985 [81]. The technique has benefited from the invention of PCR (Polymerase Chain Reaction) by Kary Banks Mullis, American biochemist, is a polymerase chain reaction of DNA which allows to obtain substantial quantities of DNA from a single molecule. It was used for biometric identification of individuals for forensic purposes. The genetic information of an individual is unique. DNA is an identification "tool" by excellence, several states across the world have or are planning the creation of a genetic database and plan to legislate in this area. The UK is a leader in this field and has in its NDNAD base, the largest number of profiles compared to its population [80].

2.4.2 Behavior Analysis

2.4.2.1 Dynamic Signature

Everyone has his own writing style. From the signature of a person, we can define a model that can be used for identification. The signature is used in many countries as a legal or administrative element, it is used to justify the good times of a person or to lead confuse previously signed documents [80].

Advantage:

- It can be stored.
- It involves the responsibility of the individual.

Disadvantages:

- The acquisition requires a graphics tablet.
- It is sensitive to the emotions of the individual.
- Cannot be used for access control.

2.4.2.2 Keystroke dynamics

During World War II, US military intelligence could distinguish messages in Morse code of the enemy by what they called "Fist of the sender" or writing of the sender. In fact the military measured the typing rhythm to determine who the sender was. In the early eighties, the US National Science Foundation commissioned a study to determine if this feature could be used to identify people by typing rhythm on a keyboard. At that time, the National Bureau of Standards US also conducting a study concluding that there unique features when a person types on a keyboard. It gave the mandate to the Stanford Research Institute (SRI), who worked on the issue until 1985 and developed a biometric technology based on keystroke dynamics [80].

2.4.2.3 The Voice

The voice biometric process data dependent on both physiological factors of age, sex, tone, accent and behavioral factors such as speed and rhythm. They are generally not imitable. This is the only technique that can currently recognize a person from a distance and is generally well accepted by users. However, this technique is easily falsifiable and in addition requires excellent recording quality. Also little difference between the two voices makes this an unreliable technology [80].

Advantages:

- readers are easily protected
- Only information usable via telephone
- Inability to imitate the voice
- It is not intrusive

Disadvantages:

- Sensitive to the physical and emotional state of the individual
- Possible fraud by recording

- Sensitive to environmental noise
- Rate of false rejection and false acceptance are high

2.4.3 Morphological analysis

2.4.3.1 Shape of the hand

Every individual has his own hand shape. It can be acquired using a specialized scanner. The length of the fingers, their thickness and their relative position are parameters which are extracted from the image and compared to those existing in a database. However, that biometrics are subject to certain changes that are due to aging. The biometrics systems using the shape of the hand are simple to implement, and are very well accepted by users [80].

Advantages:

- Very well accepted by individuals to identify or verify
- Simple to use
- No effect on identification or verification when fingers are wet or not very clean.

Disadvantages:

- Bulky for offices, in a car or a telephone
- Risk of false acceptance for twins or of a family member.

2.4.3.2 Fingerprints (Finger-scan)

The database in the case of fingerprints is the drawing represented by the ridges and furrows of the skin. This design is unique and different for each individual (figure 3.4). In practice, it is almost impossible to use all the information provided by this drawing (because too many for each individual), so researchers prefer to extract key features such as ridge bifurcations, "islands", the lines that disappear etc. A complete fingerprint contains about a hundred of these feature points (the "minutiae"). Considering the actual scanned area can be extracted about 40 of those points. Yet again, the products offered on the market are based on a couple of these points (12 at least) or less for many of them (up to 8 minimum). For history, the number 12 comes from the rule of the 12 points that it is statistically impossible to find two individuals have the same 12 feature points, even considering a population of tens of millions of people [82].

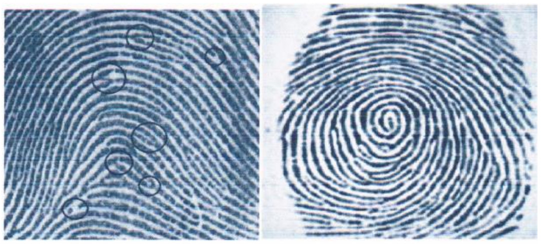


Figure 3-4 Fingerprint

2.4.3.3 *Geometry of the hand / finger (hand-scan)*

This type of biometric measurement is one of the most common, especially in the United States. This consists of measuring a number of characteristics of the hand (up to 90) as the hand shape, length and width of the fingers forms joints, inter-joint lengths, etc. the technology associated is mainly infrared imaging; in general, the system present high FAR (False Acceptance Rate, see below), especially between people of the same family or even twins [82].

2.4.3.4 Iris (iris-scan)

The first use of the pattern of the iris as a recognition means back to ophthalmology manual written by James Hamilton and Doggarts in 1949 [83]. The iris recognition uses more parameters than the other identification methods, and results a high reliability. The probability of finding two identical irises is 1/1072 based on Daugmann estimation. The first step is capturing the image of the iris. In fact, the eye is an organ (see Figure 3.5) very sensitive to light and to fatigue, both factors which can vary its size and sharpness. In addition, it is often obscured by eyelashes, eyelids, lenses, light reflections or uncontrolled movements of the person [80].

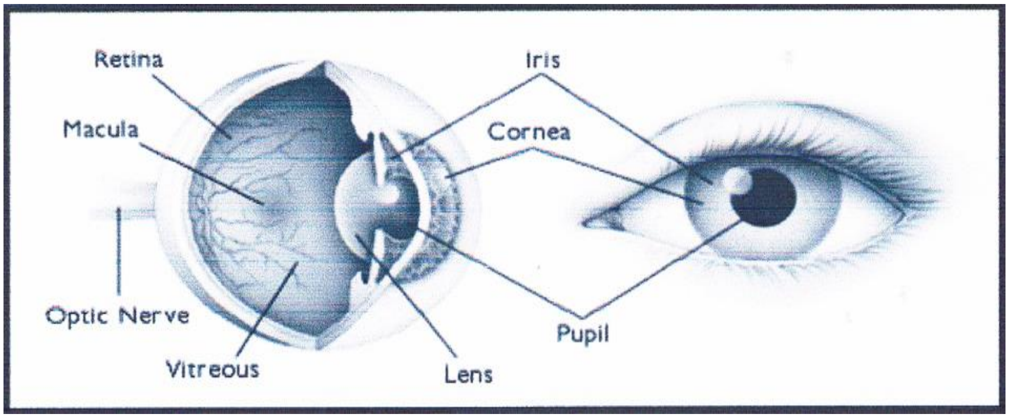


Figure 3-5 Characteristic of the eye [77]

Benefits:

- The iris contains a large amount of information
- No confusion for twins

Disadvantages:

- Invasive and non-friendly method
- the iris can be easily photographed

2.4.3.5 Retina (retina-scan)

This biometric measurement is older than that using the iris, but was less well accepted by the public and users, probably because of his character too restrictive: the measurement must be done at very small distance from the sensor (a few centimeters), which then performs a scan of the retina. It is physically impossible to carry out a retinal measurement at a distance of 30cm or more on a moving subject as can be seen in some movies. This method requires cooperative and trained subjects [77].

2.4.3.6 Face (facial-scan)

This is to make a photograph more or less evolved to extract a set of factors that are specific to each individual. These factors are chosen for their high and invariability involve areas of the face such that the top of the cheeks, the corners of the mouth, etc. and preventing the other types of hairstyles, areas occupied by hair in general or any area subject to change during the person's life (Figure 3.6).

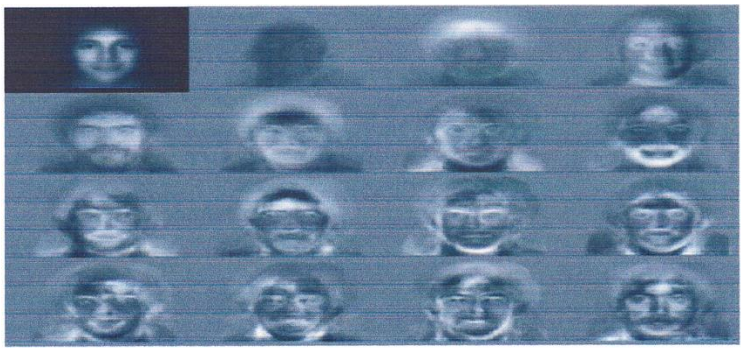


Figure 3-6 The face features [77]

There are several variations of facial recognition technology. The first is developed and supported by MIT and was called "Eigen face". It consists in breaking the face images made of several shades of gray, each highlighting a particular feature.

2.4.3.7 System configuration of veins

This technique is usually combined with another, as the study of the geometry of the hand. This is to analyze the pattern formed by the network of veins on a body part of an individual (the hand) to save some characteristic points [77].

2.5 Biometric devices

Authentication biometrics is used in all fields requiring controlled access such as banking applications, high security locations such as the seats of government, parliament, army, security service etc. As for recognition, it is often used by police and immigration authorities at airports and in search of criminal databases. It is found also in civil applications where authentication of credit cards, driving licenses and passports is becoming more common. With the advent of the Internet and its extension and with the development of various services through the fabric and especially with the emergence of electronic commerce (e-commerce), all suppliers of products and services are now supplying considerable efforts in order to secure against all possible fraudulent intrusions. Here is a partial list of applications that use biometrics to control access:

Physical access control to premises: Computer room, sensitive site (search service, nuclear plants, military bases ...).

Logical access control to information systems: Launch of the operating system, computer network access, e-commerce transaction (financial for banks, data between enterprises), and all software using a password.

Communication facilities: Internet access terminals, mobile phones.

Machines & Other equipment: Safe deposit with electronic lock, ATM, checking membership in a club, loyalty card, management and control time and attendance, car (immobilizer) etc. (Figure 3.7)

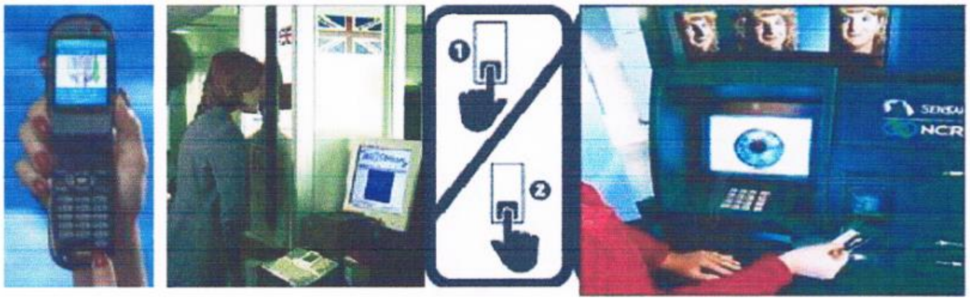


Figure 3-7 various biometric machines

2.8 Conclusion

Biometrics technology has already found its place in various domains; the visual surveillance, user authentication and access control, but unfortunately it still has a weakness, because the biometric measures can be not accurate because it is indeed a major feature of any living organism: it adapts to the environment, we get, we suffer more or less significant trauma in short, we evolve and actions change. Consider the simplest case, that of fingerprints (but note that the same applies to any natural given). Depending on the case, we present more or less sweating; finger temperature is anything but regular (on average, 8 to 10 'Celsius above ambient temperature). This affects the biometric authentication process.

3. State of the art on the technology RFID

Introduction

The Radio frequency identification (RFID) is a booming technology. It is increasingly used worldwide, it allows the identification without contact nor direct vision of the people or objects. For that, it is based on radio frequencies waves to exchange data between intelligent tags and readers. Once the data, associated with an object or a person is recovered by the reader, they will be sent towards the information system (middleware) which is responsible for managing them. The first part of this section will present the general concepts of the RFID: Definition, function, classification and application. The second part of this section will interest the security in RFID systems: Presentation of the deferent problems and attacks related to the RFID [84] [85] [86].

3.1 What is the RFID?

Definition

The RFID is a technology allowing the identification of people or objects without contact nor direct vision based on radio frequencies. It is articulated around three principal components:

- **The tag**: or label, transponder, smart label, which is the equipment associated with the object or the identified person. It stores the relative data to this object.
- **The reader:** or base station, interrogator, which is the equipment able to interrogate the tag remotely and retrieve (or to register) data related to the traced object.
-**The middleware:** which is the software that is responsible for managing, collecting and to format the data for the final application, which is dedicated to the company.

Figure 3.8 illustrates these components and their interconnections. Several interconnected readers via the information network of a company read the data presented on the tags associated to different objects. Middleware is responsible for managing RFID infrastructure as well as data from the readers, in order to provide to the finale application the needed data [87] [88].

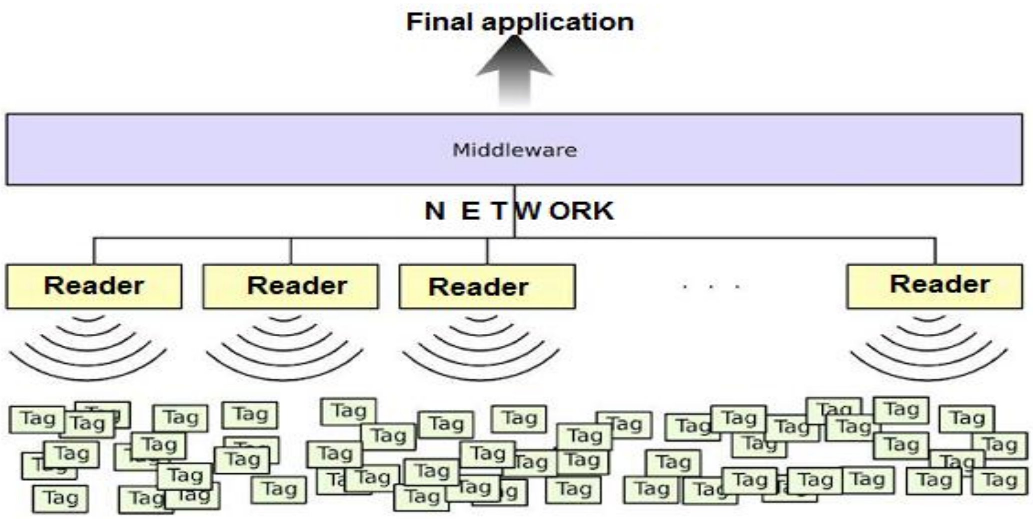


Figure 3-8 Overview of an RFID system.

3.2 The evolution of RFID technology

Contrary to what we might think, Radio Frequency Identification (RFID) is not a technological revolution of the twenty century, but the first half of the twentieth. However, it has evolved since then and the RFID which surrounds us today has not very changes of the RFID back then, of course, the physical principles on which it is based are the same, but advances in electronics have radically changed: the price of a tag can reach fifteen cents and its size is sometimes smaller than a grain of rice. These extreme values must not however hide the reality, because each application has a corresponding tag that is suitable to it, there is no need to use a tiny tag (it must be expensive) for an application that does not require it, and it is impossible using a tag of 15 cents for an application that requires security. So there is a wide range of tags with very different characteristics, from simple memory without computing capacity to the RFID card with a chip capable of using public key cryptography [89].

3.3 RFID Classification

Global standard EPC (initiative to innovate and develop industry-driven standards for the Electronic Product Code™ (EPC) to support the use of Radio Frequency Identification (RFID)) distinguishes four classes of tags.

Class 1: corresponds to the least performing tags and therefore cheaper. They have a memory accessible in read-only, which contains a unique identifier (typically 128 bits). When the tag is questioned by a reader, it simply sends its identifier. Class 1 tags can be found in libraries, supply chains, etc.

Class 2: allows you to implement functions on the tag, typically a symmetric cryptographic algorithm and possess few hundred bits of rewritable memory. However, the tags of classes 1 and 2 are passive which means they don’t have a battery and must be present in the field of the reader to communicate and perform calculations. These tags have a relatively small distance of communication: a few decimeters at high frequency and up to a few meters at ultrahigh frequency. Finally, it considers that their resistance to physical attacks is very limited: it is generally advised that the same secret information must not be shared by multiple tags to limit the consequences of such an attack.

Class 3: Class 3 tags are semi-passive, which means they have an internal power source to perform calculations, but the energy provided by the reader is always necessary for communication.

Class 4: Class 4 tags are active, with a battery used in both calculations and communication, allowing them to initiate their own exchange with a reader and possess greater communication distance. This standard also considers that the Class 4 tags can communicate with each other's [87].

There are several other ways to classify RFID systems. Like the classification based on the frequency of the used wave for communications (readers / tags). Indeed, this frequency is directly related to the physical phenomena concerned to carry out the communication, table 3.2 presents the different frequencies used in RFID.

Table 3.2 Selected frequencies and / or authorized in RFID

Radio frequency waves			**Selected frequencies and / or authorized in RFID**
From 30 to 300 KHz	LF	Low frequency	< 135 kHz
From 3 to 30 MHz	HF	High frequency	13,56 MHz
From 300 to 3 000 MHz	UHF	Ultra high frequency	433 MHz & from 860 to 960 MHz & 2,45GHz
From 3 to 30 GHz	SHF	Super high frequency	5.8 GHz

The frequency used by an RFID system will directly impact the distances of the possible readings. Thus, the low frequencies LF and the high frequencies HF will be used mainly for applications of short distances < 1cm from proximity " few centimeters " and neighborhood "tens of centimeters" when the ultra-high frequency UHF and super-high frequencies will be used primarily for long distance applications "few meters" even very long distance "several meters", as shown in Figure 3.9.

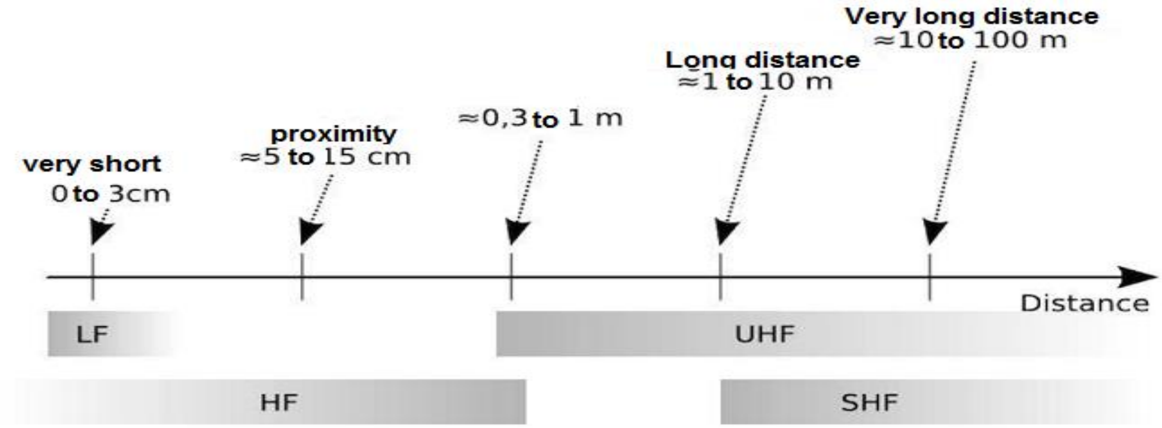


Figure 3-9 Distances of Operating RFID systems

3.4 Operation

The main feature of RFID systems is the use of the transmitted wave by the reader: the tags receive energy from the reader to operate and use the received wave from the reader to communicate. The following paragraphs explain in detail the operation of RFID systems from the point of view of the remote supply and the specific communication of RFID systems in which one of the devices (the tag) has not a transmitter. [85]

3.4.1 Physical principle of operation between tag and reader

These systems typically operate in the far field because the distances between tags and readers are sometimes large (meters), the coupling between the tag and the reader is radiative. The main technique used is the far-field known as retro-modulation, or backscattering: the tag will reflect the wave emitted by the reader as shown in Figure 3.10

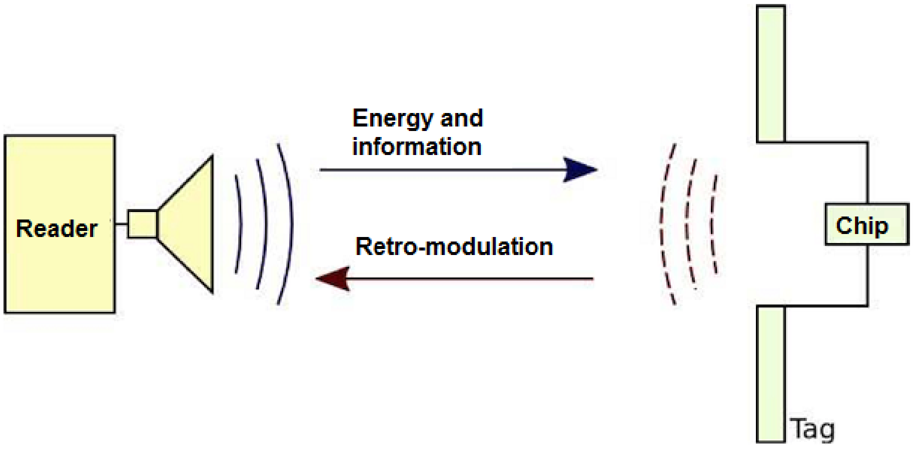


Figure 3-10 Technique of retro-modulation, or backscattering

In order to be understood by the reader, the tag changes the amount of energy reflected varying the charge across its antenna. Figure 3.11 illustrates the retro modulation for 3 deferent loads. In normal operation (a), the impedance of the chip and the antenna are adjusted. Thus, part of the absorbed wave by the antenna is transmitted to the chip and another part is reflected. This reflection is minimal, because in this configuration the power of the chip is optimal.

In the case of an open circuit (b) there is no load connected to the antenna: it's an open circuit. In this case, there is no power transmitted to the chip which is disconnected, and the reflected wave is negligible in most cases. In the case of a closed circuit (C), the antenna is short-circuited. Here, the reflected power is very important but no power is transmitted to the chip. We have seen how, despite the absence transmitter, the tag is capable of transmitting a signal to the reader. The following paragraph explains the techniques used in RFID to encode information.

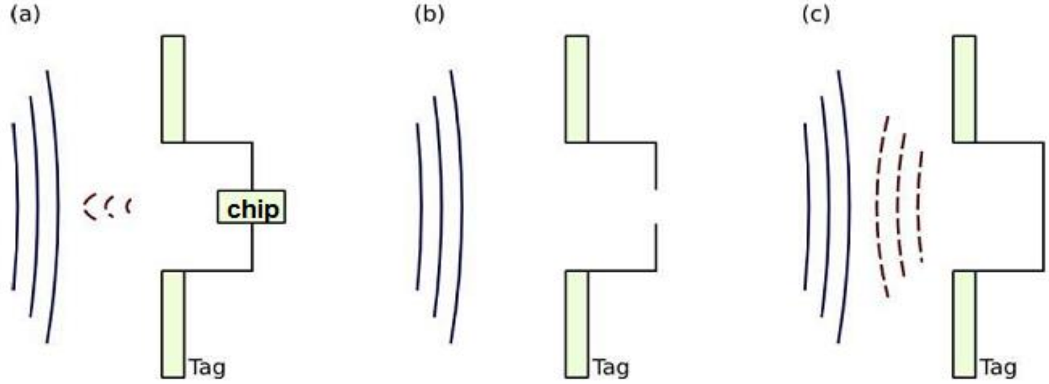


Figure 3-11 Modulation of reflected power (a) matched load, (b) open circuit and (c) short circuit

3.5 Security Issues

3.5.1 Identity Theft

If there are multiple types of tags, it is because there are also several types of applications. We must distinguish those whose main objective is the identification of objects or of subjects (replacement of bar codes, animal tattoo, etc.) from whose purpose is authentication of the same objects or of subjects (badge to access a building, startup key of a car, subscription to public transport, etc.).

The identification is not intended to prove the identity of a person or an object, but only to announce an identity. Anyone who listens to the communication between a reader and a tag is able to hear this identity but it is not the theft.

In contrast, an authentication protocol must ensure to the reader that it communicates with the rightful person or the supposed object [85].

While it is possible to design authentication protocols that are safe, it is not uncommon to see in practice attacks on authentication systems based on RFID, particularly access control systems. Several reasons explain this. First, many firms offer authentication systems that hide in fact only an identification protocol. Then, the constraints of RFID, particularly in terms of calculation, encourage the use of cryptographic algorithms “light” in terms of calculation, but also unfortunately “light" in terms of security. Two high-profile examples are the DST module Texas Instrument breaks in 2005 and the NXP Mifare Classic chip has sold hundreds of millions of copies and as always sale is totally broken since 2008 [85].

Finally, note that a serious generic attack may thwart any existing authentication protocol, this attack, called relay, it exploits the fact that tags are willing to answer without the prior consent of the holder. It involves two partners linked by a sufficiently rapid communication channel (for example, a radio communication) for data transmission. One of the accomplices is located nearby a legitimate RFID reader, example: a cinema ticket distributer, while the second is located near to RFID victim for example: tag of a customer waiting for his turn in the chain to buy a ticket. This technique allows somehow to create an extension cord between the victim and the distributor, the two attackers simply relay the messages between the two parties, making the victim believes that he is communicating directly with a legitimate distributor and vice versa.
The protection against relay attacks is not an easy thing because the use of cryptography alone does not ensure security against this type of attack.

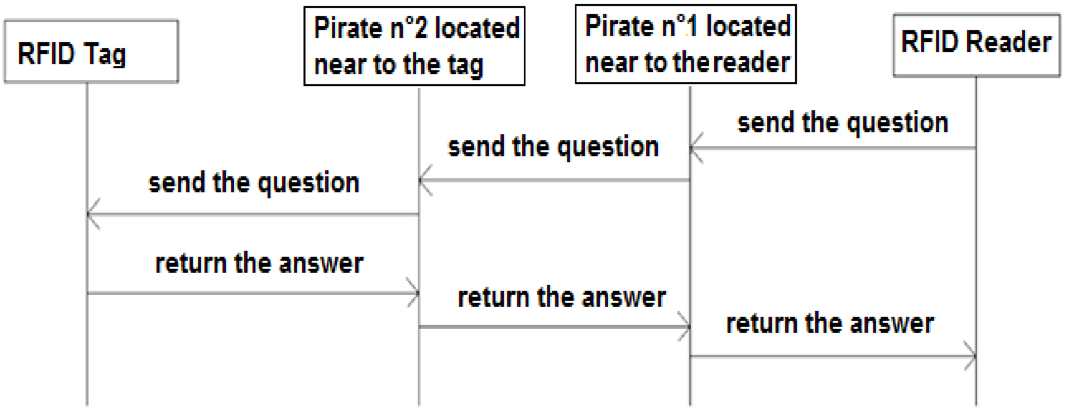


Figure 3-12 scheme of an attack by relay using the mafia fraud attack

3.5.2 Leak of information

Whereas the usurpation of identity only concerns the tags that have the objective to achieve the authentication, the problem of the flight or leak of information concerns all tags potentially. This problem lands at the time when data sent by the tag reveal the information on the object or the person that carries it. For example, a document of identity or a payment card can reveal confidential information, a card of public transportation can reveal the dates and places of its carrier's last passes. More preoccupying, the pharmaceutical products marks electronically, as recommended by the Food and Drug Administration in the United States, could reveal a person's pathologies indirectly, etc.

But the leak of information is not only the flight of personal information. A rarely evoked problem is the industrial spying. This one can take different shapes. Instead of raising the tilt of a truck of the competitor firm, it is today easier to discover their content in the scanning when they leave the warehouse or when they park on the rest stops.

Number of cardboards, palettes and containers are already in effects marks today with RFID tags. The limit between the theoretical attacks and the practical attacks are difficult to fix because it depends mainly on the attacker's motivation to achieve his misdeed [90].

3.5.3 Malicious Traceability

The problem of malicious traceability is more difficult to treat. Whatever the information sent from the tag, it can potentially be used to trace the tag in the space or in time. To not allow malicious traceability, the tag should send to readers only the answers that appear to be random except for the authorized reader. This technique is almost never used because it has several major drawbacks: (1) the tag must have sufficient capacity to use cryptography; (2) to effectively read the received data, the reader needs to know the identity of the tag (to know which secret it uses), but to know the identity of the tag, it must be able to read the received data; (3) to communicate, the RFID system uses a collision avoidance protocol that is based on the fact that each tag has a unique and fixed identifier of collisions avoidance (UID); accordingly, even if the identification or authentication protocol prevents malicious traceability, the collision avoidance protocol may allow traceability of the tag and therefore its holder. The only example we know or the problem of malicious traceability is considered secured is the biometric passport. Indeed, in the case of the passport, the tag does not provide intelligible information until the moment when the reader is properly authenticated. In addition, the collision avoidance identifier is not fixed: it is randomly generated each time the tag is requested by a reader. [90]

3.5.4 Malevolent Traceability

(1) the tag must have the sufficient capacities to use cryptography; (2) to be able to read the received data effectively, the reader must know the identity of the tag (to know which secrecy to use), but to know the identity of the tag, it must know to read the received data; (3) to be able to communicate, system RFID uses a protocol of avoidance of collisions which often rests on the fact that each tag has a single login of avoidance of collisions and fixes (UID); consequently, even if protocol of identification or authentication avoid the malevolent traceability, the protocol of avoidance of collisions can allow the traceability of the tag and thus of its carrier. The only example that we

know or the problem of the malevolent traceability is taken into account in a secure way is the biometric passport. Indeed, in the case of the passport, the tag delivers understandable information only from the moment or the reader is correctly authenticates. Moreover, the login of avoidance of collisions is not fixed: it is generated by chance each time the tag is requested by a reader [91].

3.5.5 Denial of service

Finally, piracy cannot concern a given tag, but a given system, by seeking to destabilize its infrastructure. This can be done in an interested way, the same way that a hacker deface a website or an offender draws gratis on the walls, or it may be the result of an elaborate and premeditate work.

The latter is quite possible in a situation of competition between two companies. It might be tempting to destabilize his rival by destroying the RFID system that controls its production chain. The techniques that can make it are many and varied and depend on the RFID technology. This can go from the electromagnetic interference that prevents the reading of tags to their destruction using inexpensive devices, through the operation of exploiting the vulnerabilities in readers or spreading viruses. While the latter threat seems unrealistic at present, while exploiting vulnerabilities in the readers to destabilize a system is quite real. For example, a 2006 study about the compatibility of passport verification systems with the document 9303 published by the Organization of International Civil Aviation, shows that implementations of this standard generally suffer from many problems, sometimes until the non-verification of embedded security measures on passports. The study of denials service in RFID systems is in its infancy. This domain benefits of a long history and experience in the information technology field, which can be used in good or bad purpose, in the narrower field of RFID. [92]

3.6 Conclusion

In this section, we introduced RFID technology, its evolution, its Classification and its operation we have also raised the security concerns related to this technology. We realized that it is difficult to find an authentication system perfectly secure and assure the specifications and constraints of RFID, particularly in terms of calculation, which has encouraged the use of “light” cryptographic algorithms in terms of calculation.

4. The Zero-Knowledge Proof

4.1 zero knowledge definition

The Zero-Knowledge proof is a popular concept used in many cryptographic systems. In this concept, two parties are involved, the party A and the Auditor B. Using this technique, the user A can prove that he has a title (for example, a credit card number) without having to give B the exact number.

The reason for using a Zero-Knowledge Proof in this situation for an authentication system is because it has the following properties:

4.2 zero knowledge properties

Completeness: If the statement is true, the honest prover (is someone who is following the protocol properly) will be able to prove that the statement is true to an honest verifier each time.

Durability: If the statement is false, it is not possible (with a little luck) to fake the result to the auditor.

Zero-Knowledge: If the statement is true, the auditor will know nothing except that the statement is true. The information on the details of the declaration will not be disclosed.

4.3 The zero knowledge scheme of Fiat-Shamir

The Fiat-Shamir protocol is a zero-knowledge protocol that is based on the complexity of calculating a square root in “ $\frac{Z}{nZ}$ ” where “n” is the product of two large prime numbers “p” and “q”, so “n” is an integer RSA.

The objective of the Fiat-Shamir protocol is to allow “A” (prover) to prove knowledge of “s” to “B” (Auditor) in “t” executions. This is a probabilistic protocol with a probability of 2^{-t} for an adversary to mislead the auditor. While Fiat-Shamir is executed for t = 20 to 40 executions, the probability for an adversary to mislead the auditor for all executions of “t” is very low. Fiat-Shamir is protocol of 3 pass depending on the difficulty of factorization.

Initial Setup

1. A trust center (T) selects “n” such that “ n = p q”

   “n” is public “ p” and “q” are secrets.

2. The user “A” chooses “s”: $1 \le s \le n-1$

   Calculates $I = s^2 \bmod n$

Protocol

1. The prover chooses a random number “r” in the range [1, n - 1].
2. Computes $x = r^2 \bmod n$, and sends “x” to the auditor.
3. The auditor chooses random “e” (e = 0 or e =1) and sends it to the prover.
4. The prover computes $y = r \cdot s^e \bmod n$ and sends it to the auditor.

verification

1. The auditor refuse if $y = 0 \quad or \quad y \neq x \cdot I^e$.
2. The auditor accepts if $y^2 = x \cdot I^e \bmod n$

4.4 Conclusion

In this section we presented a general overview on zero knowledge protocol which is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true, and we provided an example of Fiat Shamir scheme. The zero knowledge protocol can be applied to achieve the user authentication.

5. Authenticated encryption

Introduction

In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed during transmission (its integrity).

A MAC algorithm, sometimes called a (cryptographic) hash function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

5.1 Approaches to Authenticated Encryption

There are three main approaches for authenticated encryption

5.1.1 MAC-then-Encrypt (MtE)

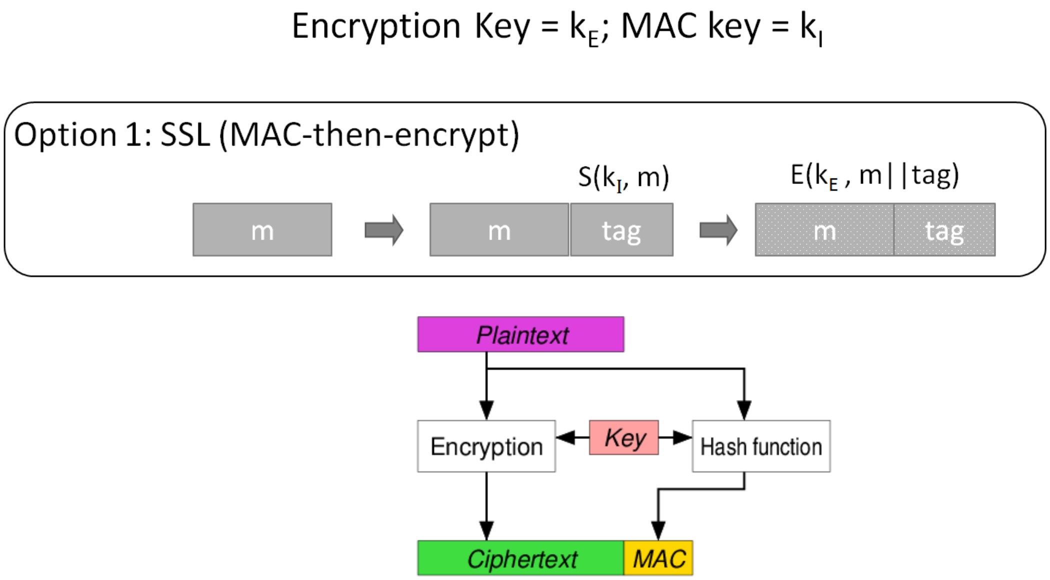


Figure 3-13 Mac then encrypt scheme

In this approach, a MAC is produced based on the plaintext, then the plaintext and MAC are together encrypted to produce a cipher text based on both. The cipher text (containing an encrypted MAC) is sent. This method is used in, SSL/TLS [93].
The SSL/TLS implementation has been proved to be strongly unforgeable by Krawczyk [94] who showed that SSL/TLS was in fact secure because of the encoding used alongside the MtE mechanism.

5.1.2 Encrypt-then-MAC (EtM)

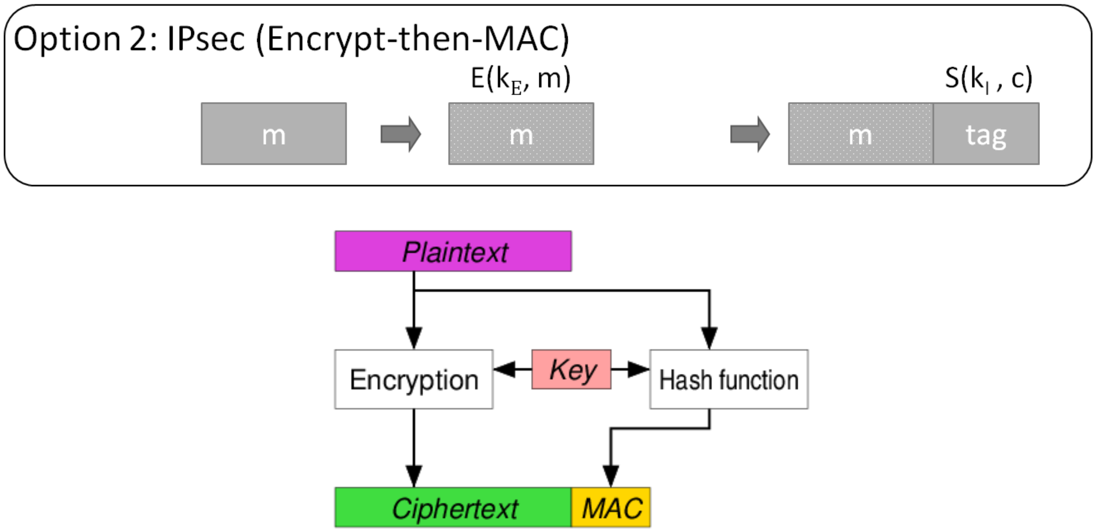


Figure 3-14 Encrypt then MAC scheme

In the second approach, the plaintext is first encrypted, then a MAC is generated based on the resulting ciphertext. The ciphertext and its MAC are sent together. This method is used in IPSec [95]. The standard method according to ISO/IEC 19772:2009 [96]. This is the only method which can reach the best level of security in Authenticated encryption, In November 2014, TLS and DTLS extension for EtM has been published as RFC 7366 [96].

5.1.3 Encrypt-and-MAC (E&M)

A MAC is produced based on the plaintext, and the plaintext is encrypted without the MAC. The plaintext's MAC and the cipher text are sent together. Used in SSH [97]. Even though the E&M approach has not been proved to be strongly unforgeable in itself, [98] it is possible to apply some minor modifications to SSH to make it strongly unforgeable despite the approach.

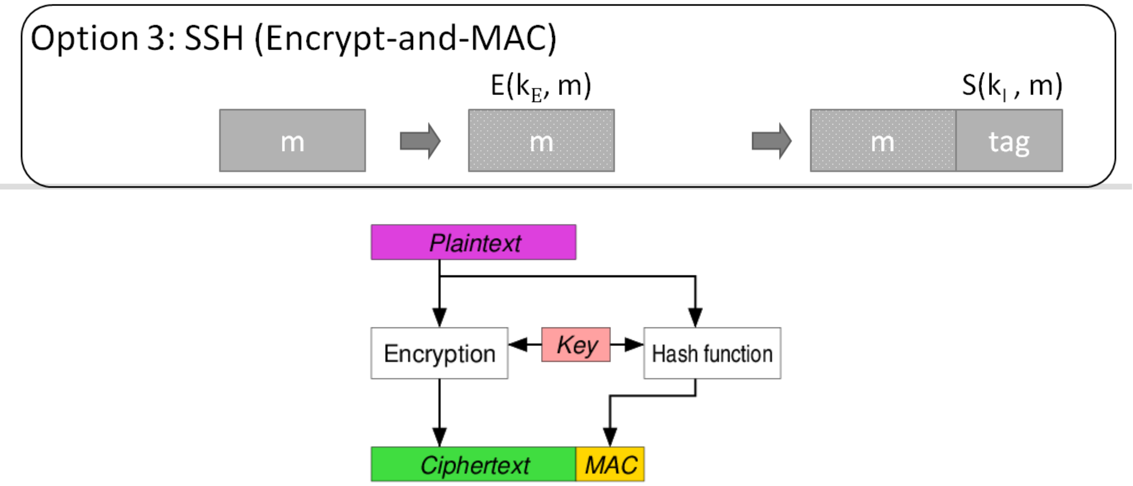


Figure 3-15 Encrypt and MAC scheme

6. Advantages and disadvantages of different user authentication techniques

The following table lists the main advantages and disadvantages of some authentication techniques:

Table 3.3 Advantages and disadvantages of different user authentication techniques

Techniques	Advantages	Disadvantages
Static password	+ easy to implement + easy to use	- theft password by looking over the shoulder - can be forgotten. - fragile (easy to guess or "crackable")
Static password stored in a magnetic card activated by a PIN code.	+ robust password (possible to select a random password, including special characters) + no need to memorize the password	- Shareable, and too often shared. - Theft, lost or forgotten card. - Shareable card.
Dynamic password generated by an application or a software.	+ Strength of the password (often random password and including special characters) + Ease of use for the user (no memorization password)	- Little ease of use (need to use software with each new connection). - problem of the use of the

		software by an unauthorized person
Dynamic password generated by a hardware.	+ Ease of use for the user (no memorization password). + robustness password (single use)	- Theft, lost or forgotten of the password generator. - The generator can get out of synchronization with the server that controls the verification of password.
X.509 certificate in the browser of a computer. X. 509 certificate in a token USB.	+ Multi usage. + Robustness of the authentication method. + Ease of use for the user. + Multi usage. + Robustness of the authentication method. + Similar attitude to the possession of keys (home. car).	- Theft or fraudulent use of the computer and copy the private key associated with the certificate. - Theft, lost or forgotten of the token.
X.509 certificate in a smartcard	+ Multi usage. + Robustness of the authentication method. + Similar attitude to the possession of a bank card.	- Theft, lost or forgotten of the smartcard.
Biometrics and reference characteristics in a networked database.	+ Theft, lost or forgotten is not possible	- Technology immature. - Falsifiable
Biometrics associated with a magnetic card		- Technology immature. - Theft, lost or forgotten of the magnetic card. - High cost.
Biometrics associated with a X509 certificate in a USB token	+ Multi usage. + Similar attitude to the possession of keys (home. car).	- Technology immature. - Theft, lost or forgotten of the USB token. - High cost.
Biometrics associated with a X509 certificate in a smartcard	+ Multi usage. + Similar attitude to the possession of a bank card.	- Technology immature. - Theft, lost or forgotten of the smartcard. - High cost.

Part two

Contributions

Proposed authentication schemes

Chapter 4 Secure image encryption scheme based on polar decomposition and chaotic map

Abstract

Security is an important issue in communication and storage of images, encryption is one of the ways to ensure security. In this work, we propose a new symmetric encryption scheme using an algebraic method which is the polar decomposition of matrices and a chaotic map. For the key generation we present a simple and fast algorithm for generating an orthogonal matrix from a random vector, Through the experiment results and the security analysis, we find that our scheme has good encryption effect and large secret key space, Furthermore, it can resist most known attacks, such as cipher image only attack, known and chosen plain image attacks, statistical analysis, differential and exhaustive attacks. Also it’s shown in the comparison of our method with existing methods in speed factor that our algorithm is fast. It is shown that the use of polar decomposition with chaotic map gives a fast and secure encryption.

Keywords

Polar decomposition, Image encryption, Singular values decomposition (SVD), Chaotic Map.

1. **Introduction**

Generally, the procedure of image encryption is separated into two stages, scrambling the image and then encrypting the scrambled image. Image scrambling throws the image elements into confusion by modifying the position of pixel in such a way that the original image is not identifiable. The scrambling is done by various reversible methods depending on magic square transform, chaos system, gray code etc. In second phase, the scrambled image is passed through some cryptographic algorithm like SCAN based methods [99, 100, 101], DNA sequence [100-106] and chaos-based methods [107-122].

Several algorithms based on chaotic map have been proposed in recent years, but most of these methods suffer from small key space, which make them vulnerable to brute force attacks.

This work aims to overcome these weaknesses by designing a novel symmetric image encryption method based on polar decomposition of matrices and 1 D logistic map, our method possesses large key space to resist brute force and good statistical properties to avoid differential attacks. It is shown that the use of polar decomposition with a chaotic map gives a fast and secure encryption.

Organization of the rest of this chapter is as follows: Section 2 presents the proposed method. Section 3 throws light on Performance and security analysis, whereas the summary of results and the conclusion is presented in Section 4.

2. Proposed scheme

In this scheme we will use some mathematical background that have been presented in (Chapter 1 Related knowledge, section three mathematical background), for more details [123-125].

Note that the SVD of a matrix A is not unique, even if A is invertible but the polar decomposition is unique if the matrix A is invertible, this uniqueness motivates us to use the polar decomposition in the proposed scheme.

Our proposed method has three main steps: key generation, encryption process and decryption process.

2.1 Key generation

The secret key consists of three parts K_0, K_1, K_2 .

Generate a random sequence $K_0 = (c_{01},..,c_{0n})$ where $c_{0i} \in [1, n]$ and put $K = (K_0)^t K_0 = (k_{ij})$, $i, j = 1,..,n$.

Create a random diagonal matrix $D = diag(d_1,..,d_n)$ of size n, its diagonal values are positive with *descending order, put* $K_1 = (d_1,..,d_n)$.

Generate an orthogonal matrix M from a random sequence $K_2 = (a_1,..,a_{n-1})$

In order to generate the orthogonal matrix M we can use our proposed Theorem:

2.1.1 Proposed method of generating orthogonal matrices

The main objective of the following Theorem is to generate easily an $n \times n$ orthogonal matrix M from a random sequence $K_2 = (a_1,..,a_{n-1})$

Theorem

For every sequence $(a_1,..,a_{n-1})$ put $A = \begin{pmatrix} 0 & -a_1 & \cdots & -a_{n-1} \\ a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & 0 & \cdots & 0 \end{pmatrix}$

and $\delta = \sqrt{a_1^2 + .. + a_{n-1}^2}$

Then the matrix $A' = I_n + \frac{\sin\delta}{\delta} A + \frac{1-\cos\delta}{\delta^2} A^2$ is orthogonal

Proof

The matrix A is skew symmetric real matrix: $A^t = -A$, so

$e^A \cdot (e^A)^t = e^A \cdot e^{A^t} = e^A \cdot e^{-A} = I$

and e^A is orthogonal.

It is easy to verify that $A^3 = -\delta A$ hence we can apply the corollary 4.3 in [126] and we give explicit formula for $e^A = A' = I_n + \frac{\sin\delta}{\delta} A + \frac{1-\cos\delta}{\delta^2} A^2$

2.1.1.1 Butterfly orthogonal matrices $Q^{(n)}$ *[127]*

Recently, Butterfly orthogonal matrices are used to precondition linear systems, these matrices are suitable to randomize integration rules, they are most easily described for the case where n is a power of two.

Put $n = 2^k$, $c_i = \cos\theta_i$, $s_i = \sin\theta_i$ for $i = 1, .., n-1$.

A recursive definition for $Q^{(n)}$ starting with $Q^{(1)} = [1]$,

$$Q^{(2n)} = \begin{pmatrix} Q^{(n)} c_n & -Q^{(n)} s_n \\ Q'^{(n)} s_n & Q'^{(n)} c_n \end{pmatrix}$$

where $Q'^{(n)}$ has the same form of $Q^{(n)}$ except that the c_i and s_i indices are all increased by n. In this case the orthogonal matrix M can be generated by $c_1, ..., c_{n-1}$.

Example:.

Put $Q^{(1)} = 1$, then $Q^{(2)} = \begin{pmatrix} Q^{(1)} c_1 & -Q^{(1)} s_1 \\ Q'^{(1)} s_1 & Q'^{(1)} c_1 \end{pmatrix} = \begin{pmatrix} c_1 & -s_1 \\ s_1 & c_1 \end{pmatrix}$

$$Q^{(4)} = \begin{pmatrix} c_1 c_2 & -s_1 c_2 & -c_1 s_2 & s_1 s_2 \\ s_1 c_2 & c_1 c_2 & -s_1 s_2 & -c_1 s_2 \\ c_3 s_2 & -s_3 s_2 & c_3 c_2 & -s_3 c_2 \\ s_3 s_2 & c_3 s_2 & s_3 c_2 & c_3 c_2 \end{pmatrix}$$

for $c_1 = \cos\theta_1$, $c_2 = \cos\theta_2$, $c_3 = \cos\theta_3$

2.1.1.2 Comparison of butterfly [127] and the proposed method of generating orthogonal matrices from a random sequence.

We compare the speed of the two methods, the measured execution time listed in Table 4.1 indicates that the proposed method is indeed faster than the butterfly method.

Table 4.1 Execution time of butterfly and proposed methods of generating orthogonal matrices

Size of the orthogonal matrix generated	64 × 64	128 × 128	256 × 256	512 × 512
Time required of the proposed method (s)	0.00397	0.023245	0.173783	1.134365
Time required of Butterfly method [126] (s)	0.01214	0.144718	0.989703	9.581574

2.2 Encryption process

The proposed encryption scheme follows these steps:

Step1: Let $A = (a_{ij})$ be a gray scale image of size $n \times n$.

Define $f(A) = A_0 = (c_{ij})$ by

$$c_{ij} = (a_{ij} + c_{i-1\ j}) \oplus k_{ij}$$

Here the initial values are $c_{01},..,c_{0n}$ defined by the key K_0,

Step 2: Apply polar decomposition to A_0 :

$$A_0 = PQ$$

where $A_0 = U\,S\,V^t$ and $P = U\,S\,U^t$, $Q = U\,V^t$.

And compute P^{-1} by

$$P^{-1} = US^{-1}U^t$$

Step 3: Using the key $K_1 = (d_1,..,d_n)$,we define the circulant matrix [128] C by

$$C = cir\,(x_0,..,x_{n-1})$$

with $(x_0,..,x_{n-1})$ is the sequence obtained by the logistic map:

$$x_{n+1} = \mu\, x_n(1-x_n)$$

where $\mu = 3.57$ and $x_0 = \frac{\sum d_i}{256} \bmod 1$

Step 4: By using the key K_1 and the matrix C we calculate

$$A_1 = DP^{-1}Q^t + C$$

Step 5: Use the key K_2 to calculate the cipher image A_2 :

$$A_2 = M\,A_1\,M^t$$

All the encryption's steps are concluded in figure 4.1.

2.3 Decryption process

Let B be a cipher image, the plain image can be recovered as follows:

Step 1: Using the key K_2 calculate:

$$B_1 = M^t\,BM$$

Step 2: use the key $K_1 = (d_1,..,d_n)$ and invert the diagonal matrix D and by using the matrix C compute:

$$B_2 = D^{-1}(B_1 - C)$$

Step 3: Apply the polar decomposition to B_2

$$B_2 = U_2 S_2 V_2^t = P_2 Q_2$$

Step 4: Calculate B_3

$$B_3 = (P_2)^{-1} (Q_2)^t = (c'_{i\,j})$$

Step 5: Finally, by the key K_0, compute the entries $a_{i\,j}$ of A and deduce the plain image using the following formula:

$$a_{i\,j} = c'_{i\,j} \oplus k_{i\,j} - c'_{i-1\ j}$$

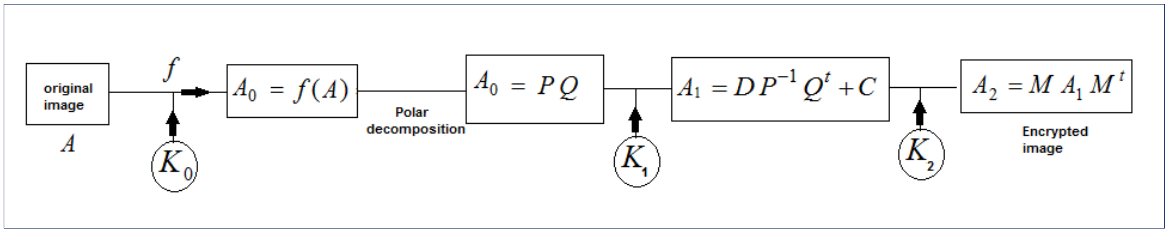


Figure 4-1 Block diagram of the encryption procedure

3. Performance and security analysis

To prevent the feasibility of our image encryption, we analyze its security. The proposed method should resist several types of attacks, as it is symmetric the keys which would be used during both encryption and decryption have to be transmitted through a secure channel.

For the implementation of the proposed scheme we choose *n* = 256 or *n*= *512*.

3.1 Key space analysis.

The secret key consists of three parts: K_0, K_1, K_2.

The orthogonal matrix M is generated by the key $K_2 = (a_1,..,a_{n-1})$ which is a pseudo random sequence with $n = 256$.

If we use the proposed key generation method with $a_i \in \{1,..,256\}$, this provides 256^{255} key combinations, as the elements of D are not zero we have 255^{256}combinations for the key K_1, by the same way we have 256^{256}combinations to obtain the key K_0, the used one dimensional logistic map has interesting properties such as a periodicity and sensitive dependence on initial values, but it has a weak security, to overcome the drawback of its small key space we must use the key K_2 in the first phase of decryption process, thus the size of key space of the proposed scheme is greater than $256^{255} \times 255^{256} \times 256^{256}$ and the key space is large enough that a brute force attack is infeasible.

3.2 Cipher image only attack

For two $n \times n$ matrices M , N we write $N^M = M N M^t$.

The illegal user needs to obtain the keys from the cipher image A_2 .

If $A = U S V^t = P Q$ then $A_2 = [D P^{-1} Q^t + C]^M$.

To deduce D , C and M the illegal user must solve the equation: $X^Y = A_2$

where the variables X and Y are two unknown $n \times n$ matrices; this makes the concerned attack ineffective. A special case of the previous equation is the equation $B^Y = A_2$ what is the conjugacy search problem (CSP) which is a generalization of discrete logarithm problem in a group $(G, \cdot)$ For $a, b \in G$ find $x \in G$ such that $b^x = a$ with $b^x = x^{-1} b x$.

3.3 Known plain image attack

For the construction of *f* in step 1 we are inspired by the Cipher Block Chaining [127] which is very useful for enhancing the security against known-plaintext and chosen plaintext attacks. Step 1 is designed so that it does not allow such attacks because the encryption of a pixel by *f* depends on the current one and all pixels before it, so the repeated elements are encrypted differently.

3.4 Statistical analysis

In this subsection, the proposed image encryption scheme is examined using different statistical measures. These measures involve histogram, information entropy analysis and Correlation analysis. Each of these measures is described in detail in the following subsections. We used six test images, four of size 256 Lena, Peppers, Baboon, Barbara, and two of size 512 Lake and boat for the statistical analysis.

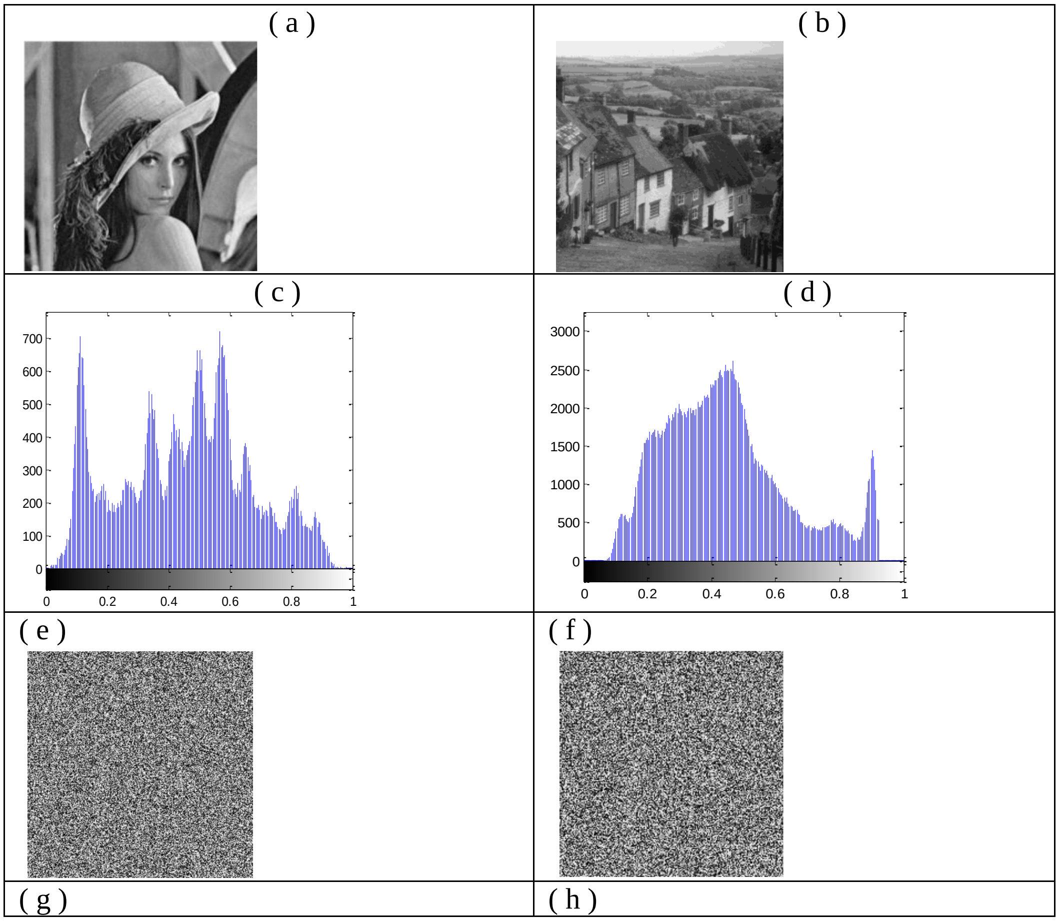
3.4.1 Histogram

In an image processing perspective, the histogram of an image normally represents a histogram of the pixel intensity values. It is a chart displaying the variety of pixels in an image at each different intensity value in that image. For an 8-bit gray scale image there are 256 different possible extremes, and so the histogram will graphically show 256 numbers displaying the distribution of pixels amongst those grayscale values. The histogram of the encryption system image has to be uniform as it shown in our encryption scheme in figure 4.2 Histogram of our encrypted images is nearly uniform and considerably different from the histogram of the plain-images which makes statistical attacks difficult.

The uniformity is justified by chi-square test, which is described by the following expression:

$$x^2 = \sum_{k=1}^{256} \frac{(V_k - 256)^2}{256}$$

Where k is the number of gray levels (256), v_k is the observed occurrence frequencies of each gray level (0–255). The lower value of the chi-square value indicates a better uniformity.



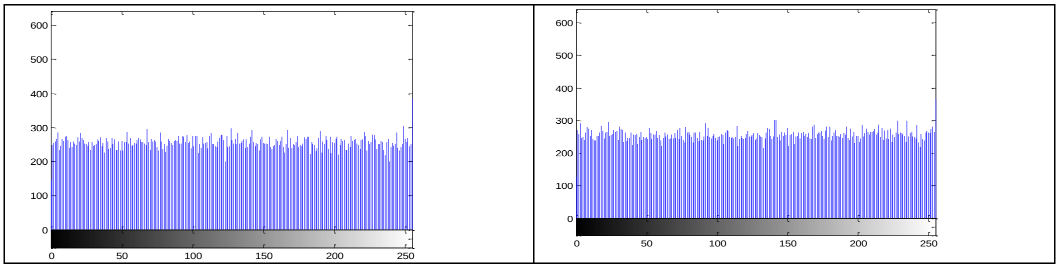


Figure 4-2 encrypted test images and the corresponded histogram

(a) Lena image; (b) Goldhill image, (c) Histogram of Lena; (d) Histogram of Goldhill; (e) Lena encryption; (f) Goldhill encryption , (g) Histogram of Lena encryption and (h) Histogram of Goldhill encryption

3.4.2 Information entropy analysis

The entropy is one of the best functions for calculating and measuring the randomness of image encryption algorithm. The information entropy H(m) of a message source m can be computed as:

$$H(m) = \sum_{i=0}^{2^{n}-1} p(m_i)\log_2\frac{1}{p(m_i)}$$

Ideally the information entropy should be 8 bits for gray scale images. If an encryption scheme generates an output cipher image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security. Information entropy is calculated by using the previous equation. Simulation results for entropy analysis are shown in Table 4.2.

The value of entropy is very close to theoretical value of 8 bits. This implies that our encryption algorithm is secure against entropy attack.

Table 4.2 Entropy results for the Cipher-Images

Encrypted image	Entropy
Lena	7.9966
Peppers	7.9961
Baboon	7.9958
Barbara	7.9975
Lake	7.9991
Boat	7.9993

3.4.3 Correlation analysis of two adjacent pixels

Correlation determines the connection between two variables. In other terms, correlation is a measure that determines level of similarity between two variables. Correlation coefficient is a useful evaluation to judge encryption quality of any cryptosystem. Any image cryptosystem is said to be good, if encryption method hides all attributes and features of a plaintext image, and encrypted image is totally random and extremely uncorrelated. For a regular image, each pixel is highly associated with its nearby pixels. An ideal encryption technique should generate the cipher images with no such correlation in the adjacent pixels. In this section, correlation coefficient of two adjacent pixels in original image and encrypted image is studied.

We have examined the correlation vertically, horizontally and diagonally between two adjacent pixels. 2000 pairs of two adjacent pixels in horizontal, vertical, and diagonal direction from plain image and its cipher image were randomly selected and the correlation coefficients were calculated using the following equations:

$$C = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \overline{x})^2)\,(\frac{1}{N}\sum_{i=1}^{N}(y_i - \overline{y})^2)}}$$

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$\overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

Where x and y are grey-level values of the two adjacent pixels in the image. Table 4.3 lists the correlation coefficients of the image Lena and its cipher-image, while their correlation distributions are shown in Figure 4.3.

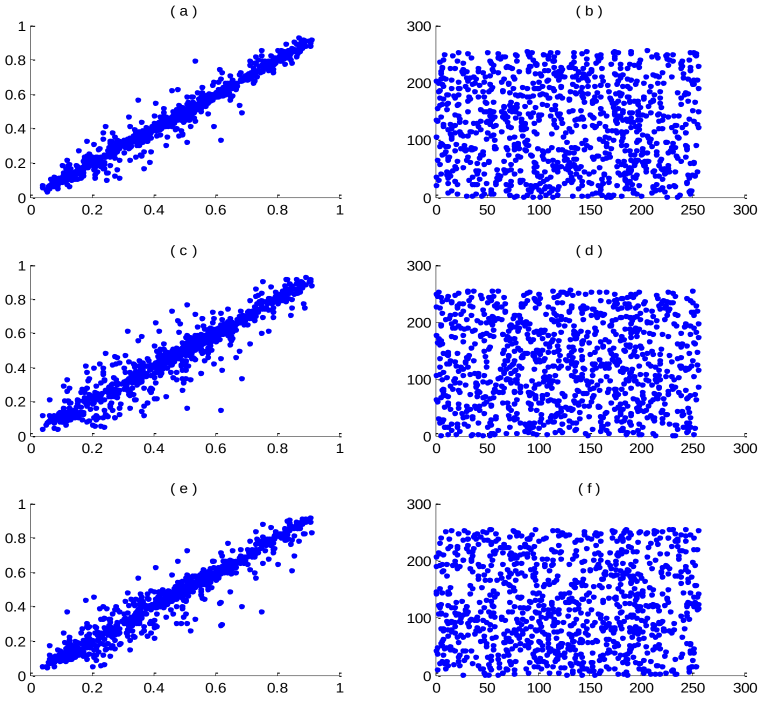


Figure 4-3 Correlation of two adjacent pixels

(a) Distribution of two horizontally adjacent pixels in the plain image, (b) Distribution of two horizontally adjacent pixels in the cipher-image, (c) Distribution of two diagonally adjacent pixels in the plain-image, (d) Distribution of two diagonally adjacent pixels in the cipher-image, (e) Distribution of two vertically adjacent pixels in the plain-image, and (f) Distribution of two vertically adjacent pixels in the cipher-image.

Table 4.3 Correlation coefficient of two adjacent pixels

Direction of adjacent pixels	Lena image 256 × 256		Peppers image 256 × 256		Baboon image 256 × 256		Barbara image 256 × 256		Lake image 512 × 512		Boat image 512 × 512	
	Original	Cipher	Origina l	Cipher	Origina l	Cipher	Origina l	Cipher	Origina l	Cipher	Origina l	Cipher
Horizontal	0.9864	0.0024	0.9456	0.0017	0.9697	0.0070	0.9854	0.0018	0.9854	0.0002	0.9791	0.0030
Vertical	0.9857	0.0002	0.9911	0.0122	0.9892	0.0024	0.9152	0.0050	0.9214	0.0007	0.9897	0.0013
Diagonal	0.9921	0.0062	0.9854	0.0003	0.9913	0.0006	0.9711	0.0114	0.9696	0.0084	0.9641	0.0011

3.5 Sensibility analysis

3.5.1 Differential attack

NPCR and UACI: Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) are Two common measures are used to examine the impact of one pixel modify on the whole image, encrypted by an algorithm.

NPCR measures the percentage of the number of different pixel to the total number of pixels. In brief NPCR, means the number of pixels change rate of ciphered image while one pixel of plaintext image is changed. To examine the average intensity of differences between the images, UACI is used to check the impact of one pixel change, tests were performed on Lena, Peppers, Baboon, Barbara, Lake and boat images.

Let C_1 and C_2 be two different cipher-images whose corresponding plaintext images are differ by only one bit. Label the grayscale value of the pixel at grid (i, j) in C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$ respectively. Define an array, D, the same size as images C_1 and C_2. Then $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$ namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$, otherwise, $D(i, j) = 1$

The *NPCR* is defined as:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\%$$

Where *W* and *H* are the width and height of cipher images C_1 and C_2.

UACI can be defined as :

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i, j) - C_2(i, j)}{255}\right] \times 100\%$$

Simulation results are shown in Table 4.4. The higher the values of NPCR and UACI are, the better the encryption algorithm is.

Table 4.4 NPCR and UACI of cipher-images.

Images	NPCR	UACI
Lena	99.6427	33.5354
Peppers	99.6848	33.6365
Baboon	99.5586	33.6312
Barbara	99.6332	33.6384
Lake	99.7964	33.5349
Boat	99.8727	33.7348

3.6 Speed analysis

Encryption speed is highly reliant on the CPU/MPU structure, RAM size, operating system platform, the programming language and also on the compiler options.
More details of algorithm speed in comparison with other algorithms are discussed as follows:

Table 4.5 compares the encryption time of the proposed cryptosystem, Benyamin Norouzi's [130] Congxu Zhu's algorithm [131], Zhi-liang Zhu's algorithm [132], and Gao's algorithms [133, 134]. The experiments are all performed using MATLAB 8 on a personal computer (PC)with a CPU Intel(R) Atom(TM) N455 @1.66 1.67 GHz, 2 GB Memory, 320 GB hard-disk capacity, and the operating system is Microsoft Windows 7.

In the proposed cryptosystem, we only need one round diffusion process; so, it just requires us 0.38s to finish the whole process for a gray image of size 256×256. Therefore, the encryption technique proposed in this method is fast.

Table 4.5 The comparison of encryption time between our proposed method and the other cryptosystems

Algorithm	Encryption time (s)	System characteristics
Proposed algorithm	0.38	CPU Intel(R) Atom(TM) N455 @1.66 1.67 GHz, Ram 2 GB
Benyamin Norouzi's [130]	0.4	CPU 2.4 GHz, Ram 4 GB
Congxu Zhu's [131]	0.69	
Zhi-liang Zhu's [132]	>2.9	
Gao's [133]	0.83	
Gao's [134]	>3	

Remarks

a) The logistic map alone does not provide a sufficient security [135], hence it is required to use the other steps.

b) The proposed scheme has a variable key length, this flexibility may be operated following the desired security.

c) We have the ability to reduce the size of the key, for example the elements of the key K_0 can be obtained only by $x_0 \in]0,1]$, and its elements are

$$C_{0m} = \lfloor 1000\,x_m \rfloor \bmod(256)$$

$1 \le m \le 256$ sequence where x_m is the m^{th} element of logistic map sequence defined by $x_{n+1} = \mu\, x_n(1 - x_n)$

where $\mu = 3.57$ and $x_0 \in]0,1]$, here $\lfloor\ \rfloor$ is the integer part, according to the IEEE floating point standard, the number of possible values of x_0 is about 10^{15}, however to maintain a good level of security, the space of the other parts K_1 or K_2 must be large enough.

4. Conclusion

In this chapter, we proposed a novel image encryption method using an algebraic method which is the polar decomposition of matrices and a chaotic map.

For the key generation we present a simple and fast algorithm for generating an orthogonal matrix from a random vector; through the experiment results and security analysis, we find that our scheme has good encryption effect and large secret key space. Furthermore, the proposed algorithm can resist most known attacks, such as cipher image only attack; known and chosen plain image attacks; statistical analysis; differential and exhaustive attacks. Also it’s shown in the comparison of our method with existing methods in speed factor that our algorithm is fast. All these features show that our algorithm is very suitable for digital image encryption.

Chapter 5 A Robust Blind and Secure Watermarking Scheme Using Positive Semi Definite Matrices

Abstract

In the last decade the need for new and robust watermarking schemes has been increased because of the large illegal possession by not respecting the intellectual property rights in the multimedia in the internet. In this chapter we introduce a novel blind robust watermarking scheme which exploits the positive circulant matrices in frequency domain which is the SVD, Different applications such as copyright protection, control and illicit distributions have been given. Simulation results indicate that the proposed method is robust against attacks as common digital processing: compression, blurring, dithering, printing and scanning, etc. and subterfuge attacks (collusion and forgery) also geometric distortions and transformations. Furthermore, good results of NC (normalized correlation) and PSNR (Peak signal-to-noise ratio) have been achieved while comparing with recent state of the art watermarking algorithms.

1. Introduction

Recently, many watermarking schemes have been proposed in spatial and frequency domains, the watermarking schemes in [136-139] are in spatial domain they are robust against geometrical attacks but they suffer from the poor capacity of data embedding, this drawback led other researchers to propose watermarking schemes in frequency domain [140-159], most of those methods are semi or non blind like [140, 141, 142, 143, 144, 148, 149, 154] which means the host image is required in the extraction procedure, also some methods have a good robustness but they don't offer a good transparency like [148, 149, 151, 154]. In most applications of watermarking the main concern has been the robustness against common digital attacks but usually resolving rightful ownership deadlock is ignored, the deadlock problem occurs where multiple ownership claims are made and the rightful ownership of digital content cannot be resolved.

In this chapter we propose a novel blind robust digital image watermarking scheme based on positive semi definite matrices and singular values decomposition. The proposed scheme has a variable watermark size, this flexibility may be operated following the desired data hiding capacity.

The rest of the chapter is organized as follows: section two explains the proposed digital watermarking method. The simulation and the experimental results are discussed in section three also a performance comparison was given, section four presents applications of the scheme in copyright protection, illicit distribution and copy control, finally, conclusions are drawn in section five.

2. proposed method

In this scheme we will use some mathematical background that have been presented in (Chapter 1 Related knowledge, section three mathematical background), for more details [123-125].

As the matrix $CC^t = C^tC$ is positive semi- definite its spectral decomposition coincides with its SVD decomposition, it is easy to verify that

$$CC^t = U_0 diag(\delta_1, \delta_2, \delta_3, \delta_4) U_0{}^t \tag{1}$$

with

$$\delta_1 = (c_1 + c_2 + c_3 + c_4)^2$$
$$\delta_2 = (c_1 - c_2 + c_3 - c_4)^2$$
$$\delta_3 = \delta_4 = (c_1 - c_3)^2 + (c_2 - c_4)^2 \quad (2)$$

are the singular values and U_0 is the constant matrix :

$$U_0 = \begin{pmatrix} 1/2 & -1/2 & 0 & -\sqrt{2}/2 \\ 1/2 & 1/2 & -\sqrt{2}/2 & 0 \\ 1/2 & -1/2 & 0 & \sqrt{2}/2 \\ 1/2 & 1/2 & \sqrt{2}/2 & 0 \end{pmatrix} \quad (3)$$

We note that the main idea of our scheme is presenting a watermarking method using positive semi-definite matrices for which the spectral decomposition coincides with the singular value decomposition [153]. The watermark W is generated as positive semi definite matrix and its singular value decomposition is $U_W \times S_W \ \times {V_W}^t$ with $U_W = V_W$.

Now we will present more details on the proposed scheme.

2.1. Construction of watermark

Before considering the proposed method, we consider a circulant matrix $C_1 = cir(c_1^1, c_2^1, c_3^1, c_4^1)$ and we are going to discuss the choice of $c_1^1, c_2^1, c_3^1, c_4^1$ so that the singular values of the positive definite circulant matrix $C_1 C_1^t = C_1^t C_1$ verify:

$$\delta_1^1 \geq \delta_2^1 \geq \delta_3^1 \geq \delta_4^1 \quad (4)$$

To this end, we put $S_1^1 = c_1^1 + c_3^1,\ S_2^1 = c_2^1 + c_4^1,\ D_1^1 = c_1^1 - c_3^1,\ D_2^1 = c_2^1 - c_4^1$

Then, according to (2), to obtain the decreasing sequence (4) it is enough to take

$c_1^1 = \dfrac{S_1^1 + D_1^1}{2}$, $c_2^1 = \dfrac{S_2^1 + D_2^1}{2}$, $c_3^1 = \dfrac{S_1^1 - D_1^1}{2}$, $c_4^1 = \dfrac{S_2^1 - D_2^1}{2}$

Where $D_1^1 > 0$, $D_2^1 > 0$, $S_2^1 > 0$, $h^1 > 0$, are four arbitrary positive numbers and $S_1^1 = r_1 + S_2^1 + h^1$ with $r_1 = \sqrt{(D_1^1)^2 + (D_2^1)^2}$.

Hence $U_0 diag(\delta_1^1, \delta_2^1, \delta_3^1, \delta_4^1) {U_0}^t$ is the SVD decomposition of $C_1 C_1^t$.

If A is an image of size $4m \times 4m$, to every arbitrary vector $(D_1^1, D_2^1, S_2^1, h^1)$ is associated a vector $c_1 = (c_1^1, c_2^1, c_3^1, c_4^1)$, as mentioned above, a 4×4 circulant matrix $C_1 = cir(c_1)$ and a watermark as $4m \times 4m$ matrix with one block

$$W_1 = \begin{pmatrix} C_1C_1^t & 0 & . & 0 \\ 0 & 0 & & . \\ . & & . & . \\ 0 & . & . & 0 \end{pmatrix} \qquad (5)$$

To obtain a watermark W_k with k blocks

$$W_k = \begin{pmatrix} C_1C_1^t & 0 & . & . & . & 0 \\ 0 & C_2C_2^t & & & & . \\ . & & . & & & . \\ . & & & C_kC_k^t & & . \\ & & & & 0 & \\ . & & & & & . \\ & & & & . & \\ 0 & . & . & . & . & 0 \end{pmatrix} \qquad (6)$$

We construct iteratively the nth block $C_nC_n^t\ , n \geq 2$ as follows:

Let

$0 < D_1^n < D_1^{n-1} < .. < D_1^1$, $0 < D_2^n < D_2^{n-1} < .. < D_2^1$

and

$r_n = \sqrt{(D_1^n)^2 + (D_2^n)^2}$, $S_1^n = \frac{r_{n-1} + r_n}{2}$, $S_2^n = \frac{r_{n-1} + r_n}{4}$

Put $c_1^n = \frac{S_1^n + D_1^n}{2}$, $c_2^n = \frac{S_2^n + D_2^n}{2}$, $c_3^n = \frac{S_1^n - D_1^n}{2}$, $c_4^n = \frac{S_2^n - D_2^n}{2}$

then

$c_n = (c_1^n, c_2^n, c_3^n, c_4^n)$

$C_n = cir(c_n)$

and the watermark with k blocks is

$$W_k = \begin{pmatrix} U_0 & 0 & . & 0 \\ 0 & . & & . \\ . & & U_0 & 0 \\ 0 & . & 0 & I \end{pmatrix} \times$$
$$diag(\delta_1^1,..,\delta_4^1,\delta_1^2,..,\delta_4^2...\delta_1^k,..,\delta_4^k,0,..,0)\times \tag{7}$$
$$\begin{pmatrix} U_0^t & 0 & . & 0 \\ 0 & . & & . \\ . & & U_0^t & 0 \\ 0 & . & 0 & I \end{pmatrix}$$

with $\delta_1^1 \geq \delta_2^1 \geq \delta_3^1 \geq \delta_4^1 \geq \delta_1^2 \geq \cdots \geq \delta_4^k \geq 0$ and I is $4(m-k)\times 4(m-k)$ identity matrix. Hence to generate a watermark W_k with k blocks we need four arbitrary positive numbers $D_1^1 > 0$, $D_2^1 > 0$, $S_2^1 > 0$, $h^1 > 0$ for the first block and two random sequences

$$0 < D_1^k < D_1^{k-1} < .. < D_1^1$$
$$0 < D_2^k < D_2^{k-1} < .. < D_2^1$$

for other blocks; that is, the insertion key K_1 is of length 2k+2.

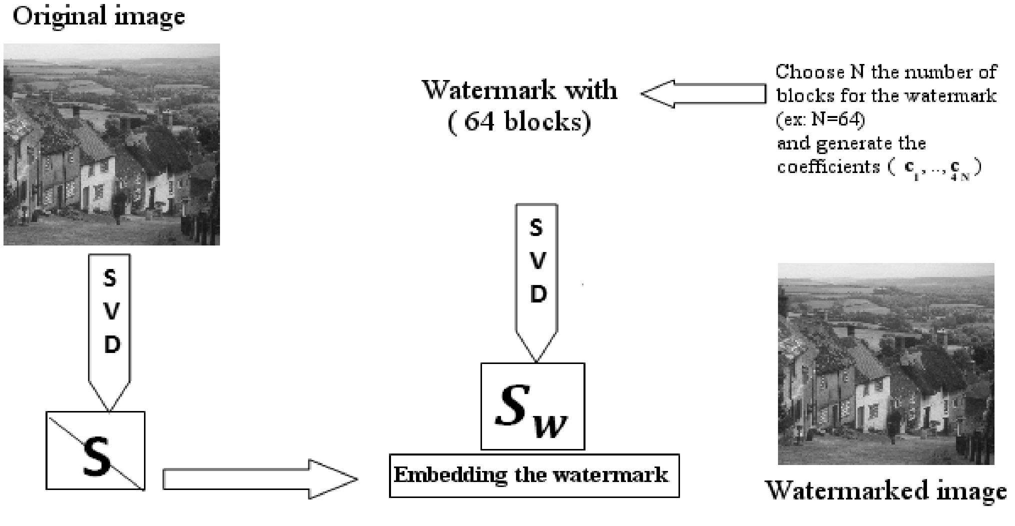

Original image
S
V
D
S
Watermark with
(64 blocks)
Choose N the number of blocks for the watermark (ex: N=64) and generate the coefficients (c_1, .., c_{4N})
S
V
D
S_W
Embedding the watermark
Watermarked image

Figure 5-1 The proposed watermarking embedding procedure

2.2. Watermark insertion procedure

To watermark a given original image A of size $4m \times 4m$, we will use a watermark with one block as following:

1) We define the insertion key $K_1 =$ (D_1^1, D_2^1, S_2^1, h^1) by using four arbitrary positive numbers and construct the watermark W_1 as mentioned above.
2) Apply SVD on A : $A = U \times S \times V^t$ with $S = diag(S_i)$
3) Perform SVD on W_1:

$$W_1 = \begin{pmatrix} U_0 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} \partial & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} U_0{}^t & 0 \\ 0 & I \end{pmatrix} \tag{8}$$

With $\partial = diag(\delta_1^1, \delta_2^1, \delta_3^1, \delta_4^1)$ and I is $4(m-1) \times 4(m-1)$ identity matrix.

4) Put

$$Y_i = S_i + \alpha \partial_i^{'} \tag{9}$$

with $\partial_1^{'} = \delta_1^1, \partial_2^{'} = \delta_2^1, \partial_3^{'} = \delta_3^1, \partial_4^{'} = \delta_4^1$ and $\forall i > 4$ $\partial_i^{'} = 0$.

So $$A^* = U \times diag(Y_i) \times V^t \tag{10}$$

A^* is the watermarked image.

The figure 5.1 conclude the watermark insertion procedure.

2.3. Watermarking detection and extraction procedure

We don't require the original image A to detect the watermark, we only require the watermarked image A^*, the scaling factor α and the key $K_2 = (S_1, S_2, S_3, S_4)$ formed by the first four values of S .

1) Apply SVD to A^*

$$A^* = U^* \times S^* \times V^{*t} \tag{11}$$

2) Calculate

$$x_i = \frac{S_i^* - S_i}{\alpha} \tag{12}$$

for the first four elements.

If $x_3 = x_4$ then the mark is detected else the watermark is not present on the image.

To extract the mark we compute:

$$W^* = \begin{pmatrix} U_0 & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} X & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} {U_0}^t & 0 \\ 0 & I \end{pmatrix} \qquad (13)$$

where $X = diag(x_1, x_2, x_3, x_4)$ and I is $4(m-1) \times 4(m-1)$ identity matrix.

Remarks:

If we use a watermark W_k with k blocks, to detect or extract the watermark we only require the scaling factor α and a key $K_2 = (S_1,...,S_{4k})$of length 4k which contains the first 4k values of S. In this case the sequence X $= (x_i)$is of length 4k and the mark is detected if $x_{4i-1} = x_{4i}$ for $i = 1,...,k$.

In Chandra algorithm [141], to extract the watermark W, (U_W, V_W) are required, in the proposed scheme $U_W = V_W$ is a constant matrix and independent of the watermark, thus our proposed algorithm is blind.

3. Experimental results

To demonstrate the efficiency and the performance of the proposed image watermarking scheme we implemented the proposed algorithm in Matlab, we used eight test images, of size 512 Cameraman Lena, Peppers, Baboon, Zelaine, Barbara, Goldhill and boat (Figure 5.2).

The quality of the watermarked image is assessed with the PSNR (Peak signal-to-noise ratio):

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})\ db \qquad (14)$$

In order to evaluate the quality of the extracted watermark, we use normalized correlation (NC) metric as:

$$NC(W,W') = \frac{1}{W_h \times W_w} \sum_{i=0}^{W_h-1} \sum_{j=0}^{Ww-1} W(i,j) \times W'(i,j) \qquad (15)$$

Where W_h and W_w are the height and width of the watermarkes, respectively. $W(i,j)$ and $W'(i,j)$ denote the coefficients of the inserted signature and the extracted signature respectively.

The PSNR values of the watermarked images by our method indicate that our method in general achieves very good quality as it is shown in (Table 5.1). So the proposed method preserves good transparency for the watermarked images.

In the proposed method we have a variety for generating the watermark which can be created using n blocks, Table (5.2) shows the quality of the extracted watermark defined by NC under deferent image processing attacks using deferent Watermarks, the values of the NC in the table are the average values of the NC for the watermarks of the eight test images, And the scale factor $\alpha = 0.03$.

Table 5.1 The PSNR values of the watermarked images of our method using variety of watermarks

Number of blocks	Lena	Peppers	Barbara	Baboon	GoIdhiII	Zelaine	Cameraman	Boat
1	56.6994	55.9094	56.9139	55.6458	57.2825	52.5031	56.2456	57.1737
3	55.5982	55.2634	55.5102	54.6902	55.5499	50.5651	57.7976	55.6458
5	55.7382	55.1153	57.1737	55.0781	55.4955	55.4154	55.5001	55.2064
10	55.0831	53.5932	55.2064	55.1058	55.1460	53.1938	52.1151	54.6902
30	55.8089	54.5946	53.3403	51.6568	54.6665	57.5347	52.2868	51.5035
64	56.0630	55.4747	51.5035	50.4369	54.6762	51.4444	50.4884	52.9705
80	55.4090	56.2183	50.2628	49.4199	52.9705	56.4001	49.2424	52.8710
100	55.4366	56.2190	50.1065	49.1576	52.8710	53. 321	49.2372	52.8454
128	55.3805	56.2759	50.0764	49.2020	52.8454	51.5657	51.0011	52.8710

It is clear from the table that our method achieves a good robustness against variety of image processing attacks, furthermore, it can be seen that the rotation process is the only attack that can take a less effect on the watermark while increasing the number of blocks, while it makes the watermark more robust to other attacks.

To prove the robustness and imperceptibility of our method we compare the simulation results with many state of the art schemes

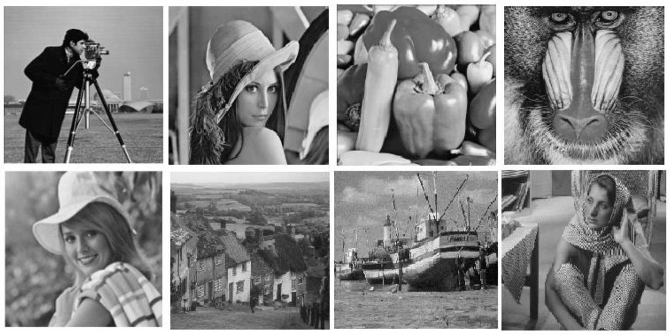
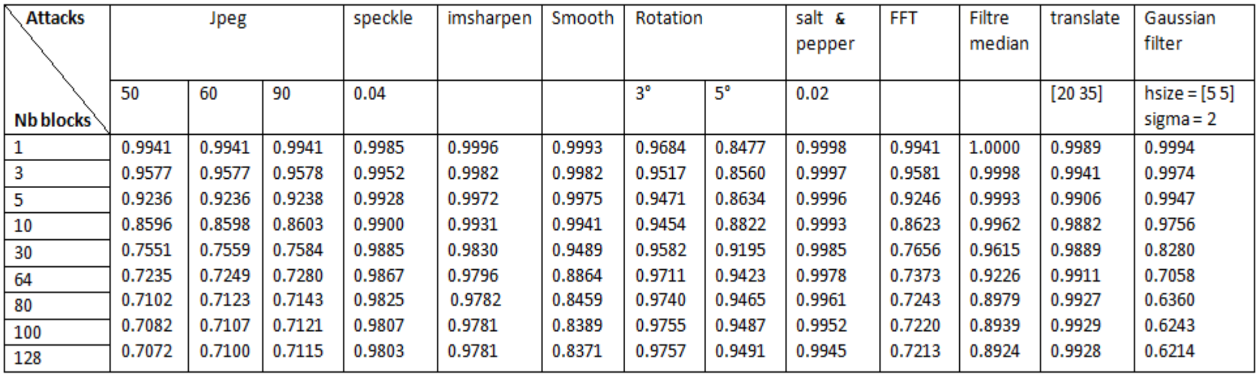


Figure 5-2 The host test images.

The NC values shown in table 5.3 indicate that our scheme achieve better robustness than other schemes in most attacks, and in the attacks that our scheme doesn't seem to be the more robust in it still achieve a good NC values > 8.5.

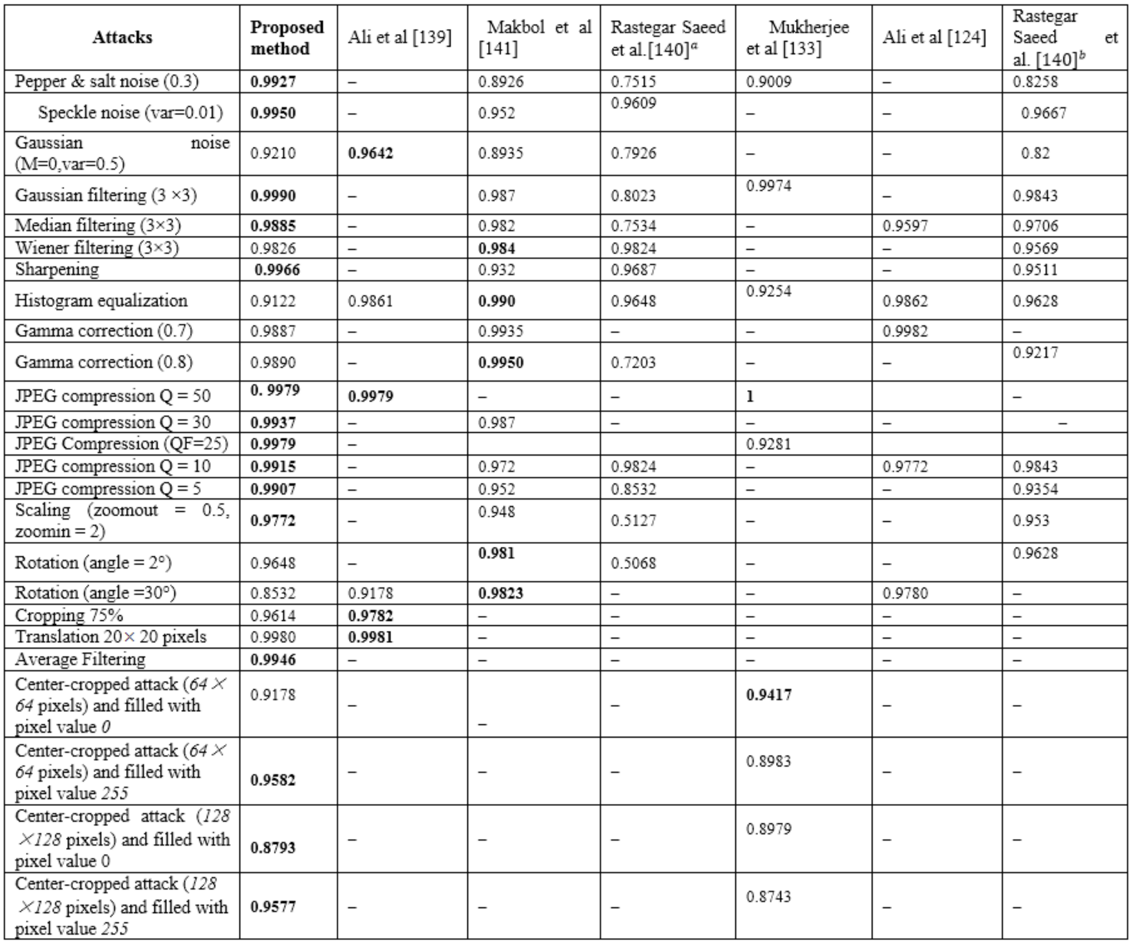
Table 5.2 the robustness of the proposed method against image processing attacks using variety of watermarks



Attacks	Jpeg			speckle	imsharpen	Smooth	Rotation		salt & pepper	FFT	Filtre median	translate	Gaussian filter
Nb blocks	50	60	90	0.04			3°	5°	0.02			[20 35]	hsize = [5 5] sigma = 2
1	0.9941	0.9941	0.9941	0.9985	0.9996	0.9993	0.9684	0.8477	0.9998	0.9941	1.0000	0.9989	0.9994
3	0.9577	0.9577	0.9578	0.9952	0.9982	0.9982	0.9517	0.8560	0.9997	0.9581	0.9998	0.9941	0.9974
5	0.9236	0.9236	0.9238	0.9928	0.9972	0.9975	0.9471	0.8634	0.9996	0.9246	0.9993	0.9906	0.9947
10	0.8596	0.8598	0.8603	0.9900	0.9931	0.9941	0.9454	0.8822	0.9993	0.8623	0.9962	0.9882	0.9756
30	0.7551	0.7559	0.7584	0.9885	0.9830	0.9489	0.9582	0.9195	0.9985	0.7656	0.9615	0.9889	0.8280
64	0.7235	0.7249	0.7280	0.9867	0.9796	0.8864	0.9711	0.9423	0.9978	0.7373	0.9226	0.9911	0.7058
80	0.7102	0.7123	0.7143	0.9825	0.9782	0.8459	0.9740	0.9465	0.9961	0.7243	0.8979	0.9927	0.6360
100	0.7082	0.7107	0.7121	0.9807	0.9781	0.8389	0.9755	0.9487	0.9952	0.7220	0.8939	0.9929	0.6243
128	0.7072	0.7100	0.7115	0.9803	0.9781	0.8371	0.9757	0.9491	0.9945	0.7213	0.8924	0.9928	0.6214

Beside the robustness the proposed method has a good PSNR values and the quality of the watermarked image is very good as it is shown in Table 5.4 where we compared the PSNR of the watermarked images of the proposed scheme with Lai, Chih-Chin et al [155] scheme and Tsai, Hung-Hsu et al [156] scheme, the scale factors were in an interval from 0.01 to 0.09 during this the results indicate that our method has a better imperceptibility. The watermarked images of our proposed method look exactly the same as the host images, so the watermarking procedure preserves the quality of the images.

Table 5.3 Comparison of robustness of our scheme and other state of the art schemes



Attacks	**Proposed method**	Ali et al [139]	Makbol et al [141]	Rastegar Saeed et al.[140]^{a}	Mukherjee et al [133]	Ali et al [124]	Rastegar Saeed et al. [140]^{b}
Pepper & salt noise (0.3)	**0.9927**	–	0.8926	0.7515	0.9009	–	0.8258
Speckle noise (var=0.01)	**0.9950**	–	0.952	0.9609	–	–	0.9667
Gaussian noise (M=0,var=0.5)	0.9210	**0.9642**	0.8935	0.7926	–	–	0.82
Gaussian filtering (3 ×3)	**0.9990**	–	0.987	0.8023	0.9974	–	0.9843
Median filtering (3×3)	**0.9885**	–	0.982	0.7534	–	0.9597	0.9706
Wiener filtering (3×3)	0.9826	–	**0.984**	0.9824	–	–	0.9569
Sharpening	**0.9966**	–	0.932	0.9687	–	–	0.9511
Histogram equalization	0.9122	0.9861	**0.990**	0.9648	0.9254	0.9862	0.9628
Gamma correction (0.7)	0.9887	–	0.9935	–	–	0.9982	–
Gamma correction (0.8)	0.9890	–	**0.9950**	0.7203	–	–	0.9217
JPEG compression Q = 50	**0. 9979**	**0.9979**	–	–	**1**		–
JPEG compression Q = 30	**0.9937**	–	0.987	–	–	–	–
JPEG Compression (QF=25)	**0.9979**	–			0.9281		
JPEG compression Q = 10	**0.9915**	–	0.972	0.9824	–	0.9772	0.9843
JPEG compression Q = 5	**0.9907**	–	0.952	0.8532	–	–	0.9354
Scaling (zoomout = 0.5, zoomin = 2)	**0.9772**	–	0.948	0.5127	–	–	0.953
Rotation (angle = 2°)	0.9648	–	**0.981**	0.5068	–	–	0.9628
Rotation (angle =30°)	0.8532	0.9178	**0.9823**	–	–	0.9780	–
Cropping 75%	0.9614	**0.9782**	–	–	–	–	–
Translation 20× 20 pixels	0.9980	**0.9981**	–	–	–	–	–
Average Filtering	**0.9946**	–	–	–	–	–	–
Center-cropped attack (*64 × 64* pixels) and filled with pixel value *0*	0.9178	–	–	–	**0.9417**	–	–
Center-cropped attack (*64 × 64* pixels) and filled with pixel value *255*	**0.9582**	–	–	–	0.8983	–	–
Center-cropped attack (*128 ×128* pixels) and filled with pixel value 0	**0.8793**	–	–	–	0.8979	–	–
Center-cropped attack (*128 ×128* pixels) and filled with pixel value *255*	**0.9577**	–	–	–	0.8743	–	–

Table 5.4 Comparison of PSNR for Lai, Chih-Chin et al [149] Tsai, Hung-Hsu et al [150] and our scheme.

Method	The scale factors α				
	0.01	0.03	0.05	0.07	0.09
Lai, Chih-Chin et al [155]	51.14	51.14	50.89	49.52	47.49
Tsai, Hung-Hsu et al [156]	47	37	33	28	about 25
Proposed method	56.70	56.68	56.53	55.97	55.87

4. System security

System security of the proposed method is based on proprietary knowledge of keys which are required to embed or extract an image watermark.

As the security level is the number of observations the opponent needs to successfully estimate the secret key, the key space must be very large.

If we use a watermark with one block and for example we suppose that each of the four components $D_1^1 > 0$, $D_2^1 > 0$, $S_2^1 > 0$, $h^1 > 0$ of the key K_1 has r decimal digits, in this case the size of key space of K_1 equals $10^{4r} \succ 2^{12r}$; then for $r \geq 15$ the size of key space of K_1 is very large, we have the same result for the extraction key K_2 .

The security of our technique can be improved by increasing *k* the number of watermark blocks and the complexities can be controlled by manipulation of *k*.

5. Applications

We now describe some applications of the proposed method.

5.1. Copyright protection

Protection of intellectual property has become a prime concern for creators and publishers of digital contents. To solve the problem of legal ownership for digital multimedia data, it must use “digital watermark”, there is need to be associated additional information with a digital content, a copyright notice may need to be associated with an image to identify the legal owner, a serial number to identify a legitimate user.

For our method the distributor generates an insertion key

$$K_1 = (D_1^1, D_2^1, S_2^1, h^1)$$

Where h^1 is the information about the copyright owner and S_2^1 is the information about the receiver, he embeds the associated watermark in the host image and sends the watermarked image to the legitimate receiver. The extraction key K_2 or the algorithm will only be known by the distributor and other trusted parties. For the proof of the ownership of the embedded image, using the key K_2 , the distributor extracts the mark and calculates the singular values $(\delta_1^1, \delta_2^1, \delta_3^1, \delta_4^1)$ and according to the choice of $c_1^1, c_2^1, c_3^1, c_4^1$ and by (4) deduces the copyright notice

$$h^1 = \sqrt{\delta_2^1} - \sqrt{\delta_3^1}$$

and serial number of the user

$$S_2^1 = \frac{\sqrt{\delta_1^1} - \sqrt{\delta_2^1}}{2}$$

In order to solve the deadlock problem [154], in generation of K_1 , D_1^1 and D_2^1 can be computed from the host image A using a secure hash function f for example let:

$$D_1^1 = f(A)$$

$$D_2^1 = f(A^t)$$

The second key K_2 is also original image dependent, this makes counterfeiting very difficult. The proposed scheme for copyright protection is resumed in figure 5.3.

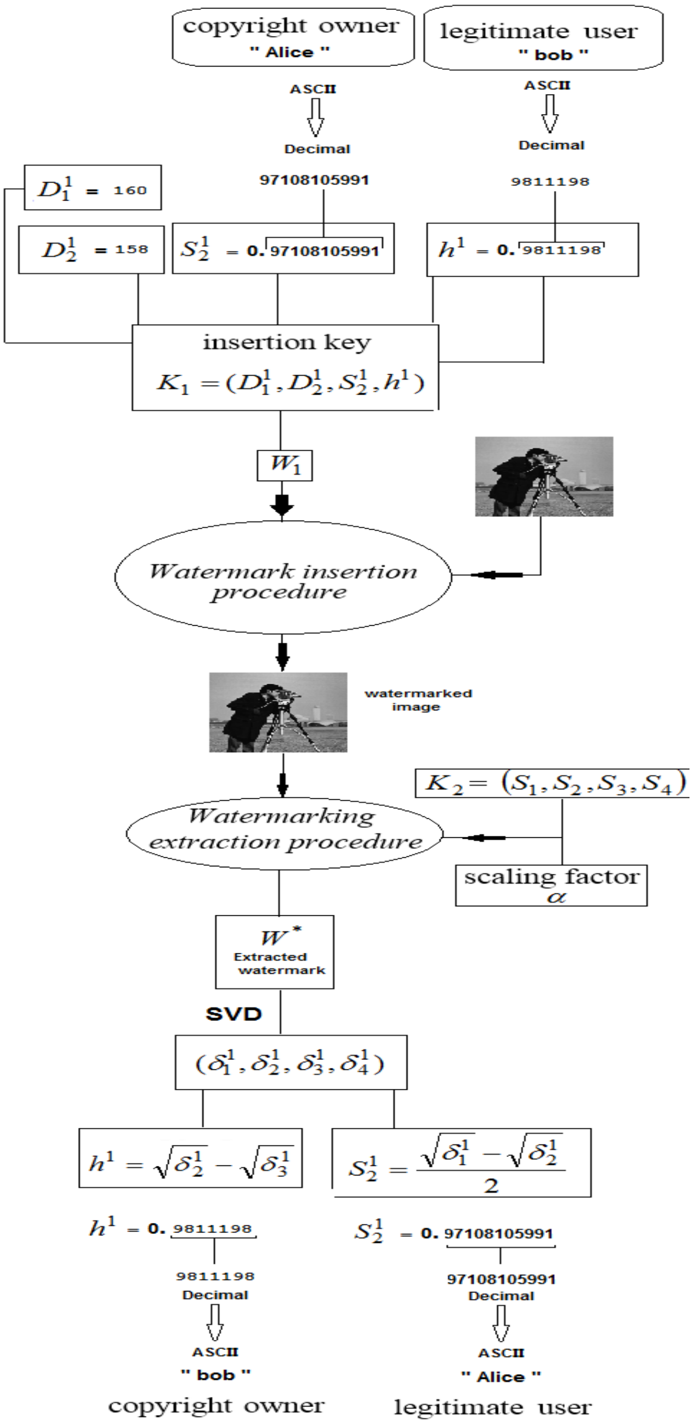


Figure 5-3 the proposed scheme for copyright protection

5.2. Illicit distribution

By using the internet, the online purchasing and distribution of digital images can be performed easily. The good distribution scheme is to distribute data without the possibility for the receivers to redistribute it to unauthorized user.

If a user illegally distributes an image then, as above by extraction procedure, we obtain

$$h^1 = \sqrt{\delta_2^1} - \sqrt{\delta_3^1}$$

the serial number of the user, so that redistributed copies can be traced back to the pirate.

5.3. Copy control

Embedding mark in an image can prevent illegal copying, for our proposed scheme we can use the second bloc and we take $D_1^2 < D_1^1$,$D_2^2 < D_2^1$ then by (4) we have

$$(D_1^2)^2 + (D_2^2)^2 = \delta_3^2 = \delta_4^2$$

Hence δ_3^2 can be considered for example as information about “no copy”, in this way a copying device might inhibit coping of image if it detects an information (δ_3^2) in watermark that indicates coping is prohibited, for this application, copying device must include watermark detection circuitry. We can increase the number of blocks of W_k so that the mark contains other information as addresses or distribution path parameters. Then the number of blocks of the watermark is related to the desired capacity.

6. Conclusion

In this chapter we have proposed a new blind robust watermarking technique which originality stands on using positive semi-definite matrices for which the spectral decomposition coincides with the singular value decomposition. The proposed watermarking scheme is robust against a wide variety of attacks, as indicated in the experimental results Moreover, the scheme overcomes the drawbacks of the deadlock problem, and the comparison analysis shows that our scheme provides a higher capacity and achieves better image quality for watermarked images, and it can be used for discouraging illicit copying and distribution of copyright material.

Chapter 6 Strict authentication of images using polar decomposition and QR codes

Abstract

Because of the prevalence of interconnected networks and the development in the digital image technologies and editing software. Digital images are easily distributed, duplicated and modified. This aspect is now so important that image content protection has become a significant security issue. Recently, fragile watermarking has been used as a technique to achieve image authentication. In this work, a blind fragile watermarking algorithm based on Polar decomposition and QR code for image authentication has been presented. Because of the non-uniqueness of the singular value decomposition (SVD), the use of polar decomposition can overcome this limitation, the watermarked image is obtained by multiplying the host image by a suitable positive semi definite matrix, the experimental results indicate the validity of the proposed algorithm in watermark transparency and fragility factors, thus the proposed watermarking scheme can be applied for image authentication.

Keywords—Digital image watermarking, Singular value decomposition, polar decomposition, Image authentication, QR code.

1. Introduction

In the past decade many different semi fragile watermarking methods have been proposed for different purposes, for watermarking medical images [161] proposed a blind semi fragile watermarking in wavelet domain, and it is robust against some common attacks such as salt and pepper noise and JPEG compression. Chune Zhang *et al*. [162] presented a scheme for both content authentication, and copyright verification. Ching-Yung Lin and Shih-Fu Chang [163] proposed a semi fragile watermarking algorithm that accepts JPEG lossy compression and rejects malicious attacks. Haohao Song *et al*. [164] proposed a novel semi fragile image watermarking scheme based on wavelet, Shi, Jianping, and Zhengjun Zhai, [165] also proposed a semi fragile watermarking, they showed that the watermark keeps good tolerate against JPEG compression. But their method is non-blind. Also other fragile watermarking methods has been proposed, Palma Hernandez,*et al*. [166] proposed a fragile watermarking scheme for image authentication in mobile devices, Helvie *et al*. [167] introduced a reversible fragile watermarking Based on difference expansion using manhattan distances for 2D vector map. Di Xiao *et al*. [168] proposed an improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing. Jassim, T *et al*. [169] presented a new robust and fragile watermarking scheme for images captured by mobile phone cameras. Most of the methods mentioned above are semi or non blind and they don't use SVD and QR code which we based on in our watermarking scheme.

This chapter concerns a strict authentication hence we propose a blind fragile watermarking scheme based on singular value decomposition and QR code for image authentication.

The rest of the chapter will be organized as follows, the second section will present the related knowledge by giving a brief definition of the QR code, the third section will explain the different steps of the proposed digital watermarking scheme. To validate our scheme we present a performance analysis in section four, and we conclude the chapter in section five.

2. Related knowledge

2.1 QR Code (Quick Response Code)

QR Code is a matrix symbol that contains a range of nominally rectangle segments organized in an overall square pattern. QR Code includes unique finder pattern located at three corners of the symbol and intended to assist in easy location of its position, size and Inclination. A wide variety of sizes of symbol is provided for together with four levels of error correction. [171], [172] and it is defined in (“QR Code Essentials”, [173] as follows: “A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted; data is then extracted from patterns present in both horizontal and vertical components of the image”.

3. Proposed method

Several SVD based watermarking schemes have been proposed, a disadvantage of the SVD method is its non-uniqueness, to overcome this drawback we proposed a watermarking scheme based on polar decomposition, this method consists to multiply the host image by a suitable positive definite matrix , it will also make the embedding and extraction procedure fast by using matrix operations. To achieve a high sensitivity detection we choose the exponential modulation, also we based on QR code because it is more practical with smart phones devices and QR matrix is sensitive to a small change of source data which help to make the watermarking more fragile.

Proposition. SVD decomposition is not unique, indeed any matrix A $\in R^{n\times n}$ has at least 2^n singular value decompositions.

Proof: Given an SVD decomposition $A = US\ V^t$ of the matrix A, consider a random sequence $(d_i) = \langle \pm 1 \rangle$ of length n and the diagonal matrix D = diag(d_i) then $A = (UD)S\ (VD)^t$ with $DD^t = I_n$. As the product of two orthogonal matrices is orthogonal, UD and VD are orthogonal matrices and $A = (UD)S\ (VD)^t$ is another SVD decomposition of A, to obtain the diagonal matrix D, we can use 2^n combinations.

Remark

As the SVD decomposition is not unique, in SVD based watermarking schemes to insert or extract the watermark we must use the same machine or the same SVD algorithm.

The proposed method divided into three subsections as follow:

Given an image A of size $n \times n$

3.1. Construction of watermark

Let $R>0$, $h>0$ be two arbitrary positive numbers. Consider a decreasing sequence

$(W_m)_{m\geq 1}$ defined by

$$W_1 = h+(n-1)R \text{ and } W_m = W_1-(m-1)R \tag{1}$$

Define the watermark by the QR code of $W=(W_1,..,W_n)$.

3.2. Watermark insertion procedure

1) Apply the right polar decomposition on A:

$$A = U\times S\times V^t = (UV^t).(\mathrm{VSV}^{\mathrm{t}}) = \mathrm{Q.P} \tag{2}$$

with $S = diag\ (S_i)$ and $\det P = \prod_{i=1}^{n} S_i \neq 0$.

2) Using *the exponential modulation*

$$Y_i = S_i e^{\alpha\, W_i} \tag{3}$$

Put $$D = diag\,(e^{\alpha W_1},\, ...,\, e^{\alpha W_n})\,,\ P_0 = VDV^t \tag{4}$$

So the watermarked image is

$$\begin{aligned} A^* &= Udiag\,(Y_i\ )V^{\,t} = (UV^t)(Vdiag\,(Y_i\ )V^{\,t}) = \\ &(UV^t)(Vdiag\,(S_i\,e^{\alpha W_i})V^{\,t}) = QPP_0 \end{aligned} \tag{5}$$

3.3. Watermark extraction procedure

Input: A^*, α and the keys: $K_1 = W_1;\ K_2 = \det(P) = \prod_{i=1}^{n} S_i$

1) Apply the right polar decomposition on A^*:

$$A^* = U^*\ diag(Y_i^*)\,V*^t = (U^*.V^{*^t})\,(V^*diag\,(Y_i^*)V^t\,) = = Q^*P^* \tag{6}$$

2) As the determinant of the orthogonal matrix is ±1, then

$\left|\det A^*\right| = \prod_{i=1}^{n} Y_i^* = \prod_{i=1}^{n} S_i \; e^{\alpha \sum_{i=1}^{n} W_i}$ where ‘ | | ’ indicates the absolute value.

$$\text{So put } \bar{S} = \sum W_i \text{ ; then } \bar{S} = \frac{1}{\alpha} \log \frac{\prod Y_i^*}{K_2} \qquad (7)$$

3) According to equations (1) and assuming that the watermarked image is manipulated then

$$R^* = \frac{1}{n-1}(2K_1 - \frac{2}{n}\bar{S}) \qquad (8)$$

4) The extracted watermark is the QR of $W^* = (\; K_1, \;\; K_1 - R^*,.., \;\; K_1 - (n-1)R^* \,)$

If the image A is not altered, R^* must be equal to R and the QR of W^* coincides with the QR of W , Otherwise the content of image is modified.

Our proposed image watermarking method can be concluded in (Figure 6.1).

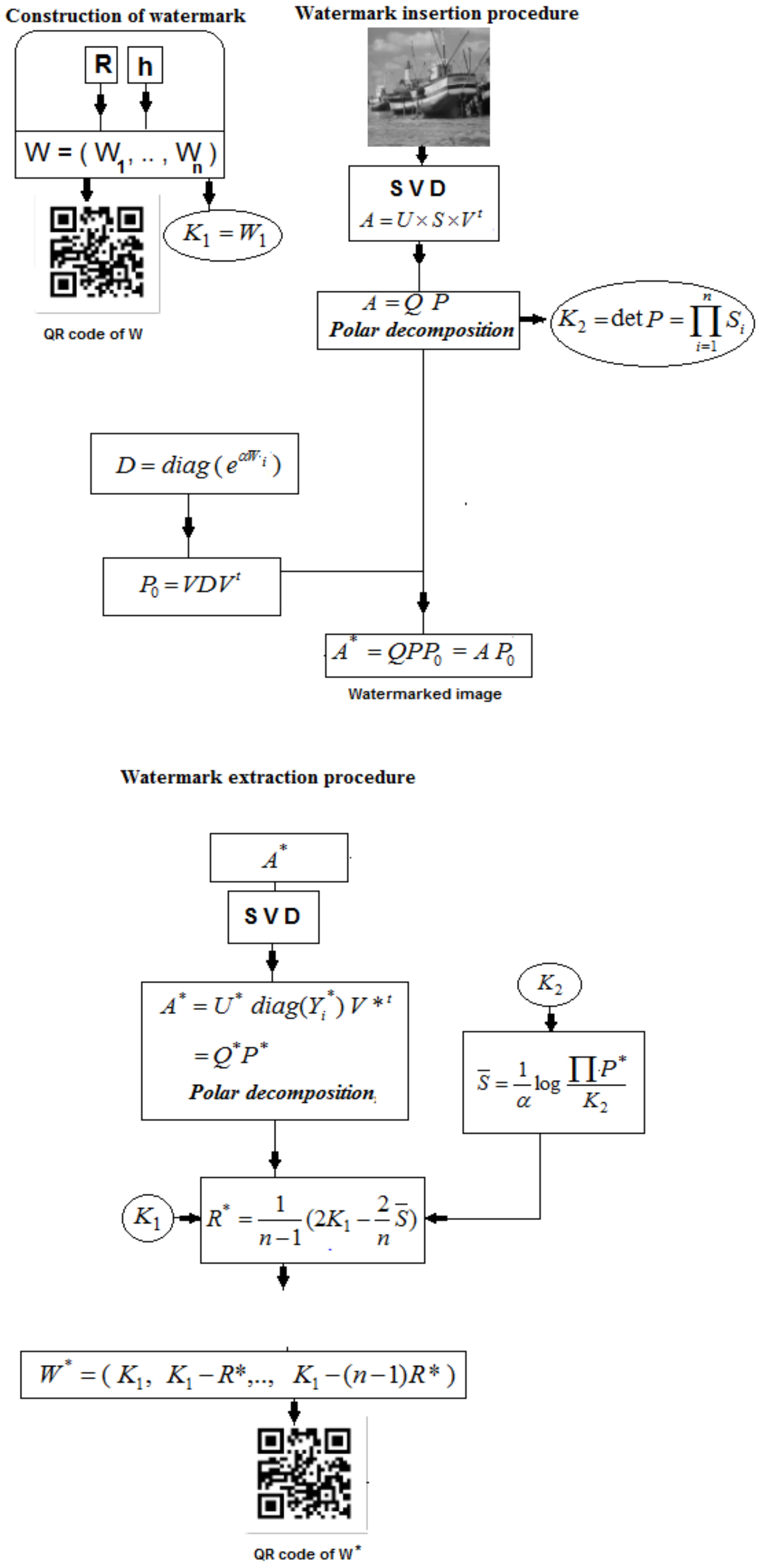

Construction of watermark
R
h
W = (W$_1$, .. , W$_n$)
$K_1 = W_1$
QR code of W
Watermark insertion procedure
S V D
$A = U \times S \times V^t$
$A = Q\ P$
Polar decomposition
$K_2 = \det P = \prod_{i=1}^{n} S_i$
$D = diag\,(e^{\alpha W_i})$
$P_0 = VDV^t$
$A^* = QPP_0 = A\,P_0$
Watermarked image
Watermark extraction procedure
A^*
S V D
$A^* = U^*\ diag(Y_i^*)\ V^{*t}$
$= Q^* P^*$
Polar decomposition
K_2
$\bar{S} = \frac{1}{\alpha} \log \frac{\prod P^*}{K_2}$
K_1
$R^* = \frac{1}{n-1}(2K_1 - \frac{2}{n}\bar{S})$
$W^* = (\,K_1,\ K_1 - R^*, ...,\ K_1 - (n-1)R^*\,)$
QR code of W*

Figure 6-1 The proposed scheme

4. Experimental results

To demonstrate the efficiency and the performance of the proposed image watermarking scheme we implemented the proposed algorithm in Matlab, we used eight test images, of size 512 Cameraman Lena, Peppers, Baboon, Zelaine, Barbara, Goldhill and boat. (figure 6.2). Using eight test images is widely enough to make a conclusion about the sensitivity of the watermarking scheme.

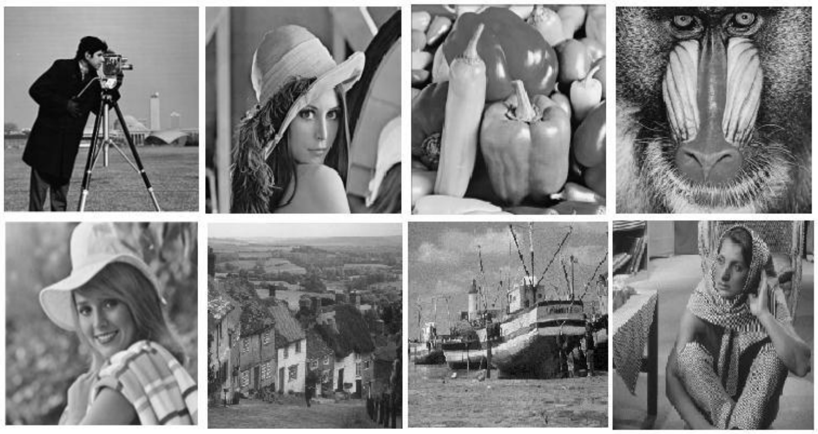


Figure 6-2 The original test images

The quality of the watermarked image is assessed with the PSNR (Peak signal-to-noise ratio):

$$PSNR = 10\log_{10}(\frac{255^2}{MSE})db \tag{9}$$

with MSE is the mean squared error between the original and watermarked image. The PSNR values of the watermarked images by our method indicate that our method in general achieves very good quality as it shown in (Table 6.1). So the proposed method preserves good transparency for the watermarked images.

Table 6.1 Relationship between the scale factor (α) and transparency in terms of the PSNR value (dB).

	the scale factor (α)								
Images	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
Lena	56.89	56. 96	56. 85	56.76	56.57	55.89	55.63	55.29	54.87
Goldhill	58.54	58.86	58.76	58.23	57.43	57.37	56.93	56.56	56.40
Baboon	56.67	56. 85	56. 26	56.15	55. 67	55.56	55.51	55.42	55.09

Barbara	56.26	56. 69	56.43	56.21	56. 17	55. 96	55. 39	55. 37	55. 28
Peppers	56.94	56. 81	56. 32	55.96	55. 30	55.16	54. 48	54. 26	53.43
Boat	55.97	56.72	56.12	55.23	55.14	55.00	54.35	54.03	53.14
Zelaine	54.44	56. 31	55.22	56.70	55. 89	57. 02	55. 11	53. 14	54. 27
cameraman	55.01	56. 43	55. 10	56.31	56. 29	55.78	55. 50	55. 85	54.89

In order to evaluate the quality of the extracted signature, we use normalized correlation (NC) metric as:

$$NC(W,W') = \frac{1}{W_h \times W_w} \sum_{i=0}^{W_h - 1} \sum_{j=0}^{Ww-1} W(i,j) \times W'(i,j) \qquad (10)$$

where W_h and W_w are the height and width of the watermarked image, respectively. $W(i,j)$ and $W'(i,j)$ denote the coefficients of the inserted signature and the extracted signature respectively.

(Table 6.2) presents the NC results between the QR image of the original watermark and QR image of extracted watermark after each attack, and with different test images. The table shows that our method is fragile for every attack and it affects on the quality of the watermark, this option makes our method detect any small change in the image and authenticate the original images against common processing attacks.

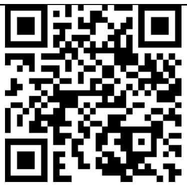
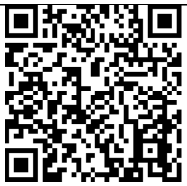
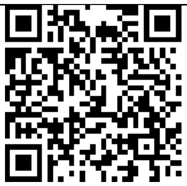
Table 6.2 Resulted NC for different image attacks.

	Image processing attacks							
Images	Jpeg 60	Speckle 0.04	imsharpen	FFT	Salt & pepper	Filter median	Gaussian filter	Rotation 5°
Lena	0.161	0.187	0.191	0.039	0.028	0.011	0.088	0.006
Goldhill	0.126	0.125	0.026	0.008	0.011	0.086	0.067	0.042
Baboon	0.198	0.192	0.049	0.118	0.102	0.109	0.0139	0.001
Barbara	0.114	0.032	0.038	0.021	0.012	0.075	0.0138	0.162
Peppers	0.100	0.001	0.031	0.013	0.091	0.028	0.032	0.013
Boat	0.091	0.140	0.104	0.113	0.008	0.043	0.174	0.010
Zelaine	0.063	0.110	0.041	0.128	0.023	0.013	0.048	0.022
cameraman	0.116	0.024	0.025	0.137	0.100	0.018	0.015	0.014

(Table 6.3) shows the extracted watermarks and the NC between each of them and the original watermark, the experiment was done using a test image Lena under different attacks, it is clear that each attack makes a change in the watermark and the NC values of all the extracted watermarks from the attacked images are close to zero which means an attack is detected and the extracted watermark is damaged.

The comparison of the results obtained by our proposed method and with the results of state of the art schemes mentioned above, shows that the sensitivity of the watermark in our method is higher than most methods and any small attack can be detected easily, also the quality of the watermarked images used presented by the PSNR values indicates that the obtained watermarked images have a very good quality, furthermore our scheme is blind so no need to resort to the original image. Thus the proposed fragile watermarking scheme can be applied as a solution to authenticate medical images, because medical tradition is very strict with the quality of medical images, and it requires a strict authentication solution.

Table 6.3 The extracted watermarks from attacked images and their NC values.

		Extracted watermark after Attacks	NC
Attacks	Original watermark (extracted watermark without attacks)		1
	Jpeg 60		0.0155
	Speckle 0.04		0.0185

	Imsharpen		0.0409
	FFT		0.0036
	Salt & pepper		0.0113
	Filter median		0.0024
	Rotation 5°		0.0200

5. Conclusion

This chapter concerns a strict authentication and presents a fragile watermarking method for image authentication based on polar decomposition and QR code, this method consists to multiply the host image by a suitable positive definite matrix, in the extraction procedure the original image is not required, so the proposed method is blind. Simulation results indicate that our method achieves good imperceptibility and fragility against image processing attacks, and it is sensitive to a very small change in the image, our perspective is to improve our watermarking scheme and make it able to locate the modification area in the attacked image.

Chapter 7 A robust watermarking scheme in frequency domain for ownership protection and deadlock prevention

Abstract

The digital watermarking is used to protect the intellectual property rights in the multimedia. In this chapter, we present a blind robust watermarking procedure to embed the watermark into an image A using the polar decomposition, the watermark is constructed by using a secret key K_1 (the owner's identities) and inserted between the positive component and the orthogonal component of A. The watermark extraction process requires a secret key K_2 which is image dependent. Our scheme is based on matrix multiplication (not commutative), in case of deadlock, this leads to know who watermarked the image first and determines the rightful owner, this scheme is thus performed to avoid the deadlock attack and for ownership protection. Experimental results show the high robustness of the proposed scheme under different image processing attacks.

Keywords— Watermarking, Polar decomposition, copyright protection, deadlock, robustness.

1. Introduction

In the last years many watermarking schemes have been proposed but most of them are vulnerable against deadlock attack, as those in [174] [175] [176] [177] [178].

So in order to solve this, Craver et al. [179] took the initiative in presenting and solving this problem. They provided a counterfeit watermarking scheme from a watermarked image to allow several claims of rightful ownership. To prevent counterfeit attack, they suggested that the owner should use a watermarking scheme that is both non-invertible and non quasi-invertible and the watermark should be a bit sequence from the image via a one way hash function. Qiao and Nahrstedt also solved the problem of rightful ownership and were the first to provide protection of customers' rights [180].Zeng and Liu[181] they proposed for resolving rightful ownerships of digital images a statistical watermarking detection without using original images, they concluded that in the watermark detection processing the original image should not be indirectly involved. They claimed the watermark series should be produced with from some significant signature or registered proprietor ID via an one way hash function.

In this chapter we introduce a novel blind robust watermarking scheme which exploits the polar decomposition of matrices and solve the deadlock problem.

Organization of the rest of this chapter is as follows: section two presents the proposed method, and section three provides an application for solving the deadlock problem, section four throws light on performance and security analysis, finally the summary of results and the conclusion is presented in Section five.

2. Proposed method

To watermark a given original image A of size $n \times n$

we need two secret keys K_1, K_2.

We use the following notation:

$$M^N = N\,M\,N^{-1} \qquad (1)$$

for every square matrix *M* and every invertible matrix *N*.

Let $A = P\,Q = U\,S\,V^t$

2.1. Key generation

Choose random positive numbers $K_1 = \left\{ D_1^1 \ D_2^1 \ldots \right\}$ to generate a watermark $W_1 = \{ w_1, w_2, w_3, w_4, \ldots \}$ of length n, for example if we use the key generation method of [160], to every key

K_1 of length $2k+2$ is associated a decreasing sequence of length *4k*:

$\delta_1^1 \geq \delta_2^1 \geq \delta_3^1 \geq \delta_4^1 \geq \ldots \geq \delta_1^k \geq \delta_2^k \geq \delta_3^k \geq \delta_4^k$

In particular we will take k = 1, then to every insertion key K_1 of length 4 is associated a sequence $w_1 = \delta_1^1 \geq w_2 = \delta_2^1 \geq w_3 = \delta_3^1 \geq w_4 = \delta_4^1 \geq \ 0 \geq \ \ldots \geq 0$

Now we construct the watermark $(w_1, w_2, w_3, w_4, 0, \ldots, 0)$.

Put $K_2 = (S_1, S_2, S_3, S_4, \alpha \ )$ the extraction key with α is the scaling factor and (S_1, S_2, S_3, S_4) are the first four singular values of the host image.

2.2.Watermark insertion procedure

To watermark the image we use four steps:

1. Apply SVD to A : $A = US \ V^t$.
2. Deduce the polar decomposition $A = PQ$
3. By using the insertion key K_1, put $W_1 = diag\ (w_1, w_2, w_3, w_4, 0, \ldots, 0)$ and calculate

$$H_1 = (I + \alpha W_1)^{\ U} \qquad (2)$$

with *I* is an identity matrix of order *n* .

4. Calculate the watermarked image

$$A_1 = P \ H_1 \ Q = USU^t.U(I + \alpha W_1 \ )U^t.UV^t \qquad (3)$$

$$= US(I + \alpha W_1)V^t$$

2.3. Watermark extraction procedure

We present our procedure for detecting the presence of a watermark in a given image A_1^* and extracting the concerned watermark.

Apply SVD to $A_1^* = U_1^* \ S_1^* \ V_1^{*t}$

with $S_1^* = diag\ (s_i^*)$ for i = 1, .., n

By using K_2 compute

$$w_i^* = \frac{1}{\alpha}\left(\frac{s_i^*}{s_i} - 1 \right) \text{ for i = 1, .., 4} \qquad (4)$$

If $\frac{s_3^*}{s_4^*} = \frac{s_3}{s_4}$ or $\begin{vmatrix} s^*{}_3 & s_3 \\ s^*{}_4 & s_4 \end{vmatrix} = 0$

then the mark is detected and the obtained mark is $(w_1*,...,w_4*,..,)$

else the watermark is not present in the image.

Remark

The watermark can be constructed with *4k* non zero values, then in this case, the extraction key is $K_2 = (S_1,..,S_{4k},\alpha\ )$ and the watermark will be detected if

$$\begin{vmatrix} s^*{}_{4i-1} & s_{4i-1} \\ s^*{}_{4i} & s_{4i} \end{vmatrix} = 0 \text{ for } i=1,.., k. \qquad (5)$$

The proposed watermarking algorithm support square images, in case of not-square images, we can divide the image into square blocks (for example of size 32 *32) then the watermarking scheme can be applied to every block. If the size of the plain image is not multiple of 256 a padding scheme can be used.

The security of the watermarking scheme is based on the secret keys, which are required in insertion and extraction procedure, the key space is larger enough to resist the brute force attack and the security of the watermarking scheme can be augmented by increasing the number of watermark blocks [160].

3. **Applications**

3.1 Protection ownership

In order to use our scheme for protection ownership we prove that it is robust against a wide range of common image processing attacks and achieves higher robustness compared to other known watermarking methods (See Experimental results and Table 7.2).

3.2 Solve the deadlock problem

3.2.1 Second variant of watermarking scheme to overcome the deadlock problem

In this section we introduce a second variant of our watermarking method to solve the multiple claims of ownership, an attacker can embed his watermark into the already watermarked image and claim the ownership of such image, by the second watermark the pirate attempts to discredit the legitimate owner of the image, he inserts an additional watermark this way it is unclear who has watermarked the image first.

We assume that the attacker knows the watermarking and the extraction algorithms, and he has a watermarked image available A_1 but he has not the secret keys of insertion and extraction of A_1.

So let A be an image of size $n \times n$

Choose random positive numbers $K_1 = \left\{ D_1^1 \; D_2^1 \ldots \right\}$ to generate a watermark $W_1 = \left\{ w_1, w_2, w_3, w_4, 0, \ldots 0 \right\}$ of size n

Apply SVD to $A = U\, S\, V^t$, with $S = diag(s_i)$, $i = 1, .., n.$

Apply normal SVD, to $A = U_0\; S\, V_0^{\,t}$

where $U_0 = UP_0$, $V_0 = VP_0$ with $P_0 = diag < \pm 1 >$ is a diagonal matrix chosen such that the first non zero element of each column of U_0 is positive.

Calculate the watermarked image

$$A_1 = U_0\; S(I + \alpha_1 W_1)\, V_0^{\,t} \qquad (6)$$

With
$$I + \alpha_1 W_1 = \begin{pmatrix} 1+\alpha_1 w_1 & 0 & \cdots & 0 \\ 0 & 1+\alpha_1 w_2 & & \\ \vdots & & \ddots & \\ 0 & & & \end{pmatrix}$$

Note that A_1 can be expressed by

$$\begin{aligned} A_1 &= (U_0 S U_0^t)(U_0 (I + \alpha_1 W_1)\, U_0^t)\,(\,U_0\, V_0^{\,t}) \\ &= PH_1\, Q \end{aligned}$$

Where $P\,Q$ is the polar decomposition of A and $H_1 = U_0 (I + \alpha_1 W_1)\, U_0^t$. According to [12] the normal SVD of A is unique if the singular value s_i are pairwise distinct and non zero, then the image A and the watermarked image A_1 have the same U_0.

For the watermark extraction procedure we use the same method cited in 3.3.

3.2.2 Double Watermarking

Suppose that a pirate generates a counterfeit original A_2 by embedding an additional watermark W_2 in A_1 (the publicly available image) then there is a double watermarking, so the same image is watermarked twice (figure 7.1).

So we will have:

$$\begin{aligned} A_2 &= U_0\, S\, (I + \alpha_1 W_1)\, (I + \alpha_2 W_2)\, V_0^{\,t} \\ &= U_0\, S\, (I + \alpha_1 W_1) V_0^{\,t}\; V_0 (I + \alpha_2 W_2)\, V_0^{\,t} \\ &= A_1 Q^t H_2 Q \qquad (7\,) \end{aligned}$$

where $Q = U_0 V_0^t$ is the same orthogonal component of A_1 or A_2 and $H_2 = U_0 (I + \alpha_2 W_2)\, U_0^t$

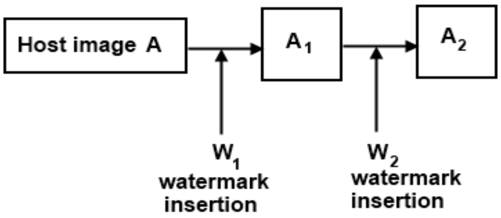


Figure 7-1 Double watermarking diagram

3.2.3 Multiple claims of ownership

In case of deadlock let us assume two parties F and G claim ownership of an image, to determine the right owner, the arbitrator or the court must establish who watermarked the image first, for this he requests from both F and G to bring the respective images I_F and I_G and their watermarks W_F and W_G and the scaling factors α_F and α_G .

The arbitrator performs a normal SVD to one of the two images I_F , I_G and deduce U_0 , V_0 and $Q = U_0 V_0^t$.

By using the watermarks W_F and W_G he computes

$H_F = U_0 (I + \alpha_F W_F) U_0^t$ and $H_G = U_0 (I + \alpha_G W_G) U_0^t$.

According to equation (7), only one of the equalities is verified

$$I_F = I_G Q^t H_F Q \tag{8}$$

$$I_G = I_F Q^t H_G Q \tag{9}$$

for example if (8) is true, then the ownership belongs to *G* and *F* is the pirate, and its image I_F is derived from I_G the watermarked copy produced by the real owner G.

Practically in order to prove that (8) is true, one can calculate:

$C_1 = I_F - I_G Q^t H_F Q$, $C_2 = I_G - I_F Q^t H_G Q$

and verify that

$trace(C_1 C_1^t) = 0 \quad and \quad trace(C_2 C_2^t) \neq 0$, otherwise

$trace(C_1 C_1^t) \neq 0 \quad and \quad trace(C_2 C_2^t) = 0$

imply that *F* is the real owner.

Our method is based on polar decomposition and multiplicative embedding. As the matrix multiplication is not commutative, this leads to know who watermarked content first. (Figure 7.2)

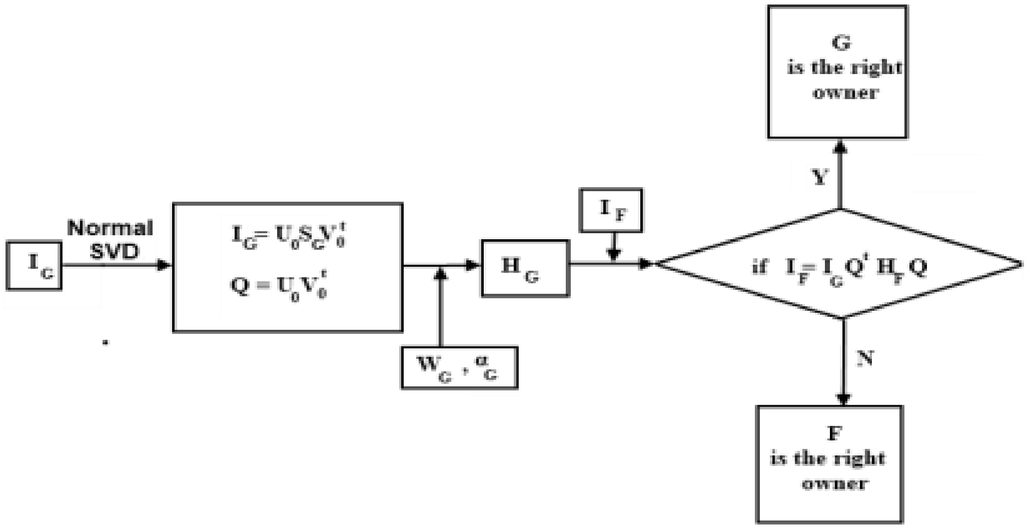


Figure 7-2 Arbitration process: claim of G

3.2.4 Illustrative example

Consider for illustrative example a scenario where G is the real owner of a test image Lena and take:

$$W_G = \{125,\ 114,\ 103,\ 72,\ 0,\ldots,0\} \qquad \alpha_G = 0.001$$

$$W_F = \{212,\ 143,\ 120,\ 88,\ 0,\ldots,0\} \qquad \alpha_F = 0.001$$

By following the above steps we calculate C_1 and C_2 to know who is the real owner, in this example we'll obtain

$$trace(C_1 C_1^t) = 2476.21 \qquad trace(C_2 C_2^t) = 0$$

This values indicate that the person G is the rightful owner of Lena image, our scheme must correctly identify the rightful owner and solve the deadlock problem. (figure 7.3)

Figure 7-3 Illustrative exemple

4. Experimental results

To demonstrate the efficiency and the security of the proposed image watermarking scheme, we used six test gray scale images of size 512 ×512 (figure 7.4), and in all experiments we took the average results of those six images. We use the PSNR (Peak Signal to Noise Ratio) to define the similarity of the watermarked and original image

$$PNSR = 10\log\left(\frac{255^2}{MSE}\right) \quad db \qquad (10)$$

Where MSE (Mean Square Error) is defined as:

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[X(i,j)-Y(i,j)]^2 \qquad (11)$$

m and n are the size of images X and Y.

the higher PSNR values shows the better quality of the watermarked image .

In the first experiment we compared the PSNR values of the watermarked images of the proposed scheme with other schemes, the results are illustrated in Table 7.1, it is clear from the table that the quality of the watermarked image is high and the achieved transparency is better than other schemes.

Figure 7-4 Test images

Table 7.1 Comparison of PSNR for Lai, C. C. et al.[155] , Tsai, H. H et al. [156] and our scheme

Method	the scale factors				
	0.01	0.03	0.05	0.07	0.09
Lai, C. C. et al.[155]	51.14	51.14	50.89	49.52	47.49
Tsai, H. H et al.[156]	47	37	33	28	about 25
Proposed method	53.91	55.26	54.38	53.82	55.31

Table 7.2 NC values obtained from different watermarking techniques under several attacks.

Method	geometrical attack		noise attack		image-processing attack		compression attack
	cropping	rotation	Gaussian noise	average filtering	histogram equalization	darken	Jpeg 50
Proposed	**0.9951**	0.9696	**0.9753**	**0.9978**	0.9959	0.9861	**0.9991**
Lagzian et al.[182]	0.9512	0.8630	0.9792	0.9942	0.8530	-	0.9983
Gaurav et al. [183]	0.3166	0.4803	0.4223	0.49525	0.8542	-	0.98755
Chin Lai[184]	0.9948	**0.9936**	0.9735	0.9840	**0.9984**	**0.9995**	0.9951
R. Liu [185]	0.9896	0.9890	0.9677	0.9780	0.9955	0.9971	0.9900
C.-C. Lai [192]	0.9925	0.9917	0.9717	0.9819	0.9971	0.9983	0.9925

In order to prove, the robustness of the proposed watermarking scheme, we apply a variety of attacks on the watermarked image, then we extract the watermark and calculate the correlation between the original and the extracted watermark, the normalized correlation is defined as follows:

$$NC(W,W') = \frac{1}{W_h \times W_w} \sum_{i=0}^{W_h-1} \sum_{j=0}^{Ww-1} W(i,j) \times W'(i,j) \qquad (12)$$

where W_h and W_w are the height and width of the watermarked image, respectively. $W(i,j)$ and $W'(i,j)$ denote the coefficients of the inserted signature and the extracted signature respectively.

In the second experiment we compared the results of the normalized correlation of the extracted watermarks after applying image attacks of our method with other methods. As can be seen in table 7.2, the proposed method achieves good robustness against all attacks, and when we compare the results with other schemes it appears that it works better than them in most attacks, and in those which it was not the best, the NC values still high.

5. Conclusion

Digital watermarking has been proposed as a means to identify the owner, the watermark must be invisible and robust to manipulations, distortions, and readily extracted to characterize the copyright owner. The deadlock problem occurs when multiple ownership claims are made, in this chapter we propose a blind watermarking scheme to resolve the rightful ownership of an image, this technique exploits the polar decomposition, to enhance the security, two secret keys are used, one key is author dependent and is required to embed the watermark into the host image, the second key is image dependent and is required for the watermark extraction, without it, it will be impossible to extract the watermark. Our scheme is based on matrix multiplication (not commutative) in case of deadlock, this leads to know who watermarked the image first and determines the rightful owner.

Simulation results indicate that the proposed method is robust against a wide range of common image processing attacks and achieves higher robustness compared to other known watermarking methods.

General Conclusion

In this thesis we have presented a study of one of the main objectives of the cryptography science, which is the authentication.

Authentication means the techniques and the protocols used to prove the identity of a person or a document, and for this it can be divided into user authentication and content authentication, this concept has been existed for many centuries, but Since the extraordinary technical revolution from analog to digital at the end of 20th century, the authentication methods took a new forms, challenges and high importance.

The development of the technology and the digitalization led to develop new technologies, devices and algorithms in order to achieve the authentication of users and of the digital contents in the digital world.

In our thesis we have studied the most developed techniques to assure content authentications such as handwritten signature recognition system, Digital signature, Digital watermarking. In the other hand we have presented the technologies and technique to achieve the user authentication, we started with the classic and dynamic password, then the biometric techniques including their three types, biological analysis techniques, behavior analysis technique (dynamic signature, keystroke dynamics, the voice) and morphological analysis techniques (shape of the hand, fingerprints, iris, retina, facial scan and the configuration system of veins).

Furthermore we have presented the state of the art of RFID technology to achieve authentication and access control, finally we have presented the zero knowledge proof

In the second part of our thesis we have provided mainly four contributions that took place in content authentication schemes, starting with a secure image encryption scheme based on polar decomposition and chaotic map then a robust blind and secure watermarking scheme using positive semi definite matrices, furthermore a novel blind watermarking scheme based on SVD and QR code for image authentication and finally a robust watermarking scheme in frequency domain for ownership protection and deadlock solution.

The four proposed schemes have achieved very good experimental results, and they showed a good security compared to the state of the art schemes, each of the proposed scheme’s stand on an originality that makes it avoid the weakness and vulnerabilities that other state of the art schemes suffer from. The proposed schemes have many applications for content authentication, copy control, illicit distribution, deadlock prevention, content confidentiality and integrity, and they can be improved to support and be applied in other technologies and different areas.

References

[1] Arnaud, N. (2009). La diffusion des fonds photographiques patrimoniaux et scientifiques: analyse d'outils et d'interfaces. Propositions pour la photothèque de l'Observatoire de Paris (Doctoral dissertation, Institut national des techniques de la documentation du CNAM).

[2] Aujol, J. F. (2005). Traitement d'images par approches variationnelles et équations aux dérivées partielles.

[3] Pignat, J. M. (2005). Etude de la perception visuelle du mouvement et de la couleur par IRMf (Doctoral dissertation, University of Geneva).

[4] serge paulus (2008) Mémento prépresse, les formats d'image, la résolution, les espaces colorimétriques.

www.serge-paulus.be/cours/

[5] A. Manzanera,(2006) "TERI : Traitement et reconnaissance d'image", Cours Traitement et reconnaissance d'image, Master, Université Pierre et Marie CURIE, Paris 2006.

[6] A. Manzanera, (2005)" Les images numériques", cours traitement et reconnaissance d'image, Master IAD, Ecole Nationale Supérieure de Techniques Avancées/Unité d'Électronique et d'Informatique, Université Pierre et Marie CURIE, Paris 2005.

[7] d'Hardancourt, A., & Bavagnoli, J. (1995). *Fou de multimédia*. Sybex.

[8] R.C. GONZALES et P. WINTZ, (1997) « Digital Image Processing », Addition Wessley » .

[9] nrtailleau (2007) , « Chapitre 1 : L'image numérique » http://lyc-renaudeau-49.ac-nantes.fr/spip.php?article724

[10] Rivest, R. (1992). The MD5 message-digest algorithm.

[11] Eastlake, D., & Jones, P. (2001). US secure hash algorithm 1 (SHA1).

[12] Dobbertin, H., Bosselaers, A., & Preneel, B. (1996, January). RIPEMD-160: A strengthened version of RIPEMD. In *Fast Software Encryption* (pp. 71-82). Springer Berlin Heidelberg.

[13] Zheng, Y., Pieprzyk, J., & Seberry, J. (1993, January). HAVAL—a one-way hashing algorithm with variable length of output. In *Advances in Cryptology—AUSCRYPT'92* (pp. 81-104). Springer Berlin Heidelberg.

[14] Rijmen, V., & Barreto, P. S. L. M. (2001). The WHIRLPOOL hash function. *World-Wide Web document*, 72.

[15] G. H. GOLUB AND C. F. VAN LOAN, (1983) Matrix Computations, Johns Hopkins University Press, Baltimore,MD.

[16] Higham, N.(1986), 'Computing the Polar Decomposition—with pplications' SIAM Journal on Scientific and Statistical Computing 1986 7:4, 1160-1174

[17] J. F. Yang and C. L. Lu,(1995) "Combined Techniques of Singular Value Decomposition and Vector Quantization for Image Coding," *IEEETransaction on Image Processing, Piscataway, New Jersey, USA*, 4, pp. 1141–1146,.

[18] Bhatia, Rajendra. (2009)Positive definite matrices. Princeton University Press.

[19] Plamondon, R., & Lorette, G. (1989). Automatic signature verification and writer identification—the state of the art. *Pattern recognition*, *22*(2), 107-131.

[20] Han, K., & Sethi, I. K. (1996). Handwritten signature retrieval and identification. *Pattern Recognition Letters*, *17*(1), 83-90.

[21] M. Wirotius, (2005)Authentification par Signature manuscrite sur support nomade, thèse de doctorat en Informatique, université de Tours.

[22] A. Lahyane, (2002)Vérification de Signatures Manuscrites, mémoire en Mathématique et Informatique, université du Québec à Trois-Rivières.

[23] R. Sabourin et G. Genest, (1995)'Définition et Evolution d'une Famille de Représentations pour la Vérification hors-ligne des Signatures', Traitement du Signal, vol.12, no.6, pp. 586-596.

[24] R. Plamondon and N. Sargur, (2000) 'On-line and Off-line Handwriting Recognition: A Comprehensive Survey', IEEE Transactions on Pattern Recognition and Machine Intelligence, vol.22, no.1.

[25] S. Sanjay, K. Gharde, P. Adhiya, H. Harsha, and G. Chavan, (2012)'Offline Handwritten Signature Verification Approaches: A Review', IJCST, vol.3, no.2, pp. 265-269.

[26] N. Athamena,(2010) Reconnaissance de l'écriture Arabe Manuscrite, thèse de Doctorat en Electronique, université de Batna.

[27] Herkt, A. (1986). Signature Disguise or Signature Forgery?. *Journal of the Forensic Science Society*, *26*(4), 257-266.

[28] A. Boukharouba, (2011) Contribution à la Segmentation et à la Reconnaissance de l'écriture Arabe Manuscrite, thèse de Doctorat en Sciences, université de Mentouri-Constantine.

[29] M. Bhatia, (2013)'Off-Line Handwritten Signature Verification using Neural Network', IJAIEM, vol.2, no.5.

[30] R. Bendana, (2007) Sélection d'Attributs Basée sur un Algorithme Génétique Neural : Application à la Reconnaissance des Caractères manuscrits, mémoire de Magister en Informatique, université Mentouri de Constantine.

[31] R.O. Duda, P.E. Hart, and D.G. Stork, (2001) *Pattern Classification*, Wiley-Interscience, New York-USA.

[32] N. Benhamed, (2002) Optimisation de Réseaux de Neurones pour la Reconnaissance de Chiffres Manuscrits Isolés : Sélection et Pondération des Primitives par Algorithmes Génétiques, mémoire de la Maîtrise en Génie de la Production Automatisée, université de Québec-Montréal.

[33] L. Miclet, (1984) Méthodes structurelles pour la reconnaissance des formes, Eyrolles, Paris-France.

[34] G. Gaillat, (1983) *Méthodes statistiques de reconnaissance de formes*, Centre d'édition et de documentation de l'École Nationale de Techniques Avancées.

[35] R. Plamondon and G. Lorette, (1989) 'Automatic Signature Verification and Writer Identification the State of the Art', Pattern Recognition, vol.22, no.2.

[36] Shanker, A. Piyush, and A. N. Rajagopalan. (2007) "Off-line signature verification using DTW." *Pattern Recognition Letters* 28.12: 1407-1414.

[37] Justino, E. J., Bortolozzi, F., & Sabourin, R. (2005). A comparison of SVM and HMM classifiers in the off-line signature verification. *Pattern recognition letters*, *26*(9), 1377-1385.

[38] Vélez, José F., Ángel Sánchez, Ana B. Moreno, and José L. Esteban. (2006)"Combining snakes and neural networks for off-line signature verification." In *Tenth International Workshop on Frontiers in Handwriting Recognition*. Suvisoft,.

[39] Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, Deepsikha Chaudhury, (2007), "Handwritten signature authentication scheme using integrated statistical analysis of bi -color images", IEEE ICCSA 2007 Conference, August, pp.72-77

[40] Samaneh, Moghaddam, (2009)"Off- Line Persian Signature Identification and Verification Based on Image Registration and Fusion", Journal of Multimedia, vol. 4, vol. 3.

[41] Ramachandra, Ravi, Raja, Venugopal, Patnaik, (2009)"Signature Verification using Graph Matching and Cross-Validation Principle", Int. 1. of Recent Trends in Engineering (IJR TE), vol. 1, no.1, , pp.57-61

[42] Emre, M. Elif Karsligil, (2005)"Off-line signature verification and recognition by support vector machine", Pattern Recognition Letters, vol. 26, Nov, pp.2390-2399

[43] ElGamal, T. (1985, January). A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology* (pp. 10-18). Springer Berlin Heidelberg.

[44] Dimitrios, Poulakis, and Robert Rolland. (2013)"A Digital Signature Scheme Based on Two Hard Problems." Computation, Cryptography, and Network Security.

[45] Chen, Haipeng, Xuanjing Shen, and Yingda Lv. (2010)"A New Digital Signature Algorithm Similar to ELGamal Type." Journal of Software 5.3: 320-327.

[46] Saxena, Navrati, and Narendra S. Chaudhari. (2012)"Secure encryption with digital signature approach for Short Message Service." Information and Communication Technologies (WICT), 2012 World Congress on. IEEE.

[47] Yang, Chou-Chen, Ting-Yi Chang, and Min-Shiang Hwang. (2013) "A New Group Signature Scheme Based on RSA Assumption." Information Technology And Control 42.1: 61-66.

[48] N. KOMATSU et H. TOMINAGA (1988): Authentication system using concealed image in telematics. Memoirs of the School of Science & Engineering, Waseda University, (52):45-60.

[49] KHALED LOUKHAOUKHA, (2010) 'Tatouage numérique des images dans le domaine des ondelettes basé sur la décomposition en valeurs singulières et l'optimisation multi-objective', Ph.D thesis 2010, LAVAL university. Quebec

[50] Lie, W. N., & Chang, L. C. (1999). Data hiding in images with adaptive numbers of least significant bits based on the human visual system. In *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on* (Vol. 1, pp. 286-290). IEEE.

[51] Santhi, V., & Thangavelu, D. A. (2009). DWT-SVD combined full band robust watermarking technique for color images in YUV color space. *International Journal of Computer Theory and Engineering*, *1*(4), 424-429.

[52] Kapre Bhagyashri, S., & Joshi, M. Y. (2011, June). All frequency band DWT-SVD robust watermarking technique for color images in YUV color space. In *Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on* (Vol. 3, pp. 295-299). IEEE.

[53] Dharwadkar, N. V., Amberker, B. B., & Gorai, A. (2011, February). Non-blind watermarking scheme for color images in RGB space using DWT-SVD. In *Communications and Signal Processing (ICCSP), 2011 International Conference on* (pp. 489-493). IEEE.

[54] Bas, P., Le Bihan, N., & Chassery, J. M. (2003, April). Color image watermarking using quaternion Fourier transform. In *Acoustics, Speech, and Signal Processing, 2003. Proceedings.(ICASSP'03). 2003 IEEE International Conference on* (Vol. 3, pp. III-521). IEEE.

[55] Daubechies, I. (1992). *Ten lectures on wavelets* (Vol. 61, pp. 198-202). Philadelphia: Society for industrial and applied mathematics.

[56] V.Darmstaedter, J-F. Delaigle, D. Nicholson and B. Macq. (1998) « A Block Based Watermarking Technique for MPEG-2 Signals : Optimisation and Validation on real Digital TV Distribution Links ». In Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST'98).

[57] J-F. Delaigle, C. De Vleeschouwer and B. Macq. (1997) « Watermarking Using a Matching Model Based on The Humain Visual System ». Ecole Thématique CNRS GDR-PRC ISIS : Information Signal Images Marly le Roi.

[58] J-F. Delaigle, J-M. Boucqueau, J-J. Quisquarter and B. Macq. (1996) « Digital Images Protection Techniques in a Broadcast Framework : Overview ». In Proceeding of European Conference on Multimedia Applications, Services and Techniques (ECMAST'96), pp. 711-728, Louvain-la-Neuve, Belgium,.

[59] J.R. Hernandez, F. Pérez-Gonzalez, J.M. Rodriguez and G. Nieto. (1998) « The impact of Channel Coding on The Performance of Spatial Watermarking for Copyright Protection » In Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP'98), vol. 5, pp. 2973-2976.

[60] H.Maître and S.Baudy. (1999) « Modèles Théoriques de Prédiction de Performance » Technical Report, Réseau National de la Recherche en Télécommunication, Projet Aquamars, Paris, . Vit Fan

[61] A.J. Viterbi. (1967) « Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm » IEEE Transactions on Information Theory, vol. IT-13, pp. 260-269,.

[62] R. M. Fano. (1963) « A Heuristic Discussion of Probabilistic Decoding » IEEE Transactions on Information Theory, vol. IT-9, pp. 64-73.

[63] Ammar Dahmani, (2014) these de doctorat en electronique,CONTRIBUTION AU DEVELOPPEMENT D'UNE TECHNIQUE DE WATERMARKING POUR IMAGES .université de batna

[64] les attaques sur les mots de passe. [Online] http://wiki.korben.info/mots_de_passe_statique.

[65] VAISSET Antoine, TORILLEC Olivier. *Attaque de mots passes à l'aide de Rainbow Table.* lyon : université claude bernard.

[66] SAUVAGE, Sébastien**.** C'est quoi SSL, SSH, HTTPS. *Comprendre l'ordinateur.* [Online] http://www.sebsauvage.net/comprendre/ssl/.

[67] Decouvrez OpenID un systeme d'authentification decentralise. [Online] http://connect.ed-diamond.com/Linux-Pratique/LP-048/Decouvrez-OpenID-un-systeme-d-authentification-decentralise.

[68] Haller, N.M. (1994) The S/KEY one-time password system. Symposium on Network and Distributed Systems Security.

[69] Ismael, Belghiti.(2011) Preuves à divulgation nulle de connaissance.

[70] A. Shimizu, T. Horioka, and H. Inagaki. (1998) A password authentication method for contents communication. s.l. : IEICE Transactions on Communications.

[71] Pansa, D., & Chomsiri, T. (2011). Web Security Improving by using Dynamic Password Authentication. In 2011 International Conference on Network and Electronics Engineering, IPCSIT (Vol. 11, pp. 32-36).

[72] Das, A. K., Sharma, P., Chatterjee, S., & Sing, J. K. (2012). A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. *Journal of Network and Computer Applications*, *35*(5), 1646-1656.

[73] ntrg.cs.tcd.ie/undergrad/. .ibiometrics/history.html

[74] A. K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” 1EEE Trans. on Circuits and Systems for Video Technology, vol. 14, pp. 4—20, Jan 2004.

[75] wwwbiometricnewsportal.comIbiometrics_definition.asp

[76] wwwtomsguide.fr/article/biometrie-focus,2-629.html

[77] Fernando L. Podiol and Jeffrey S. Dunn; Biometric Authentication Technology: From the Movies to Your Desktop

[78] www.biometrie-online.net/

[79] thèse présentée par M. Mohamad El Abed ,Evaluation de systèmes biométriques, et soutenue le 9 décembre 2011.

[80] D. Hoang Vu, Biométrie pour l’Identification, Rapport final, Institut de la Francophonie pour l’Informatique, Hanoï-Vietnam, 2005.

[81] Jeffreys, A. J., Wilson, V. & Thein, „Hypervariable ‘minisatellit& regions in human DNA S. L. *Nature* 314, 67—73 (1985)

[82] www. securiteinfocomIconsei1sIbiometrie. Shtml

[83] James Hamilton Doggart, Ohptalmic Medicine, First Edition, London Churchill 1949, AS1N B000L5N9T8

[84] Landt, J. (2005). The history of RFID. *Potentials, IEEE*, *24*(4), 8-11.

[85] Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The evolution of RFID security. *IEEE Pervasive Computing*, *5*(1), 62-69.

[86] Srivastava, B. (2004). Radio frequency ID technology: The next revolution in SCM. *Business Horizons*, *47*(6), 60-68.

[87] Want, R. (2006). An introduction to RFID technology. *Pervasive Computing, IEEE*, *5*(1), 25-33.

[88] Miles, S. B., Sarma, S. E., & Williams, J. R. (Eds.). (2008). *RFID technology and applications* (Vol. 1). Cambridge: Cambridge University Press.

[89] Ilie-Zudor, E., Kemeny, Z., Egri, P., & Monostori, L. (2006). The RFID technology and its current applications. *ISBN*, *963*(86586), 5.

[90] Ahson, S. A., & Ilyas, M. (2008). RFID handbook: applications, technology, security, and privacy. CRC press.

[91] Sarma, S. E., Weis, S. A., & Engels, D. W. (2003). RFID systems and security and privacy implications. In *Cryptographic Hardware and Embedded Systems-CHES 2002* (pp. 454-469). Springer Berlin Heidelberg.

[92] Phillips, T., Karygiannis, T., & Kuhn, R. (2005). Security standards for the RFID market. *Security & Privacy, IEEE*, *3*(6), 85-89.

[93] Rescorla, Eric. SSL and TLS: designing and building secure systems. Vol. 1. Reading: Addison-Wesley, 2001.

[94] Krawczyk, Hugo. "The order of encryption and authentication for protecting communications (or: How secure is SSL?)." Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001.

[95] Doraswamy, Naganand, and Dan Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall Professional, 2003.

[96] "Information technology -- Security techniques -- Authenticated encryption". 19772:2009. ISO/IEC. http://www.iso.org/iso/catalogue_detail.htm?csnumber=46345 Retrieved March 29, 2016.

[97] Ylonen, Tatu, and Chris Lonvick. (2006) "The secure shell (SSH) protocol architecture.".

[98] Bellare, Mihir, and Chanathip Namprempre. (2000)"Authenticated encryption: Relations among notions and analysis of the generic composition paradigm."Advances in Cryptology—ASIACRYPT 2000. Springer Berlin Heidelberg,. 531-545.

[99] Maniccam, S.S., Bourbakis, N.G.: (2004) Image and Video Encryption using Scan Patterns. Pattern Recognition 37, 725–737

[100] Bourbakis, N.: (1997) Image Data Compression Encryption using G-SCAN Patterns. In: Proceedings of IEEE Conference on SMC, Orlando, FL, pp. 1117–1120

[101] H. T. Panduranga and S. K. Naveen Kumar (2012) ' Multiple Image Encryption Using Phase Manipulation and SCAN Methods' Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012), Lecture Notes in Electrical Engineering 222

[102] X. Xue, Q. Zhang, X. Wei, L. Guo, and Q. Wang, (2010) "An image fusion encryption algorithm based on DNA sequence and multi-chaotic maps," Journal of Computational and Theoretical *Nanoscience*, vol. 7, no. 2, pp. 397–403,.

[103] H. Liu, X. Wang, and A. Kadir, (2012)"Image encryption using DNA complementary rule and chaoticmaps," *Applied Soft Computing Journal*, vol. 12, no. 5, pp. 1457–1466,.

[104] Qiang Zhang, Xiaopeng Wei, (December 2013) A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system, Optik - International Journal for Light and Electron Optics, Volume 124, Issue 23, , Pages 6276-6281, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2013.05.009.

[105] RasulEnayatifar, Abdul Hanan Abdullah, Ismail FauziIsnin, (May 2014) Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence, Optics and Lasers in Engineering, Volume 56, , Pages 83-93, ISSN 0143-8166, http://dx.doi.org/10.1016/j.optlaseng.2013.12.003.

[106] Shihua Zhou; Qiang Zhang; Xiaopeng Wei, (2010) "Image Encryption Algorithm Based on DNA Sequences for the Big Image," Multimedia Information Networking and Security (MINES), 2010 International Conference on , vol., no., pp.884,888, 4-6 Nov. 2010doi: 10.1109/MINES.2010.188

[107] M. Amin, O. S. Faragallah, and A. A. Abd El-Latif, (2010) "A chaotic block cipher algorithm for image cryptosystems," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no.11, pp. 3484–3497,.

[108] S.-J. Xu, X.-B. Chen, R. Zhang, Y.-X. Yang, and Y.-C. Guo, (2012) "Animproved chaotic cryptosystem based on circular bit shift andXOR operations," *Physics Letters A*, vol. 376, no. 10-11, pp. 1003–1010,.

[109] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, (2012) "An imageencryption scheme based on quantum logisticmap," *Communicationsin Nonlinear Science and Numerical Simulation*, vol. 17,no. 12, pp. 4653–4661,.

[110] X. Y. Wang and X. M. Bao, (2013) "A novel block cryptosystem basedon the coupled chaotic map lattice," *Nonlinear Dynamics*, vol.72, pp. 707–715,.

[111] G. D. Ye, (2009) “A chaotic image cryptosystem based on toeplitz andhankel matrices,” *Imaging Science Journal*, vol. 57,no. 5, pp. 266–273,.

[112] X.-F. Li, A. C.-S. Leung, X.-J. Liu, X.-P. Han, and Y.-D. Chu, (2010)“Adaptive synchronization of identical chaotic and hyperchaoticsystems with uncertain parameters,” *Nonlinear Analysis.RealWorld Applications*, vol. 11, no. 4, pp. 2215–2223,.

[113] H. Liu and X.Wang, (2011) “Color image encryption using spatial bitlevelpermutation and high-dimension chaotic system,” *OpticsCommunications*, vol. 284, no. 16-17, pp. 3895–3903,.

[114] H.Wang, X.Wang,X.-J. Zhu, andX.-H.Wang, (2012)“Linear feedbackcontroller design method for time-delay chaotic systems,”*Nonlinear Dynamics*, vol. 70, no. 1, pp. 355–362,.

[115] X. Wang and L. Teng, (2012) “An image blocks encryption algorithmbased on spatiotemporal chaos,” *Nonlinear Dynamics*, vol. 67,no. 1, pp. 365–371,.

[116] F. Sun, Z. L¨u, and S. Liu, (2010) “A new cryptosystembased on spatialchaotic system,” *Optics Communications*, vol. 283, no. 10, pp.2066–2073,.

[117] Z. Wang, X. Huang, N. Li, and X. N. Song, (2012) “Image encryptionbased on a delayed fractional-order chaotic logistic system,”*Chinese Physics B*, vol. 21, Article ID 050506,.

[118] X.-y. Wang, F. Chen, and T. Wang, (2010) “A new compound mode ofconfusion and diffusion for block encryption of image basedon chaos,” *Communications in Nonlinear Science and NumericalSimulation*, vol. 15, no. 9, pp. 2479–2485,.

[119] J.He, H. Qian, Y. Zhou, and Z. Li, (2010) “Cryptanalysis and improvementof a block cipher based on multiple chaotic systems,”*Mathematical Problems in Engineering*, vol. 2010, Article ID590590, 14 pages,.

[120] Guoyan Liu, Jie Li, Hongjun Liu, (February 2014) Chaos-based color pathological image encryption scheme using one-time keys, Computers in Biology and Medicine, Volume 45, 1, Pages 111-117, ISSN 0010-4825, http://dx.doi.org/10.1016/j.compbiomed.2013.11.010.

[121] Dinghui Zhang, Fengdeng Zhang, (January 2014) Chaotic encryption and decryption of JPEG image, Optik - International Journal for Light and Electron Optics, Volume 125, Issue 2, , Pages 717-720, ISSN 0030-4026, http://dx.doi.org/10.1016/j.ijleo.2013.07.069.

[122] Paul, A.; Das, N.; Prusty, A.K., (2013)"An advanced gray image encryption scheme by using discrete logarithm with logistic and HEH64 chaotic functions," Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.1114,1120, 22-23 Feb. 2013doi: 10.1109/IAdCC.2013.6514383

[123] G. H. GOLUB AND C. F. VAN LOAN, (1983) Matrix Computations, Johns Hopkins University Press, Baltimore,MD,.

[124] Higham, N., (1986) 'Computing the Polar Decomposition—with pplications' SIAM Journal on Scientific and Statistical Computing 7:4, 1160-1174M

[125] J. F. Yang and C. L. Lu, (1995) "Combined Techniques of Singular Value Decomposition and Vector Quantization for Image Coding," *IEEETransaction on Image Processing, Piscataway, New Jersey, USA*, 4, pp. 1141–1146,.

[126] Dennis S.Benstein and wasinso (August 1993) “Some explicit formulas for the matrix exponential”, IEEE transaction on automatic control, Vol 38, No 8,.

[127] Alan Genz, (1998) Methods for generating Random orthogonal matrices, Proceeding of the MCQMC 98 Meeting.

[128] Oussama, Noui, and Noui Lemnouar. (2014) "A blind robust watermarking scheme based on SVD and circulant matrices." Second International Conference on Computational Science & Engineering (CSE - 2014), pp65-77..

[129] Furht, Borko, and DarkoKirovski. (2006) Multimedia encryption and authentication techniques and applications. CRC Press,.

[130] Norouzi Benyamin, MirzakuchakiSattar, SeyedzadehSeyedMohammad, MosaviMohammadReza (2012)'A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process' Multimedia Tools and Applications DOI 10.1007/s11042-012-1292-9

[131] Zhu C (2012) A novel image encryption scheme based on improved hyperchaotic sequences. J Opt Commun 285:29–37

[132] Zhu ZL, Zhang W, Wong KW, Yu H (2011) A chaos-based symmetric image encryption scheme using a Bit-level permutation. J Inform Sci 181:1171–1186 .

[133] Gao T, Chen Z (2008) A New image encryption algorithm based on hyper-chaos. J PhysLett A 372:394–400

[134] Gao T, Chen Z (2008) Image encryption based on a new total shuffling algorithm. J Chaos SolitonsFractals 38:213–220

[135] Wang, Bin, Xiaopeng Wei, and Qiang Zhang. (2013) "Cryptanalysis of an image cryptosystem based on logistic map." Optik-International Journal for Light and Electron Optics 124.14: 1773-1776.

[136] Surekha, B., and G. N. Swamy. (2011)"A spatial domain public image watermarking." International Journal of Security and Its Applications 5.1: 12.

[137] Nasir, Ibrahim, Ying Weng, and Jianmin Jiang. (2007) "A new robust watermarking scheme for color image in spatial domain." Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. Third International IEEE Conference on. IEEE,.

[138] Mukherjee, Dipti Prasad, SubhamoyMaitra, and Scott T. Acton. (2004)"Spatial domain digital watermarking of multimedia objects for buyer authentication." Multimedia, IEEE Transactions on 6.1: 1-15.

[139] Wang, Feng-Hsing, Lakhmi C. Jain, and Jeng-Shyang Pan. (2004) "Genetic watermarking on spatial domain." Intelligent Watermarking Techniques 7: 377.

[140] Chandra, DV Satish. (2002)"Digital image watermarking using singular value decomposition." Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on. Vol. 3. IEEE,..

[141] Chang, Chin-Chen, Piyu Tsai, and Chia-Chen Lin. (2005) "SVD-based digital image watermarking scheme." Pattern Recognition Letters 26.10: 1577-1586.

[142] Al-Haj, Ali. (2007) "Combined DWT-DCT digital image watermarking." Journal of computer science 3.9: 740.

[143] W. H. Lin, Y. R. Wang, and S. J. Horng, (2008)"A Blind Watermarking Scheme Based on Wavelet Tree Quantization," The Second International Conference on Secure System Integration and Reliability Improvement, , pp. 89-94

[144] Ghouti, Lahouari, et al. (2006) "Digital image watermarking using balanced multiwavelets." Signal Processing, IEEE Transactions on 54.4: 1519-1536.

[145] Zheng, Dong, Jiying Zhao, and Abdulmotaleb El Saddik. (2003) "RST-invariant digital image watermarking based on log-polar mapping and phase correlation." Circuits and Systems for Video Technology, IEEE Transactions on 13.8: 753-765. . .

[146] Ouhsain, Mohamed, and A. Ben Hamza. (2009) "Image watermarking scheme using nonnegative matrix factorization and wavelet transform." Expert Systems with Applications 36.2: 2123-2129.

[147] Oussama Noui and Lemnouar Noui, (2014) 'Blind Watermarking Scheme for Image Authentication' ,3ème édition de la conférence JEESI'14. Ecole superieur d'informatique ESI.

[148] R. Liu and T. Tan, (2002) "A SVD-based watermarking scheme for protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121-128,.

[149] E. Ganic and A. M. Eskicioglu, (2004) "Robust DWT-SVD domain image watermarking: embedding data in all frequencies," ACM Multimedia and Security Workshop 2004, Germany, , pp. 20-21.

[150] C.H. Lin, J.C. Liu, and P.C. Han, (2008) "On the security of the full-band image watermark for copyright protection," IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, , pp. 74-79.

[151] Mukherjee, Soumya, and Arup Kumar Pal. (2012) "A DCT-SVD based robust watermarking scheme for grayscale image." In Proceedings of the International Conference on Advances in Computing, Communications and Informatics, pp. 573-578. ACM,.

[152] Yang, Jar-Ferr, and Chiou-Liang Lu. (1995) "Combined techniques of singular value decomposition and vector quantization for image coding." Image Processing, IEEE Transactions on 4, no. 8: 1141-1146.

[153] Bhatia, Rajendra. (2009) Positive definite matrices. Princeton University Press,.

[154] Craver, Scott, Nasir Memon, Boon-Lock Yeo, and Minerva M. Yeung. (1998)"Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications." Selected Areas in Communications, IEEE Journal on 16, no. 4: 573-586..

[155] Lai, Chih-Chin, and Cheng-Chih Tsai. (2010) "Digital image watermarking using discrete wavelet transform and singular value decomposition." Instrumentation and Measurement, IEEE Transactions on 59, no. 11: 3060-3063.

[156] Tsai, Hung-Hsu, Yu-JieJhuang, and Yen-Shou Lai. (2012) "An SVD-based image watermarking in wavelet domain using SVR and PSO." Applied Soft Computing 12, no. 8: 2442-2453.

[157] Ali, Musrrat, and Chang WookAhn. "An optimized watermarking technique employing SVD in DWT domain." In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, p. 86. ACM, 2013.

[158] Rastegar, Saeed, FatemeNamazi, KhashayarYaghmaie, and Amir Aliabadian. "Hybrid watermarking algorithm based on Singular Value Decomposition and Radon transform." AEU-International Journal of Electronics and Communications 65, no. 7 (2011): 658-663.

[159] Makbol, Nasrin M., and Bee EeKhoo. (2013) "Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition." AEU-International Journal of Electronics and Communications 67, no. 2: 102-112.

[160] Oussama Noui and Lemnouar Noui , (2014), "a robust blind and secure watermarking scheme using positive semi definite Matrices", International Journal of Computer Science & Information Technology (IJCSIT) Vol 6, No 5, October 2014, pp 97-110

[161] Liu Xin; Lv Xiaoqi; Wang Ying, (May 2008) "A Semi-Fragile Digital Watermarking Algorithm Based on Integer Wavelet Matrix Norm Quantization for Medical Images," Bioinformatics and Biomedical Engineering, 2008. ICBBE 2008. The 2nd International Conference on , vol., no., pp.776,779, 16-18

[162] Chune Zhang; Cheng, L. L.; Zhengding Qiu; Cheng, L.M., (2008) "Multipurpose Watermarking Based on Multiscale Curvelet Transform," Information Forensics and Security, IEEE Transactions on , vol.3, no.4, pp.611,619, Dec. 2008. doi: 10.1109/TIFS.2008.2004288.

[163] Ching-Yung Lin and Shih-Fu Chang (2000) "Semifragile watermarking for authenticating JPEG visual content", Proc. SPIE 3971, Security and Watermarking of Multimedia Contents II, 140 (May 9, 2000); doi:10.1117/12.384968;

[164] Haohao Song; Zihua Qiu; Jian Gu, (2010) "A novel semi-fragile image watermarking scheme based on wavelet," Audio Language and Image Processing (ICALIP), International Conference on , vol., no., pp.1504,1510, 23-25 Nov. 2010,

[165] Shi, Jianping, and Zhengjun Zhai. "Curvelet transform for image authentication. (2006)" In Rough Sets and Knowledge Technology, pp. 659-664. Springer Berlin Heidelberg,. ISBN 978-3-540-36299-9

[166] Palma Hernandez, C.; Torres-Huitzi, C., (2011) "A fragile watermarking scheme for image authentication in mobile devices," *Electrical Engineering Computing Science and Automatic Control (CCE), 2011 8th International Conference on* , vol., no., pp.1,6, 26-28 doi: 10.1109/ICEEE.2011.6106601.

[167] helvie Nidya Neyman, Benhard Sitohang, Sobar Sutisna, Shelvie Nidya Neyman, Benhard Sitohang, Sobar Sutisna, (2013) Reversible Fragile Watermarking based on Difference Expansion Using Manhattan Distances for 2D Vector Map, Procedia Technology, Volume 11, 2013, Pages 614-620, ISSN 2212-0173, doi:10.1016/j.protcy.2013.12.236

[168] Di Xiao, Frank Y. Shih, (2012) An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing, Optics Communications, Volume 285, Issues 10–11, 15 May 2012, Pages 2596-2606, ISSN 0030-4018.

[169] Jassim, T.; Abd-alhameed, R.; Al-Ahmad, H., (2013) "A new robust and fragile watermarking scheme for images captured by mobile phone cameras," Communications, Signal Processing, and their Applications (ICCSPA), 2013 1st International Conference on , vol., no., pp.1,5, 12-14 Feb.

[170] Jar Ferr Yang; Chiou-Liang Lu, (Aug 1995) "Combined techniques of singular value decomposition and vector quantization for image coding," Image Processing, IEEE Transactions on , vol.4, no.8, pp.1141,1146,

[171] Yue Liu; Ju Yang; Mingjun Liu, (2008) "Recognition of QR Code with mobile phones," Control and Decision Conference, 2008. CCDC 2008. Chinese , vol., no., pp.203,206, 2-4

[172] Vongpradhip, S.; Rungraungsilp, S., (2012)"QR code using invisible watermarking in frequency domain," *ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2011 9th International Conference on* , vol., no., pp.47,52, 12-13

[173] "QR Code Essentials". Denso ADC. 2011. Retrieved 20 September 2014 , http://www.nacs.org/LinkClick.aspx?fileticket=D1FpVAvvJuo%3D&tabid=1426&mid=4802

[174] Musrrat Ali and Chang Wook Ahn. (2013). An optimized watermarking technique employing SVD in DWT domain. In *Proceedings of the 7th International Conference on*

Ubiquitous Information Management and Communication (ICUIMC '13). ACM, New York, NY, USA, , Article 86 , 7 page.

[175] Ghaderi, K.; Akhlaghian, F.; Moradi, P., (2013)"A new robust semi-blind digital image watermarking approach based on LWT-SVD and fractal images," *Electrical Engineering (ICEE), 2013 21st Iranian Conference on* , vol., no., pp.1,5, 14-16 May 2013
doi: 10.1109/IranianCEE.2013.6599633

[176] Soumya Mukherjee and Arup Kumar Pal. (2012). A DCT-SVD based robust watermarking scheme for grayscale image. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (ICACCI '12). ACM, New York, NY, USA, 573-578.

[177] Nasrin M. Makbol, Bee Ee Khoo, (2013) Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition, AEU - International Journal of Electronics and Communications, Volume 67, Issue 2, February 2013, Pages 102-112, ISSN 1434-8411

[178] Chinmayee Das, Swetalina Panigrahi, Vijay K. Sharma, K.K. Mahapatra, (2013) A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation, AEU - International Journal of Electronics and Communications, Available online 3 September 2013, ISSN 1434-8411, http://dx.doi.org/10.1016/j.aeue.2013.08.018.

[179] **S.** Craver, N. Memon, **B.** L and M. M Yeung (1998) “Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, andimplications,” BEE Journal on Selected Areas in Communications, Vol. 16 Issue: 4 , May 1998, pp. 573 - 586.

[180] L.Qiao and K.Nahrstedt. (1998) "Watermarking Schemes and protocolos for protecting ownerships and customer's rights. *Journal of visual Communication and image representation*, 9(3):194-210,

[181] Wenjun Zeng and B. Liu, (1999)“A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images”1mage Processing, IEEE Transactions on , Volume: 8 no. 11.

[182] Lagzian, S., Soryani, M., & Fathy, M. (2011). A new robust watermarking scheme based on RDWT-SVD. International Journal of Intelligent Information Processing, 2(1), 22-29.

[183] Bhatnagar, G., & Raman, B. (2009). A new robust reference watermarking scheme based on DWT-SVD. Computer Standards & Interfaces, 31(5), 1002-1013

[184] Lai, C. C. (2011). A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. Digital Signal Processing, 21(4), 522-527.

[185] Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. Multimedia, IEEE Transactions on, 4(1), 121-128.

[186] Lai, C. C., Huang, H. C., & Tsai, C. C. (2008, August). Image watermarking scheme using singular value decomposition and micro-genetic algorithm. In Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on (pp. 469-472). IEEE.