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

Thèse

En vue de l'obtention du diplôme de

Doctorat en Informatique

Partage de Secret en Utilisant des Métaheuristiques Bionispirées

Présentée Par

ZENDER Rouia

Soutenue le : 04/07/2024

Membres du jury :

Président :	Bilami Azeddine	Professeur	Université de Batna 2
Encadreur :	Noui Lemnouar	Professeur	Université de Batna 2
Co-encadreur	Abdessemed Mohamed Ridha	MCA	Université de Batna 2
Examinateurs :	Seghir Rachid	Professeur	Université de Batna 2
	Melkemi Lamine	Professeur	Université de Batna 1

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

Secret Sharing Scheme based on Bioinspired Metaheuristics

Presented by:

ZENDER Rouia

04/07/2024

Members of the jury:

President:	Bilami Azeddine	Professor	University of Batna 2
Supervisor:	Noui Lemnouar	Professor	University of Batna 2
Co-Supervisor:	Abdessemed Mohamed Ridha	MCA	Université de Batna 2
Examinators:	Seghir Rachid	Professor	University of Batna 2
	MelkemiLamine	Professor	University of Batna 1

Acknowledgements

I would like to express my sincere gratefulness to my supervisor, Prof. Noui Lemnouar, Professor at the Mathematics Department of the University of Batna for his continuous encouragements and suggestions that led to this thesis, during many years. This thesis would not have been accomplished without his invaluable support.

I also show all my appreciation to Prof. Bilami Azeddine, Professor at the Computer Science Department of the University of Batna 2, for the honour that he makes to preside this jury.

I sincerely thank Prof. Seghir Rachid Professor at the Computer Science Department of the University of Batna 2, for accepting to judge this work and to be part of my thesis jury.

I also show all my appreciation and gratitude to Prof. Melkemi Lamine, Professor at the University of Batna 1, for accepting to judge this work and to be part of my thesis jury.

I sincerely thank Dr. Abdessemed Mohamed Ridha, MCA at the University of Batna 2, for cooperating with me during this research.

Finally, it is my pleasure to thank my parents, sister and my husband for supporting me for my education.And they have given me the support and comfort that accompanied me during this path.

Abstract

Technology has progressed a lot in recent decades, especially in terms of computing power and will probably continue to do so in the future, Moore's law is there to support it. This had disastrous repercussions on the information security; although cryptography has also evolved a lot in terms of encryption algorithms, recent supercomputers are capable of overcoming some cryptosystems. This has led researchers in this field to investigate new avenues, such as secret sharing, which over time has proven to be the most secure solution currently used for protecting its secret.

The main axis around which revolves the subject of this thesis is precisely this secret sharing paradigm, requiring cooperation and collaboration on the part of secret keepers based on distributed trust and jointly managed control of the security situation.During these last years, various sharing algorithms have been proposed. Indeed, security in the field of IT in general and computer systems in particular have contributed a lot in the evolution of this discipline which belongs to cryptography and which is based on strong theoretical pillars such as: modular arithmetic and coding theory.

Contribution in this research work consists of the proposal of a new secret sharing scheme based on bioinspired hexagonal structure and integer decomposition. As a metaheuristic inspiration, hexagonal structure was inspired from nature where it’s common in constructs made by biological systems and the intelligent behaviours of a bee swarm.

For integer decomposition, it is known that the oldest method is Fermat’s factorization, which is based on the representation of an odd integer as the difference of two squares, while for the proposed decomposition every positive integer has a unique factorization into two factors.

To check functionality and efficiency of the proposed scheme, it was applied to digital images processing domain where it has exhibited good properties: it is lossless and ideal, its flexibility allows many extensions to handle additional situations, it can add new or delete an old participant and it can detect and identify cheater. Aside these interesting features, experimental results demonstrate that this scheme has a good security level.

Keywords

Secret Sharing Scheme, Quasi-Square Decomposition, Bioinspired Metaheuristic, isoperimetry.

Résumé

La technologie a beaucoup progressé ces dernières années, notamment en termes de puissance de calcul et continuera probablement à le faire dans le futur, la loi de Moore est là pour le soutenir. Cela a eu des répercussions désastreuses sur la sécurité de l'information ; bien que la cryptographie ait aussi beaucoup évolué en termes d'algorithmes de chiffrement, les supercalculateurs récents sont capables de parvenir à bout de certains cryptosystèmes. Cela a conduit les chercheurs dans ce domaine à explorer de nouvelles pistes, telles que le partage de secret, qui au fil du temps s'est avéré être la solution la plus sécurisée actuellement utilisée pour protéger son secret.L'axe principal autour duquel s'appuie le sujet de cette thèse est précisément ce paradigme de partage du secret, nécessitant une coopération et une collaboration de la part des gardiens du secret basée sur la confiance distribuée et le contrôle collectif de la situation sécuritaire. Au cours de ces dernières années, divers algorithmes de partage ont été proposés. En effet, la sécurité dans le domaine de l'informatique en général et des systèmes informatiques en particulier a beaucoup contribué à l'évolution de cette discipline qui appartient à la cryptographie et qui repose sur de solides piliers théoriques tels que : l'arithmétique modulaire et la théorie du codage.

La contribution à ce travail de recherche consiste en la proposition d'un nouveau schéma de partage secret basé sur la structure hexagonale bioinspirée et la décomposition entière. En tant qu'inspiration métaheuristique, la structure hexagonale a été inspirée de la nature où elle est courante dans les constructions faites par des systèmes biologiques et le comportement intelligent d'un essaim d'abeilles.Pour la décomposition d'entiers, on sait que la méthode la plus ancienne est la factorisation de Fermat, qui est basée sur la représentation d'un entier impair comme la différence de deux carrés, tandis que pour la décomposition proposée, tout entier positif a une factorisation unique en deux facteurs.

Pour vérifier la fonctionnalité et l'efficacité du schéma proposé, il a été appliqué au domaine de traitement d'images numériques où il a présenté de bonnes propriétés : il est sans perte et idéal, sa flexibilité permet à de nombreuses extensions de gérer des situations supplémentaires, il peut ajouter un nouveau ou supprimer un ancien participant et il peut détecter et identifier le tricheur. Outre ces caractéristiques intéressantes, les résultats expérimentaux démontrent que ce système a un bon niveau de sécurité.

Mots-clés

Schéma de partage de secret, décomposition quasi-carrée, métaheuristique bio-inspirée, isopérimétrie.

ملخص البحث

لقد تقدمت التكنولوجيا كثيرا في العقود الأخيرة، خاصة فيما يتعلق بقوة الحوسبة ومن المحتمل أن تستمر في القيام بذلك في المستقبل، قانون مور موجود لدعمها. كان لهذا تداعيات كارثية على أمن المعلومات. على الرغم من أن التشفير قد تطور أيضا كثيرا من حيث خوارزميات التشفير، إلا أن أجهزة الكمبيوتر العملاقة الحديثة قادرة على التغلب على بعض أنظمة التشفير. وقد دفع هذا الباحثين في هذا المجال إلى البحث عن طرق جديدة، مثل مشاركة السرية، والتي أثبتت بمرور الوقت أنها الحل الأكثر أمانا المستخدم حاليا لحماية سرها.

المحور الرئيسي الذي يدور حوله موضوع هذه الأطروحة هو بالضبط نموذج المشاركة السرية هذا، والذي يتطلب التعاون والتآزر من جانب حفظة السر على أساس الثقة الموزعة والسيطرة المدارة بشكل مشترك على الوضع الأمني. خلال هذه السنوات الأخيرة، تم اقتراح خوارزميات مشاركة مختلفة. والواقع أن الأمن في مجال تكنولوجيا المعلومات بشكل عام وأنظمة الكمبيوتر بشكل خاص قد ساهم كثيرا في تطور هذا التخصص الذي ينتمي إلى التشفير والذي يقوم على ركائز نظرية قوية مثل: الحساب المعياري ونظرية الترميز.

تتكون المساهمةفي هذا العمل البحثي من اقتراح مخطط مشاركة سري جديد يعتمد على بنية سداسية مستوحاة بيولوجيا وتحلل عددصحيح . كمصدر إلهام للطرق الكشفية ،تم استلهام البنية السداسية من لطبيعة حيث أنها شائعة في التركيبات التي تصنعها الأنظمة البيولوجية والسلوك الذكي لسرب النحل.

بالنسبة للتحلل الصحيح، من المعروف أن أقدم طريقة هي تحليل ،Fermat والذي يعتمد على تمثيل عدد صحيح فردي كفرق بين مربعين، بينما بالنسبة للتحلل المقترح، يحتوي كل عدد صحيح موجب على عامل واحد في عاملين.

للتحقق من وظائف وفعالية المخطط المقترح، تم تطبيقه على مجال معالجة الصور الرقمية حيث أظهر خصائص جيدة: إنه سريع ومثالي، ومرونته تسمح للعديد من الامتدادات بالتعامل مع مواقف إضافية، ويمكن إضافة مشارك جديد أو إزالة مشارك قديم كما يمكن اكتشاف كل مشارك غشاش وتحديده. بالإضافة إلى هذه الميزات المثيرة للاهتمام، تظهر النتائج التجريبية أن هذا النظام يتمتع بمستوى جيد من الأمان.

كلمات مفتاحيه

مخطط المشاركة السرية، التحليل شبه المربع، الاستدلالات المستوحاة من البيولوجيا الحيوية، قياس النظائر.

Publications

R. Zender, L. Noui, M.R Abdessemed, “A Secret Sharing Scheme based on Integer Decomposition and Hexagonal Structure”, Inderscience Journal IJICT.Vol. 24, No. 4, 2024

Abbreviations and Acronyms

–AI: Artificial Intelegens

–IT: Information Technology

–SSL: Secure Socket Layers

–RSA: Rivest Shamir Adleman cryptosystem

–DES: Data Encryption Standard

–SSS: Secret Sharing Scheme

–CC: Cloud Computing

–IoT: Internet of Things

–MPC: Multy Party C omputation

–TSS: Threshold Signature scheme

–CDMB: Global Dogma of Molecular Biology

–HVS: Human Visual System

–GA: Genetic Alogorithm

–Γ : Access Structure

–D: Dealer

–TS: Trusted Center

–C: Combiner

–$\bar{\Gamma}$: adversary structure or unauthorized groups

–A : qualified subsets or authorized groups

–Class P : class Polynomial

–Class NP: Non-deterministic in Polynomial time

–GFq:

–VSS: verifiable secret sharing schemes

–PSS : Proactive secret sharing

–SSRS : Secure Secret Reconstruction Scheme with verifiable shares

–DNSSEC: Human-memorable Internet domains

–ICANN: Internet Corporation for Assigned Names and Numbers

–SA: Swarm Algorithms

–EA: Evolutionary Algorithm

–EC: Evolutionary Computing

–ACO: Colony Optimization

−**ABC:** Artificial Bee Colony

−**PSO**: Particle Swarm Optimization

−**SI:** Swarm Intelligence

−**QSD:**Quasi Square Decomposition

−**LFSR:** Linear feedback shift Register

−**E**: Encryption function

Table of contents

List of figures

List of Tables

General Introduction

In the virtual world, data protection is the main mission of a security manager; Given the complexity of performing a security mission, data encryption(cryptography) is the fundamental tool of computer security. Indeed, the implementation of cryptography allows Many researchers to realize it in different ways, using mathematical or cryptographic tools, in a generic context of dealing with security-related risk problems, such as: authentication, integrity and confidentiality. In reality, protecting the electronic data includes, among other things, the control of the environment against the target of malicious acts (theft of smart materials, data, hostage of computer resources) or illegal action (blackmail, embezzlement, money laundering, deny of service).

In addition, the concept of security recursion has been well defined as the fact that security solutions such as: the password, the private key, also need to be protected and secured so that beings can offer a certain level of security.

From this effect; the original motivation for the "secret sharing", is to protect data against loss or theft. Generally, sharing cryptography deals with situations where the authority of possession of security infrastructures is distributed between certain shareholders, in order to distribute the role of the authority a set of entities in a cooperative mission.

Unfortunately, the approaches applied today to solve the secret sharing problem only prove effective for small sizes of this problem; the sharing schemes used lead to an exponential increase in the amount of data that each participant needs to hold. This classifies the NP-complet secret sharing problem. A secret sharing scheme based on hexagonal structure and integer decomposition comes for this purpose, to try not only to solve this secret sharing problem in innovative ways but also to increase the size of the problem to be solved. It also opens up new perspectives for proposing adaptive secret sharing schemes;

In the other side, traditional optimization techniques have proven effective for small problems. However, for large real-world problems, traditional methods either do not scale, provide suboptimal solutions, or provide long-term solutions. Even previous

artificial intelligence-based techniques used to solve these problems have failed to produce acceptable results. However, last two decades have seen many new methods in AI based on the characteristics and behaviours of the living organisms in the nature which are categorized as bioinspired or nature inspired optimization algorithms. These techniques, also known as metaheuristic optimization techniques, which have been theoretically tested and implemented using simulations and have been used to create many useful applications. Because they are easy to understand, flexible, and adaptable to problems, they have been widely used to solve many complex industrial and engineering problems. In this topic, we will present new bioinspired metaheuristic,

This thesis presents two main contributions related to secret sharing schemes. In this thesis we focus on two concepts: Firstly,the use of hexagonal structure which is common in biological modelling;and secondly, a new integer decomposition, it is known that the oldest method is Fermat's factorization, which is based on the representation of an odd integer as the difference of two squares, while for our proposed decomposition every positive integer has a unique factorization into two factors. As well, in order to apply a symmetric encryption to greyscale bitmap image, we suggest the use Vendermond matrix generation method instead of encryption by the Hill Cipher.

Our thesis is divided into two parts, the first part presents an introduction to the research domain, starting by an overview on computer security and cryptography, we focus on a state of the art about the secret sharing scheme and its applications; then, we present an overview on the metaheuristic and bioinspired modelling, we ended by the mathematical tools, and the second part shows our major contributions.

The first chapter, provides introduction to computer security and cryptography algorithms with some useful concepts on digital image.

In the second chapter we present the topic of secret sharing scheme, with general model for secret sharing schemes,the basics techniques, complexity measures, classification and properties, and the proposed schemes with extended capabilities and applications.

The third chapter was on bioinspired metaheuristic and hexagonal biological modelling

The fourth chapter of this thesis explains the tools and methods of our contributions, we present the mathematical tools such as the isoperimetric problem, and presentation of the matrix key generation used for image encryption.

The contribution was presented in **chapter five**, and it is about a novel secret sharing scheme based the bioinspired hexagonal modelling inspired from the beehive form, and a novel approach of factorization we called it **Quasi Square Decomposition**, in the same chapter, we have presented a novel effective algorithm for producing a secret sharing scheme for image, using a new type of orthogonal matrix from a random vector, which has many applications in cryptography. We also show the experimental results, analysis and discussion, and we winded up our thesis by general conclusion.

Chapter 1.Overview on Domain of Researches

1.1Introduction

Computer security is important because it keeps your information and data safe. It could be your business, health or personal data. We talk in this chapter about Computer security which provides properties such as availability, integrity, and confidentiality to computer systems. Computer security is considered important for protecting personal information, also Company Properties, To Prevent data theft; To protect from unauthorized Access. In general, the implementation of a cryptographic system makes it possible to carry out services of **confidentiality**, **authentatio**n and verification of the **integrity** of data.This chapter provides also an introduction to digital images. In this chapter we will talk about some concepts about the image and its different types.

1.2Computer security

1.2.1Computer Security issues

With the wide application of network technology, the development of electronic communication, e-mail, electronic payment, automatic retail business, etc., various computing and communication systems have become an important part of the human living environment, they collect, analyse, store, display and disseminate information in multimedia formats, and as independent products or combined with other physical products. People should be concerned about their own information security issues human political, economic, military and cultural services. Most of modern social work data is transmitted at high speed by computer as a carrier, whether it is personal or corporate data, there is a danger of being hacked and deciphered, resulting in different degrees of loss, as shown in (Figure 1). In this context, how to use all kinds of information safely and effectively has become an important cornerstone to ensure the development of human society; How to ensure that information is not illegally stolen, eavesdropped, forged and tampered with during the transmission and processing of information on the public network, that is, the issue of information authentication and confidentiality, which has become a problem that people are concerned about.

Computer security is essentially the protection of computer systems and information from damage, theft and unauthorized uses; The concept of information systems security covers a set of methods, techniques and tools responsible for protecting the resources of an information system.

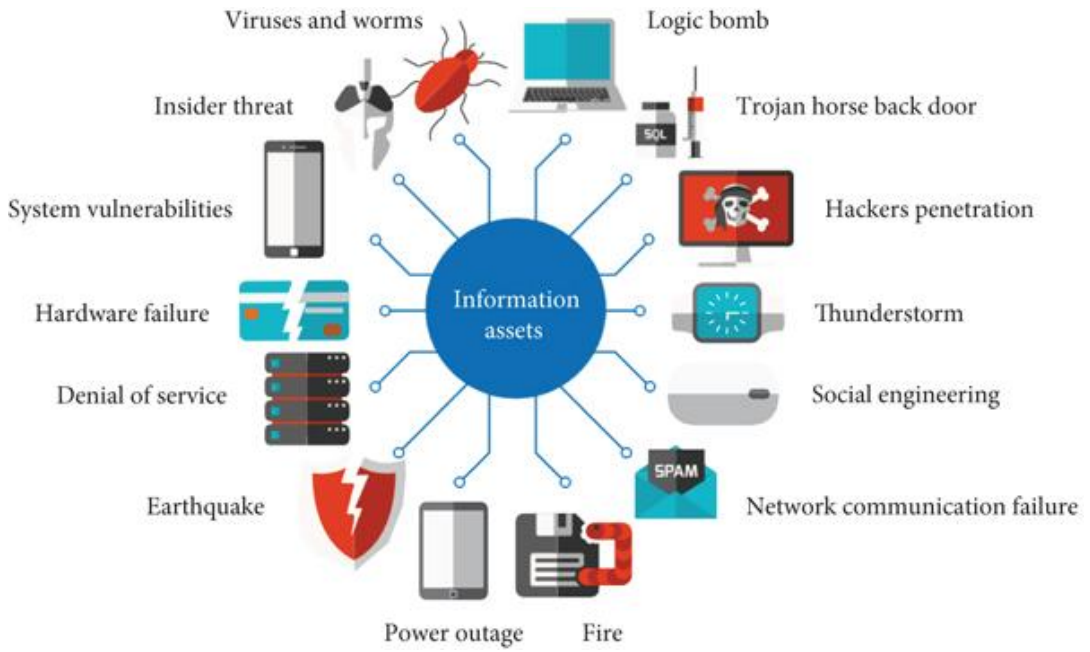

Figure 1 Computer security issues

1.2.2 Computer Security Measures

The concept of information systems security covers a set of methods, techniques and tools responsible for protecting the resources of an information system.The role of computer security is to reduce the risk to an acceptable level in a given context, and depends on the importance given by managers to the assets to be protected and the painful risks. Computer security must be understood in a comprehensive way. It goes through the definition of measures and the security policy, the motivation and the control of the risks, then the implementation of measures, as well as the optimization of appropriate security techniques and means. In addition, several techniques (conventional cryptography, firewalls, intrusion detection system and biometric devices) make it possible to provide a particular response to a specific security problem [1][2].

Measuring the security of a system should quantify the intuitive concept of "the ability of the system to resist attacks" [3]. That is, it should be operational and reflect the degree to which the system can be expected to remain non-destructive under specific operating conditions, including attacks.These are classification criteria of security measures:

-**Confidentiality:** Confidentiality ensures that only authorized users have access to information. We must protect our confidential information. An organization must guard against malicious actions that endanger the confidentiality of its information.

-**Authentication:** Is to guarantee the identity of a given entity or the origin of a communication or document. i.e. authentication of the origin of the data: it is used to prove that the data received has indeed been issued by the declared sender. In this case, authentication often designates the combination of two services: authentication and integrity in off-line mode. These two services have no sense separately and are often provided together.

-**Integrity:** Integrity ensures that an electronic message or document has not been tampered with, i.e, it has not been maliciously modified during transfer or storage; Integrity means that changes should be made only by authorized entities using authorized mechanisms.

-**Non repudiation:** Is to protect against the contention of sending or receiving a message or an electronic document during a transaction. In other words, it is ensure that neither the sender nor the receiver of a message be able to deny the transmission.

-**Access control:** Requires that access to information resources may be controlled by or the target system.

-**Availability:** Requires that computer system assets be available to authorized parties when needed.

1.2.3 Possible attacks and threats

Ensuring security should and must become the responsibility of each system administrator.When we trying to improve security of information systems,we generally used six categories of security procedures including: general security policies and

procedures software, virus protection, digital signatures, encryption, firewalls and proxy servers.

The destruction of resources, theft of resources, theft of services, refusal of service, and corruption of data and applications; These are Security threats or intentional attacks

Security threats and attacks on information systems most often increase from the following sources: malicious user, hackers, terrorists, and computer viruses.The most common steps in the attack are as follows:

- Testing and Assessment,
- Exploitation and penetration,
-Increased privileges,
-Maintenance of access,

We can classify the different consequences of threat and attack and the most common are:

1.2.3.1Threats related to issues not specific to IT

-Accidental material risks: for this, the protection techniques are fairly well mastered (fire, explosion, flood, storm, lightning).

-Theft and sabotage of hardware: Theft of hardware equipment, destruction of equipment, destruction of backup media.

-Other risks: Anything that can lead to financial losses in a company. Losses more associated with the organization, the management of personnel (departure of strategic personnel, strikes, . . . etc).

1.2.3.2Failures and errors (unintentional)

-Hardware failures/malfunctions.

-Basic software failures/malfunctions.

-Operating errors (forgetting to save, overwriting files),

-Application design errors.

-Information manipulation errors (entry error, transmission error, user error)

1.2.3.3Intentional threats

Which are the set of malicious actions (which constitute the biggest part of the risk) which should be the main object of the protective measures. Among the objectives of the attacks:

-Misinform;

-Prevent access to a resource;

-Take control of a resource;

-Retrieve information present on the system.

-Use the compromised system to bounce back.

-Establish a network of "botnet" (or network of zombie machines).

An intentional threat is called an attack; There are several kinds of attacks but,generally, all attacks can be classified into four categories:

A.Cutting or breaking: This type of attack interrupts the flow of information in the system. This is a direct or active attack.

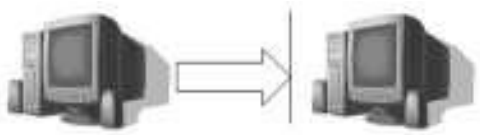

Figure 2 Cutting or interruption of information flow

B.Interception: This type of attack is generally unseen, and unlike the previous, active attacks, it is a passive attack. In this kind of attack the person trying to collect information or to perform monitoring of current performance.

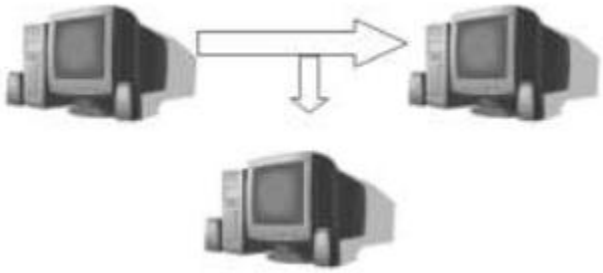

Figure 3 Interception of information

C.Changes of information: This kind of attack is classified into the category of active attacks, because it affects the integrity. And caused may be a changing of the data or the whole system.

Figure 4 Changes of information flow

D.Fabrication: This kind of attack is also an active attack, it affect the authenticity. This kind of attack is used for faking data, traffic, etc…

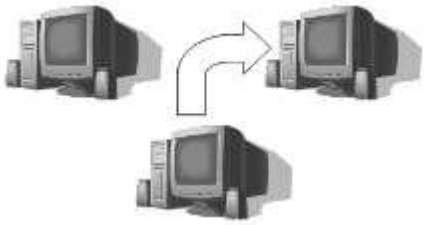

Figure 5 information Fabrication

1.2.4The Basic Steps of the security

One of the specified condition of security, is that its maintenance of the level of acceptable risk. The risk is the result of accumulation of threats and weaknesses of the consequences, and possible threats that can come from outside. We can not say with certainty that a system is fully protected, there is no absolute security. When the protection system had necessary to accept some level of risk and the possibility a certain loss, i.e. reasonable level of risk. Each process is in a dynamic state, so the safety can be implemented using several different products and services, procedures and rules. However, the very products and services, procedures and rules are not sufficient in themselves. Need a proper and timely training of authorized persons in charge of the protection system.

Security is based on four basic steps as follows:

-**Evaluation:** measure the possible risks and predictions for their exclusion;

-**Protection:** prevent potential attacks in order to reduce the possibility of compromising the system;

-**Discovery**: the process of identifying the attack,

-**Answer :**the safe recovery with the possibility of further work or restoration of the system itself.

1.2.5 Objectif of computer security

The digital revolution in communications and information has opened up many fields of investigation for cryptography, to the point where it has invaded our daily lives: smart cards, banking transactions, the Internet, mobile phones, etc.

Let's start by looking at the security services, that cryptography can guarantee and its applications in "real" life.

It is well known that the security of a security system is measured by its weakness. In general, the strength of a computer security system is not the cryptographic system but, for example, its computer implementation.

Cryptography contributes to computer security by providing primitives that achieve the objectives of authentication, confidentiality and integrity protection. Beyond this trilogy, cryptography also provides answers to the problems of service availability and fault resistance on certain cryptographic protocols. This last security objective is at the subject of the next section

1.3 Cryptography

1.3.1 Introduction and History

Cryptography was an art before being a security policy. From its first uses by the Egyptians, around 4000 years ago, until the 20th century, when it played a crucial role in both world wars[4].

Cryptography was, until the 1950s, almost reserved for the military, diplomatic and governmental sectors (it was a means of protecting national secrets). The proliferation of

computing and communication systems around the 2000s caused the civilian sector to seek security services to protect their digital information[5].

Cryptography is a process of keeping information secret and safe simply by converting it into unintelligible information; It is all about math functions and can be applied in technical solutions for increasing high level of security.

1.3.2 Cryptography Services and Mechanisms

- **-Cryptology:** Is an ancient science "science of the secret". Its purpose is the design and analysis of mathematical methods for hiding information, it has two distinct but closely related branches: cryptography and cryptanalysis.
- **-Cryptography:** Which offers solutions aimed at ensuring secrecy. The traditional concept of cryptography is encryption. It is the operation by which a message is encrypted. Indeed, encrypting or coding information makes it incomprehensible in the absence of a particular decoder.
- **-Cryptanalysis:** Is the science or art of studying ciphers, cipher-texts or cryptographic systems using mathematical techniques, in order to find weaknesses that will allow recovery of the plain-text from the cipher-text, without necessarily knowing the encryption key**.**
- **-Steganography :** A plain-text message may be hidden in any one of the two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.

1.3.3 Objectif of Cryptography

The historical and main objective of cryptography, is to allow two people to communicate through an insecure channel, in such a way, that an opponent who has access to the information circulating on the communication channel, cannot understand what is exchange. In addition, the communications exchanged between these two entities, are matter to a certain number of threats. Cryptography provides powerful functionalities to moderate these threats. On the one hand: availability, integrity and confidentiality, when the

two entities had mutual trust so it remains to protect themselves from an intruder, On the other hand: confirming the veracity, the authenticity of an action or entity and the existence of an action (Non-repudiated Transfer of Information) [6][4].

1.3.4Cryptography applications

Cryptography is used today in many applications: in mobile phones, on the Internet or for pay-TV. In the case of mobile phones, cryptography is used to ensure the confidentiality of communications. Indeed, the law on telecommunications obliges the operators to guarantee the security of the communications of the users. In particular, in the case of mobile telephones, the communications between the telephone and the radio station are encrypted; On the Internet, cryptography used to guarantee the confidentiality of certain communications, such as, the transmission of the code of a credit card, or to ensure the confidentiality. Browsers, such as Mozilla Firefox or Internet Explorer, use the SSL (Secure Sockets Layers) security protocol, which is based on a public key cryptography process: RSA.

1.3.5Cryptographic Systems (Cryptosystems)

A cryptographic system includes mechanisms and algorithms that are based on complex mathematical procedures. There are two main classes of cryptographic systems:symmetric systems and asymmetric systems.

1.3.5.1Components of cryptosystems

A basic cryptosystem includes the following components:

-**Plain-text:** Is the data that needs to be protected.

-**Encryption algorithm:** Is the mathematical algorithm that takes plain-text as the input and returns cipher-text. It also produces the unique encryption key for that text.

-**Cipher-text:** Is the encrypted, or unreadable, version of the plain-text.

-**Decryption algorithm:** Iis the mathematical algorithm that takes cipher-text as the input and decodes it into plain-text. It also uses the unique decryption key for that text.

-**Encryption key:** Is the value known to the sender that is used to compute the cipher-text for the given plain-text.

-**Decryption key:** This is the value known to the receiver that is used to decode the given cipher-text into plain-text.

1.3.6Types of cryptosystems

Cryptosystems are categorized by the method they use to encrypt data, either symmetrically or asymmetrically.

-**symmetric key encryption:** Iis when the cryptosystem uses the same key for both encryption and decryption. In this method, keys are shared with both parties prior to transmission and they are changed regularly to prevent any system attacks.

-**Asymmetric key encryption:** Is when the cryptosystem uses different keys for encryption and decryption. However, the keys are mathematically related. In this method, each party has their own pair of keys that is exchanged during transmission.

1.3.6.1Symmetric cryptosystems:

This system is fundamentally based on the notion of key. It's about an information used to encrypt and decrypt a message. The principle of this technique, is that the key must remain completely confidential, and transmitted between correspondents in an assured way.

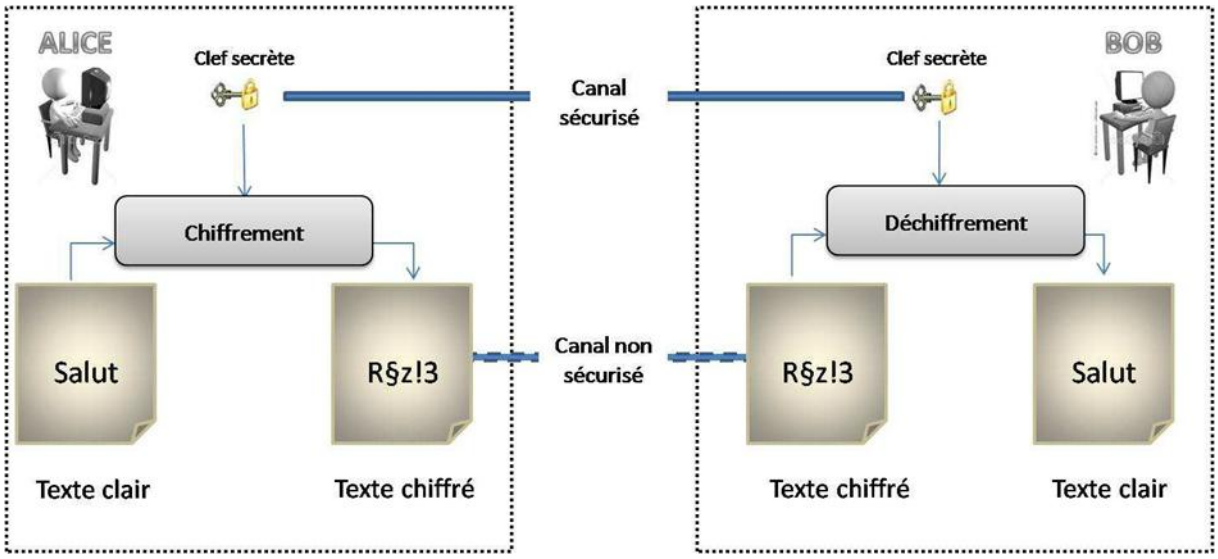

Figure 6 Representation scheme of Symmetric cryptosystems

Among the symmetric encryption algorithms, we can cite two types:

(a)bit cipher: which acts on the plain text one bit at a time:

-**Vernam cipher**: Proposed in 1917, during the First World War, as an encryption method(combining the characters typed on a machine with those of a secret key).

(b)Block cipher: which acts on the plain text by groups of bits called blocks.

-**Cryptosysteme DES:** Global encryption standard since the late 1970s.

-**AES Cryptosystem**: Successor to DES, it is a standardized block cipher in 2001.

1.3.6.2Asymmetric cryptosystems:

It is regularly referred to as public key cryptography, the encryption and decryption keys are distinct and cannot be assumed from one of the other. One of which is made public while the other remains private. If the public key is used for encryption, anyone can encrypt a message, but only the owner of the private key will be able to decrypt it.

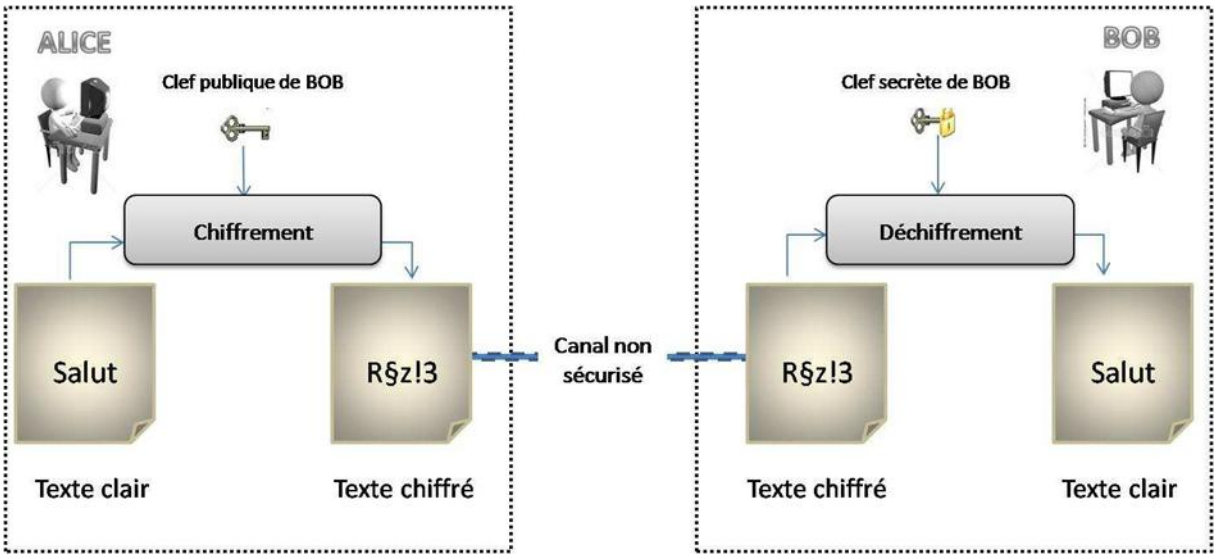

Figure 7 Representation scheme of Asymmetric cryptosystems

Public key encryption algorithms can be classified into 3 categories:

(a)Key Exchange: Principle of Diffie and Hellman,

(b)Encryption/Decryption: This provides privacy**;**

-**RSA Cryptosystem:** invented in 1978 by R.Rivest, A. Shamir and L.Adleman. Its security is closely linked to the difficulty of factoring a positive integer which is the product two large prime numbers;

-**ElGamel cryptosystem:** invented in 1985. Its security is linked to the problem of discrete logarithm.

(c)Digital Signature: This provides authentication.

1.3.7 Threshold cryptography

In modern cryptography, most schemes are designed with one sender and a single receiver scenario. In fact, there are some cases in which more than one receiver (or sender) must share the same function in a cryptosystem. The main motivation for the threshold cryptography was to develop techniques to deal with multi sender/ multi receiver scenarios. Threshold cryptography finds applications in many fields, including cloud computing, authentication, the Internet of Things, ad-hoc and sensor networks, digital signatures, and electronic voting. The technique can effectively reduce the total number of cryptographic

keys used for encryption in a group.In[7]. Desmedt,Y.studies some recent research results on this topic.

Other researches on threshold cryptography are applied in different fields, such as: encryption/decryption operations in symmetric and asymmetric cryptosystems and digital signatures.

1.3.7.1Secret Sharing Schemes (SSS)

threshold secret sharing as the name suggests, the technique shares a secret among multiple users. Each piece of the secret is called a share. The secret generating process is carried out by a trusted authority, called dealer. The secret recovery process requires a threshold number t of shares, from n shares such that $(t < n)$. In th (Chapter 2) we give details or a state of the art of secret sharing schemes.

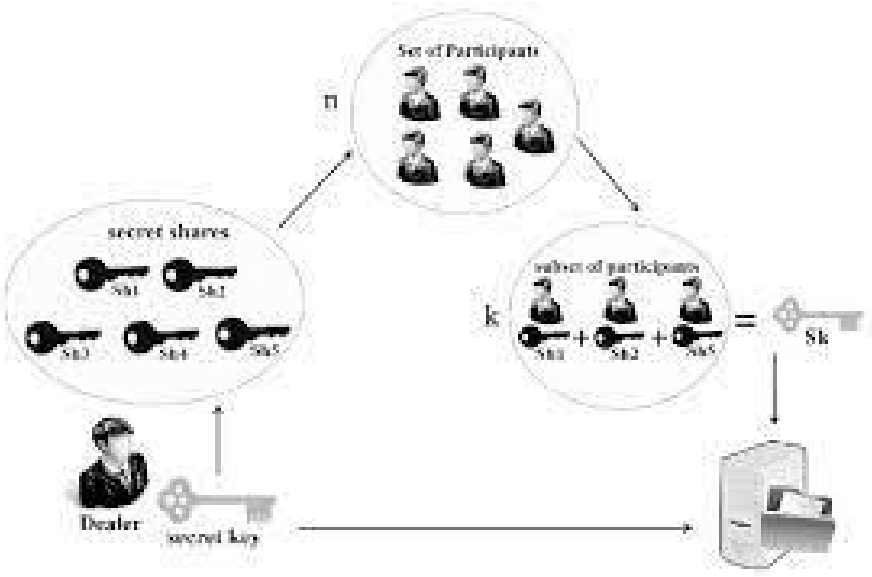

Figure 8 General Representation of threshold secret sharing scheme

1.3.7.2Cloud Computing (CC)

Cloud computing involves storing users' private data at a remote location. This breaks the implicit security of personal devices, and researchers have come up with innovative solutions to address the security concerns so as to ensure confidentiality, integrity, and access control. A major effort in cloud computing is to deploy solutions based on threshold cryptography to mitigate the problems involved private and anonymous data storage [8][9][10].

1.3.7.3The Internet of Things (IoT)

The Internet of Things (IoT) is a widely popular concept nowadays [11]. The idea of interconnectivity, with all its fancy dimensions, has started to conquer the lives of the common man. IoT helps people live and work smarter and take full control of their lives. In addition to providing smart devices for home automation, IoT is also critical for businesses. IoT can also leverage artificial intelligence (AI) and machine learning to make the data collection process simpler and more dynamic.

1.3.7.4multiparty computation (MPC)

Multi-party computation (MPC) is a branch of cryptography that started with the seminal work of Andrew C. Yao [12].

almost 40 years ago. In MPC, a set of parties that do not trust each other try to jointly compute a function over their inputs while keeping those inputs private. In fact, a major effort in cloud computing [12],is to deploy solutions based on threshold cryptography to mitigate the problems involved Private and anonymous data storage [11].

1.3.7.5threshold signature scheme (TSS)

A threshold signature scheme is a digital signature scheme in which the key generation and sign algorithms are distributed among multiple parties. i.e, (TSS) is a method for generating a single digital signature from multiple signers. In TSS, certain criteria, thresholds, must be met before a transaction can be authorized. The threshold refers to the number of major shareholders who can sign on behalf of the entire group. Signing with TSS is more efficient than other key management systems because it generates only one signature instead of multiple signatures like Multi-Signatures scheme (MSS).

Threshold signature scheme have been also considered in [13][14][15][16][17][18].

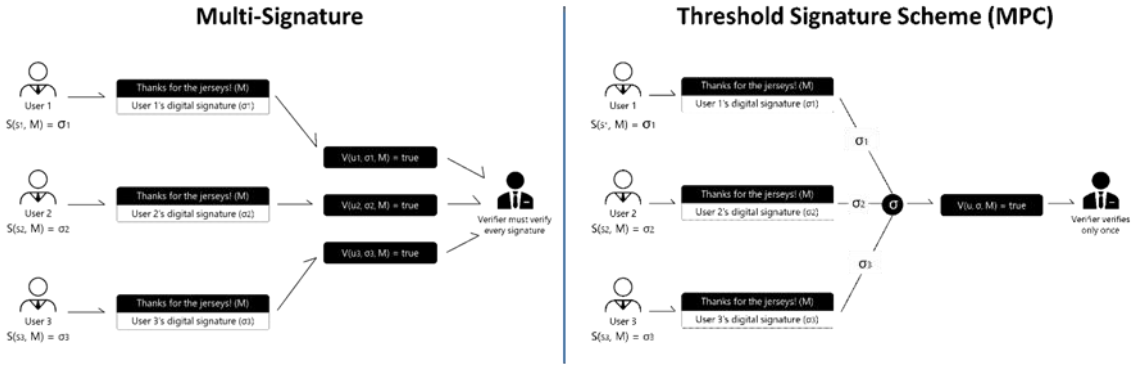

Figure 9 Multi-Signature Vs Threshold Signature Scheme

1.3.8 Bio-inspired Cryptosystems

1.3.8.1 DNA Based Cryptography

Bioinspired cryptography is a modern form of cryptography that uses nature inspiration and machine learning techniques to achieve data security. A central system based on molecular biology system (CDMB) performs encryption and decryption algorithms by simulating natural processes; Genetic coding (converts binary to DNA bases), transcription (converts DNA to mRNA) and Translation (turning mRNA into protein) and reverse processes to enable encryption and decryption respectively [19].

1.3.8.2Neural cryptography

Neural cryptography is a direction in cryptography using Artificial Neural Networks (ANN) for encryption and cryptanalysis [20].

Artificial Neural Networks (ANN) and Evolution Computing is a sub-field of artificial intelligence that includes various neural network architectures and training rules. Artificial neural networks are inspired by biological neural networks (the central nervous system, especially the brain) and can be implemented in various complex control techniques Functions approach problems in pattern recognition, data mining, forecasting, machine learning, and more. Artificial neural networks are only recently discovered the successful implementation of cryptography (especially encryption) and forms an independent branch of cryptography [21]. At least, one algorithm based on the implementation of (ANNs) in cryptography is known that uses two neural networks that can

be trained and synchronized on each other's output bits. Two neural networks sharing the same weights can be used as encryption keys.

1.3.8.3Genetic coding

Genetic coding is a bioinspired calculation that modifies the individual solution of a repeatedly selected population; the main processes of genetics are (“Population generation, crossover, and mutations”). Genetic coding exploits security as the technology structure changes from traditional security algorithms with the mathematical method; As the use of CDMB (Central Dogma of Molecular Biology) for cryptographic purposes. Because genetics has been used widely to solve optimization problems with or without restrictions applied, genetics science is used in the natural sciences, mathematics, and widely in computer science. In computer science, genetics is used for both restrictive and unrestricted security and optimization problems; it reduces huge computational complexity by solving optimization problems in the least amount of time as it can solve difficult NP problems [22]. The NP problems are explained as complexity class in (2.3.2).

1.3.9Visual cryptography

Visual cryptography research has come a long way since 1994, by Shamir [23]. Visual cryptography provides a very powerful technique that can be used to split a secret into two or more parts, called shares. If the frameworks were printed on transparencies, and then placed exactly together, the original secret could be recovered, and then, no computer participation is required, i.e without complex mathematical operations or additional hardware. VC is a unique technique because encrypted messages can be directly deciphered by the Human Visual System (HVS). Visual cryptography schemes have been also considered in [24][25][26]:

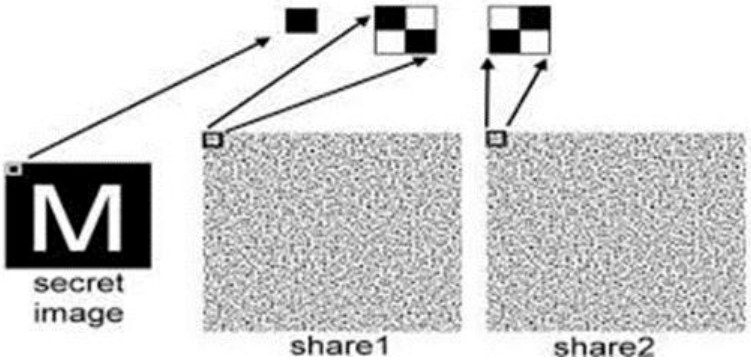

Figure 10 Visual cryptography illustration

1.4 Digital Image

1.4.1 Introduction

Nowadays, digital images represent a huge type of information involved in modern communications. Since images were introduced and processed in an electronic form, their applications have been continuously enriched. It has become digital and adopted by ordinary users and professionals (e-commerce, medicine, audiovisual, business, military...). Digital image security has become more significant with the fast progress of the internet; Therefore, it is necessary to develop tools effective protection against intrusion [27].

1.4.2 Terminology

1.4.2.1 Bitmap Image

In the most general sense, the term digital image refers to any image captured, processed and stored in coded form, which can be represented by numbers (values). Digitization is the process of enabling the state of a physical image (such as an optical image), characterized by a continuous aspect of the signal it represents (such as an infinite value of luminous intensity) to enter into the state of a digital image, characterized by a discrete aspect (the intensity of light can only be in the take quantized values at a finite number of different points). It is this digital form that enables later use by computer software tools [28].

1.4.2.2 The Pixel

The digital image is made up of a set of dots called pixels. A pixel (short for Picture Element) is defined as the smallest constituent element of a raster digital image. For a two-tone, black and white image, the pixel can be coded by a single coding bit (0 for black or 1 for white). each pixel is associated with a color, fragmented into three primary components (red, green and blue). For images in shades of gray or in color, the pixel can be coded by 2, 4, 8, 16, 24 or 32 bits.

1.4.2.3 Definition

The definition of the bitmap image is the fixed number of pixels that is used to represent the image in its two dimensions. The more pixels an image has, the greater the definition of the image. In fact, the definition of an image refers to the total number of pixels that make up a digital image. The higher the pixel count, the better the quality of the original image.

1.4.2.4 Resolution

Resolution is the number of pixels per unit length in the image. More the resolution is high (the lower the discretion step), and the better the details will be represented. Very high-resolution images provide more detailed images and facilitate the possibility of zooming in on images.

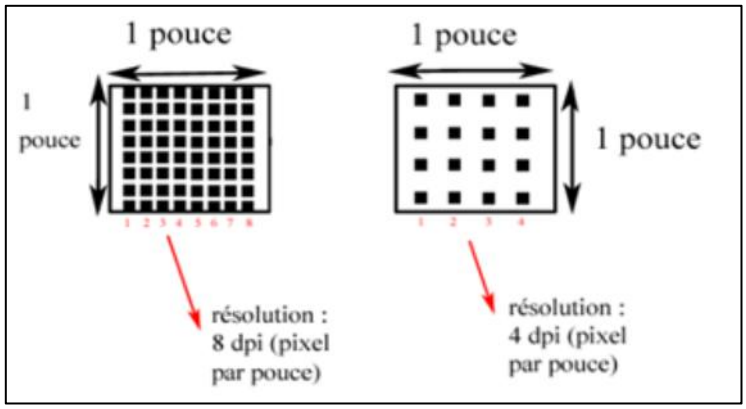

Figure 11 Resolution of 8 dpi Vs Resolution of 4dpi

1.4.3 Different types of digital image

Images can be classified into three categories according to their formats, their colors, or dimensions:

1.4.3.1 Categories of Recording formats

Concerning images, there is a wide variety of file formats, each one has its own characteristics. Consist of both bits comprising image and header information about the analysis and interpretation of the file. File formats vary in resolution, bit profundity, color capabilities, and support for compression and meta-data.

-JPEGformat: (Joint Photographic Experts Group) is a format that compresses the image. It is most commonly used in digital photography because it offers an excellent ratio between weight and image quality.

-GIF format: (Graphics Interchange Format) format that offers a compressed image while keeping good rendering but which remains limited in terms of color depth (limited to 256 colors). This format allows the production of animated images.

-BMP format (or Bitmap): Microsoft Windows default format which offers a file without compression and therefore it is very heavy.

-PNG format: (Portable Network Graphics)format that offers excellent lossless compression, PNG is robust, providing both verification file integrity and simple detection of transmission errors.

1.4.3.2 Categories of colors

Binary images: Binary images are images in witch pixels can have only two intensity values. They are displayed in black and white. Numerically, the two values are often 0 for

Figure 12 Binary image (black and white)

black, and either 1 or 255 for white.

Grayscale image : Each pixel in a grayscale image is coded on 8 bits (one byte) and can only take tints more or less gray between black and white. For a grayscale image, only one number is required per pixel, the sub-pixels receiving the same information.

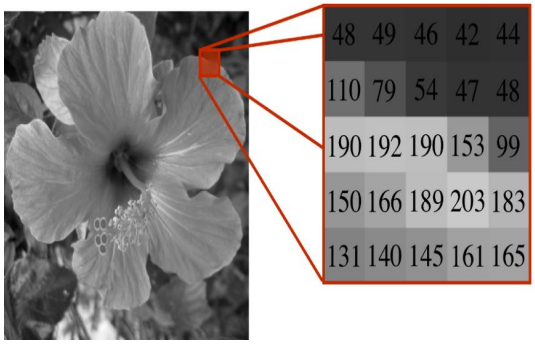

Figure 13 Grayscale image

Grayscale Bit Coding

-**One BIT** A bit is the smallest piece of data that a computer (or an image) can use. If we decide to use a bit to describe our image, we can use this on (1) or off (0) state to represent black or white without having any possible intermediate state (no gray).

-**Two BIT** If we now use two bits to describe our image, we now have four possible states: black, dark gray, light gray, white.

-**n BIT** use 3 major formats: Jpeg, Tiff or a format specific to their camera and which belongs to the Raw family. Your customers may also ask you to provide them with files in Adobe-proprietary formats such as .EPS or .PSD.

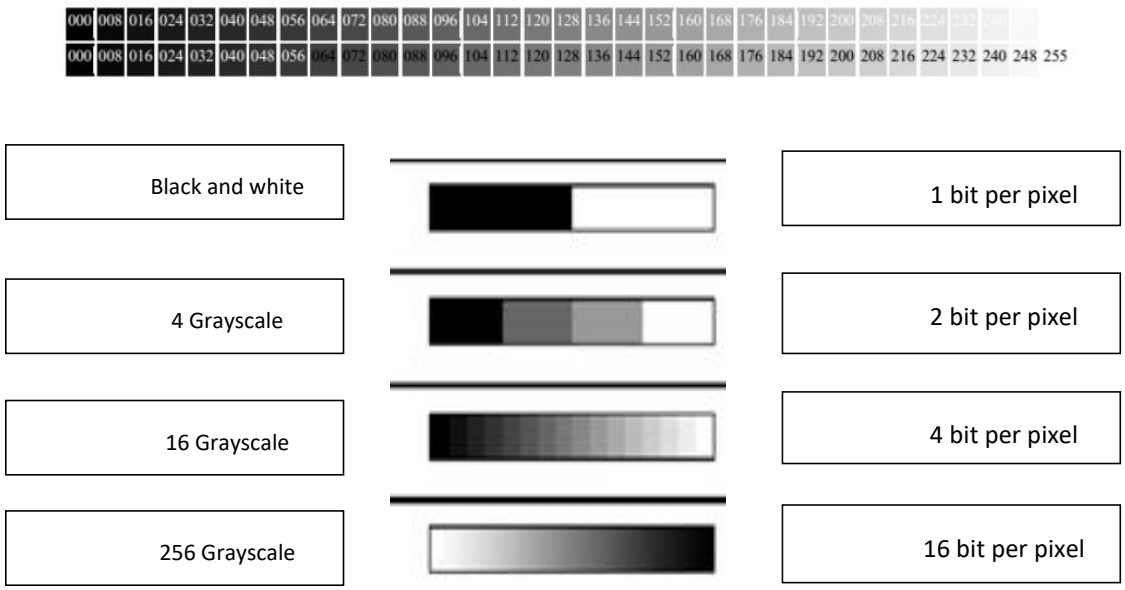

Table 1 Grayscale level degradation represented in bit per pixel

Color image: A color image is a multi-spectral image with a band for each color, thus producing a combination of the three primary colors for each pixels. A 24-bit color image, an 8-bit value for each color: red from 0 to 255, green from 0 to 255, blue from 0 to 255 , thus being able to display 224 = 16,777,216 different colors.

It is almost possible to construct all visible colors by combining the three primary colors: red, green and blue, because the human eye has only three different color receptors; each of them sensitive to one of the three colors. Different combinations of receptor stimulation allow the human eye to distinguish approximately 350,000 colors.

Figure 14Colore image

1.4.3.3Categories of dimension

Matrix dimension (bitmap image): It is composed, as its name suggests, of a matrix (array) of points with several dimensions, each dimension representing a spatial dimension (height, width, depth), temporal (duration) or other (for example, a level of resolution).

2D dimension: In the case of two-dimensional images (the most common), the points are called pixels. From a mathematical point of view, the image is considered as a function ($R \times R$) in $\mathbb{R}$ where the input couplet is considered as a spatial position, the output singleton as an encoding.

This type of image adapts well to display on a computer screen (also pixel oriented); On the other hand, it is not very suitable for printing, because the resolution of computer screens, generally from 72 to 96 dpi “dots per inch” is much lower than that achieved by printers, in minus 600 dpi today. The printed image, if it does not have a high resolution, will therefore, be more or less blurred or will show visible square pixels.

Vector image: The vector image is suitable for working on objects whose tracing parameters are known, it is described in terms of elementary shapes: (lines, circles, rectangles, The shapes are described by geometric attributes and by attributes of thickness, color, type, ...). The size of a vector image is only a function of its complexity; a very complex image is of the order of 1 to 2 MB. The spatial modifications of the image are relatively flexible, because they consist of geometric operations that do not lead to the loss of information.

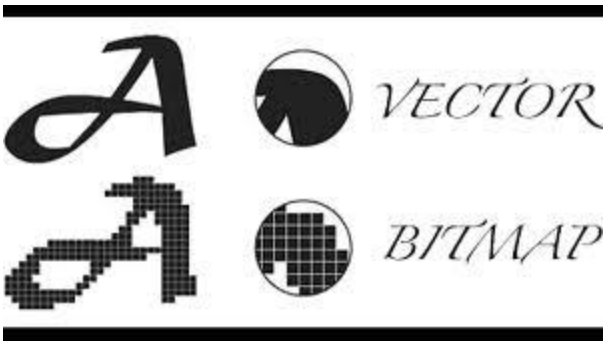

Figure 15 difference between Vector image and Bitmap image

1.4.4 Image processing in cryptography

Ensuring the security of digital images distributed or stored in an untrusted network is strongly linked to the image encryption algorithm used. However, due to its characteristic of large amounts of data and the strong correlation between pixels.

There are two major differences between textual data and digital images making text encryption methods for most cases inapplicable to encryption of images:

-**The main difference lies in the size**, indeed the amount of information contained in the image is much larger than those contained in the textual data.

-**The second difference concerns the loss of data**, when a technique of compression is applied.

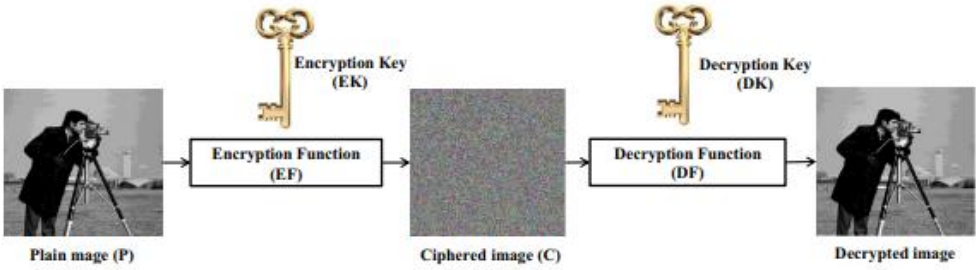

Figure 16 Encryption and decryption algorithm on grayscale image

Unlike images, using a lossy compression method is totally forbidden when encrypting a text, therefore, researchers have studied several lossy/lossless image encryption methods.

Several existing image encryption algorithms have been proposed from different technology in [29],Optic domain [30], Fourier transformation [31],[32],[33]

1.4.4.1 Encryption by confusion and diffusion methods (chaos theory)

Chaotic systems [34][35] are widely used in digital images because of their complex characteristics such as ergodicity, pseudo-randomness, and extreme sensitivity to their initial values and parameters.

The proposed chaotic image encryption schemes are based on two principles cited confusion and diffusion, where confusion is simply a rearrangement of pixels, in other words, it is based on the principle of changing the position of pixels, while the principle of diffusion changes the value of pixels.

Concept of confusion and diffusion

In cryptography, confusion and diffusion are two fundamental properties of a secure cipher:

-The confusion means that each bit of the cipher-text must depend on several parts of the key, while hiding the relationships between the two. So, the purpose of the confusion is to hide any existing bindings between the plain-text, the cipher-text and the key.

-The diffusion is a property where statistical redundancy in plain-text is dissipated in cipher-text statistics.

These two properties make cryptanalysis very difficult [36] More specifically, a cryptosystem that has good confusion and good diffusion is resistant to different attacks.

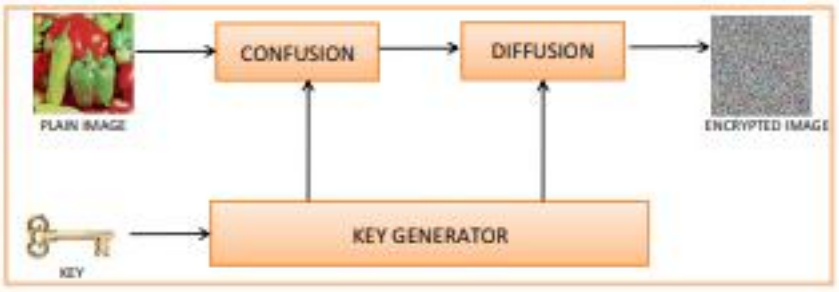

Figure 17 Encryption of color image by confusion and diffusion functions

1.4.4.2Methods based on matrix transformations

The authors of [37] adapted some matrix transformations to create a new asymmetric block image cipher scheme. First, all pixels and in each block of the original image are swapped. Then a pair of keys is created based on matrix transformation. Then, the image is encrypted using the private key. Finally, the receiver uses the public key to decrypt the encrypted messages.

Acharya et al. [38] proposed a method that allows to generate self-inverting matrix. The proposed self-inverting matrix are then used in an efficient method for image encryption using matrix transformations. The proposed method requires a lower computational complexity than other algorithms since the computation of the inverse matrix is not necessary during decryption.

1.4.4.3Encryption digital image by DNA sequencing

In [39], a new image encryption scheme based on DNA sequence addition and chaos is proposed; First, a DNA sequence matrix is obtained by encoding the original image, and then the DNA sequence matrix is divided into some equal blocks, and these blocks are added using the DNA sequence addition operation. Next, DNA sequence complement operation results of adding matrices using two logic diagrams. Finally, the scrambled image can be obtained by decoding the DNA sequence matrix obtained in the third step.

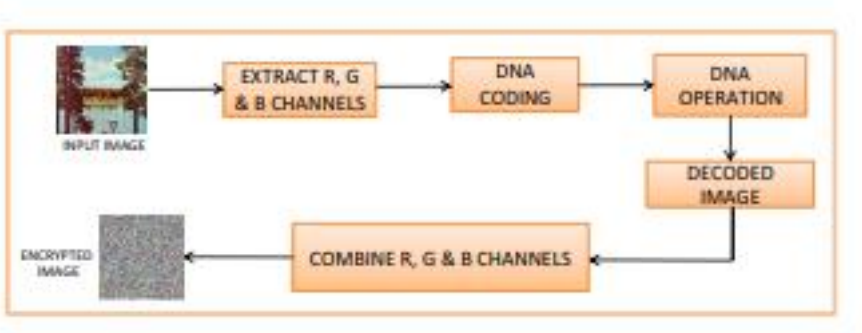

Figure 18 DNA approach applying in image encryption

In [39][40] DNA approach applying in image encryption can greatly improve the efficiency of image confusion and diffusion.

The paper [41]surveyed different image techniques and decryption in the span of 13 years (1999-2012).

1.4.4.4 Meta-heuristics Based Image Encryption Techniques

Metaheuristic techniques play an important role in optimizing NP-hard problems. The benefit of these techniques is the constant parameters needed to optimize the encryption process.

Abdullah et al. [42] used Genetic Algorithm (GA) (section 3.3.4.1) for image encryption. This technique is used to select best encrypted image from the initial population. The chaotic technique is utilized to develop a given number of encrypted images. Thereafter, GA is used to select the best encrypted image which has high entropy and low correlation coefficient.

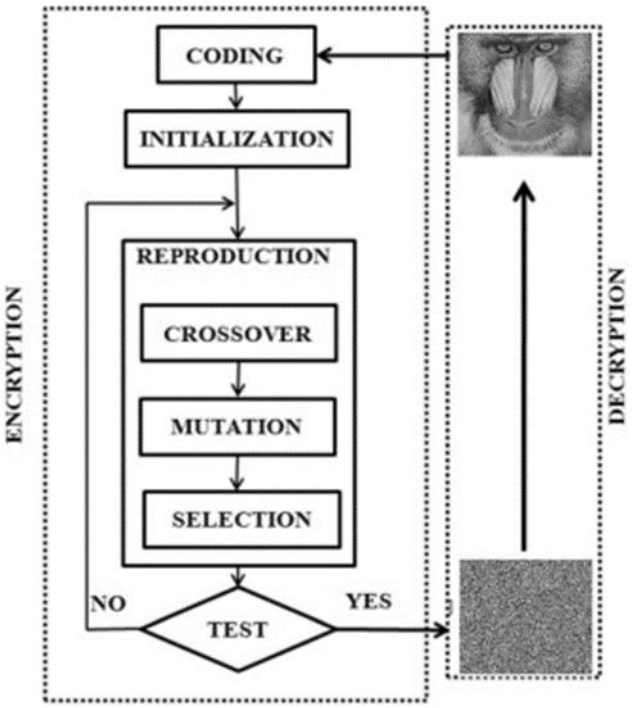

Figure19 Diagram of (GA) used for image encryption and decryption

1.4.5 Basic tools for analysing an image encryption algorithm

1.4.5.1 Key-space

The key-space size is the number of encryption/decryption key pairs that are available in the cipher system[43]. A necessary, but not sufficient, condition for an encryption scheme to be secure is that the key-space be large enough to provide security against brute force attack. the strongest method is the random generation method.

1.4.5.2 Statistical analysis

The histogram: In an image processing context, the histogram of an image refers to a histogram of pixel intensity values. This histogram is a graph illustrating the number of pixels in an image at each intensity value found in that image. For a grayscale image there are 256 different possible intensities, so the histogram is displayed graphically using 256 digits indicating the distribution of pixels between these grayscale level values [44]

In an image encryption context, the histogram of the encrypted image must be uniform so that an adversary cannot extract any information from this histogram.

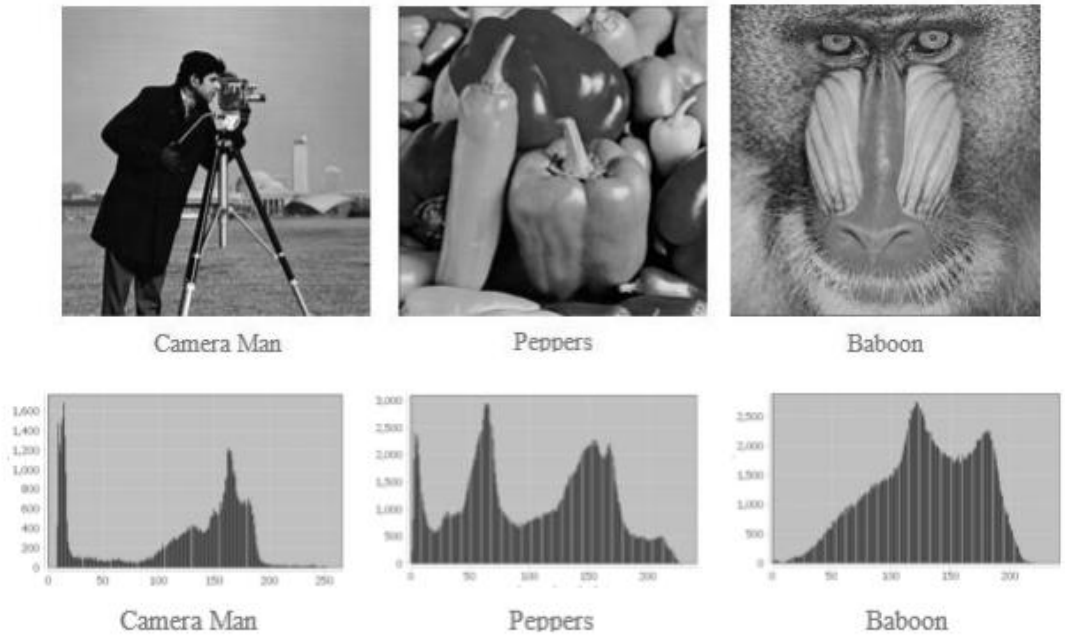

Figure 20 The plain Images and corresponding histograms.

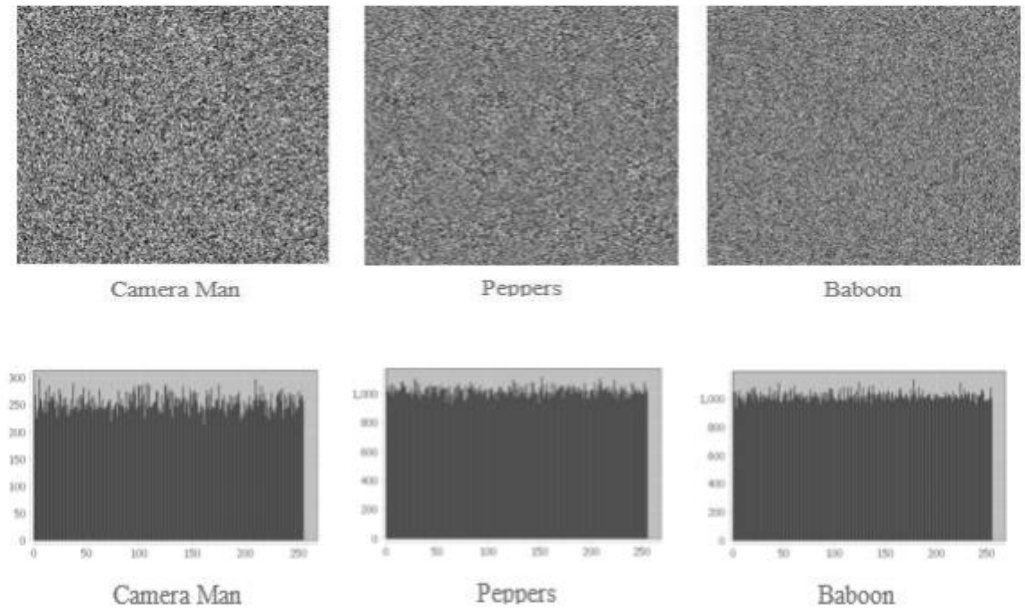

Figure 21 The cipher Images and corresponding histograms

Entopy: According to Shannon's theory [45], the entropy of information is the quantity of information absorbed or released by a source of information. Thus, it is one of the main measures of the randomness of information. High entropy values exhibit a high degree of randomness; And for any message encoded on M bits, the upper limit of the entropy is M. The formula used to calculate the entropy of a source m is as follows: So, for a perfect image encryption cryptosystem the value of entropy must be very close to 8 for each plane.

$$\boldsymbol{H(M) = \sum_{i=0}^{2^n-1} p(m_i)\, log_2(\frac{1}{p(m_i)}} \quad \textbf{(1)}$$

Correlation: it is a technique that compares two images to estimate the displacements of the pixels of one image relative to another reference image. Adjacent pixels in a standard image have a strong correlation. A good image encryption scheme should remove such correlation in order to provide security against statistical analysis.In order to test the correlation between two images, we randomly choose 10,000 pairs of two adjacent pixels of the clear image and its encrypted image and the correlation coefficients of each pair are calculated using the following formulas; Such as:

$$\mathbf{r} = \frac{\boldsymbol{cov(x,y)}}{\sqrt{\boldsymbol{D(x)}}\sqrt{\boldsymbol{D(y)}}} \quad \textbf{(2)}$$

Where:

$$\boldsymbol{Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))} \quad \textbf{(3)}$$

$$\boldsymbol{E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i\,,\ D(x) = \sum_{i=1}^{N}(x_i - E(x))^2} \quad \textbf{(4)}$$

r: the correlation.

cov: the covariance.

E: the mathematical expectation.

D: variance.

x, y: the pixel values of the images.

The result of the calculation is a real value belonging to the interval [0,1]. If the coefficient is 1 then the two images are equal. Otherwise, if the value obtained is 0 or close to 0 then the two images are different.

1.5Conclusion

In this chapter we have presented general information on computer security, we also showed how cryptography with symmetric keys and asymmetric keys is used to protect information from unauthorized or accidental disclosure.

we have tried to focus on the different image encryption techniques by mentioning some definition and concepts related to the digital image. The latter represents a very vast field of research, from which several techniques have been adapted and used.

Chapter 2. Secret sharing scheme: State of the Art

2.1Introduction to secret sharing

Due to increased reliance on technology, information security is becoming very important. Some situations require the secret to be shared among several users. For this, research in secret sharing schemes has attract a considerable attention; it is initiated in 1979 by Shamir and Blakley [46],[47]. The two authors have used Lagrange interpretation and linear projective geometry respectively.

A secret sharing scheme (SSS) is a system in which a dealer D distributes shares of a secret S to participants, such that, only authorized subset of participants can cooperate to recover the secret. The authorized subsets constitute the access structure.

For two integers k, n such that $k \leq n$. (k, n) threshold secret sharing is a special type of SSS, where among a group of participants, only k or more participants can reconstruct the secret [46], but real-world applications require more capabilities than threshold system can possess, thus, a SSS has been proposed [49][50][51].

2.2 General model for secret sharing scheme

2.2.1 The involved entities

The security of secret sharing schemes can be analysed with the help of threat models [52] Such a model takes into account distinct entities and whether they behave honestly. The entities that are assumed to be involved in secret sharing schemes are usually the following:

-**A Dealer /share builder** which shares a secret among Participants through a secure channel.

-**A Participant/ shareholders** is a member of some authorized set. He guards a share and to provides it in the reconstruction phase.

-**A Combiner** is responsible for receiving the shares from Participants and reconstructing the secret correctly.

-**An Adversary** tries to learn the secret without being authorized to.

-**The qualified subsets (access structure):** A qualified subset is a subset of the participants that should be able to rebuild the secret.

The behaviours of these entities are the following:

-**Honest Dealer** is completely honest, i.e., he shares a secret following the protocol of a secret sharing scheme.

-**A Passive Adversary** tries to capture the shares and try to recover the secret without subverting the secret sharing protocols.

-**Polarized Participants** are either completely honest (they follow the protocols correctly) or completely dishonest (they try to break the protocol).

-**Honest Combiner** is a honest party that receives all the necessary shares and reconstructs the secret.

The basic idea of secret sharing is to divide a secret according to a given access structure. **The access structure** of a given secret-sharing system is the collection of authorized subsets of shareholders who are authorized to reconstruct the secret. The secret is divided into n parts $(S_1 \dots S_n)$ such that at least one number k among n can reconstruct the secret.

2.2.2 Access Structure

The notion of access structure discusses the access authorization of a group to a system, the candidates to whom access is granted are qualified parties, who form the access structure. In the secret sharing domain, the structure of access to a shared secret is a generalized form of the threshold diagram (k, n), it represents all the subsets of participants having the right to access the reconstruction of the secret.

Let be the access structure of a secret sharing scheme Γ. The elements of the access structure are called authorized groups and the rest are called unauthorized groups. The set of all unauthorized groups is called the adversary structure. The latter is denoted $\bar{\Gamma}$. As an example, for a threshold access structure (k, n):

$$\boldsymbol{\Gamma = \{A \in 2^p : |A| \geq k} \quad \textbf{(5)}$$

$$\bar{\Gamma} = \{A \in 2^p : |A| < k \tag{6}$$

where 2^p is the set of participant groups $P = \{1, 2, \ldots, n\}$.

For each qualified set A, any set containing A will also be qualified and can reconstruct the secret. Furthermore, if a set A is unqualified, any subset of A will not be qualified and will never be able to reconstruct the secret.

$$(A \in \Gamma) \wedge (A \subseteq B) \Rightarrow B \in \Gamma \tag{7}$$

$$(A \in \bar{\Gamma}) \wedge (A \subseteq B) \Rightarrow B \in \bar{\Gamma} \tag{8}$$

The notion of a monotone structure can be deduced if the two equations **(7)** and **(8)** are both satisfied. This notion will make it possible to define one or more finite and specific subsets of participants having the possibility of reconstructing the secret in a unique way.

2.2.3 The basic phases of secret sharing scheme

Classical secret-sharing envisages an implementation which should conform to three standards phases:

-Construction phase;

-Distribution phase;

-Secret reconstruction phase.

2.2.3.1 Share construction phase

During this phase, a trusted entity, which called the dealer D, is supplied with required input to produce a share for each participants P (Figure 22).The secret can be as small as an encryption key, a safe combination or as large as a database. Without losing generality, usually the secret information is represented as integers.

Figure 22 The Dealer receives required input to produce the shares

2.2.3.2 Share distribution phase

In shares distribution phase, the shares produced in the first phase is delivered to the participants (Figure 23). Usually, secure channels are used for communication between the dealer (share-builder) and participants (shareholders).

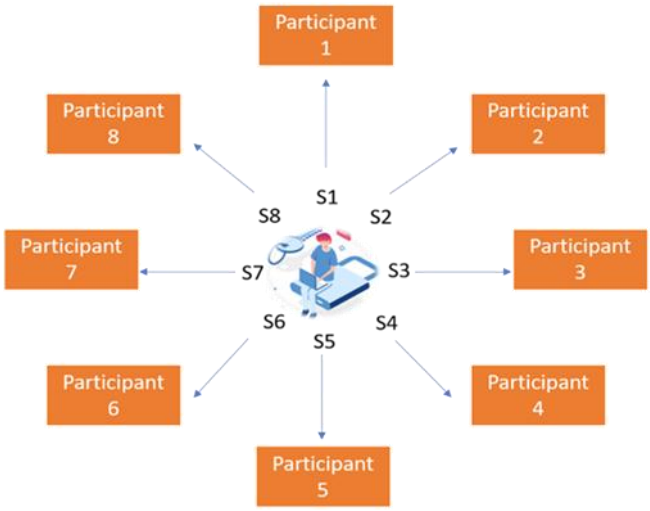

Figure 23 The dealer distributes shares to the participants

2.2.3.3 Share reconstruction phase

During Secret reconstruction phase, a qualified subset of participants will pool their shares to a trusted entity, usually called secret-builder or the combiner, to reconstruct the secret, for example in (Figure 24) participants 3, 6, 8 are not involved in this phase.

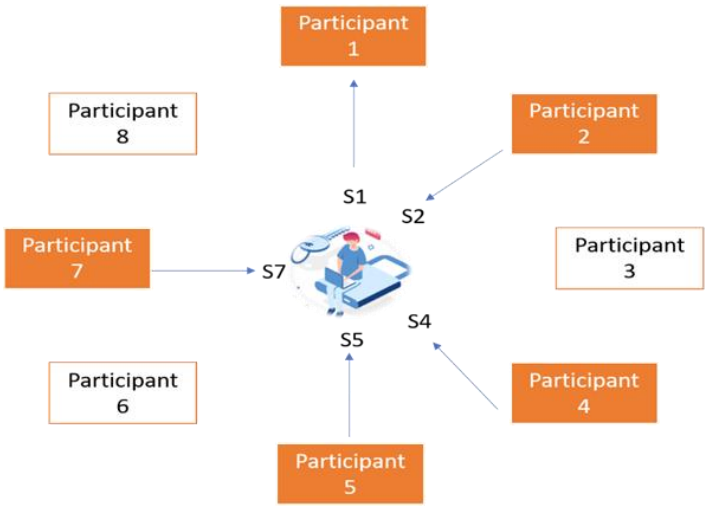

Figure 24 The combiner gets shares from a qualified subset of participants

2.3 Complexity and measures of efficiency of secret sharing scheme

In the secret sharing scheme, shares should be distributed secretly by Dealer D or Trusted Center (TC). The reconstruction of the secret can be done by a qualified set or by a trusted party called the combiner C. The class of all authorized sets is the access structure denoted by Γ. For the most schemes, access structure is considered monotone, that is, any superset of authorized group must be authorized group. We define the rank and the corank of Γ, respectively, by the maximum and the minimum cardinality of a minimal qualified subset.

One of the most important issues when designing secret sharing schemes is the size of the shares, most general access structures require shares of size exponential in the number of parties, even if the domain of the secret is binary.

2.3.1information rate

The length of the shares, when compared to the length of the secret value, is usually considered as a measure of the efficiency of a secret sharing scheme. Specifically, the complexity, or information rate [53][63], of a secret sharing scheme is defined as the ratio between the maximum length of the shares and the length of the secret. The average complexity, or average information rate, is defined analogously from the average length of the shares. In every secret sharing scheme, the length of every share is at least the length of the secret.

The information rate of SSS is defined by:

$$\boldsymbol{e = \frac{Thesizeof S}{Max(thesizeofshares)}} \quad \textbf{(9)}$$

And it is used to measure the efficiency of the system.

2.3.2 Complexity classes

One can formally define the complexity classes *P*, *NP*, and *BPP*. We only consider the time complexity here. The complexity is analysed in terms of asymptotic behaviour; This convention allows us to eliminate some small inputs on which the machine could

perform exceptionally well, and we can then focus on the "general" functionality of the machine.

A.The complexity class $\mathcal{P}$

A Turing machine is said to run in polynomial time if there is a polynomial P, such that the number of instructions is less than $P(n)$ where n is the size of the input; The complexity class $\mathcal{P}$ (Polynomial) represents the set of languages L that can be recognized "efficiently", i.e., by a deterministic Turing machine in polynomial time[54][55].

B.The complexity class $\mathcal{NP}$

The complexity class $\mathcal{NP}$ (Non-deterministic in Polynomial time), represents the set of languages that can be accepted 11 "efficiently" by a non-deterministic Turing machine [55]. In the computation tree, there is at least one branch that leads to a final state accepting if the input word is in the language. However, the discovery of this branch is not always easy to find because the number of branches in the tree of calculations can be exponential. Thus, in polynomial time, the machine cannot not explore all branches.

Informally, we can also see $\mathcal{NP}$ as the class of all languages that admit a certificate of belonging to a language. This certificate is, for example, the representation of the branch that leads to an accepting state. Given this certificate, also called a witness, membership in a language can be efficiently verified, i.e., in polynomial time.

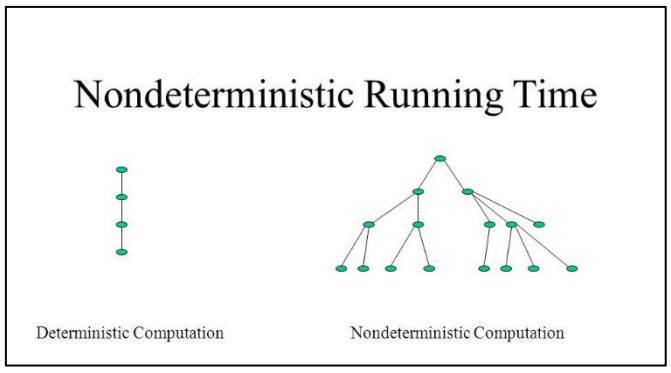

Figure 25 Deterministic (class *P*) Vs Non-deterministic (class *NP*) complexity

2.4 Secret Sharing Techniques

2.4.1 Technique of Adi Shamir

2.4.1.1 Polynomial interpolation

In numerical analysis, interpolation is a mathematical operation allows to construct a curve from a finite number of points, or a function from a finite number of values. There are several types of interpolation such as: Linear interpolation, cosine interpolation, cubic interpolation, and Polynomial interpolation[56]; Polynomial interpolation is a technique of interpolating a data set or a function by a polynomial. In other words, given a set of points, we have to looking for a polynomial that passes through all these points.

2.4.1.2 Algorithm

Shamir's scheme [46] is based on polynomial interpolation; The basic idea of Adi Shamir is that 2 points are sufficient to define a line, 3 points are enough to define a parabola, 4 points to define a cubic curve, etc. In other words, it takes k points to define a polynomial of degree $k - 1$.

In other words, in a finite field, we generate a polynomial of degree k whose constant term is the secret information. Each participant is given the coordinates of a separate point chosen on the curve. Thus, k participants can, by polynomial interpolation, find the coefficients of the polynomial, and therefore the secret information.

A.Construction and distribution phase

Suppose we want to use a threshold scheme (k, n) to share our secret S, which we assume to be an element in a finite field, without loss of information. We need to follow the following steps:

-**Step 1)** Select randomly $(k - 1)$ coefficients $a_1, \ldots, a_{k-1}$ in F, and set the constant term:$a_0 = S$

-**Step 2)** Construct the polynomial of degree $k - 1$:

$$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots + a_{k-1} x^{k-1}$$

-**Step 3)** Calculate n points from this polynomial, for example; $i = 1, \ldots, n$ which give the points $(i, f(i))$;

-**Step 4)** Each participant receives one point.

B.Reconstruction Phase

We can find the coefficients of the polynomial, using polynomial interpolation, by the Lagrange polynomial:

$$f(x) = \sum_{j=0}^{k-1} y_j \; l_j(\mathrm{x}) \tag{10}$$

$$l_j(x) = \prod_{m=0, m\neq j}^{k-1} \frac{x - x_m}{x_j - x_m}(\mathrm{x}) \tag{11}$$

Where, the l_j are the basic Lagrange polynomials.$l_j\,(x)$ are calculated by (11).

Then we calculate the final polynomial and hence, we find a_0, which represent the secret S value.

2.4.1.3 Graphic interpretation

(Figure 26) shows, for 4 points$(-9, 5), (-4, 2), (-1, -2), (7, 9)$, the polynomial interpolation L(x) (of degree 3), which is the sum of the basic polynomials $(\mathrm{y}_0.\mathrm{l}_0(\mathrm{x}))$, $(\mathrm{y}_1.\mathrm{l}_1(\mathrm{x}))$, $(\mathrm{y}_2.\mathrm{l}_2(\mathrm{x}))$, and $(\mathrm{y}_3.\mathrm{l}_3(\mathrm{x}))$. The interpolation polynomial passes through the 4 control points, and each basic polynomial passes through its respective control point (0) for the x corresponding to the other control points.

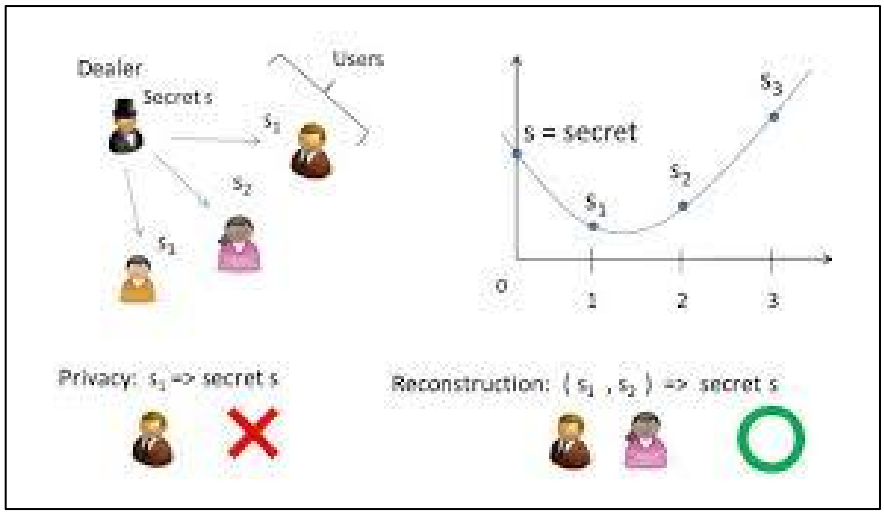

Figure 26 Shamir SSS with Interpolation polynomial.

2.4.1.4 Example

Phase 1: Construction and distribution

Suppose our secret is S=224. We would like to share the secret in 6 parts, or shares (n = 6), where any assembly of 3 parts (k = 3) is enough to reconstruct the secret.

-**Step 1)** Generate randomly $k - 1$ numbers greater than 0; in our case we get 2 numbers: 118, 56.

$$a_0 = S = 224,\ a_1 = 118,\ a_2 = 56$$

The polynomial to produce the keys is written as follows:

$$f(x) = 224 + 118x + 56x^2 \quad \textbf{(12)}$$

-**Step 2)** We can constructed 6 points using the polynomial (12):

(1, 398), (2, 684), (3, 1082), (4, 1592), (5, 2214), (6, 2948)

-**Step 3**) We give each participant a different point at a time $(x, f(x))$.

Phase 2: Reconstruction

-**Step 1**) In order to reconstruct the secret, 3 points will be enough. For example :

$$(x_0, y_0) = (2, 684),\ (x_1, y_1) = (4, 1592),\ (x_2, y_2) = (6, 2948).$$

-**Step 2)**The associated Lagrange polynomial is written:

$$f(x) = \sum_{j=0}^{k-1} y_j\ l_j(x),\ \ l_j(x) = \prod_{m=0, m\neq j}^{k-1} \frac{x - x_m}{x_j - x_m} \qquad \textbf{(13)}$$

Where the $l_j$are the basic Lagrange polynomials

$$l_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x-4}{2-4} \cdot \frac{x-6}{2-6} = \frac{x-4}{-2} \cdot \frac{x-6}{-4}$$

$$= \frac{(x^2 - 6x - 4x + 24)}{8} = \frac{1}{8}x^2 - \frac{5}{4}x + 3$$

$$l_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x-2}{4-2} \cdot \frac{x-6}{4-6} = \frac{x-2}{2} \cdot \frac{x-6}{-2}$$

$$= \frac{(x^2 - 6x - 2x + 12)}{-4} = -\frac{1}{4}x^2 + 2x - 3$$

$$l_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x-2}{6-2} \cdot \frac{x-4}{6-4} = \frac{x-2}{4} \cdot \frac{x-4}{2}$$

$$= \frac{(x^2 - 4x - 2x + 8)}{8} = -\frac{1}{8}x^2 - \frac{3}{4}x + 8$$

$$f(x) = 684(\tfrac{1}{8}x^2 - \tfrac{5}{4}x + 3) + 1592(-\tfrac{1}{4}x^2 + 2x - 3) + 2948(\tfrac{1}{8}x^2 - \tfrac{3}{4}x + 1)$$

$$f(x) = 244 + 118x + 56x^2$$

-**Step 2)** the secret S is: 244.

2.4.2 Technique by George Blakely

2.4.2.1 Algorithm

Blakely secret sharing scheme[47] uses the geometry of hyperplanes to solve the secret sharing problem[57][58]; The secret is a point in the t-dimensional plane where the n parts are affine hyperplanes passing from this point as shown in (Figure 27). We can write

the coordinates of an affine hyperplane in a t-dimensional plane with a linear equation of the form:

$$a_1x_1 + a_2x_2 + \ldots + a_tx_t = b \quad \textbf{(14)}$$

The common point will be found by the intersection of t hyperplanes among the n hyperplanes. The secret is one of the coordinates of the point of intersection. We can manage to put the secret in the first coordinate.

In other words, in a finite field GFq, we build a linear system with n equations and t, and whose only solution is the secret information. The constant term is public, and each participant receives a line from the system.

A. Construction and distribution phase

Suppose we want to use the threshold scheme (k, n), and consider our secret denoted by S. We will pursue the following steps:

-**Step 1)** Generate a k-dimensional point x note that the first coordinate is our secret S, and the others are randomly chosen;

-**Step 2)** generate Random$k$ coefficients;

-**Step 3)** From k coefficients and the coordinates of the point x, we write them in the form of a linear equation of k;

-**Step 4)** For $n$participants repeat steps 1), 2) and 3)for n times;

-**Step 5)** Each participants is given an equation.

B. Reconstruction Phase

To find the coordinates of the point of intersection x we simply look for the solution of the system of equations of t equations (n ≥ t ≥ k) and k unknowns values.

-**Step 1)** Constitution of a system of equations of t equations as follows:

$$\begin{cases} a_{11}x_1 + a_{21}x_2 + \ldots + a_{k1}x_k = b_1 \\ a_{12}x_1 + a_{22}x_2 + \ldots + a_{k2}x_k = b_2 \\ a_{1t}x_1 + a_{2t}x_2 + \ldots + a_{kt}x_k = b_t \end{cases}$$

-**Step 2)** Find the solution of the system whose solution is represented by the coordinate values of the intersection point x.

-**Step 3)** We compare the secret by the first coordinate.

2.4.2.2 Graphic interpretation

Each part of the secret is a plan, and the secret is the point of intersection between the three parts. Two shares only intersect at a line of intersection.

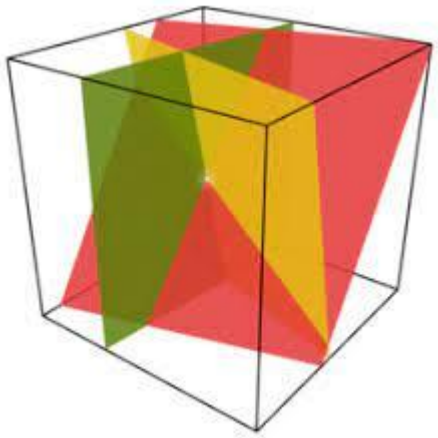

Figure 27 the geometry of hyperplanes of Blackly SSS

2.4.2.3 Example

Suppose that our secret is S=224. We want to divide the secret into 6 parts (n = 6), where any meeting of 3 parts (k = 3) is enough to reconstruct the secret.

Phase 1: Construction and distribution

-**Step 1)** Generate the coordinates of a k-dimensional point x ; $X = [x_1, x_2, x_3] = [224, 75, 13]$, note that the first coordinate x_1 = 224 is our secret S;

-**Step 2)** Choose random k coefficients for n equations;

$$\begin{gathered} \boldsymbol{a_{11} = 12,\quad a_{21} = 25,\quad a_{31} = 35} \\ \boldsymbol{a_{12} = 20,\quad a_{22} = 10,\quad a_{32} = 11} \\ \boldsymbol{a_{13} = 16,\quad a_{23} = 5,\quad a_{33} = 7} \\ \boldsymbol{a_{14} = 2,\quad a_{24} = 13,\quad a_{34} = 6} \\ \boldsymbol{a_{15} = 3,\quad a_{25} = 5,\quad a_{35} = 17} \\ \boldsymbol{a_{16} = 43,\quad a_{26} = 9,\quad a_{36} = 21} \end{gathered}$$

-**Step 3)** Writing data in the form of linear equations.

$$a_1x_1 + a_2x_2 + a_3x_3 = b \qquad \textbf{(15)}$$

And calculate:

$$a_1x_1 + a_2x_2 + a_3x_3 = b$$
$$12(224) + 25(75) + 35(13) = 5018$$
$$20(224) + 10(75) + 11(13) = 5373$$
$$16(224) + 5(75) + 7(13) = 4050$$
$$2(224) + 13(75) + 6(13) = 1501$$
$$3(224) + 5(75) + 17(13) = 1620$$
$$43(224) + 9(75) + 21(13) = 10580$$

Each participant receives the values $(a_1, \ldots, a_k, b)$.

$P_1(12, 25, 35, 5018)$, $P_2(20, 10, 11, 5373)$, $P_3(16, 5, 7, 4050)$, $P_4(2, 13, 6, 1501)$, P_5 (3, 5, 17, 1620), P_6 (43, 9, 21, 10580).

Phase 2: Reconstruction

-**Step 4)** In order to reconstruct the secret, 3 equations will be sufficient. For example: P1, P3, P6: $P_1(12, 25, 35, 5018)$,, $P_3(16, 5, 7, 4050)$, P_6 (43, 9, 21, 10580).

The system is written:

$$\begin{cases} 12x_1 + 25x_2 + 35x_3 = 5018 \\ 16x_1 + 5x_2 + 7x_3 = 4050 \\ 43x_1 + 9x_2 + 21x_3 = 10580 \end{cases}$$

-**Step 5)**Solve this system to find the coordinates of the point of intersection.

The system solution is:

x_1= 224.00000000000003

x_2 = 75.00000000000007

x_3 = 12.999999999999952

-**Step 6)** Result: the secret is the first coordinatex_1 = 224

2.4.3 Chinese Remainder technique

2.4.3.1 Algorithm

The Chinese remainder theorem, is a result of modular arithmetic dealing with the resolution of systems of congruences [59][60][61] .This result, initially established onZ/nZ, and it can be generalized in number theory.

A. Construction and distribution phase

Suppose we want to use the threshold scheme (k, n), and take our secret denoted S. We will follow the following steps:

-**Step 1)** generate a Random $n+1$ Relatively prime numbers noted m

$m_0, m_1, \ldots, m_n$ satisfying the following conditions: m_0 is a prime number.

$$0 < m_0 < m_1 < \ldots m_n \tag{16}$$

$$\mathrm{M} = m_1 \times m_2 \times \ldots m_k > m_0 \times m_n \times m_{n-1} \times \ldots \times m_{n-k+2} \tag{17}$$

Where:

$$m_0 \times \prod_{i=1}^{k-1} m_{n+1-i} < \mathrm{M} = \prod_{i=1}^{k} m_i \tag{18}$$

-**Step 2)** Choose a random integer α such that:

$$0 \leq y = S + \alpha m_0 < \mathrm{M} \tag{19}$$

-**Step 3)** Compute $y_i \equiv y \bmod m_i$ for $i = 1, 2, \ldots, n$

The y_i are the values that we want to distribute over n participants.

C. Reconstruction Phase

In order to reconstruct the secret, we will have to follow the following steps:

-**Step1)** Collect at least k shares of $k$participants:(y_i, m_i)

-**Step2)** Use the Chinese remainder theorem to solve the following system of congruences:

$$\begin{cases} y \equiv y_1 \bmod m_1 \\ y \equiv y_2 \bmod m_2 \\ \vdots \\ y \equiv y_k \bmod m_k \end{cases}$$

The system has a unique solution ,Only if the m_i are Relatively prime,

-**Step 2)** Calculate M $= m_1 \dots m_k$ and then, calculate S = (Y mod M) mod m_0.

2.4.3.2 Example

Suppose our secret is S = 4. We want to divide the secret into 5 parts ($n = 5$), where any group of 3 shares (k = 3) is enough to reconstruct the secret.

Phase 1: distribution

-**Step 1)** Generate random (n + 1 = 5 + 1 = 6) relatively prime numbers;

- $m_0 = 5,\ m_1 = 13,\ m_2 = 17,\ m_3 = 19,\ m_4 = 21,\ m_5 = 23$

- M $= m_1 \times m_2 \times m_3$

$= 13 * 17 * 19 = 4199$;

M > $5 * 21 * 23 > 2415$, The condition is satisfied;

-**Step 2)** Choice of a random integer $\alpha = 29$ which satisfies the condition:

$0 < S + \alpha \times m_0 <$ M ;

$y = 4 + 29 \times 5 = 149 < 4199 < M$

-**Step 3)** Computesy_i for $i = 1 \dots n$,

$y_1 = 149\ mod\ 13 = 6, y_2 = 149\ mod\ 17 = 13, y_3 = 149\ mod\ 19 = 16, y_4 = 149\ mod\ 21 = 2, y_5 = 149\ mod\ 23 = 11.$

Phase 2: Reconstruction

-**Step 1)** Choosing 3 values will be sufficient. For example: $y_1 = 6$, $y_1 = 2$ and $y_1 = 1$;

$$\begin{cases} y \equiv 6\ mod\ 13 \\ y \equiv 2\ \ mod\ 21 \\ y \equiv 11\ mod\ 23 \end{cases}$$

-**Step 2)** Calculate:M $= m_1 \times m_2 \times \dots \times m_k$, $M = 13 \times 21 \times 23 = 6279$;

-**Step 3)** The solution of the system is: $y = 6e_1 + 2e_2 + 11e_3\ mod$ M ; Each e_i is calculated using the extended Euclid algorithm[62]. $e_i = s_i \times \frac{\mathrm{M}}{\mathrm{m_i}}$;

$$\begin{cases} e_1 = -6 \times 483 = -2898 \\ e_2 = -4 \times 299 = -1196 \\ e_3 = -8 \times 273 = -2148 \end{cases}$$

$$y_0 = \big(6 \times (-2898)\big) + \big(2 \times (-1196)\big) + \big(11 \times (-2148)\big)$$
$$= -43804\ mod\ M = 149\ mod\ m_0 = 4$$

The result optined is the secret information S=4.

2.5 Secret Sharing Scheme Properties

different secret sharing schemes with specific properties, were developed. Some of secret sharing schemes properties are described next.

2.5.1 Perfect secret sharing scheme

A secret can be shared across n individuals via a secret sharing method, and only certain subsets of those people are allowed to recover the secret. Perfect secret sharing methods satisfy the extra requirement that unqualified subsets can obtain zero knowledge of the secret. Several SSS were designed to be perfect such as [63][64][65][66].

2.5.2Non-perfect secret sharing scheme

The advantage of perfect SSS is that unqualified subset of participants cannot use their shares to gain any information about the secret. Thus, in a non-perfect secret sharing scheme, unqualified subset of participants may cooperate to uncover some information about the secret. This partial information has been found useful in some cases.

2.5.3Ideal secret sharing scheme

A secret sharing scheme is ideal [67], if any subset of participants who can use their shares to determine any information about the secret can in fact actually determine the secret, and if the set of possible shares is the same as the set of possible secret. i.e. A secret-sharing scheme is ideal if the domains of the shares are the same as the domain of the secrets. By a mathematical proof; A secret sharing scheme is called ideal if the information rate for all shares is equal to one. The information rate of SSS is defined by formula (9) in (section 2.3.1). And it is used to measure the efficiency of the system. As an example, consider the Shamir's (k, n) threshold scheme, then:

$$\left|\Gamma\right| = C_n^k = \frac{n!}{k!(n-k)!} \qquad \textbf{(20)}$$

2.5.4 Secret sharing homomorphism

Homomorphism property attained by several other secret sharing schemes, which allows multiple secrets to be combined by direct computation on shares. This property reduces the need for trust among agents, and allows secret sharing to be applied to many new problems. A description of the homomorphism property of secret sharing was given first in 1987 by Benaloh [68].

2.5.5 Linear secret sharing schemes

linear secret-sharing schemes is a class of schemes based on linear algebra. which are schemes in which the secret can be reconstructed from the shares by a linear mapping.

Most known secret-sharing schemes are linear. For example, the schemes of [46][47]. However, the schemes in [69][70] are non-linear SSS.

2.6 Classification of secret sharing scheme

2.6.1 Threshold secret sharing

Definition 1: Let a secret S to be protected and divided into n parts, and t a positive integer;
In a secret sharing scheme (t, n), the secret is divided between n participants so that:

-for a threshold t; any set of $(t \leq n)$ participants who collaborate can reconstruct the secret, whereas;

-less than t participants cannot get any relevant information on the secret.

in [46] Shamir proposed a scheme like (t, n) threshold scheme (2.4.1), the principle is: in a finite field, generates a polynomial of degree t in which the constant term is the secret S, and the reconstruction is done by applying the polynomial interpolation.

A (t, n) threshold schemes have been proposed by Blackly [47] based on the geometry of hyperplanes over finite fields (section 2.4.2). The secret is a point of a $t-$dimensional space, and n secret shares are affine hyperplanes passing through this secret point.

The secret sharing scheme based on threshold level has been categorized into four forms:

-(t, n) threshold sharing scheme;

-(n, n) threshold sharing scheme;

-$(2, 2)$ threshold sharing scheme;

-$(2, n)$ threshold sharing scheme.

The chronological order of threshold based sharing schemes are shown in [71]

Another variant of a secret-sharing scheme based on modular arithmetic, using a simultaneous congruence system, see (section 2.4.3), of which the parts of the secret S are residual classes associated with the secret S. In [72] The patterns of Mignotte and Asmuth Bloom are almost similar, they used a special sequence of prime integers between them.

This threshold secret sharing schemes are considered as perfect schemes because a subset of fewer than t participants cannot determine any partial information regarding the secret S, even with infinite computational resources. they considered two as ideal schemes because the length of every share is the same as the length of secret S.

In the literature, there is scenarios in which non-threshold secret sharing schemes are required because, for instance, Somme participants should be more authorized to reconstruct the secret then others. for this type of case a hierarchical secret sharing and general access structure are proposed.

2.6.2 General access structure

we consider that generalized secret sharing scheme as flexible extension of the perfect threshold secret sharing [66], so it is natural to expect that the participants are not equal their privileges or authorities. In [73][74] and [75] they describe a general method of threshold secret sharing where: P is the set of all participants with the following proprieties:

-If an authorized subset of participants $B \subseteq P$ pool their shares, so that they can determine the value of the secret S;

-If an unauthorized subset of participants $C \subseteq P$ pool their shares, then they can determine nothing about the secret S.

In [74] secret sharing scheme with general monotone access have been proposed.

2.6.3 Hierarchical access structure

Secret sharing in hierarchical groups has been studied extensively in the past [76][77], where the secret is shared among a group of participants partitioned into levels. such problems may occur in setting where the participants differ in their authority or level of confidence [78]. for example, a bank transfer should be signed by some bank employees, at least one of them must be a department manager. in [78] they presented a hierarchical threshold secret sharing based on the theory of Birkhoff interpolation [79].

2.6.4 Visual secret sharing scheme

Moni Naor and Adi Shamir introduced another sharing scheme called '$(2, 2)$ sharing scheme'. This sharing scheme creates a concept called 'Visual Cryptography'[23]. The shares are generated based on contrast level of the pixel. While this scheme fails in obtaining the contrast level when a greater number of shares are shared and combined together. To overcome this problem '$(2, n)$ sharing scheme' was introduced. Even though improvement was made in the sharing scheme, it lagged to provide the perfect contrast proposition which was addressed by [80]. Hofmeister improved the contrast level and he tried to provide the perfect reconstructed image with perfect contrast.

2.7Threat models in some Secret sharing scheme

There are threat models where some secret sharing schemes cannot guarantee secret's security.

2.7.1Security limitations of Shamir's secret sharing

In [81] very interest vulnerabilities were mentioned; for example, the use of super singular curves or anomalous curves leads to weaknesses in elliptic curve cryptosystems, for RSA cryptosystem there are some attacks for low public exponent or small private exponent. In certain circumstances the secret sharing scheme is required to decentralize the risk. By this context, the well-known Shamir's secret sharing is not always perfect and that the uniform randomization before sharing is insufficient to obtain a secure scheme.

2.7.2 Secret Sharing Schemes with Hidden Sets

One example, is a variation on Shamir's scheme, where a malicious dealer can distribute wrong shares to participants. In this way, different groups of Participants could reconstruct different secrets without knowing whether the secret obtained is the correct one. To guarantee security with these threat models, verifiable secret sharing schemes were proposed (see section 2.8.1).

In [75] paper, they demonstrate that there exists a different threat model, where a malicious dealer can compute shares such that a subset of less than t shares is allowed to reconstruct the secret. We refer to such subsets or unauthorized access structure as a **hidden set**[1]. Two significant implications of hidden sets were mentioned in [52].

2.8 Proposed secret sharing scheme with extended capabilities

2.8.1 Verifiable secret sharing schemes (VSS)

In order to solve the reasonable distrust between the dealer and participants, Verifiable secret sharing (VSS) was introduced by Feldman in [82]. In a VSS scheme, participants are able to verify whether the shares distributed by the dealer or submitted by other participants are valid. Which ensures the security of the scheme. However, the verification phase of a VSS can only performed between participants, in [83] a system of publicly verifiable secret sharing was proposed and it consist of verification of shares in the distribution phases, and decryption of the share in the reconstruction phases.

2.8.2 Proactive secret sharing (PSS)

Proactive secret sharing (PSS) was proposed by Herzberg et al [84] This is a stronger scheme by means of security. PSS is effective in the sharing of the shares to the participants when the secret is kept. The participants get the new pieces of the secret. These pieces are independent of the old ones and then the old pieces are removed. PSS protects the secret s from possible attacks [85].

[1] Given a variation on Shamir's scheme (t, n), where t shares are required to obtain a polynomial f, when the Dealer is malicious there is a non-negligible probability that $1 < l < t - 1$ out of these shares can lead to another polynomial $g \neq f$ of degree $l - 1$ such that $g(0) = f(0)$ is the secret.

2.8.3 Secure Secret Reconstruction Scheme with verifiable shares (SSRS)

Based on bivariate polynomials, A novel design for an efficient SSRS with verifiable shares is introduced in [86]. SSRS can prevent both active and passive attackers. Moreover, they propose a verification scheme which can verify all shares at once, i.e., it allows all participants to efficiently verify that their shares obtained from the dealer are generated consistently without revealing their shares and the secret. the proposed scheme is really attractive for efficient and secure secret reconstruction in communications systems.

2.8.4 Protecting against cheating

Cheating problem in (k, n) secret sharing is an important issue, such that dishonest participant(s) (i.e., cheater(s)) can always exclusively derive the secret by submitting faked share(s) during secret reconstruction to fool honest player and thus the other honest participants get nothing but a faked secret. Cheater detection and identification are very important to achieve fair reconstruction of a secret. During periods of research on cheating prevention, vast (k, n) secret sharing schemes against cheating have been proposed [87][88][89][90][91][92][93].

2.9 Secret Shering Shceme Applications

2.9.1 Cloud systems and spatial domain embedding process

Spatial domain embedding process in digital watermarking techniques was introduced in visual cryptographic technique in [94]. This concept ensured more security with less computation cost. The secret sharing schemes were distributed to cloud system so that they can distribute data to multiple servers. The sharing scheme in cloud is resistant to system failures caused by natural disasters (or) human error [95]. Initially, the SS scheme was distributed to cloud system to use secret sharing for health data in multi-provider clouds [46].

2.9.2 Human-memorable Internet domains (DNSSEC)

The DNS system converts human-rememberable Internet domains like irs.gov into machine-readable IP addresses like 166.123.218.220. You might have a rough day if an

attacker can trick your computer into believing that irs.gov actually resides at a different IP address by posing as the DNS system. A successor known as DNSSEC has been suggested to defend against these kinds of assaults. A domain-name mapping cannot be falsified thanks to DNSSECs usage of cryptography. Although the cryptography needed to verify DNS mappings is intriguing, a more important question still has to be asked: Who can be trusted with the system's master cryptographic keys? The following scheme has been chosen by ICANN, a non-profit organization in charge of such matters. The master key is split into 7 pieces and distributed on smart cards to 7 geographically diverse people, who keep them in safe-deposit boxes. The question proposed was, how is it possible that any 5 out of the 7 key-holders can reconstruct the master key, but (presumably) 4 out of the 7 cannot? The solution lies in a cryptographic tool called a secret-sharing scheme.

2.9.3 E-Voting protocol based on SSS

For electronic voting protocols, where a single authority supports the full execution; The voting process cannot guarantee the protocol's security requirements. For Instance; If the private key used to decrypt votes is owned by a single institution, the latter can decrypt voters' votes and know each one. to avoid this kind in some situations, private keys must be shared rather than held by a single authority between some authorities. This process spreads trust to reach higher levels ensure security and reduce the risk of the presence of rogue authorities. Between the voting process, secret sharing, can be used in three different ways:

- **Class 1:**A secret is a private key shared by authorities; this private key is used to decrypt all votes.
- **Class 2**: The secret is a ballot. Each voter uses a secret sharing scheme to share its ballot between authorities.
- **Class 3:**A secret is the decryption key for a single vote. each voter A secret-sharing scheme for sharing decryption keys for his votes among authorities. Based on these three approaches, a classification of e-voting protocols using SST is proposed in [96]

Chapter 3. Metaheuristics and Bioinspired Modelling

3.1 Motivation

At the area where the fastest software on the world can no longer solve certain problems (complexity), man is progressively inspired by the nature that surrounds him to set up algorithms simulating the behaviour of animals, their actions or reactions vis-with a problem and even the methods they use to deal with it. Even if these methods are subject to many arguments, they make it possible to find easily and quickly the closest solution to the optimal one if it exists, and remains a very effective way to treat complex problems that can take years of calculations without results [97][98]

In real life, problems are more complex, including NP-hard problems. There are two types of methods to solve them: exact methods and approximate methods. Where the exact method gives the optimal solution in an unacceptable time, the approximation method gives a good solution in a reasonable amount of time. There are two types of approximation methods: heuristics and metaheuristics. The first is problem-specific, whereas metaheuristics are agnostic problems. Many metaheuristics are inspired by nature, especially biology. These bioinspired metaheuristics are easy to implement and produce interesting results. This chapter aims to provide a comprehensive overview of bioinspired metaheuristics, their taxonomies, principles, and application domains.

3.2 Optimization Problems

In mathematics and engineering, an optimization problem is the problem of finding the best solution from all possible solutions. Such a problem is usually defined as an objective function of one or more variables with a set of constraints. These problems can be discrete or continuous, depending on whether the variables involved are discrete or continuous. The complexity of an optimization problem is directly related to the objective function and the number of variables considered. However, many real-world optimization problems are classified as NP (non-deterministic polynomial time). This means that it can be solved in polynomial time using non-deterministic algorithms [97], see (section 2.3.2).

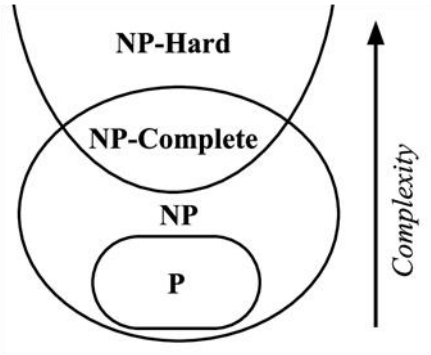

Figure 28 complexity measure levels

For these optimization problems, the goal of an efficient metaheuristic is to find a global solution to keep track of in different environments, or to find a robust solution that performs best in the presence of uncertainty. Many metaheuristics are inspired by nature, especially biology [99]. These bioinspired metaheuristics are easy to implement and produce interesting results. In this topic. we will present new bioinspired metaheuristic.

In contrast to numerical optimization algorithms, metaheuristics cannot guarantee finding a globally optimal solution. However, a reasonable solution can be obtained faster with much less computation. Many metaheuristics also use stochastic optimization, and the solution found depends on random variables. Most importantly, it works even with incomplete or imperfect information.

Metaheuristics are an increasing by preferred resolution strategy.One of the important peculiarities of metaheuristics is the absence of particular hypotheses on the regularity of the objective function. No hypothesis on the continuity of this function is required, its successive derivatives are not necessary, which makes the field of application very wide.

3.2.1 Metaheuristic Optimization Process

Each metaheuristic explores the solution space to find the best or at least good solution. It uses her two key processes of diversification and intensification[100]:

-In **the diversification** step, the metaheuristic explores the global search space to find promising areas;

-In **the intensification** process, metaheuristics make use of local regions to improve the solution.

Due to the exponential nature of the search space, metaheuristics search randomly in hopes of finding a high-quality solution in a reasonable amount of time. This trade-off between reasonable time investment and good solution quality is one of the most important key advantages of metaheuristics.

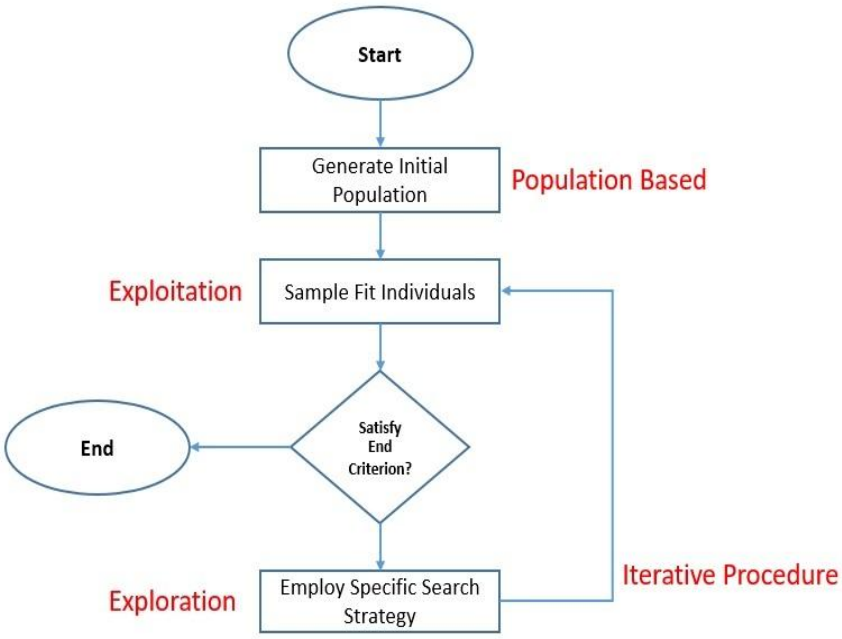

Figure 29 MetaheuristicAlgorithm

3.2.2 Advantages of Metaheuristics

One of the key aspects of the metaheuristic approach is finding the right balance between **exploration** and **exploitation**. The goal of **exploration** is to explore as many feasible areas as possible and avoid suboptimal solutions. The purpose of the **exploitation** is to discover the neighbourhood of promising regions to find the optimal solution.

-They are used where the exact method fails.

-Most of the time we find nature as a source of inspiration biology, physical phenomena;

-Their concepts are simple and free from the complexity of the gradient of the objective function.

-They are common. They are therefore associated with different issues.

-Enhanced duality, diversification, so that exploring neighbours, first can improve the quality of the solution. and a second process of exploring promising areas of the search space to improve global solutions.

-They accept degradation of current solution jumps to avoid local optimum traps and find interesting solutions.

3.2.3 Disadvantages of metaheuristics

-Convergence to the optimal solution is not guaranteed.

-It does not give information about how close the solution obtained is to the optimal solution.

-Their behaviours depend on the parameter settings. As a result, it depends on the user's experience and emotions.

-They suffer from a lack of theoretical research.

-Difficult to analyse its performance.

3.3 Bioinspired metaheuristic

The most metaheuristics are inspired by nature. This last offers some natural ways to tackle complex ordinary problems. In nature, insects, animals, and other organisms have evolved the ability to deal with complex real-life problems. The methods used and the results achieved by these "unintelligent" creatures to solve complex ordinary problems are surprising. Inspired by nature, researchers and engineers have developed ingenious solutions to solve industrial, health, transportation and other problems. It is based on the fact that a large number of studies have transmitted significant information about bioinspired metaheuristics.

Recently, bioinspired algorithms in combinatorial environments have attracted increasing interest, due to its practical utility. Many applications can be expressed as combinatorial optimization problems. The most common case is where the objective function varies over time. typical examples are dynamic automobile routing, scheduling, inventory planning, tracking a moving object, etc. The objective function may also be uncertain or noisy due to simulation, measurement or approximation errors. In addition, design variables or environmental conditions may also be disturbed, or change over time.

3.3.1 Definition of Bioinspiration

Bioinspiration is a paradigm shift that leads designers to take inspiration from nature to develop new systems. Bioinspiration is often based on biomimetics. She can draw inspiration from the world of plants, animals and insects, or bacteria and viruses. It has already contributed to applications in fields as varied as aeronautics, pharmacy, marine, medicine, green chemistry, composite materials, robotics, artificial intelligence and nanotechnologies.

3.3.2 Some application of Bioinspired techniques

It is used by non-industrial actors (in fields such as design, art, architecture, urban planning, teaching, software design, genetic algorithm and/or evolutionary algorithm) and in a way better known to the general public by engineers who sometimes adapt methods derived from the retro-engineering.

3.3.3 Classification of bioinspired metaheuristic

bioinspired metaheuristic are methods whose exploration strategies are inspired by systems in nature. Overhead, Euler diagram(figure 30)from [97]

is created for classifying different metaheuristics based on local vs. global search and single-based vs. population-based search properties.

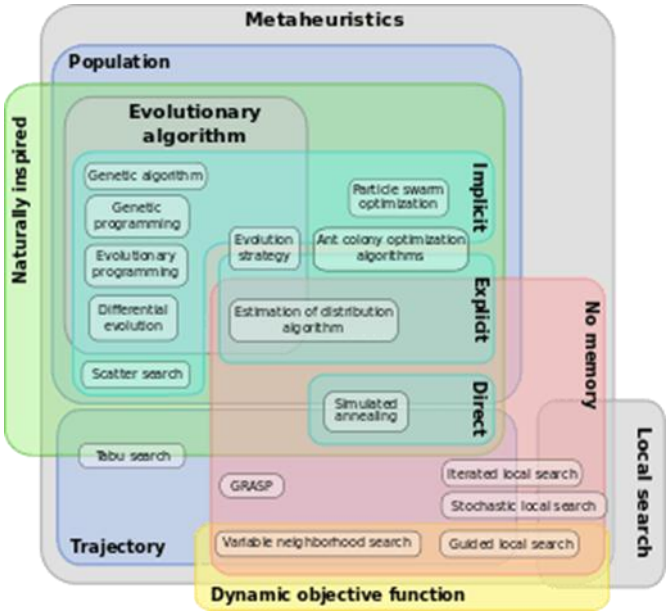

Figure 30 Euler Diagram shows classification of Metaheuristics

Evolutionary Computation forms a sub-field of artificial intelligence using a family of global optimization algorithms inspired by biological evolution. bioinspired metaheuristics can be categorized in different ways based on their characteristics. However, we will focus specifically on a class of bioinspired metaheuristics known as evolutionary computation (EC) [101][102]. Evolutionary computation[103] has a complex taxonomy of algorithms. However, it focuses on the Bode Evolutionary computation classification into evolutionary algorithms (EA)in [104], and swarm algorithms (SA) in [105] and [106].

In evolutionary computing. Both use a population-based representation of candidate solutions and an iterative approach with probabilistic search.

3.3.4 Evolutionary Algorithms

Evolutionary Algorithm (EA) is a general term used to describe population-based probabilistic direct search algorithms that in some ways mimic natural evolution. Prominent representatives of such algorithms are genetic algorithms, evolutionary strategies, evolutionary programming and genetic programming [104].

Evolutionary Algorithms (EA) are a class of algorithms inspired by Darwin's evolutionary theory [107]. his theory postulates that mutations between members of a species occur by chance. these take inspiration from this theory to identify near-optimal

solutions in the search space. Each iteration of such an algorithm is called a generation and consists of parent selection, recombination (crossover), mutation, and survivor selection. While crossovers and mutations drive exploration, parental and survivor selection brings exploitation to the fore.

3.3.4.1 Genetic algorithms

Genetic algorithms are probably one of the oldest and most popular bioinspired metaheuristics known today. Firstly, introduced in [108] by John Holland in 1975

As a search optimization algorithm based on the mechanism of the natural selection process. At its principal, it seeks to emulate the concept of "survival of the fittest", where the weak tend to perish, while the strong tend to adapt and survive. Individual solutions to problem areas are genetically represented as **chromosomes**. We characterize the solution by a set of parameters called **genes.** All genes are then linked to forma chromosome.

Start by selecting an initial population, either randomly or using heuristics. We then use the fitness function to score the population members and rank them based on their performance. This eliminates the low order chromosomes [108]. The rest of the population participates in the reproductive process. The next two operators, crossover and mutation, are important to genetic algorithms.

- **Crossover** randomly selects the two chromosomes from the population and sets them by exchanging their genes.
- **Mutation** consists of taking a chromosome and randomly mutating its genes. These operators allow the algorithm to emphasize exploration of the search space.

This cycle continues to create new populations until the termination measures are met. This is done by reaching a maximum number of generations or finding an optimal solution. Other strategies can also be used to allow subordinate chromosomes to participate in reproduction. Additionally, elitism can be used to prevent optimal solutions from being discarded during crossovers and mutations[109].

3.3.5 Popular Swarm Algorithms

The Swarm Algorithm (SA) is a relatively new and very active research area in Evolutionary Computing (EC). Recite the literature on new meta-heuristics inspired by

collective behaviour of new agents. However, we mention a few popular algorithms in this area, such as Ant Colony Optimization (ACO) artificial bee colony (ABC) and Particle Swarm Optimization (PSO).

3.3.5.1 Particle swarm optimization PSO

The algorithmic concept of particle swarm optimization (PSO) is inspired from the collective behaviours of social animals and insects, like organisms, such as: fishing and flocking birds. A swarm consists of multiple agents. A single agent's behaviours are very simple, local and stochastic. Without a centralized structure to manage agent behaviours, interactions between agents generate global intelligent behaviours called swarm intelligence (SI). These algorithms are inspired by the collective behaviours of natural agents such as ants and bees. The goal of such algorithms is the information shared within the swarm that can directly affect the movement of each agent. By controlling the exchange of information between agents in the swarm.PSO particles cooperate with each other as a group to achieve their goals [110].

3.3.5.2 Ant artificial colony algorithm:

Ant colony optimization [114] was introduced in the early 1990s. The source of inspiration for ant colony optimization is the searching behaviour of real ant colonies. This behaviour is exploited in artificial ant colonies to search for approximate solutions to discrete optimization problems, continuous optimization problems, and important problems in telecommunications such as routing and load balancing.

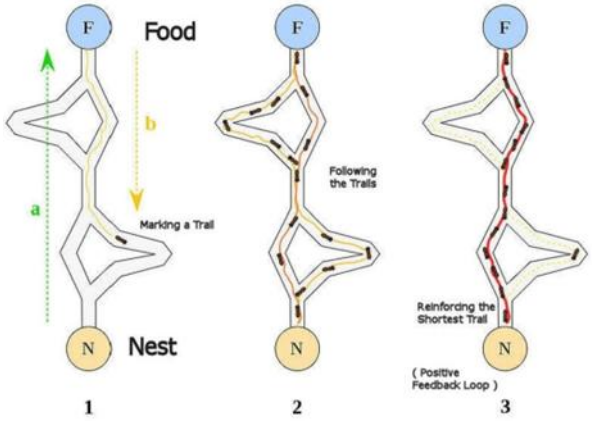

Figure 31 Ant colony optimization scheme

3.3.5.3 Artificial bee colony algorithm:

The Artificial Bee Colony (ABC) algorithm is a swarm-based metaheuristic algorithm introduced by Karaboga [111] in 2005, for optimization of numerical problems. Inspired by the intelligent foraging behaviour of bees. This algorithm is based specifically on the honeybee colony foraging behaviour model proposed by Tereshko and Loengarov [112].

This model consists of his three main components: **Employed** and **unemployed foragers** and **food sources**. At ABC, we look for artificial food sources (appropriate solutions to specific problems) that are enriched with colonies of artificial foraging bees (agents).

To apply ABC, the considered optimization problem is first transformed into the problem of discovery the optimal parameter vector that minimizes the objective function. Artificial bees then randomly discover a population of initial solution vectors and iteratively improve them using the following strategy:It uses the Neighbour Discovery mechanism to give up on bad solutions while moving to better ones[113].

3.4 Bioinspired Hexagonal Modelling

3.4.1 Why nature prefers Hexagons?

Basalt columns of an old volcanic eruption. snowflake. honeycomb. Corals, crystals, and many other biological and non-biological structures feature hexagons. Why does nature, which often appears chaotic and irregular, seem to prefer this form? Actually, it's all about geometry and physics [115].

3.4.2 The Hexagonal shape of the Beehives

Bees spend a lot of their time working, but they don't like working for free. It doesn't matter if it's not efficient. Bees make combs efficiently, and hexagons help with that. Hives are made from beeswax produced by worker bees. They produce wax from special glands on their bodies and mix it with chewed honey and pollen to make beeswax.

Figure 32 The Hexagonal shape of the Beehives

Ancient Greek philosophers wondered about this. Pap-pus of Alexandria supposed that the bee "has a certain geometrical foresight", while entomologist William Kirby believed that the bee was "heaven-instructed mathematicians". Even Charles Darwin was fascinated by the hexagonal shape of bees, and conducted an experiment to see if honeybees were able to make hexagonal combs purely by instinct, or if it was a learned behaviour.

By Darwin's time, people had a pretty good understanding of the geometry of the hexagon. Especially when it comes to covering surfaces. If you use just only one shape to cover the plane, here are only three shapes that will work. Equilateral triangle, square, hexagon. From all of these, hexagons have the least number of partitions, so it makes sense that bees prefer them because they require less beeswax. This was declared by the 18th century, i.e., Darwin declared that hexagonal hive has to be "absolutely perfect in saving labour and wax". Darwin thought that natural selection gave bees the instinct to build these wax chambers. This had the advantage of requiring less energy and time than other shapes [116].

3.4.2.1 Dragonflies' hexagonal eyes

The extinct coral Cyathophyllumhexanum is named for its hexagonal shape, and some diatoms (a major group of algae) are also hexagonal. But there may be no more hexagonal biological structure than the eye of a dragonfly.

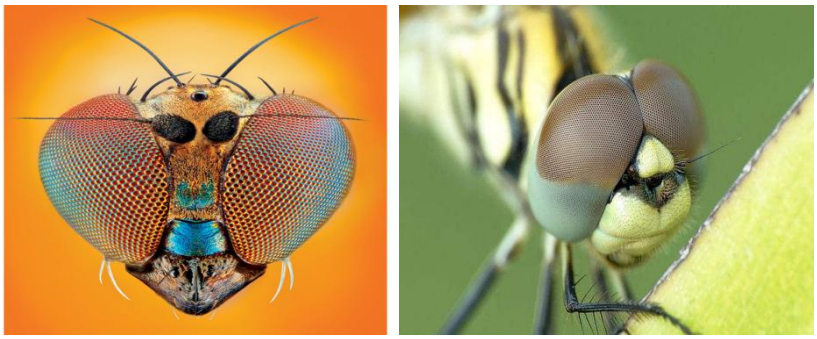

Figure 33 Hexagonal shape of the eyes of dragonflies

Dragonflies have two big compound eyes with thousands of hexagonal lenses (and three eyes with simple lenses). The hexagonal lenses are connected by underlying elongated retinal cells. In fact, there seems to always be a rule, that the eyes of many insects are hexagonal, with no more than three cell walls meeting at the apex.

3.4.2.2 Snowflakes Hexagonal structures

Certainly, every snowflake has its own, but every snowflake has six sides or tips. This is due to the way snowflakes are shaped to reflect their internal structure. The hexagonal structure groups water molecules (containing one oxygen atom and two hydrogen atoms) this in most efficiently to group up together.

In reality, snowflakes have not only crystals with a hexagonal structure. Zoom in further and you'll find yet another hexagon. As any chemistry student quickly realizes, hexagons are the foundation of organic chemistry. When six carbon atoms are joined, the angle is 120 degrees. By now it should already be known, that Combining the six carbon atoms form a perfect hexagon, also called a benzene ring.

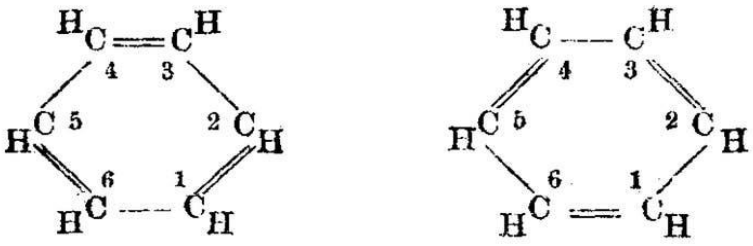

Figure 34 Hexagonal forme of a Benzene ring

3.4.2.3 Deduction

hexagons modelling proved that are an efficient way to conserve mass or energy, or simply arrange atoms in a way that stabilizes them. It may simply be due to its shape.
Nature is necessarily not always precise. Nature tends not to like very solid things, but she does like designs, and precisely hexagons.

3.4.3 Isoperimetrically Optimal Hexagon in a large grid

The isoperimetric, see (section 4.4),and uniform connectivity of the hexagonal grid make it a naturally excellent way to tile a plane. Recent work on hexagonal frames has led to significant advances in frame construction, encoding, indexing, storage and related operations [117].

Proprieties:

- A hexagon is regular if all sides are congruent and all interior angles are congruent.
- Each interior angle of a regular hexagon is 120°. The sum of its interior angles is 720°.
- A great and large planes can be covered with regular hexagons.

3.4.4 Hexagonal grids advantages

A hexagonal grid uses hierarchical subdivisions to cover an entire plane or sphere. The six-fold rotational symmetry of square and triangular lattices makes them suitable for tasks dealing with spatial information processing and intelligent decision making [116].
The hexagonal lattice defined in the previous section has some advantages over square and triangular lattices (e.g. isoperimetric, additional equidistant neighbours, uniform connections, etc.) and the information present in them helps to handle the Inspired by these advantages and natural occurrences (insect and human visual systems, honeycombs, etc.), hexagonal lattices can be indexed using the above coordinate system. These systems diverge in three important characteristics [116]:

- Storage efficiency when stored in a rectangular storage area, availability of mapping between coordinate system convolutions and traditional 2D convolutions,

- Ability to reuse square convolution kernels for hexagonal convolution,
- Simple rotation and reflection calculations in coordinate system.

Chapter 4. Mathematical Tools and Background

4.1 Motivation

The main topic of this thesis is the hexagonal structure of the Beehive, we used it because it is an optimal shape; In order to understand this mathematical structure involved in our study, we will start by introducing two simple problems: Shape optimization and isoperimetric problems.

The so-called isoperimetric problem dates back to ancient literature and geometry Physical insight into natural phenomena and answers to questions" why bees build hives with cells that are in a hexagonal shape".

It is known that the isoperimetric problem is one of the most classical shape optimization problems. it studies sets of finite perimeter and compactness of their characteristic function. This is very useful in shape optimization when the perimeter appears in the minimizing functional, it can be formulated as:

"Among all closed curves of a given length, the optimal one which encloses maximum area"

Shape optimization[117] is along-standing, classical and ubiquitous research field that has influenced not only profound mathematical theories,but numerous important industrial and engineering applications. Rising raw material constants the need to reduce energy consumption. These requirements, along with increasing computing power and the development of advanced mathematical programming techniques, have made shape and topology optimization a very popular field in industrial design, especially civil engineering, with unprecedented capabilities. Where it has successfully predicted the conceptual design. The concept of shape and topology optimization is very influential in science. Of course, it is also used in multi-purpose data processing issues such as image segmentation, shape detection and reconstruction[118][119], for modelling structural mechanics such as civil engineering and architecture [120], fluid dynamics [121] and in connection with aerospace applications or with the design of cooling devices [122][123],and biology [124].

A phenomenon when explaining the "optimal" complex patterns observed in biology. B.General purpose data processing problems such as , electromagnetic morphophonemics [125].

4.2 Definition of Shape Optimization

Shape optimization is a technique that optimizes the outer boundary of a shape. The structure is modified to solve the optimization problem.Using the finite element model, the shape is defined by the positions of the grid points, shape optimization changes these positions to update the shape.

Shape optimization is more general than parametric optimization. The shape of the component is changed by identifying the appropriate design variables. Component geometry plays an important role in many problems. Topology and topography optimization offer great concepts, but even the most promising new designs need fine-tuning. This is where size, shape, and free-shape optimizations take place.

Topology and topography optimization offer great concepts, but even the most promising new designs need fine-tuning. This is where size, shape, and free-shape optimizations take place.

4.2.1 Size optimization

Size optimization is commonly used to find optimal solutions for key product characteristics, such as: section thickness, material selection, and other part parameters. Designers look to form and free-shape optimizations to reduce the likelihood of product failure when initial concept analyse is reveals high stress concentration

Shape optimization strengthens the existing geometry by adjusting the height, length, or radius of the design and deforms the part to distribute stresses more evenly.

4.2.2 Free-shape optimization

Free-shape optimization provides additional flexibility by allowing designers to mark areas for compression reduction. The software then creates new and improved geometry for that area of the part. However, this increased degree of free-shape optimization in simulation comes with a trade-off. Free-shape optimization does not preserve small design

features such as fillets. Therefore, it is important to understand the detailed geometric constraints of your design to be able to confidently choose which tools to use for fine tuning.

4.2.3 Methods of Shape Optimization

A.The Eulerian approach to shape optimization

The Eulerian approach to shape optimization differs from the Lagrange approach by having nodes that do not move. Instead, the shape is contained within a rectangular "box" with an associated function describing and assigning values of "state" according to coordinates of the grid, which are fixed. The Eulerian approach was discussed in [125]**Hadamard's boundary variation method**

The shape optimization approach developed is a gradient-based method and uses the Hadamard's boundary variation method [126]. The gradient, called shape gradient, is computed by means of adjoint system method.

The shape optimization approach developed involves the differentiation with respect to the domain also called derivative in the sense of Hadamard [127][128].

4.3 Historic of isoperimetry

Isoperimetry (the study of geometric figures of equal perimeters) was a topic well embraced by the ancient Greeks. Isoperimetric problem on a surface is to enclose a given area with the shortest possible curve. The classical isoperimetric theorem asserts that in a plane the unique solution is a circle; we know that Greek mathematicians treated the isoperimetric proprieties of the circle and the sphere.

The first proof of the isoperimetric property of the circle is due to Zenodorus [130], who wrote a lost treatise on isoperimetric figures, known through the fifth book of the Mathematical Collection by Pappus of Alexandria. Zenodorus proved that among polygons enclosing a given area, the regular ones have the least possible length.

Isoperimetric problems restricted to a subclass of curves, for example triangles, rectangles, or n-sided polygons are of interest and appear throughout the early Greek literature.

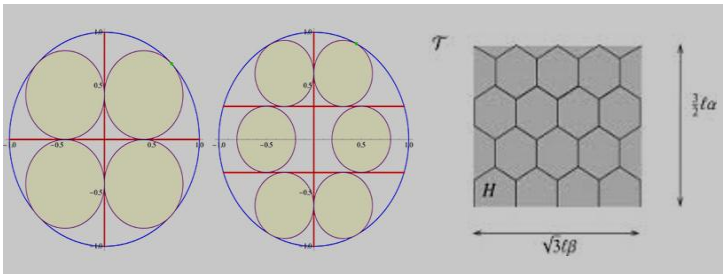

Figure 35 Isoperimetric Figures and Areas

4.4 Isoperimetric problems

Isoperimetric problems deal with relationship between area and perimeter of a planar region.

We'll take for granted the Jordan Curve Theorem [131], which says that a simple closed curve in the plane divides the plane into two regions, one compact and one non compact, and is the common boundary of both regions. When we talk of the region bounded by a simple closed curve in the plane, we'll always mean the compact region.

Irregular shapes (curves) make bees uncomfortable, so it means equilateral and equiangular regular shapes. Bees used their intelligences to concept a beehive that contained more honey, and chose the one that was the most angled for their work. Bees know a very useful fact that hexagons are greater than squares and triangles and absorb more honey for the same amount of material.

4.4.1 Types of isoperimetric problems

Theorem. Let C be a simple closed curve in the plane with length L and bounding a region of area A; Then:

$$\boldsymbol{L^2 \geq 4\pi A} \qquad \textbf{(21)}$$

with equality if and only if C is a circle.Thus, among all simple closed curves in the plane with a given length, the circle bounds the largest area.

The proof of the theorem discusses here can be found in[132]

Continuous Version: It is easy to show that for a fixed area, the rectangle with the least perimeter is a 2n-sided polygons.

Lemma. Among all 2n-sided polygons with the same length L, the regular 2n-gon has the largest area.

Existence of a maximize among such 2n-gons is evident, since the vertices may be restricted to a compact region of the plane, for example, a disk of radius L. Hence the set of such 2n-gons is itself compact, and since the area is a continuous function, it is certainly maximized.

There are several types of isoperimetric problems, let us take a look at some examples:

-Among the triangle, the square, the hexagon, with the same perimeter, the hexagon has the largest area.

-Among all rectangles of a given area, which rectangle minimizes the perimeter?

In [133] authors assumed that the optimal way to cover a large region with shapes of the same area while minimizing the perimeter is to use the hexagonal structure. This conjecture is proved by Thomas Hales [134] in according with this conjecture, bees know that the hexagonal shape of cells is the best will hold more honey and require less building wax.

Discrete Version: For a fixed area A, "minimal perimeter for a rectangle with integer sides" may be considered as the discrete analogue of the previous problem. Let x, y be two positive integers, consider x the width and y the length of a rectangle that has the given area A and a minimum perimeter. Then A can be represented as a product of x and y: $\mathrm{A} = \mathrm{xy}$ such that $\mathrm{x} \leq \mathrm{y}$ and$\mathrm{x} + \mathrm{y}$ is a minimum. As:

$$(x + y)^2 = (y - x)^2 + 4\mathrm{A} \qquad \textbf{(22)}$$

$(\mathrm{x} + \mathrm{y})$ is decreasing if and only if $(\mathrm{y} - \mathrm{x})$ is so. Hence the answer of the discrete version is the unique pair (x, y) such that $\mathrm{A} = \mathrm{xy}$, $\mathrm{x} \leq \mathrm{y}$ and $\mathrm{y} - \mathrm{x}$ is minimal. To prove the uniqueness of the pair (x, y), suppose that $\mathrm{A} = \mathrm{xy} = \mathrm{x'y'}$, as the minimum is unique, $\mathrm{y} - \mathrm{x} = \mathrm{y}' - \mathrm{x}' = \mathrm{S}$, so (x, y), (x', y') verify:

$$\begin{cases} y + (-x) = S \\ y(-x) = -A \end{cases} \quad \textbf{(23)}$$

$$\begin{cases} y' + (-x') = S \\ y'(-x') = A \end{cases} \quad \textbf{(24)}$$

and$(-x, y)$, $(-x', y')$ are the roots of the same equation,

$$\mathrm{x}^2 - \mathrm{S}x - \mathrm{A} = 0 \quad \textbf{(25)}$$

so: $$(x, y) = (x', y') \quad \textbf{(26)}$$

In the (section 5.2), we presented our contribution as new factorization algorithm to compute the pair (x, y).

4.5 Key generation: Vendermond matrix

4.5.1 Invertible Matrix

In linear algebra, a square n-by-n matrix is said to be invertible (non singular or non degenerate) if the product of the matrix and its inverse is the identity matrix.

4.5.2 Self-Invertible Matrix Encryption

A is called a self-invertible matrix if $K = K^{-1}$.

The authors of [135]suggests efficient methods for generating self-invertible matrix for Hill Cipher algorithm. The analysis for generation of self-invertible key matrix is valid for matrix of positive integers, that are the residues of modulo arithmetic of a number.

In 1929 Hill proposed an encryption algorithm using self-invertible matrices [136]. The basic theory of the algorithm is to use a matrix to convert plain-text into cipher-text, and the key is the matrix itself. The encryption method is described as:

$$C = KM(mod\ R) \quad \textbf{(27)}$$

Where; M is a plain-text matrix, C is a cipher-text matrix, R is a range of plain-text values (R=256 in image encryption processing), K is an encryption key, and matrix K must be an invertible matrix. becomes a matrix. The Hill encryption algorithm is uncompressed, the encryption formula is detailed in [137].

4.5.3 Vendermond matrix

A matrix whose rows (or columns) consist of monomials of successive powers is called a Vandermonde matrix and can be used to describe several useful concepts and has properties that can be used to solve many types of problems.

A Vandermonde matrix has the property that it is a matrix that is always invertible modulo p and therefore the corresponding linear system of congruence equations has a unique solution. An example of this was shown in [138] for implementation of Shamir's scheme that is using both interpolating polynomials and linear system of congruence equations.

The Vandermonde matrices are an essential topic in applied mathematics, natural science and engineering. a few examples are cited in [139][140]. they appear in the fields of numerical analysis, mathematical finance, statistics, geometry of curves and control theory. Moreover, Vandermonde matrices have gained much interest in wireless communications due to their frequent appearance in numerous applications in signal reconstruction, cognitive radio, physical layer security, and MIMO channel modelling.

Definition. The Vandermonde matrix is a matrix that is always invertible. It is an $n \times m$ matrix of the form :

$$V_{mn}(x_n) = \left[x_j^{i-1}\right]_{i,j}^{m,n} = \begin{bmatrix} 1 & & 1 & \cdots & 1 \\ & \vdots & & \ddots & \vdots \\ x_1 & & x_2 & \cdots & x_n \\ x_1^{m-1} & x_2^{m-1} & & \cdots & x_n^{m-1} \end{bmatrix}$$

where $x_i \in \mathbb{C}$, $i = 1, \ldots, n$. If the matrix is square, $n = m$, the notation $V_n = V_{nm}$ will be used.

To show the usefulness of the proposed scheme for image we need the following Proposition.

Proposition.

$$\text{Let } V=\begin{pmatrix}\alpha_1\\ .\\ \alpha_n\end{pmatrix}\in\left(\frac{Z}{256Z}\right)^n \sum_{i=1}^{256}\alpha_i^{\,2}\equiv 2 \tag{29}$$

such that: $\sum_{i=1}^{256}\alpha_i^{\,2}\equiv 2$, put $A=(V.V^t)$ where V^t is the transpose of V and I_n the identity matrix of order n, then $K=A-I_n$ is orthogonal $(K=K^t)$ and involutory $(K=K^{-1})$.

Proof. We have:

$$A^2=V.(V^t.V).V^t=(V^t.V).(V.V^t)=\mathbf{2A} \tag{30}$$

$$V^t.V=\sum_{1}^{n}\alpha_i^2\equiv 2[256] \tag{31}$$

Hence ;

$$K^2=(A-I_n)^2=\ A^2-2A+\ I_n=I_n \tag{32}$$

that is, K is involutory $(K\ =\ K\ -1\ )$, K is orthogonal because:

$$K^t=(A-I_n)^t=A^t-I_n=K \tag{33}$$

Since the Vandermonde self-invertible matrix is used as the key matrix, the in verse of the key matrix always exists and there is no need to compute the inverse of the key matrix while decrypting the cipher-text. This helps reduce the computational complexity associated with the process of finding the inverse of the key matrix.

Chapter 5. CONTRIBUTION

5.1 Introduction

In this section, an integer decomposition is combined with a hexagonal representation to obtain a new secret sharing scheme. Consider the scenario in which a dealer D or Trusted Center (TC) splits a secret S into n pieces, and to increase the security, he uses a symmetric encryption E, and then, he sends the shares to participants P_1, ..., P_n

For the reconstruction phase, the combiner C (trusted party) or a dictatorial participant (if the SSS possess a such participant) takes the key K submitted by the dealer and collects shares sent from an authorized subset A, the secret will be obtained and returned to each participant in A.

5.2 Proposed factorization(QSD)

In this subsection, we introduce the proposed decomposition, which is the major building block of our scheme. According to the previous subsection, we obtain the following factorization.

Proposition 5.2. For every natural number A there is a unique decomposition into two factors x and y such that: $A = xy$, such that $x \leq y$ and $y - x$ is minimum. The obtained decomposition is called **"Quasi Square Decomposition",** or **(QSD)**.

Proof.

-Put $m = [\sqrt{A}]$ (the integer part of the root square of A).

-Let $E = \{i \in \mathbb{N}: m - i divides A\}$. E is not empty because $i = m - 1 \in E$.

-As E is a subset of $\mathbb{N}$, it has a least element i_0, then:

$$A = (m - i_0)\, h \tag{34}$$

-Put $x = m - i_0$ and $y = h$, by definition of x, $x \leq \sqrt{A}$.

We have $\sqrt{A} \leq y$, (else $y < \sqrt{A}$ and $x \leq \sqrt{A}$ imply $xy = A < A$), so $x \leq y$.

As x is the largest divisor of A smaller than m, $y - x$ is minimal.

To prove the uniqueness of the quasi-square decomposition suppose we have two decompositions of $A = xy = x'y'$ According to **(**section 4.4.1**)** and the equation (26), we have: $(x, y) = (x', y')$.

Algorithm of QSD

Input: Natural number A.

Output: QSD of A.

(1) Compute $m = [\sqrt{A}]$ (the integer part of square root of A) and (x, y) = (1, A)

(2) For i =0,...,m-1

(a) Test if m - i divides A ?

(a1) If no, increment i by 1 ,

(a2) If yes, write $x = m - i,\ y =$ A/x and exit the loop For,

Return: x, y

Table 2 Quasi Square DecompositionAlgorithm

According to this algorithm, we have:

$$x \leq [\sqrt{A}] = m. \quad \textbf{(35)}$$

Remark. It is known that Fermat's Factorization is based on the representation of an odd integer n as the difference of two squares but this factorization is not unique: For example, let n = 105, then:

With Fermat's Factorization

$$105 = 11^2 - 4^2 = (11 - 4)(11 + 4) = 7 \times 15$$
$$= 11^2 - 8^2 = 5 \times 21$$
$$= 19^2 - 16^2 = 3 \times 35$$

With QSD Factorization Algorithm

$\left|\sqrt{105}\right|$=10, from 0 to 9, we get 7 divides 105, then $x = 7$ and $y = 15$.

$105 = 7 \times 15$ (Unique solution).

The uniqueness of the QSD decomposition is required for the use in encryption of secret sharing.

5.3 Bioinspired Hexagonal Structure of SSS

In this Hexagonal secret sharing, a set of participants is partitioned into disjoint levels. So, participant at first levels have more importance than the others. so, each level i contain 2^i shareholders see (figure 36).

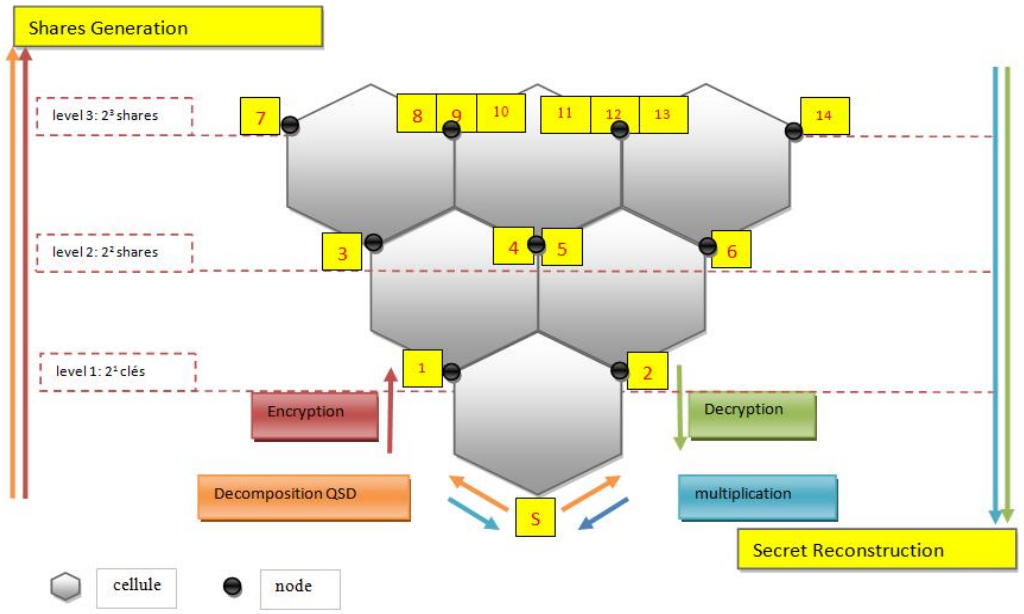

Figure 36 Bioinspired Hexagonal secret sharing scheme

In biology the first concern of bees is to cover the area in order to pave the space; among several regular polygons which serve to pave the plan and offer the smallest perimeter is the hexagon as detailed in (Chapter 3). inspiring of this idea, the design of our scheme after decomposition, and encryption is based on the hexagonal structure that give us a diagram with the starting point of up to Several levels with the following proprieties:

-In level i we have exactly 2^i participants;

-Paving space: nodes sharing (sharing of space between the distant participants);

-Possibility to distribute multiple shares to a trusted person (more than a single share in a node);

-The hierarchy of levels (several choices of distribution of participants according to several levels;

-Several path back to the secret (variation of the access structures).

The (figure 36) representing the general model with distribution phase and reconstruction phase is detailed in the next sections.

5.4 Secret sharing scheme (general case)

Let $\mathbb{N}$ denote the set of all natural numbers and Q, Pr_1, Pr_2, be the mappings defined by :

Q: $\begin{matrix}\mathbb{N} & \longrightarrow \mathbb{N}\times\mathbb{N} \\ A & (\mathrm{x},\mathrm{y})\end{matrix}$ with $A = xy$ is the QSD of A defined in (section5.2).

$$\mathrm{Pr}_1\colon \begin{matrix}\mathbb{N}\times\mathbb{N} & \longrightarrow \mathbb{N} \\ (x,y) & \mathrm{x}\end{matrix} \quad \text{and} \quad \mathrm{Pr}_2\colon \begin{matrix}\mathbb{N}\times\mathbb{N} & \longrightarrow \mathbb{N} \\ (x,y) & \mathrm{y}\end{matrix}.$$

Consider $E : \mathbb{N} \longrightarrow \mathbb{N}$ an encryption function and denote by E^{-1} the corresponding decryption function. Put:

$$\psi_1 = E\ o\ \mathrm{Pr}_1 o\ \mathrm{Q} \tag{36}$$

$$\psi_2 = E\ o\ \mathrm{Pr}_2 o\ \mathrm{Q} \tag{37}$$

Assume that a dealer D and combiner C share the same key K. Let $S \in \mathbb{N}$ be a secret.

5.4.1 Distribution phase

Step 1) First, to compute $\mathrm{S}_1^1 = \psi_1(\mathrm{S})$ the dealer applies the QSD to S, S_1^1 is the encryption by E of the first component, while $\mathrm{S}_1^2 = \psi_2(\mathrm{S})$ is the encryption of the second component, then D obtains two shares in the first level.

Step 2) In order to obtain the shares in level 2 the dealer D computes:

$$\mathrm{S}_2^1 = \psi_1\left(\mathrm{S}_1^1\right),\ \mathrm{S}_2^2 = \psi_2\left(\mathrm{S}_1^1\right) \tag{38}$$

$$S_2^3 = \psi_1(S_1^2),\ S_2^4 = \psi_2\ (S_1^2) \tag{39}$$

D repeats the same operations until reaching the desired level, (Figure 37).

In the general case, for S_n^i, n indicates the level and i is the index that specifies the position of the share in the level n.

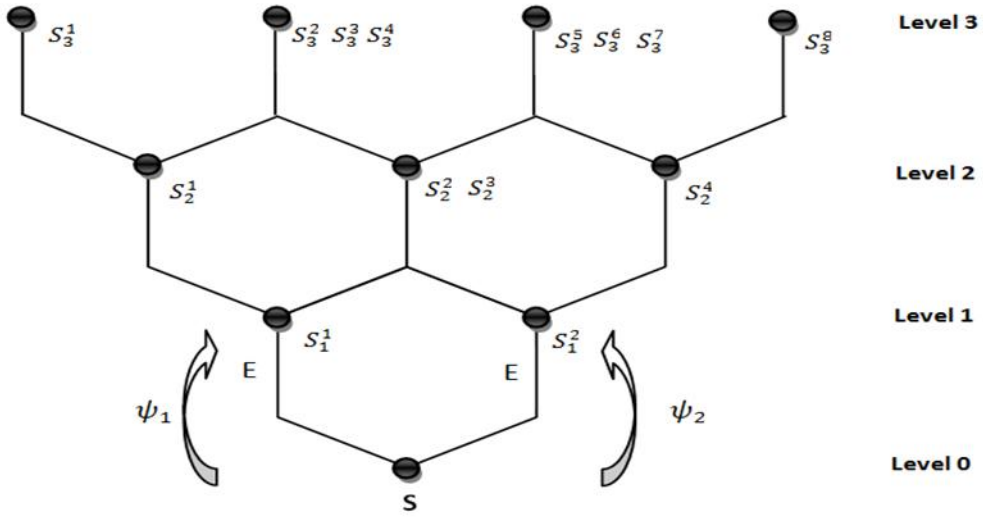

Figure 37 Hexagonal structure of the secret sharing scheme in three levels (construction phase)

-In the level n there are $n+1$ nodes: $N_0, N_1, \cdots, N_n$.

-In the node N_k , there are:

$$C_n^k = \frac{n!}{k!(n-k)!} \tag{40}$$

shares, so the number of shares constitute the Pascal's Triangle:

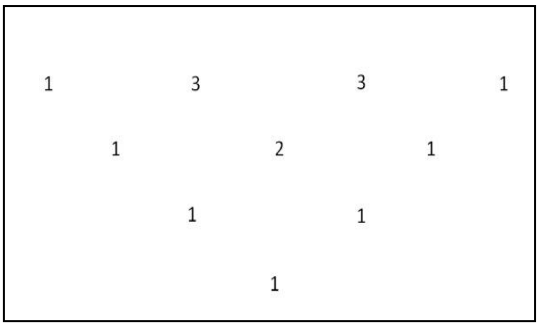

Figure 38 Pascal's Triangle

-Then in the level n, there are 2^n participants:

$$\sum_{k=0}^{n} |N_k| = C_1^0 + \cdots + C_n^n = 2^n \quad \textbf{(41)}$$

5.4.2 Reconstruction phase

To reveal the secret S that was distributed by the dealer D,

Step 1) It is assumed, for example, that the dealer sends the shares to participants up to level n, then:

$$|\mathrm{P}| = 2 + \cdots + 2^{\mathrm{n}} = 2^{\mathrm{n}+1} - 2 \quad \textbf{(42)}$$

where P denotes the set of all participants.

Step 2) An authorized set sent their shares to a combiner C. using the key K the combiner C consider the transition from one level to a lower level:

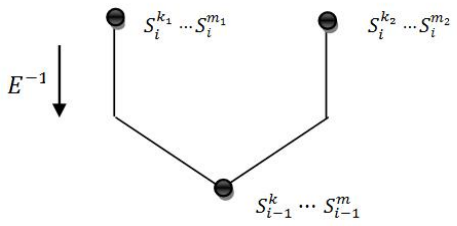

Figure 39 Transition to lower level

Where:

$$S_i^{k_1} = \psi_1\left(S_{i-1}^k\right),\ S_i^{k_2} = \psi_2\left(S_{i-1}^k\right) \tag{43}$$

Step 3)C computes:

$$S_{i-1}^k = E^{-1}\left(S_i^{k_1}\right)E^{-1}\left(S_i^{k_2}\right) \tag{44}$$

$S_i^{k_2}$ is called the homologous share of $S_i^{k_1}$;

Step 4) The combiner repeats the process until reaching the level 0 and obtains the secret

An illustrative example will be provided in the next section.

5.5 Secret sharing scheme for Digital Image

In this section, we describe the application of the proposed method to the secret image sharing. The secret image can be reconstructed by combining the sufficient number of shares together. The process responsible for share generation is called the 'dealer' and share reconstruction is called 'combiner'.

First, we recall the definition of Shur product (or Hadamard product):

Let $A = \left(a_{ij}\right)$ and $B = \left(b_{ij}\right)$ be two $k \times n$ matrices, the Shur product of A and B, denoted $A \odot B$, is defined by:

$$(A \odot B)_{ij} = \left(a_{ij}\right)\left(b_{ij}\right) \tag{45}$$

The proposed scheme consists of two phases: distribution phase and recovery phase.

5.5.1 Distribution phase

Input: A grayscale secret image S of size $m \times m$; (for tests we take $m = 256$).

Output: Generate shadows up to level n.

Step 1) According to the subsection (4.5.3), generate an orthogonal involutory matrix K of

order m.

Step 2) Perform the QSD to matrix S: $S = S_1 \odot S_2$ where $(S_1)_{ij} \leq [256] = 16$ and $(S_1)_{ij} \leq (S_2)_{ij}$.

Step 3) Generate a random binary sequence R of length m.

Step 4) Use the random sequence $R = (R_i)_{1 \leq i \leq m}$ to balancing the elements of the two matrices S_1 and S_2 , indeed, if $R_i = 1$ we permute between the i^{th} column of S_1 and the i^{th} of S_2. If $R_i = 0$ the corresponding columns remain unchanged.

so $S = S_1 \odot S_2$ is replaced by $S = S_1^* \odot S_2^*$.

Step 5) Encrypt $S_i^*, i = 1,2$ by $S_i^{**} = K S_i^* K = E(S_i^*)$, put $S_1^1 = S_1^{**}, S_1^2 = S_2^{**}$

Step 6) Repeat Step 2) through Step 5) for $S_i^{**}, i = 1,2$.

Step 7) Repeat the process until the desired level.

Remarks:

-In this system we used one key K but for more security we can use a key K_i at each level i.

-To have a good balancing for the elements of the two matrices S_1, S_2 we have chosen a random sequence because it has a nearly equal number of 1's and 0's, so for example, this sequence can be generated by LFSR [141] (Linear feedback shift Register).

Hence, each level requires the decomposition QSD, a balancing and encryption.

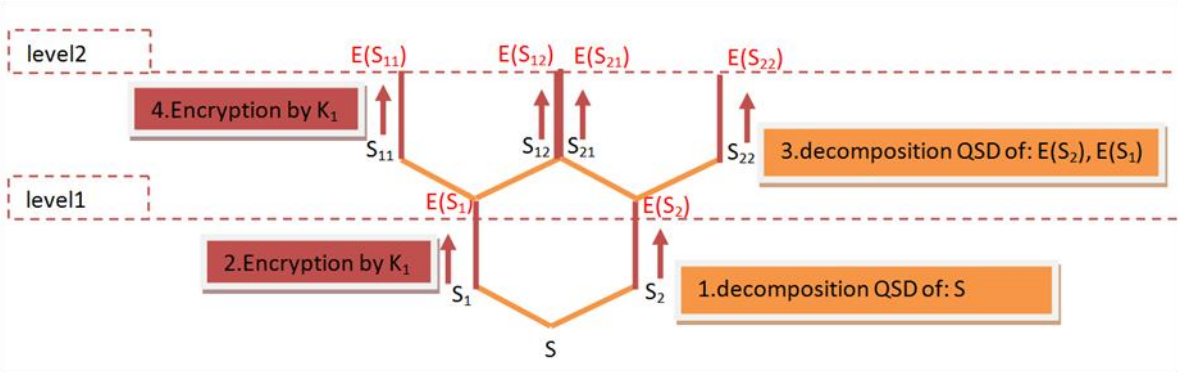

Figure 40 Geometric representation of Sharing Phase

5.5.2Reconstruction phase

Given an authorized set of participants in level n, how to recover the image secret S?

Let $M_n\left(\frac{\mathbb{Z}}{256\,\mathbb{Z}}\right)$ denote the set of $n \times n$ matrices with entries in $\frac{\mathbb{Z}}{256\,\mathbb{Z}}$ .The encryption function E is defined by :

$$E: M_n\left(\frac{\mathbb{Z}}{256\,\mathbb{Z}}\right) \rightarrow M_n\left(\frac{\mathbb{Z}}{256\,\mathbb{Z}}\right), E(A) = KAK \tag{46}$$

As K is involutory $(K^{-1} = K)$, $E^{-1} = E$. Define the mapping:

$$\varphi: M_n\left(\frac{\mathbb{Z}}{256\,\mathbb{Z}}\right) \times M_n\left(\frac{\mathbb{Z}}{256\,\mathbb{Z}}\right) \rightarrow M_n\left(\frac{\mathbb{Z}}{256\,\mathbb{Z}}\right) \tag{47}$$

by:

$$\varphi(X, Y) = E^{-1}(X) \odot E^{-1}(Y) = (K\,X\,K) \odot (K\,Y\,K) \tag{48}$$

Hence:

-for $n = 1$ we have $S = \varphi\left(s_1^1, s_1^2\right)$;

-for $n = 2$ we have $S = \varphi(\varphi\left(s_2^1, s_2^2\right), \varphi\left(s_2^3, s_2^4\right))$;

-for the general case we use the transition to a lower level

with:

$$S_{i-1}^{k} = \varphi\left(s_i^{k_1}, s_i^{k_2}\right) = \left(K\, S_i^{k_1}\, K\right) \odot \left(K\, S_i^{k_2}\, K\right) \quad \textbf{(49)}$$

This process is repeated until reaching the level 0.

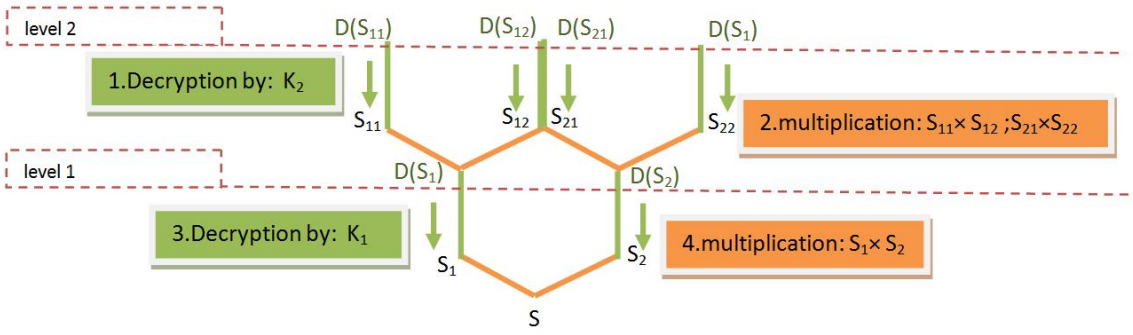

Figure 41 Geometric representation of reconstructing secret Phase

5.6 Experimental results, analysis and discussions

5.6.1 Simulation

The security of the proposed scheme is based on the security of the secret image; we applied the proposed method on two kinds of standard grayscale images with the size of 256×256.

We consider two scenarios:

5.6.1.1 Case of one level.

Level 1: When $P = \{P_1, P_2\}$, for the distribution phase we apply the QSD to the secret image S: $S = S_1 \odot S_2$ we use a random binary sequence R to balance the elements of the two components: $S = S_1^* \odot S_2^*$ and we encrypt S_1^* and S_2^* by:

$$S_i^{**} = \mathrm{E}(S_i^*) = K\, S_i^* K,\ i = 1,2 \quad \textbf{(50)}$$

Then $S_1^1 = S_1^{**}$, $S_1^2 = S_2^{**}$ are the two image shadows, (Figure 42):

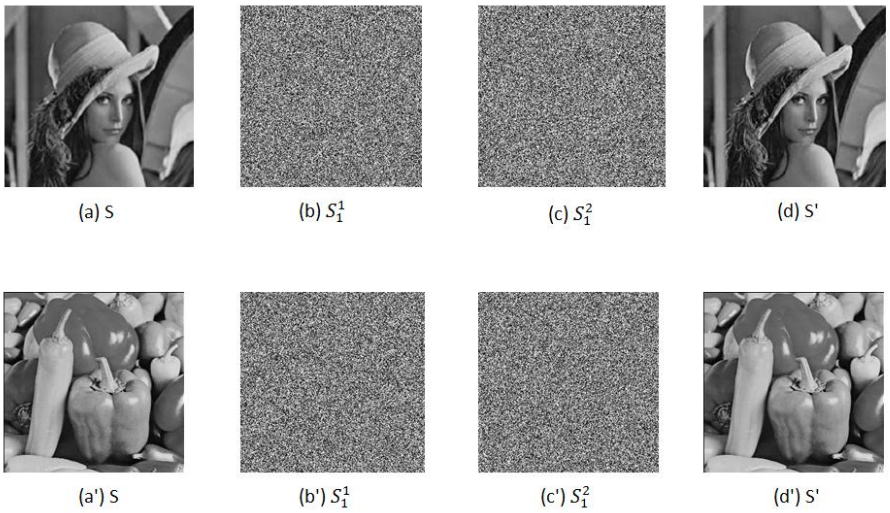

Figure 42 The secret image S, the two shadow images, and the reconstructed image.

For the recovery phase we have:

$$S' = \left(K\, S_1^1\, K\right) \odot \left(K\, S_1^2 K\right). \tag{51}$$

5.6.1.2 Case of two levels.

Here we consider the case where the dealer sends the shares to participants until up the level 2, hence, the SSS has 6 participants and 4 qualified subsets: $|P| = 6, |\Gamma| = 4$, (figure 43).

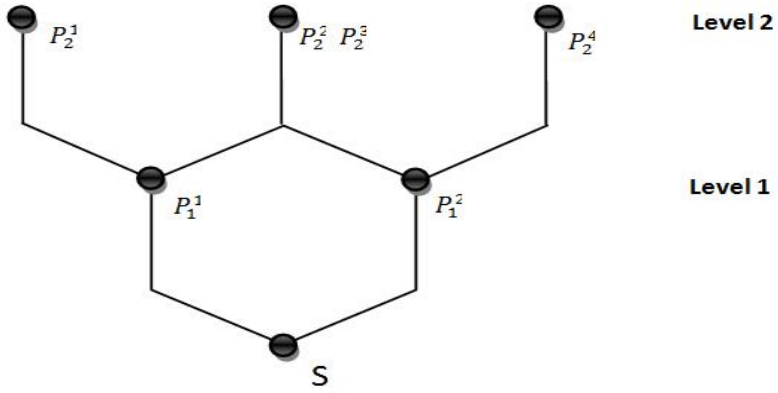

Figure 43 Hexagonal structure of the SSS with two levels

$P = \{P_1^1, P_1^2, P_2^1, P_2^2, P_2^3, P_2^4\}$

$\Gamma = \{\{P_1^1, P_1^2\}, \{P_1^1, P_2^3, P_2^4\}, \{P_2^1, P_2^2, P_1^2\}, \{P_2^1, P_2^2, P_2^3, P_2^4\}\}$

We have already calculated S_1^1 and S_1^2, to compute S_2^1 and S_2^2 we repeat the same operation to S_1^1 (QSD, balancing and encryption). In the same way we obtain S_2^3 and S_2^4. (Figure 44) shows the four image shadows: $S_2^1, S_2^2, S_2^3, S_2^4$.

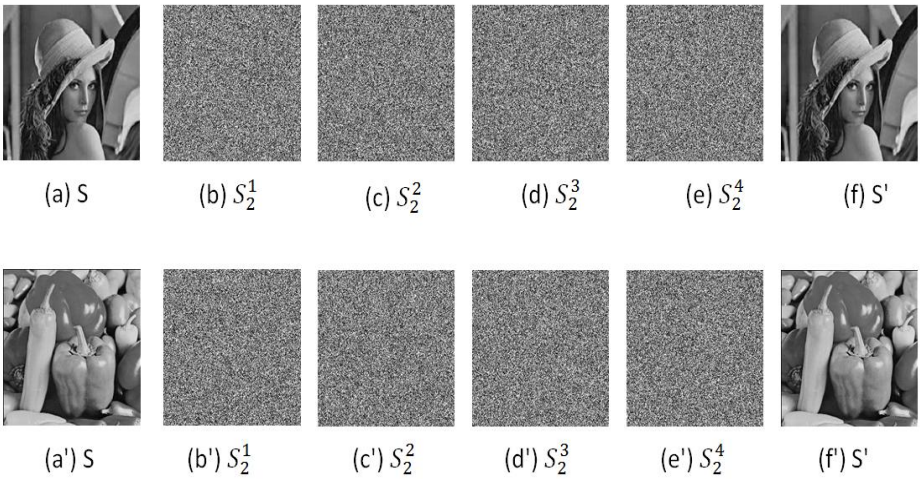

Figure 44 secret image, the four shares images, and the recovered image.

For the recovery phase, for example, we will deal with the qualified subset $\{P_2^1, P_2^2, P_2^3, P_2^4\}$, and then the recovered image is:

$$S' = \varphi\left(\varphi(S_2^1, S_2^2), \varphi(S_2^3, S_2^4)\right) = K[(K\,S_2^1\,K) \odot (K\,S_2^2\,K)]K \odot K[(K\,S_2^3\,K) \odot (K\,S_2^4\,K)]K \quad \textbf{(52)}$$

The simulation results are shown in (Figure 44).

5.6.2 Security analysis

To highlight the security of proposed system, we present some statistical analysis.

5.6.2.1 Statistical analysis

For examining the resistance of our scheme against statistical attacks, we use the correlation, histogram and entropy tests.

Correlation test: Correlation deal with the relation of neighbouring pixels in vertical, horizontal and diagonal directions, for most images, the adjacent pixels are correlated to

each other, while for shadow images, (Table 3) shows that the value of correlation of adjacent pixels is close to zero, this guarantees the confusion and diffusion of pixels.

	Lena S	S_1^1	S_1^2	S_2^1	S_2^2	S_2^3	S_2^4
Horizontal	0.9602	-0.0018	0.0009	0.0035	-0.0050	-0.0040	-0.0019
Vertical	0.9815	-0.0013	0.0066	-0.0021	-0.0029	-0.0101	-0.0033
Diagonal	0.9407	-0.0061	-0.0061	0.0028	-0.0029	-0.0057	-0.0015
	***Paper* S**	S_1^1	S_1^2	S_2^1	S_2^2	S_2^3	S_2^4
Horizontal	0.9478	-0.0056	-0.0003	0.0055	-0.0057	0.0056	-0.0006
Vertical	0.9482	-0.0018	-0.0056	-0.0027	0.0066	0.0014	-0.0007
Diagonal	0.9036	-0.0001	0.0029	-0.0029	-0.0100	0.0001	-0.0011

Table 3 Correlation coefficients of adjacent pixels for the shares and original images.

Similarity between secret images $S = (S_{ij})$ and recovered image $S' = (S'_{ij})$ is done using correlation coefficient:

$$R = corr2(S, S') = \frac{\sum_i \sum_j (S_{ij} - \overline{S}\ )(S'_{ij} - \overline{S'})}{\sqrt{\sum_i \sum_j (S_{ij} - \overline{S}\ )^2} \sqrt{\sum_i \sum_j (S'_{ij} - \overline{S'})^2}} \quad \textbf{(53)}$$

Where $\overline{S}$ = mean (S) , and $\overline{S'}$ = mean (S') and $corr2(S, S')$ is MATLAB command. (Table 4) shows that $corr2(S, S') = 1$ and $corr2(S, S_j^i)$ is close to 0, that is, S and S' are absolutely identical and S and shadows are uncorrelated.

	S_1^1	S_1^2	S_2^1	S_2^2	S_2^3	S_2^4	S'
Lena S	0.0076	-0.0040	-0.0033	-0.0012	0.0060	0.0010	1
Paper S	-0.0033	0.0038	0.0081	0.0022	4.0.392e-04	-9.4477e-04	1

Table 4 Correlation between secret image, shares and reconstructed image.

We have also $S - S' = 0$, this means that the proposed scheme is lossless.

According to (Table 4), the shadow S_j^icannot reveal any information about the secret image S.

Histogram test: The histogram represents the frequency of intensity value of each pixel. The (Figure 45) shows the histograms of original image, shadows and the reconstructed image.In a good scheme, the histogram of shadows should satisfy the uniform distribution; according to (Figure 45) the histograms of shadows are almost uniform.

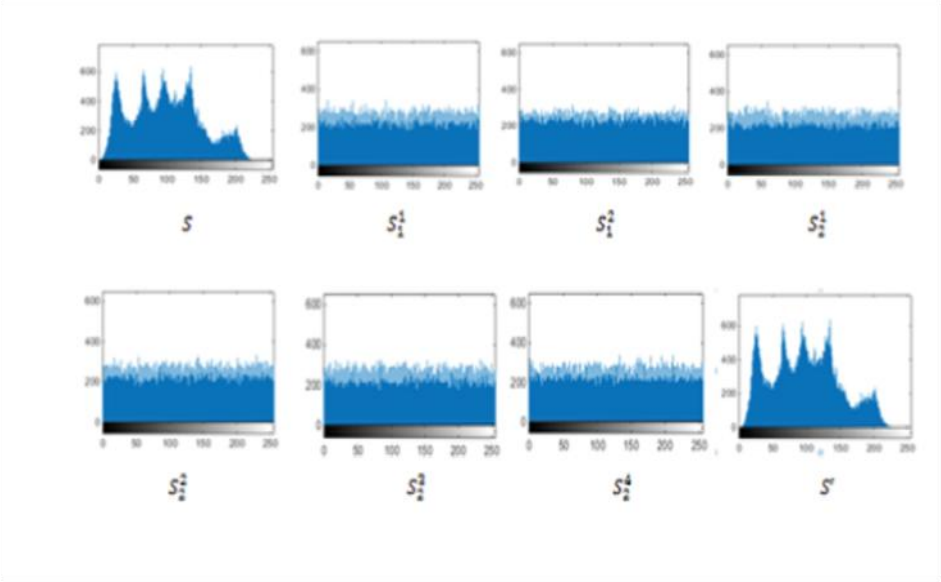

Figure 45 Histograms of Lena, shares and the reconstructed image

Entropy test: The information entropy is used to compute randomness in the image. When the entropy is nears to its ideal value 8 the image is said to be random. (Table 5) shows entropy results for secret image, shadows and reconstructed image.

Entropy	S	S_1^1	S_1^2	S_2^1	S_2^2	S_2^3	S_2^4	S'
Lena	7.5633	7.9918	7.9897	7.9931	7.9898	7.9923	7.9921	7.5633
Paper	7.5333	7.9917	7.9917	7.9929	7.9909	7.9854	7.9923	7.5333

Table 5 Entropy of secret image, shares and reconstructed image.

(Table 5) illustrates that the entropy value of the shadows is so close to 8, so the proposed scheme can resist the entropy attack.

5.6.2.2 Key space analysis.

Let $c_1, \dots, c_{255} \in \frac{Z}{256\,Z}$ such that: $c_1^2 + \cdots + c_{255}^2 = 1$

Put:

$$V = \begin{pmatrix} c_1 \\ \vdots \\ c255 \\ c_{256}=1 \end{pmatrix}, \text{ then } \sum_{i=1}^{256} {c_i}^2 = 2 \qquad \textbf{(54)}$$

according to (section 4.5.3) the matrix $K = VV^t - I_{256}$ is orthogonal and involutory, then the cardinality of the space of $K$is greater than the number of solutions of the equation (55).

To evaluate the space of the key K, we will use (lemma 2) in[143], indeed, for three positive integers: n, k, λ

Put:

$$\rho_{k,\lambda}(n) = card\{(x_1, \cdots, x_k) \in \left(\frac{Z}{nZ}\right)^k : x_1^2 + \dots + x_k^2 \equiv \lambda \ (mod\ n)\} \qquad \textbf{(55)}$$

Lemma 2 shows that for $(s \geq 3)$ and odd numberλ,

$$\rho_{k,\lambda}(2^s) = 2^{(s-3)(k-1)}\,\rho_{k,\lambda} \quad \textbf{(56)}$$

If we take $s = 8$, k= 255, $\lambda = 1$, we obtain:

$$\rho_{255,1}(256) = 2^{5(254)} \cdot \rho_{255,1}(8) > 2^{1270} \quad \textbf{(57)}$$

Hence, the construction of K provides at least 2^{1270} combinations. Thus, the size of key space is greater than 2^{1270} so the brute force attack is infeasible.

5.6.2.3 Chosen plain image attack

The distribution algorithm is probabilistic, because it uses randomness in balancing step while the recovery algorithm is deterministic, and the random permutation is not required in this case. When we apply the distribution algorithm twice to the same image we obtain different sharing, hence, the proposed scheme resists chosen plain image attack.

5.7 The cardinality of access structure

In this subsection, we will focus on the cardinality of the access structure Γ when the secret sharing scheme has participants until up to level n. To calculate easily the cardinality of Γ we permute the positions of participants such that every participant is near its homologous: (S_i^{k1}, S_i^{k2}).

After this permutation the (figure 43) is replaced by the following (figure 46):

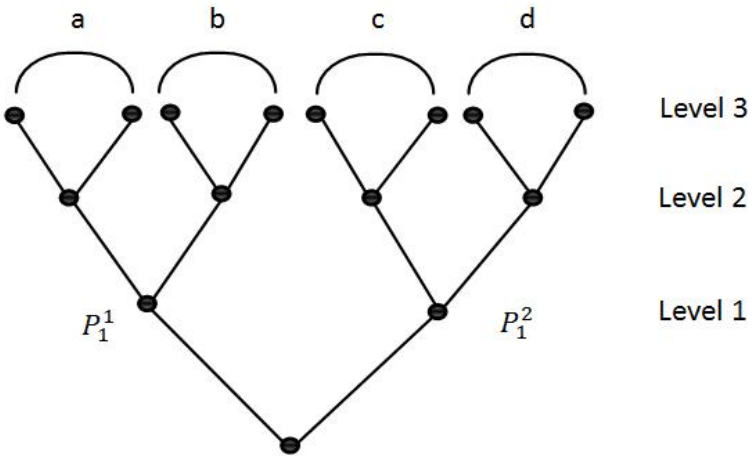

Figure 46 Binary form of the hexagonal structure of SSS used to calculate the Access structure cardinality

A.For level 1: n=1 there is one qualified subset, namely the pair (P_1^1, P_1^2),

$|\Gamma| = a_1 = 1$.

B.For n=2, we previously showed that $|\Gamma| = a_2 = 4 = 2^2$.

C.For n=3, we discuss according to c the number of pair at level n, then $c \in \{0,1,2,3,4\}$.

D.If $c = 4$, there is one qualified subset: $c_4 = 1$

E.if $c = 3$, $c_3 = 4$: abc P_2^4 , abP_2^3d, a P_2^2cd, P_2^1 bcd, and in the same way we obtain:

F.if $c = 2$, $c_2 = 8$

G.if $c = 1$, $c_1 = 8$

H.if$c = 0$, $c_0 = 4$, hence $|\Gamma| = a_3 = 1 + 4 + 8 + 8 + 4 = 25$.

I.For n=4 the number c of pairs at level 4 varies between 0 and 8, using the same method we obtain the following results:

C	0	1	2	3	4	5	6	7	8
c_i	25	80	144	168	138	82	32	8	1

Table 6 Table of Access structure cardinality

Then:$|\Gamma| = a_4 = \sum_0^8 c_i = 676 = 26^2$.

Generally, a_n verifies the recursive formula:

$$a_{n+1} = (a_n + 1)^2 \quad \textbf{(58)}$$

with: $a_0 = 0$, so:

$$\underbrace{a_n = \left(\cdots\left(((0+1)^2+1)^2+1\right)^2\cdots+1\right)^2}_{n\ squares} \quad \textbf{(59)}$$

and the cardinality of access structures :1,4,25,676, 458329, ..., a_n, ... grows faster when the number of participants increases.

5.8 Comparison and concluding remarks on the security of the proposed scheme

-In [58], the size of shares is greater than the size of secret while our scheme is ideal and has no pixel expansion.

-In [144], the quality of recovered image increases by growing the number of shares but for the proposed system, there is no loss in the recovered image.

-According to results of histograms, information entropy and correlation tests, the security in level 2 is better than the security in level 1.

-Our scheme can detect cheating and identify cheater while in the Shamir's scheme [46] a dishonest user may present a wrong share during the reconstruction phase, so that other users get an invalid secret while he exclusively obtains a valid secret.

The use of secret key K can add an additional security layer. To increase the randomness of the shadows and resist some attacks, diffusion, and confusion need to be introduced in proposed system, for this, we use permutation and orthogonal matrix respectively. The simulation results and the security analysis show that our method provides good security.

5.9 Properties of the proposed scheme

We assume both dealer and combiner are trusted. The proposed system has the following properties:

(1) It is **ideal**: share size is equal to secret size.

(2) Our scheme is **lossless**

(3) If the scheme has participants until up to level n, then for the access structure Γ we have rank:

$$(\Gamma) = 2, \{P_1^1, P_1^2\} \quad \textbf{(60)}$$

And the corank:

$$(\Gamma) = 2^n, \{P_n^1, \ldots, P_n^{2^n}\}. \quad \textbf{(61)}$$

(4) The proposed scheme **exhibits good statistical res**ults.

(5) Using an encryption function E increases the security of the proposed system.

(6) Our scheme is **perfect**: any non-qualified subset has no information about the secret, and the participants in the same node also cannot reveal any information about S because to reach the secret they have to cooperate with the combiner and go through several levels and apply gradually the mapping φ.

(7) In order to **prevent cheating**, and increase **authenticated ability**, we can add step 8 in the sharing algorithm. The dealer computes H_i^k the hash value of every share S_i^k and sends it to combiner. Hence the combiner could check the malicious behaviour of the participant by comparing H_i^k with the hash value of the share submitted by the participant. So, the combiner **detects cheatin**g and **identifies cheater.**

(8) The proposed system has the ability to **add or delete participants** without affecting the secret S, indeed, the addition and deletion operations are done **flexibly**, for example, consider the scheme which has participants until up to level n. To add a new participant the dealer splits a share S_n^k at level n into two shares at level $n+1$: $S_{n+1}^{k_1}, S_{n+1}^{k_2}$ by using the mappings ψ_1, ψ_2 respectively. He moves the participant P_n^k at position $\binom{k_1}{n+1}$ with

the share $S_{n+1}^{k_1}$ and assigns the new participant $P_{n+1}^{k_2}$ at position $\binom{k_2}{n+1}$with the share $S_{n+1}^{k_2}$. The participant S_n^k is implicitly rendered useless, then the dealer D updates N the number of participants to $N+1$ preserving the other shares and the secret S. In our scheme, the dealer can delete a member $P_n^{i_1}$ at level n and sends its share to combiner. In this case, its homologous$P_n^{i_2}$ becomes inactive and cannot be member of a minimal qualified subset, then the dealer updates N to $N-1$.

5.10 Final Discussion

In this paper, we proposed a new secret sharing scheme which is based on quasi-square decomposition and hexagonal structure. The use of QSD is significant tool of this paper. The solution of a discrete isoperimetric problem leads us to propose this novel integer decomposition called "QSD". The use of secret keys K_1, K_2 can add an additional security layer. To increase the randomness of the shadows and resist some attacks, diffusion, and confusion need to be introduced in the proposed system, for this, we use permutation and orthogonal matrix respectively. The proposed scheme has various properties, it is ideal, perfect, lossless scheme and it can detect and identify cheater. The security analyse is and the experimental results demonstrate that the proposed scheme has a good security: it uses a combination of confusion and diffusion and it is easy to implement and exhibits good statistical properties.

General Conclusion

In modern cryptography, the security of our data depends entirely on the security of the keys used. Most ciphers are public, so we can easily encrypt and decrypt messages if we know the keys involved. For some sensitive data, it's not always a good idea to have a single person to manage the keys and protect the data. This has lead to the requirement for Secret Sharing Schemes.

This project explores the concept of secret sharing and its trust features, and how this construct can be used in large organization or network to create safe accessible environments. In fact, a distributed secure system using secret threshold sharing can automatically adjust according to any organisation ability.

(k, n)-threshold SS schemes have been studied by many researchers for perfect SS schemes. But there are only a few constructions method that can be applied to a great cardinality of an access structure; Then they are much inefficient, compared with our proposed scheme, especially in the case that only in (n=5) levels with 32 shares we can get an access structure with cardinal closed to 458329.

Moreover, in this thesis, we proposed a new construction method of Secret Sharing schemes that attain almost all the security conditions: authentication, confidentiality, access control, and availability of the information.Furthermore; One of the specified conditions of a secret sharing scheme with proprieties, and extended capability is to be: Ideal, perfect, verifiable, flexible, and can detect and identify cheater; we aim to construct an efficient which attains all these proprieties and capabilities.

Inspiring from the nature, especially the structure of the beehives, and using the paradigm of the metaheuristic and the isoperimetric optimisation; We have designed our secret sharing scheme with extensible levels. In addition to this contribution, in the formal side, we proposed a new method of integer factorisation we called it Quasi Square Decomposition. In fact, we used this technique as one-way function to generate the shares of the secret, and the shares are also encrypted by the symmetric encryption techniques, and this phase makes the scheme to be stronger.

In this thesis, we applied bioinspired secret sharing scheme to the grayscale bitmap images as an extension, and the results show that the proposed scheme has a good security.

Bibliography

[1] Summers, R. C. (1984). An overview of computer security. *IBM systems journal*, *23*(4), 309-325.

[2] Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, *2*(5), 544-554.

[3] Jindal, G., Baranwal, S., & Memoria, M. (2019, March). Cryptography Using Multi-Dimensional Objects. In International Conference on Advances in Engineering Science Management & Technology (ICAESMT)-2019, Uttaranchal University, Dehradun, India.

[4] Delfs, H., Knebl, H., & Knebl, H. (2002). Introduction to cryptography (Vol. 2). Heidelberg: Springer.

[5] Kessler, G. C. (2003). An overview of cryptography.

[6] Baby, A., & Krishnan, H. (2017). Combined Strength of Steganography and Cryptography-A Literature Survey. International Journal of Advanced Research in Computer Science, 8(3).

[7] Desmedt, Y. (1998). Some recent research aspects of threshold cryptography. In Information Security: First International Workshop, ISW'97 Tatsunokuchi, Ishikawa, Japan September 17–19, 1997 Proceedings 1 (pp. 158-173). Springer Berlin Heidelberg

[8] Duan, Q., Wang, Y., Mohsen, F., & Al-Shaer, E. (2013). Private and anonymous data storage and distribution in cloud. In IEEE International Conference on Services Computing (SCC) (pp. 264–271). Santa Clara, CA, USA.

[9] Lin, H.-Y., & Tzeng, W.-G. (2012). A secure erasure code-based cloud storage system with secure data forwarding. IEEE Transactions on Parallel and Distributed Systems, 23(6), 995–1003. doi:10.1109/TPDS.2011.252

[10] Venukumar, V., & Pathari, V. (2016). A survey of applications of threshold cryptography—proposed and practiced. Information Security Journal: A Global Perspective, 25(4-6), 180-190.

[11] Yao, A. C. (1982, November). Protocols for secure computations. In 23rd annual symposium on foundations of computer science (sfcs 1982) (pp. 160-164). IEEE.

[12]Evans, D., Kolesnikov, V., & Rosulek, M. (2018). A pragmatic introduction to secure multi-party computation. Foundations and Trends® in Privacy and Security, 2(2-3), 70-246.

[13]Tillem, G., Burundukov, O., & Team, I. N. G. D. L. T. Threshold Signatures using Secure Multiparty Computation.

[14]Shoup, V. (2000). Practical threshold signatures. In Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19 (pp. 207-220). Springer Berlin Heidelberg.

[15]Boldyreva, A. (2003, January). Threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme. In Public Key Cryptography (Vol. 2567, pp. 31-46).

[16]Hwang, M. S., & Chang, T. Y. (2005). Threshold Signatures: Current Status and Key Issues. Int. J. Netw. Secur., 1(3), 123-137.

[17]Abdalla, M., Miner, S., & Namprempre, C. (2001). Forward-secure threshold signature schemes. In Topics in Cryptology—CT-RSA 2001: The Cryptographers' Track at RSA Conference 2001 San Francisco, CA, USA, April 8–12, 2001 Proceedings (pp. 441-456). Springer Berlin Heidelberg.

[18]Venukumar, V., & Pathari, V. (2016). A survey of applications of threshold cryptography—proposed and practiced. Information Security Journal: A Global Perspective, 25(4-6), 180-190.

[19]Basu, S., Karuppiah, M., Nasipuri, M., Halder, A. K., & Radhakrishnan, N. (2019). Bio-inspired cryptosystem with DNA cryptography and neural networks. Journal of Systems Architecture, 94, 24-31.

[20]Blackledge, J., Bezobrazov, S., & Tobin, P. (2015, July). Cryptography using artificial intelligence. In 2015 International Joint Conference on Neural Networks (IJCNN) (pp. 1-6). IEEE

[21]Klein, E., Mislovaty, R., Kanter, I., Ruttor, A., & Kinzel, W. (2004). Synchronization of neural networks by mutual learning and its application to cryptography. Advances in Neural Information Processing Systems, 17.

[22]Thabit, F., Alhomdy, S., & Jagtap, S. (2021). A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. International Journal of Intelligent Networks, 2, 18-33

[23]Naor, M., & Shamir, A. (1995). Visual cryptography. In Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13 (pp. 1-12). Springer Berlin Heidelberg.

[24]Ibrahim, D. R., Teh, J. S., & Abdullah, R. (2021). An overview of visual cryptography techniques. Multimedia Tools and Applications, 80, 31927-31952

[25]Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (2001). Extended capabilities for visual cryptography. Theoretical Computer Science, 250(1-2), 143-161.

[26]Weir, J., & Yan, W. (2010). A Comprehensive Study of Visual Cryptography. Trans. Data Hiding Multim. Secur., 5, 70-105.

[27]Randy Crane. Simplified approach to image processing : classical and modern techniques in C. Prentice Hall PTR, 1996

[28]Andreas Koschan andMongi Abidi. Digital color image processing. JohnWiley & Sons, 2008

[29]Pakshwar, R., Trivedi, V. K., & Richhariya, V. (2013). A survey on different image encryption and decryption techniques. International journal of computer science and information technologies, 4(1), 113-116

[30]Isha Mehra and Naveen K Nishchal. Optical asymmetric image encryption using gyrator wavelet transform. Optics Communications, 354 :344–352, 2015.

[31]Narendra Singh and Aloka Sinha. Optical image encryption using fractional fourier transform and chaos. Optics and Lasers in Engineering, 46(2) :117–123, 200.

[32]Dezhao Kong and Xueju Shen. Multiple-image encryption based on optical wavelet transform and multichannel fractional fourier transform. Optics & Laser Technology, 57 :343–349, 2014.

[33]Liansheng Sui, Kuaikuai Duan, Junli Liang, Zhiqiang Zhang, and Haining Meng. Asymmetric multiple-image encryption based on coupled logistic maps in fractional fourier transform domain. Optics and Lasers in Engineering, 62 :139–152, 2014.

[34]CK Huang, Chin-Wen Liao, SL Hsu, and YC Jeng. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommunication Systems, 52(2) :563–571, 2013.

[35]S Behnia, A Akhshani, H Mahmodi, and A Akhavan. A novel algorithm forimage encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals,35(2) :408–419, 2008.

[36]Edward Lorenz. Predictability : does the flap of a butterfly's wing in Brazil set off a tornado in Texasna, 1972.

[37]Yang Shuangyuan, Lu Zhengding, and Han Shuihua. An asymmetric image encryption based on matrix transformation. In Communications and Information Technology, 2004. ISCIT 2004. IEEE International Symposium on, volume 1, pages 66–69. IEEE, 2004

[38]Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda. Image encryption by novel cryptosystem using matrix transformation. In Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on, pages 77–81. IEEE, 2008

[39]Qiang Zhang, Ling Guo, and Xiaopeng Wei. Image encryption using dna addition combining with chaotic maps. Mathematical and Computer Modelling,52(11) :2028–2035, 2010.

[40]Noorul Hussain UbaidurRahman, Chithralekha Balamurugan, and Rajapandian Mariappan. A novel dna computing based encryption and decryption algorithm. Procedia Computer Science, 46 :463–475, 2015

[41]Pakshwar, R., Trivedi, V. K., & Richhariya, V. (2013). A survey on different image encryption and decryption techniques. International journal of computer science and information technologies, 4(1), 113-116

[42]Abdullah AH, Enayatifar R, Lee M (2012) A hybrid genetic algorithm and chaotic function model for image encryption. AEU Int J Electron Commun 66(10):806–816

[43]Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. Handbook of applied cryptography. CRC press, 1996..

[44]Ashley Walker Erik Wolfart Robert Fisher, Simon Perkins. Image processing learning resources explore with java. http://homepages.inf.ed.ac.uk/rbf/ HIPR2/hipr_top.

[45]Wyner, A. (1974). Recent results in the Shannon theory. IEEE Transactions on information Theory, 20(1), 2-10.

[46]Shamir, A. (1979) ' How to share a secret', Communications of the ACM, vol.22 No.11, pp. 612-613.

[47]Blakley, G. R. (1979) 'Safeguarding cryptographic keys', International Workshop on Managing Requirements Knowledge (MARK). IEEE,

[48]Xu, J. and Zha, X. (2007) 'Secret sharing schemes with general access structure based on MSPs', Journal of Communications, vol.2 No.1, pp. 52-55.

[49]Lein, H., Chingfang, H., Mingwu, Z., Tingting, H. and Maoyuan, Z. (2016) 'Realizing secret sharing with general access structure', Information Sciences, Vol. 367, 1 November 2016, pp.209–220. https://doi.org/10.1016/j.ins.2016.06.006.

[50]Kaboli R., Khazaei S., Parviz M. (2020). On ideal and weakly-ideal access structures. IACR Cryptol. 2020, 483 .

[51]Xu, G., Yuan, J., Xu, G., Jia, X. (2021). A New Multi-stage Secret Sharing Scheme for Hierarchical Access Structure with Existential Quantifier. Information Technology and Control, 50(2), 236-246

[52]De Souza, R. L., Vigil, M., Custódio, R., Caullery, F., Moura, L., & Panario, D. (2018, June). Secret sharing schemes with hidden sets. In 2018 IEEE Symposium on Computers and Communications (ISCC) (pp. 00713-00718). IEEE. Beimel, A. (1996). Secure schemes for secret sharing and key distribution.

[53]Padró, C., Vázquez, L., & Yang, A. (2013). Finding lower bounds on the complexity of secret sharing schemes by linear programming. Discrete applied mathematics, 161(7-8), 1072-1084

[54]Book, R. V. (1972). On languages accepted in polynomial time. SIAM Journal on Computing, 1(4), 281-287..

[55]Lin, T. (2021). Diagonalization $ of $ Polynomial-Time Turing Machines Via Nondeterministic Turing Machine. arXiv preprint arXiv:2110.06211.

[56]Nevai, P. (1984). Mean convergence of Lagrange interpolation. III. Transactions of the American Mathematical Society, 669-698.

[57]Blakley, G. R., & Kabatianskii, G. A. (1994). Linear algebra approach to secret sharing schemes. In Error Control, Cryptology, and Speech Compression: Workshop on Information Protection Moscow, Russia, December 6–9, 1993 Selected Papers (pp. 33-40). Springer Berlin Heidelberg.

[58]Shamsoshoara, A. (2019). Overview of Blakley's Secret Sharing Scheme. arXiv preprint arXiv:1901.02802.

[59]Kondracki, A. (1997). The chinese remainder theorem. Formalized Mathematics, 6(4), 573-577.

[60]Pei, D., Salomaa, A., & Ding, C. (1996). Chinese remainder theorem: applications in computing, coding, cryptography. World Scientific.

[61]Butson, A. T., & Stewart, B. M. (1955). Systems of linear congruences. Canadian Journal of Mathematics, 7, 358-368.

[62]Zhou, J., Hu, J., & Chen, P. (2010, December). Extended Euclid algorithm and its application in RSA. In The 2nd International Conference on Information Science and Engineering (pp. 2079-2081). IEEE.

[63]E. Brickell, and D. Stinson, “Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes”, Journal of Cryptology, vol. 5, no. 3, pp. 153- 166, 1992.

[64]G. Blakley, and G. Kabatianski, “On General Perfect Secret Sharing Schemes”, Advances in Cryptology-CRYPTO'95, vol. 963, pp. 367-371, 1995.

[65]C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, “Perfectly Secure Key Distribution for Dynamic Conferences”, Information and Computation, vol. 146 , no. 1, pp. 1-23, 1998

[66]Xingxing Jia, Yusheng Guo, Xiangyang Luo, Daoshun Wang, Chaoyang Zhang, A perfect secret sharing scheme for general access structures,Information Sciences,Volume 595, 2022, Pages 54-69, ISSN 0020-0255,

[67]Lin, C., Harn, L. and Ye, D. (2009),' Ideal perfect multilevel threshold secret sharing scheme' In IAS 2009: Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, IEEE Computer Society, Washington, vol.02, pp. 118–121.

[68]J. Benaloh, “Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret”, Advances in Cryptology-CRYPTO'86, vol. 263, pp. 251-260, 1986

[69]A. Beimel, and Y. Ishai, “On the Power of Nonlinear Secret-Sharing”, in Proc. IEEE Conference on Computational Complexity, Chicago, IL, June 2001, pp. 188-202.

[70]D. Stinson, and S. Vanstone, “A Combinatorial Approach to Threshold Schemes”, Advances in Cryptology-CRYPTO'87, vol. 293, pp. 330-339, 1987.

[71]Chitra, M. K., & Venkatesan, V. P. (2020). An antiquity to the contemporary of secret sharing scheme. Journal of Innovative Image Processing (JIIP), 2(01), 1-13.

[72]Iftene, S. (2007). General secret sharing based on the chinese remainder theorem with applications in e-voting. Electronic Notes in Theoretical Computer Science, 186, 67-84.

[73]Ito, M., & Saito, A. (1987). T, Nishizeki. Secret sharing scheme realizing any access structure. In Proc. IEEE Globecom (Vol. 87, pp. 99-102).

[74]Benaloh, J., & Leichter, J. (1988, August). Generalized secret sharing and monotone functions. In Conference on the Theory and Application of Cryptography (pp. 27-35). Springer, New York, NY.

[75]Patil, S., Tajane, K., & Sirdeshpande, J. (2013). An explication of secret sharing schemes with general access structure. International Journal Of Advances In Engineering & Technology, 6(2), 883

[76]Charnes, C., Martin, K., Pieprzyk, J., & Safavi-Nainil, R. (1997, November). Secret sharing in hierarchical groups. In International Conference on Information and Communications Security (pp. 81-86). Springer, Berlin, Heidelberg.

[77]Tassa, T. (2007). Hierarchical threshold secret sharing. Journal of cryptology, 20(2), 237-264.

[78]Pattipati, D. K., Tentu, A. N., Venkaiah, V. C., & Rao, A. A. (2016). Sequential Secret Sharing Scheme Based on Level Ordered Access Structure. Int. J. Netw. Secur., 18(5), 874-881.

[79]Nielsen, H. B., & Picek, I. (1983). Lorentz non-invariance. Nuclear Physics B, 211(2), 269-296.

[80]Hofmeister, T., Krause, M., & Simon, H. U. (2000). Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science, 240(2), 471-485

[81]Lemnouar, N. (2022). Security limitations of Shamir's secret sharing. Journal of Discrete Mathematical Sciences and Cryptography, 1-13

[82]Feldman, P. (1987, October). A practical scheme for non-interactive verifiable secret sharing. In 28th Annual Symposium on Foundations of Computer Science (sfcs 1987) (pp. 427-438). IEEE.

[83]Peng, Q., & Tian, Y. (2016). Publicly verifiable secret sharing scheme and its application with almost optimal information rate. Security and Communication Networks, 9(18), 6227-6238.

[84]Herzberg, A., Jarecki, S., Krawczyk, H., & Yung, M. (1995, August). Proactive secret sharing or: How to cope with perpetual leakage. In annual international cryptology conference (pp. 339-352). Springer, Berlin, Heidelberg.

[85]Çalkavur, S., & Solé, P. (2020). Some multisecret-sharing schemes over finite fields. Mathematics, 8(5), 654.

[86]Hsu, C., Harn, L., Wu, S., & Ke, L. (2020). A new efficient and secure secret reconstruction scheme (SSRS) with verifiable shares based on a symmetric bivariate polynomial. Mobile Information Systems, 2020.

[87]Liu, Y. (2016). Linear (k, n) secret sharing scheme with cheating detection. Security and Communication Networks, 9(13), 2115-2121.

[88]Cabello, S., Padró, C., & Sáez, G. (2002). Secret sharing schemes with detection of cheaters for a general access structure. Designs, Codes and Cryptography, 25(2), 175-188.

[89]Harn, L., & Lin, C. (2009). Detection and identification of cheaters in secret reconstruction. Designs, Code and Cryptography, 52(1), 15-24.

[90]Brickell, E. F., & Stinson, D. R. (1991). The detection of cheaters in thershold schemes. SIAM Journal on Discrete Mathematics, 4(4), 502-510

[91]Ma, Z., Ma, Y., Huang, X., Zhang, M., & Liu, Y. (2020). Applying cheating identifiable secret sharing scheme in multimedia security. EURASIP Journal on Image and Video Processing, 2020(1), 1-10.

[92]Liu, Y., Yang, C., Wang, Y., Zhu, L., & Ji, W. (2018). Cheating identifiable secret sharing scheme using symmetric bivariate polynomial. Information Sciences, 453, 21-29.

[93]Kandar, S., & Dhara, B. C. (2020). A verifiable secret sharing scheme with combiner verification and cheater identification. Journal of Information Security and Applications, 51, 102430

[94]Smys, S., & Raj, J. S. (2019). Internet of things and big data analytics for health care with cloud computing. Journal of Information Technology, 1(01), 9-18.

[95]Brindha, K., & Jeyanthi, N. (2015). Secured document sharing using visual cryptography in cloud data storage. Cybernetics and Information Technologies, 15(4), 111-123.

[96]Neji, W., Blibech, K., & Rajeb, N. B. (2018). A survey on e-voting protocols based on secret sharing techniques. Proc. CARI, 142, 2018.

[97] Nanda, S. J., & Panda, G. (2014). A survey on nature inspired metaheuristic algorithms for partitional clustering. Swarm and Evolutionary computation, 16, 1-18..

[98]Rahman, M. A., Sokkalingam, R., Othman, M., Biswas, K., Abdullah, L., & Abdul Kadir, E. (2021). Nature-inspired metaheuristic techniques for combinatorial optimization problems: overview and recent advances. Mathematics, 9(20), 2633.

[99]SS, V. C., & HS, A. (2022). Nature inspired meta heuristic algorithms for optimization problems. Computing, 104(2), 251-269.

[100]Kaleche, R., Bendaoud, Z., & Bouamrane, K. (2020). Bio-inspired metaheuristics: A comprehensive survey. International Journal of Organizational and Collective Intelligence(IJOCI), 10(4), 1-18.

[101]Back, T., & Schwefel, H. P. (1996, May). Evolutionary computation: An overview. In Proceedings of IEEE International Conference on Evolutionary Computation (pp. 20-29). IEEE.

[102]Spears, W. M., De Jong, K. A., Bäck, T., Fogel, D. B., & De Garis, H. (2005, June). An overview of evolutionary computation. In Machine Learning: ECML-93: European Conference on Machine Learning Vienna, Austria, April 5–7, 1993 Proceedings (pp. 442-459). Berlin, Heidelberg: Springer BerlinHeidelberg

[103]Bäck, T., & Schwefel, H. P. (1993). An overview of evolutionary algorithms for parameter optimization. Evolutionary computation, 1(1), 1-23.

[104]Bartz-Beielstein, T., Branke, J., Mehnen, J., & Mersmann, O. (2014). Evolutionary algorithms. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 4(3), 178-195

[105]Krause, J., Cordeiro, J., Parpinelli, R. S., & Lopes, H. S. (2013). A survey of swarm algorithms applied to discrete optimization problems. In Swarm intelligence and bio-inspired computation (pp. 169-191). Elsevier.

[106]Chakraborty, A., & Kar, A. K. (2017). Swarm intelligence: A review of algorithms. Nature-inspired computing and optimization: Theory and applications, 475-494

[107]Game, P. S., & Vaze, D. (2020). Bio-inspired Optimization: metaheuristic algorithms for optimization. arXiv preprint arXiv:2003.11637

[108]Holland, J. H. (1992). Genetic algorithms. Scientific american, 267(1), 66-73

[109]Lambora, A., Gupta, K., & Chopra, K. (2019, February). Genetic algorithm-A literature review. In 2019 international conference on machine learning, big data, cloud and parallel computing (COMITCon) (pp. 380-384). IEEE..

[110]Marini, F., & Walczak, B. (2015). Particle swarm optimization (PSO). A tutorial. Chemometrics and Intelligent Laboratory Systems, 149, 153-165.

[111]Karaboga, D, (2005). An idea based on honey bee swarm for numerical optimization. Technical Report TR06, Erciyes University, Engineering Faculty, Computer Engineering Department, 2005.

[112]Tereshko, V., Loengarov, A. (2005), Collective decision-making in honey bee foraging dynamics, Computing and Information Systems, 9 (3): 1-7, University of the West of Scotland, UK.

[113]Karaboga, D., & Akay, B. (2009). A comparative study of artificial bee colony algorithm. Applied mathematics and computation, 214(1), 108-132

[114]Blum, C. (2005). Ant colony optimization: Introduction and recent trends. Physics of Life reviews, 2(4), 353-373.

[115]Pearce, P. (1980). Structure in Nature is a Strategy for Design. MIT press.

[116]Ball, P. (2016). Why Nature Prefers Hexagons: The Geometric Rules Behind Fly eyes, Honeycombs, and Soap Bubbles. Nautilus Science Connected (http://nautil. us/issue/35/boundaries/why-nature-prefers-hexagons).

[117]Luo, J., Zhang, W., Su, J., & Xiang, F. (2019). Hexagonal convolutional neural networks for hexagonal grids. IEEE Access, 7, 142738-142749.

[118]G. Aubert, M. Barlaud, O. Faugeras, and S. Jehan-Besson, Image segmentation using active contours: Calculus of variations or shape gradients?, SIAM Journal on Applied Mathematics, 63 (2003), pp. 2128–2154.

[119]H.-K. Zhao, S. Osher, and R. Fedkiw, Fast surface reconstruction using the level set method, in Variational and Level Set Methods in Computer Vision, 2001. Proceedings. IEEE Workshop on, IEEE, 2001, pp. 194–201

[120]L. L. Beghini, A. Beghini, N. Katz, W. F. Baker, and G. H. Paulino, Connecting architecture and engineering through structural topology optimization, Engineering Structures, 59 (2014), pp. 716–726.

[121]V. J. Challis and J. K. Guest, Level set topology optimization of fluids in stokes flow, International journal for numerical methods in engineering, 79 (2009), pp. 1284–1308.

[122]S. Zhou and Q. Li, A variational level set method for the topology optimization of steady-state navier–stokes flow, Journal of Computational Physics, 227 (2008), pp. 10178–10195.

[123]F. Feppon, G. Allaire, F. Bordeu, J. Cortial, and C. Dapogny, Shape optimization of a coupled thermal fluid– structure problem in a level set mesh evolution framework, SeMA Journal, 76(3) (2019), pp. 413–458

[124]E. Cances, R. Keriven, F. Lodier, and A. Savin ` , How electrons guard the space: shape optimization with probability distribution criteria, Theoretical Chemistry Accounts, 111 (2004), pp. 373–380.

[125]N. Lebbe, C. Dapogny, E. Oudet, K. Hassan, and A. Gliere, Robust shape and topology optimization of nanophotonic devices using the level set method, Journal of Computational Physics, 395 (2019), pp. 710–746.

[126]Christensen, J., & Bastien, C. (2015). Nonlinear optimization of vehicle safety structures: Modeling of structures subjected to large deformations. Butterworth-Heinemann.

[127]Henrot, A., & Pierre, M. (2006). Variation et optimisation de formes: une analyse géométrique (Vol. 48). Springer Science & Business Media.

[128] Allaire, G., & Schoenauer, M. (2007). Conception optimale de structures (Vol. 58). Berlin: Springer.; Henrot, A., & Pierre, M. (2006). Variation et optimisation de formes: une analyse géométrique (Vol. 48). Springer Science & Business Media.

[129]Allaire, G., Dapogny, C., & Jouve, F. (2021). Shape and topology optimization. In Handbook of Numerical Analysis (Vol. 22, pp. 1-132). Elsevier.

[130]Wilbur R. Knorr, The ancient tradition of geometric problems, Dover Publications, Inc., New York, N.Y., 1993

[131]Kline, J. R. (1942). What is the Jordan curve theorem?. The American Mathematical Monthly, 49(5), 281-286.

[132]Courant, H. R. R., Courant, R., Robbins, H., & Stewart, I. (1996). What is Mathematics?: an elementary approach to ideas and methods. Oxford University Press, USA

[133]Brozek Boon, P., Vonck, K., van Rijckevorsel, K., El Tahry, R., Elger, C. E., Mullatti, N., ... & McGuire, R. M. (2015). A prospective, multicenter study of cardiac-based seizure detection to activate vagus nerve stimulation. Seizure, 32, 52-61.

[134]Hale, K., & Keyser, S. J. (2002). Prolegomenon to a theory of argument structure. MIT press..

[135]Panigrahy, S. K., Acharya, B., & Jena, D. (2008). Image encryption using self-invertible key matrix of hill cipher algorithm

[136]Duanhao, O., Wei, S., & Bo, L. (2012). A novel image encryption scheme with the capability of checking integrity based on inverse matrix. Journal of Graphics, 33(2), 89..

[137]Zhang, X., Wang, L., Niu, Y., Cui, G., & Geng, S. (2019). Image encryption algorithm based on the H-fractal and dynamic self-invertible matrix. Computational intelligence and neuroscience, 2019.

[138]Johansson, H. (2020). Secret Sharing with Threshold Schemes.

[139]Trivedi, P., & Swami, M. S. (2022). BEHAVIOURAL NUDGES IN THE ARENA OF MACROECONOMICS IN INDIA: MAKING A DIFFERENCE IN HEALTH AND EDUCATION. A MULTIDISCIPLINARY RESEARCH JOURNAL, 100.

[140]Rawashdeh, E. A. (2019). A simple method for finding the inverse matrix of Vandermonde matrix. Matematicki vesnik, 3(71), 207-213.

[141]Ahmad, A., & Elabdalla, A. M. (1997). An efficient method to determine linear feedback connections in shift registers that generate maximal length pseudo-random up and down binary sequences. Computers & electrical engineering, 23(1), 33-39.

[142]Noui,O., Beloucif,A. and Noui, L. (2017)'Secure image encryption scheme based on polar decomposition and chaotic map', International Journal of Information and Communication Technology , vol.10 No.4, pp.437-453.

[143]Catalina, C., Grau, J.M., Oller-Marcén, A.M. and Tóth, L . (2015) 'Counting invertible sums of squares modulo n and a new generalization of Euler's totient function',Publicationes Mathimaticae, vol. 87, No. 1-2, pp. 133-145.

[144]Merabet, N.A. and Benzid, R. (2018) 'Progressive image secret sharing scheme based on Boolean operations with perfect reconstruction capability', Information Security Journal: A Global Perspective, vol.27 No.1, pp.14-28.