République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Batna 2
Faculté des Mathématiques et de l'Informatique
Département d'informatique

Thèse

Présentée pour l'obtention du diplôme de doctorat en informatique

Par
Rafik HAMZA

Thème:

Sécuriser les images numériques par une approche probabiliste

Soutenue publiquement le 21 décembre 2017

Devant le jury composé de :

Rachid	SEGHIR	Maitre de Conférence	Université Batna2	Président
Faiza	TITOUNA	Maitre de Conférence	Université Batna2	Directeur de thèse
Lemonouar	NOUI	Professeur	Université Batna2	Examinateur
Kamal Eddine	MELKEMI	Professeur	Université de Biskra	Examinateur
Rachid	BAGHDAD	Professeur	Université de Bejaia	Examinateur
Souheila	BOUAM	Maitre de Conférence	Université Batna2	Examinateur

People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
University of Batna 2
Faculty of Mathematics and Computer Science
Department of Computer Science

A Dissertation Presented to the University of Batna
Department of Computer Science

By
Rafik HAMZA

Submitted in fulfillment of the requirement of the degree of Doctor in Computer Science

Entitled:

Secure digital images with a probabilistic approach

Defended on December, 21 2017

Committee members:

Rachid	SEGHIR	Associate Professor	University of Batna2	President
Faiza	TITOUNA	Associate Professor	University of Batna2	Supervisor
Lemonouar	NOUI	Professeur	University of Batna2	Examiner
Kamal Eddine	MELKEMI	Professeur	University of Biskra	Examiner
Rachid	BAGHDAD	Professeur	University of Bejaia	Examiner
Souheila	BOUAM	Associate Professor	University of Batna2	Examiner

إلى أبي وأمي

Acknowledgements

First and foremost, I would like to thank Allah almighty for giving me the strength, knowledge, ability and opportunity to undertake this research study.

Praise be to Allaah. الحمد لله

I would like to express my deeply-felt thanks to my thesis advisor, Dr. Faiza Titouna, for her warm encouragement and thoughtful guidance. It has been an honor and pleasure working with her during the last years.

I also thank the members of thesis committee: Prof. Lemnouar Noui, Dr. Seghir Rachid, Prof. Kamal Eddine Melkemi, Prof. Rachid Baghdad, and Dr. Souheila Bouam for having accepted to assess my thesis.

I am happy to acknowledge my deepest sincere gratitude to Prof. Naoui Lamnouar, for the truly inspiring teaching which turned me towards searching for the ciphers structures.

I want to express my gratitude to my friend Dr. Khan Muhammad. In fact, I am indebted to many friends: Meriem L, Nassim B, my little brother Djihad, Taha D, Nassim K, Maroua B, and Abdelmoumen M ... The List is long but distinguished.

An extra special recognition to my family whose love and aid have made this thesis possible, especially my parents, I love you both very much and am immensely grateful for all that you do. Thank you for everything.

Abstract

Most companies cooperate and communicate through Internet, where a significant amount of information is stored, treated and transmitted according to a digital process. However, these data becomes vulnerable to interception, duplication, falsification or corruption. Thus, the need to secure the digital images is paramount.

The principal objective of this thesis is to achieve security of digital images through modern cryptography techniques with probabilistic approaches. In this regard, the security of digital image can be enhanced with a randomized technique that will make the cryptosystem semantically secure. The focus of this dissertation in perspective, is two parts. The first part focuses on the of digital images terminology, also the characterized of these special data. Additionally, we present some security mechanisms which would ensure the digital images' privacy and provide high level of security in various communication applications. The second part focuses on our researches contributions. In this context, a pseudo random numbers' generator based on Chen chaotic system is proposed in order to produce appropriate cryptographic keys for digital images. We also proposed a new image encryption algorithm based on Zaslavsky chaotic map which guarantee the confidentiality of digital images. After that, we proposed a summarization framework based on our image encryption algorithm. The proposed technique is based on summarization of a wireless capsule endoscopy video and the preceding image encryption algorithm, which guarantee a secure transmission of the extracted informative keyframes during wireless capsule endoscopy actions. The proposed cryptosystems have a good ability to resist the chosen/known attacks and differential attacks. Furthermore, comparison with several recent state-of-the-art show that the proposed cryptosystems have excellent results, with higher performances.

Keywords : Digital Images; Modern Cryptography; Randomized Algorithms; Probabilistic Approach.

ملخص البحث

مع تطور التكتنوجيا الجديثة, أصبحت معظم الشركات تتعاون وتواصل فيما بينها عبر الإنترنت ، بحيث يتم تخزين كميه كبيرة من المعلومات وتتم معالجتها ونقلها وفقا لعمليات رقمية. غير ان هذه البيانات أصبحت عرضة لمختلف انواع الهجمات كالتزييف أو الازدواجية أو التزوير. وبالتالي ، فان الحاجة إلى تامين الصور الرقمية أصبح أمرا ضروريا ضروري.

هذه الاطروحة تهدف الي تطوير أمن الصور الرقمية، وذلك اعتمادا علي تقنيات التشفير الحديثة مع النهج الاحتمالية. وفي هذا الصدد ، ندرس امكانية تعزيز أمن الصورة الرقمية مع تقنية عشوائية والتي من شأنها ان تجعل نظام التشفير آمن من الناحية الدلالية"Semantically secure".

هذه الاطروحة ترتكزعلي جزئين. يركز الجزء الأول علي الصور الرقمية، مصطلحاتها والمميزات التي تتميز بها هذه البيانات الخاصة وأيضا مختلف طرق معالجة الصور الرقمية. بالاضافه إلى ذلك ، تقدم هذه الاطروحة أيضا بعض الأليات الامنية التي من شانها ان تضمن سرية الصور الرقمية وتوفير مستوي عال من الأمن في مختلف تطبيقات الاتصالات والمعلوماتية.

يركز الجزء الثاني علي مساهماتنا العلمية المنشورة في مجلات علمية. في هذا السياق ، قدمنا ثلاث مساهمات جديدة لتطوير امن المعلوماتية للصور الرقمية. اول بحث يشمل مولد أعداد شبه عشوائية اعتمادا علي خريطة تشن الفوضوية. النظام المقترح هو بالأساس من أجل إنتاج مفاتيح التشفير المناسبة لمتطلبات الصور الرقمية. في البحث الثاني، اقترحنا أيضا خوارزمية تشفير للصور اعتمادا علي خريطة الفوضى زاسلافسكي, المخطط المقدم يضمن سرية الصور الرقمية وبأداء جيد ويستطيع مقاومة العديد من الهجمات المعروفة حاليا. بعد ذلك، اقترحنا اطار عمل لتلخيص فعال وامن لفيديو منظار الكبسولة الاسلكي كثالث إسهام في الأطروحة. تستند التقنية المقترحة هنا علي تلخيص البيانات المستخرجة من منظار الكبسولة اللاسلكي متبوع بتشفير البيانات الملخصة. المخطط المقترح يضمن نقل أمن للإطارات المفتاحية -key frames- على شبكات المعلومات.

بصفة عامة, المخططات المقترحة في عملنا لها قدره جيدة علي مقاومة مختلف الهجمات المعروفة حاليا. وعلاوة علي ذلك ، فان المقارنة مع الخوارزميات الحديثة تشير إلى ان الاعمال المقدمة في هذه الاطروحة لها نتائج ممتازة ، مع أداء ممتاز.

كلمات مفتاحية :

الصور الرقمية ; علم التشفير الحديث; الخوارزميات العشوائية; نهج احتمالي.

Résumé

La plupart des entreprises, coopèrent et communiquent via Internet, où une quantité importante d'informations est stockée, traitée et transmise selon un processus numérique. Cependant, ces données deviennent vulnérables à l'interception, la duplication, la falsification ou la corruption. Ainsi, la nécessité de sécuriser des images numériques devient primordiale. Le principal objectif de cette thèse est d'assurer la sécurité d'images numériques au moyen de techniques de cryptographie modernes notamment les approches probabilistes. À cet égard, la sécurité de l'image numérique peut être améliorée grâce à une technique aléatoire qui rend le cryptosystème sémantiquement sécurisé. L'objectif de cette thèse est élaborée est deux parties. La première partie se concentre sur la terminologie des images numérique. En outre, nous présentons certains mécanismes de sécurité qui pourraient garantir la confidentialité des images numériques et fournir un niveau élevé de sécurité dans diverses applications de communication. La deuxième partie se concentre sur nos contributions de recherches. Dans ce contexte, un générateur de nombres pseudo-aléatoire basé sur le système chaotique de Chen est proposé, il permet de produire une séquence de clés cryptographiques appropriées pour le chiffrement des images numériques. Nous avons aussi proposé un nouvel algorithme de cryptage d'images basé sur la carte chaotique de Zaslavsky. Ce dernier garantit d'une manière efficace la confidentialité des images numériques. En plus, nous avons proposé un cadre théorique basé sur l'algorithme de chiffrement précédemment proposé. La technique ainsi élaborée est basée sur la synthèse d'une vidéo endoscopique en utilisant des capsules sans fil. Elle garantit une transmission sécurisée et ceci en effectuant une extraction des frames les plus pertinents. Les cryptosystèmes ainsi proposés ont une bonne capacité de résister aux différents types d'attaques notamment les attaques choisies, connus et

aux attaques différentielles. Une étude expérimentale a montré que les résultats trouvés sont excellents et dotés de performances de haut niveau comparés aux techniques classiques.

Mots-clés: Images numériques; Cryptographie moderne; Algorithmes randomisés; Approche probabiliste.

List of Publications

Peer Review Journals

(41) Rafik Hamza*. A novel pseudo random sequence generator for image-cryptographic applications. Journal of Information Security and Applications, 35:119-127, 2017.

(46) Rafik Hamza* and Faiza Titouna. A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. Information Security Journal: A Global Perspective, 25(4-6):162179, 2016.

(42) Rafik Hamza, Khan Muhammad, Zhihan Lv*, and Faiza Titouna. Secure video summarization framework for personalized wireless capsule endoscopy. Pervasive and Mobile Computing, Pages 436-450, Volume 41, 2017.

(55) Khan Muhammad, Rafik Hamza, Jamil Ahmad, Jaime Lloret*, Haoxiang Wang, and Sung Wook Baik. Secure Surveillance Framework for IoT systems using Probabilistic Image Encryption. IEEE Transactions on Industrial Informatics, In Press, 2018. (doi: 10.1109/TII.2018.2791944).

(43) Rafik Hamza, Khan Muhammad, Arunkumar Nachiappan, Gustavo Ramrez Gonzlez*. Hash based encryption for keyframes of diagnostic hysteroscopy. IEEE Access, In Press, 2018 (Doi :10.1109/ ACCESS.2017.2762405).

(96) Rafik Hamza*, Faiza Titouna, and Hewage, Chaminda. Investigation of 3D-images security based on Improved Image Randomized Encryption Method. NED University Journal of Research - An International Journal. In Press, 2018.

Conference Proceedings

(45) R. Hamza* and F. Titouna, A study on chaotic maps to produce randomness numbers," National Days on Applied Mathematics: Skikda-Algeria-JNMA'15, 2015.

(44) R. Hamza* and F. Titouna, A new pseudo random sequence generator based on chen chaotic map," International Workshop on Cryptography and its Applications Oran-Algeria-IWCA'16, 2016.

Contents

Cover ii

Acknowledgements iii

Abstract x

List of Publications x

List of Figures xvii

List of Tables xxi

1 General introduction 1

1.1 Problematic and motivation 1

1.2 Organization of the thesis and contributions 5

I State of the art 8

2 Digital image processing 10

2.1 Introduction 12

2.2 Digital image 12

2.3 Types of images 13

2.3.1 Vector graphics 14

2.3.1.1 Advantages 14

2.3.1.2 Disadvantages 14
2.3.2 Matrix graphics 15
2.3.2.1 Advantages 15
2.3.2.2 Disadvantages 16
2.4 Digital image characteristics 17
2.4.1 Pixels 17
2.4.2 Quantization and Sampling 17
2.4.3 Image size and resolution 18
2.4.4 Size file of an image 20
2.5 Digital images colours 20
2.5.1 Binary images 20
2.5.2 Gray images 20
2.5.3 Colours images 21
2.5.3.1 True colour images 23
2.5.3.2 Indexed colour images 23
2.6 2D images & 3D images 24
2.7 Image processing operations 26
2.8 Medical images 28
2.9 Conclusion 29

3 Security Mechanisms **30**
3.1 Introduction 32
3.2 Secure Digital Images 32
3.2.1 Cryptology 33
3.2.2 Security concepts 33
3.2.3 Cryptography 34
3.2.4 Cryptanalysis 35
3.3 Probabilistic approach 36
3.3.1 Randomized algorithms 36
3.3.2 Summarization algorithms 37
3.4 Encryption terminologies 38
3.5 Encryption types 40
3.5.1 Asymmetric encryption 40

3.5.2 Symmetric encryption 41
3.6 Ciphers modes 42
3.6.1 Cipher stream 42
3.6.2 Cipher block 42
3.6.3 Comparative study 42
3.7 Substitution-Permutation Network 43
3.7.1 Rijndael Advanced Encryption Standard (AES) 45
3.8 Chaos Theory 49
3.9 Requirements and metrics 51
3.9.1 Kerckhoffs principles 52
3.9.2 Encryption requirements 52
3.9.3 PRNG requirements 53
3.10 Semantic Security 54
3.11 Conclusion 56

II New approaches to secure digital images 57

4 Pseudo random numbers generator 59
4.1 Introduction 61
4.2 Proposed System 63
4.2.1 Chen chaotic system 63
4.2.2 Proposed algorithm structure 65
4.3 Experimental Results 67
4.3.1 Security Analysis 68
4.3.1.1 Key sensitivity 68
4.3.1.2 Key Space 69
4.3.2 Randomness tests 70
4.3.3 Encryption image simulation 72
4.3.4 Security Properties comparison 77
4.4 Conclusion 78

5 Chaos-based cryptosystem **79**
5.1 Introduction . . . 81
5.2 Proposed encryption scheme . . . 82
5.2.1 Generating encryption keys . . . 82
5.2.2 Encryption algorithm . . . 84
5.2.3 Decryption algorithm . . . 86
5.2.4 RGB image encryption . . . 88
5.3 Experimental results and discussion . . . 89
5.3.1 Histogram analysis . . . 90
5.3.2 Information entropy . . . 91
5.3.3 Correlation of two adjacent pixels . . . 91
5.3.4 Randomness tests . . . 94
5.3.5 Key Sensibility . . . 95
5.3.6 Key Space . . . 97
5.3.7 NPCR and UACI tests . . . 98
5.3.8 Known/Chosen attack . . . 100
5.3.9 Comparative analysis . . . 102
5.4 Conclusion . . . 104

6 Secure framework for wireless capsule endoscopy **106**
6.1 Introduction . . . 108
6.2 Proposed framework . . . 109
6.2.1 Summarization of video data captured during WCE . . . 110
6.2.1.1 Color space conversion: RGB to COC . . . 112
6.2.1.2 Integral image computation . . . 113
6.2.1.3 Visual saliency computation . . . 113
6.2.2 ZCM-based image encryption algorithm . . . 116
6.3 Experimental results and discussion . . . 118
6.3.1 Histogram analysis . . . 119
6.3.2 Differential attack analysis . . . 121
6.3.3 Chosen/Known attack analysis . . . 123
6.3.4 Sensibility analysis . . . 123
6.3.5 Space Key analysis . . . 126

6.3.6 Entropy analysis 126
6.3.7 Correlation coefficient analysis 126
6.4 Analysis and evaluation results 128
6.4.1 Summarization scheme 128
6.4.2 Encryption scheme 129
6.5 Conclusion 132

Conclusion and Future Work **133**

References **136**

List of Figures

2.1 A zoom for a part of a vector image 13
2.2 A zoom for a part of a matrix image 16
2.3 Different Pixel Resolutions for logo of university of Batna 2. (a) a block of [512,512] pixels, (b) have a block of [256, 256] pixels, (c) have a block of [128, 128] pixels, (c) have a block of [64, 64] pixels, (e) have a block of [32, 32] pixels. 18
2.4 (a) Binary image, (b) Gray image, (c) a colour image 19
2.5 Binary image 21
2.6 Pixels values for a gray image 21
2.7 (a) Original image, (b), (c), and (d) components Red, Green and Blue, respectively. 22
2.8 Matrix transformations effect on the visual show for a gray image. 22
2.9 RGB image colour ordering. (a) RGB colour image in component ordering. (b) RGB-colour image using packed ordering. 23
2.10 RGB indexed image. 24
2.11 3D reconstruction from multiple medical frames. 25
2.12 Left and right (Side-by-side) 3D image. 25
2.13 3D image. 26
2.14 Arithmetic mean for the components of an RGB image 27
2.15 Brightness and contrast tests. 28
2.16 Encryption of a medical image. 28

3.1 Scenarios of cryptosystem/cryptanalysis 35
3.2 Block diagram of a randomized encryption procedure (39) 36

LIST OF FIGURES

3.3 Probabilistic image Encryption/Decryption. 37
3.4 Encryption and Decryption of an image "Lenna". 39
3.5 Framework of generating the cryptographic keys. 40
3.6 Architectures of asymmetric encryption. 41
3.7 Architectures of symmetric encryption. 42
3.8 Confusion and diffusion algorithm 44
3.9 An instance of confusion algorithm of a pixels block. 45
3.10 An instance of diffusion algorithm of a pixels block. 45
3.11 First round process in 128-AES 46
3.12 schematic of 128-AES structure 49
3.13 Mechanism of PRNG for image encryption. 50

4.1 Lyapunov exponents of Chen's chaotic system 63
4.2 Chaotic behavior of Chen's system. 64
4.3 The distribution of values x using different seeds. 65
4.4 The distribution of values y using different seeds. 66
4.5 The distribution of values z using different seeds. 67
4.6 The structure of the proposed algorithm: The input: Secret-Keys, n, and l. (1) generate the Sequences $x(i)$, $y(i)$, $z(i)$ using equations 4.1 of chaotic Chen equations. (2) generate the sequence P using the equations 4.2. (3) generate a binary sequence using the equation 4.4 with $l = 2$. (4) generate numbers sequence using the equation 4.4 with $l = 256$. 68
4.7 Flowchart of the proposed PRNG algorithm 69
4.8 Histogram of the pseudo random numbers 70
4.9 **(a)** The difference Plot ($S_1 - S_2$), **(b)** Auto-correlation of these sequences 71
4.10 Basic tests of image encryption using transposition pixels position based on our proposed algorithm. 75

5.1 The initial matrix K_{init} 83
5.2 Test image encryption by our encryption scheme. (a) The plain-image, (b) The encrypted image , (c) The decrypted image 86

5.3 Illustration the encryption / decryption algorithm for gray image (the girl *lenna*) 88
5.4 Test the histogram of zeros image, and its corresponding encrypted image. (a) The zeros image. (b) Histogram for the zeros image. (c) The corresponding encrypted image. (d) Histogram for the encrypted image. 89
5.5 Test the histogram of plain image, and its corresponding encrypted image. (a) The plain image *girl 'Lena'*. (b) Histogram for the plain image. (d) The corresponding encrypted image. (d) Histogram for the encrypted image. 90
5.6 Correlation analysis of two adjacent pixels in an image and its corresponding encrypted image. (a) The plain image. (b) Distributions of two horizontally adjacent pixels in the plain image. (c) Distributions of two vertically adjacent pixels in the plain image. (d) Distributions of two diagonally adjacent pixels in the plain image. (e) The encrypted image. (f) Distributions of two horizontally adjacent pixels in the encrypted image. (g) Distributions of two vertically adjacent pixels in the encrypted image. (h) Distributions of two diagonally adjacent pixels in the encrypted image. 93
5.7 Key sensitivity results. (a) The encrypted image C using the secret key SC_1, (b) the encrypted image C_1 using the secret key SC_2, (c) the encrypted image C_2 using the secret key SC_3, (d) the image difference $|C_1 - C_2|$ (e) the decrypted image using the secret key SC_1, (f) the decrypted image D_1 using the secret key SC_2, (g) the decrypted image D_3 using the secret key SC_3, (h) the image difference $|D_1 - D_2|$. 97
5.8 $NPCR$ and $UACI$ tests. (a) NPRC test for 1000 modified plain-images in one bit with a single pixel. (b) UACI test for 1000 modified plain-images in one bit with a single pixel. 101
5.9 plainimage sensitivity results. (a) The plain image I. (b) The modified image J. (c) The image difference $|I - J|$. (d) The encrypted image CI. (e) The encrypted image CJ. (f) The image difference $|CI - CJ|$ 102

LIST OF FIGURES

6.1 Framework of the proposed system. 111
6.2 Experimental test of ciphering the extracted keyframe 112
6.3 Encryption algorithm. 117
6.4 Decryption algorithm. 118
6.5 Overall procedure of the proposed framework. 119
6.6 Selected test keyframes with frame numbers from our proposed scheme. 120
6.7 Sample non-keyframes with frame numbers from our proposed scheme. 120
6.8 Histogram of a frame 0065. 121
6.9 NPRC tests (a) and UACI tests (b) for 100 plain-images (randomized) 123
6.10 Key sensitivity analysis at the encrypted/decryption stage. 124
6.11 Tests of the keyframe sensitivity. 125
6.12 Correlation coefficient diagrams (blue channel). 128

List of Tables

4.1 Results of the NIST SP 800-22 randomness tests for 1000000 *bits* 72
4.2 Results of the NIST SP 800-22 randomness tests for 8000000 bits 73
4.3 DIEHARD statistical test results 74
4.4 Variances of histograms compared among all secret keys in the proposed algorithm. 76
4.5 Percentage of variances difference of histograms compared among all secret keys in the proposed algorithm. 77
4.6 Security Properties comparison 78

5.1 Entropy of the plain and cipher image of different size images . . 92
5.2 Correlation coefficients of two adjacent pixels in the Plain and cipher images 94
5.3 Results of the NIST SP 800-22 randomness test on encrypted image 95
5.4 NPCR and UACI between cipher images with slightly different keys $+10^{-15}$. 96
5.5 NPCR & UACI tests 100
5.6 The speed analysis between our proposed method and the other chaotic-cryptosystems 103
5.7 Comparison between our proposed method and the other cryptosystems 104

6.1 NPCR and UACI tests results for each channel of RGB frame. . . 122
6.2 NPCR and UACI tests results for a set of keyframes. 122
6.3 Tests of secret keys sensibility. 124
6.4 The Entropy tests for a set of data keyframe. 126

LIST OF TABLES

6.5 The correlation coefficient of adjacent pixels tests. 127
6.6 Summarization Scheme Evaluation. 130
6.7 Recall (R), Precision (P), and F-measure (F) results compared with different summarization techniques. 130
6.8 Comparison of the proposed image encryption method with recent state-of-the-art encryption algorithms based on multiple performance evaluation metrics. 131

1

General introduction

1.1 Problematic and motivation

In recent years, digital images have become an important source of information. These data are widely used in various fields of works. Consequently, digital images were given great attention and become an increasingly common tool for communication, especially in the last decade where the social media become a part of our daily life. Many examples are given in our lifestyle such as smart-phone, smart-cars, and smart-homes. As a result, a huge amount of digital images are employed for several applications in communication and information systems. Yet, the general public uses these data without considering the potential security and privacy risks. Thus, cryptography and security are of vital importance today more than yesterday.

To guarantee the security of digital images, researchers proposed several solutions which would ensure the privacy of the information. For instance, ensuring the confidentiality of the information by encryption algorithms and ensuring the integrity of the information by hash functions. In fact, data security can be included during the transmission over an open network, safeguarding accurate the data, verify who is really the sender of the data, and which data was really sent by the sender. In this regard, information security aspects could elucidate

the mechanisms of ensuring data security. Cryptography techniques can ensure the information security within four aspects: authentication, confidentiality, integrity, and non-repudiation. All of these mechanisms should be applied to the digital image to guarantee its security.

Probabilistic algorithms are very important and widely used in cryptography. To put it another way, probabilistic techniques play an important role in applications extending from combinatorial optimization and machine learning to communication networks and secure protocols (76). Probabilistic techniques are employed in encryption and digital signature schemes often include random sources such as embedded noises bits in the original image (98). Furthermore, study cryptanalysis usually allows to analyze and crack the cryptographic schemes using probabilistic techniques (22). A randomized encryption involves procedure ciphered messages (randomly) corresponding to the same message under the current secret key (98). Here, a probabilistic encryption is a semantically secure cryptosystem, which means that an intruder is infeasible to learn anything about the original data from the ciphered data.

In order to enhance the level of security for digital images, several encryption algorithms have been presented in the last decades. Mainly because the traditional cipher techniques could not meet the requirements of digital images characteristics (61, 91). Although most common encryption schemes such as Data Encryption Standard "DES" (49), Advanced Encryption Standard "AES" (95) are designed with good confusion and diffusion properties, but also are not really appropriate for digital images (16, 85). This specific data have different inherent properties such as high correlation among adjacent pixels, and have large sizes compared with texts or binary data (61).

Even though researchers created new solutions, many image security applications have been analyzed recently, and became insecure against the hackers. As known, cryptography applications should be resistant to all cryptanalysis attacks. However, some security issues with image encryption algorithms have been exposed including various serious privacy issues.(57, 59, 63, 122). These

ciphers schemes have been analyzed mainly from three points: structures of the cryptographic key, the structures of encryption scheme, and their combination. The weakness of the cryptographic keys could be in secret keys, pseudo-random number generator (PRNG), and the poor employing of the cryptographic keys among the encryption scheme. Basically, the attackers try always to use several attacks in order to collect the informative data. For instance, one common attack is using special images like a black-image (all pixels equal to zero) (117). The main issue that allows cryptanalysis to break many encryption schemes is the problem of low security-sensitivity to plain-image change (117). The structures of an encryption scheme should have high sensitivity for all input (plain-image, secret keys). The attackers could propose cryptanalysis based on low sensitivity in plain-image change and weakness of the encryption architecture that does not guarantee encryption characteristics (confusion-diffusion). Therefore, any amendment in plain-image pixels should change completely its corresponding encrypted image.

Correspondingly, cryptographic keys are very important in cryptography applications.These keys should be infeasible to find or estimate without the correct secret keys due to the fact that the secrecy depends only on keeping the keys secret (58). The cryptographic keys require numerous properties such as statistical randomness and avoid the short periodic and predictable non-randomness keys. Pseudo-random number algorithms considered as a solution to produce the cryptographic keys to encrypt digital images.

Researchers in the last two decades have become aware of relationship between the chaotic systems and cryptography (36), where the unpredictable behaviour of the chaotic maps used in order to produce random numbers. This means that the chaotic maps produce good pseudo-stochastic sequences that can be applied to design cryptography keys (108). Mainly due to their valuable properties such as sensibility and large space of the initial values and controlling parameters. The idea of using a chaotic system as a pseudo-random generator is about the ability of producing a sequence of numbers, which appears like a random source. In fact, chaos-pseudo-random number generators (PRNG) demonstrated their importance within numerous fields, especially among cryptographic applications,

where the keys-cryptographic are very required in image encryption algorithm (17, 31, 62).

Additionally, a further point to be considered with the medical images. These significant data are employed mainly for diagnosis of diseases additionally to clinical examination and other investigations such as biological examinations, but also utilizes several different physical principals or imaging modalities. As a matter of fact, the medical technologies are improved for a better life with enhancing diagnosis decisions including to make the critical decisions easier and faster.

Wireless capsule endoscopy (WCE) can directly capture images in the gastrointestinal tract of a patient (33). The initial capsule endoscope model was developed by "*Given Imaging*" and approved in developed countries in 2001 (84), and it was approved in several countries such as Japan in April 2007 (84). The first capsule endoscope model in the world, called M2A (84), while the most famous WCE is known by "PillCam". This capsule allows to carry out endoscopy by applying the principle of miniaturization in medicine. Unlike "classical" endoscopies where access to part of small intestine is uncomfortable for the patient, WCE capsule is easy to swallow and runs through the entire digestive tract. In fact, the device is quite tiny that it can ultimately pass over tight strictures without any problems (118).

Generally speaking, the transmitting the data to healthcare centers and doctors can be really challenging as well as wastage of several resources including energy, memory, computation, and bandwidth. Also, it is very difficult and time consuming tasks for the specialist to find the desired contents from a huge amount of the collected video. Mainly, the captured data contains critical information with distinguishing visual representations of the interior of a body (83, 102).As a result of capturing images for many hours inside the body, a huge number of frames are important and sent for diagnosis by the specialist (33, 65). In this pursuit, it is time-consuming and difficult inherently for doctors to find the desired frames from a huge amount of video data.For this reason, it is necessary

to employ extra techniques to extract the informative frames from capsule endoscopy video. Equally important, the problem of secure dissemination of secret information over Internet is very challenging.

In this dissertation, we provide some solutions, to surmount the above issues, of digital image security with different cryptography techniques with probabilistic items. Our proposal attempts to meet this objective and has been validated in three application areas. First, a new stream cipher algorithm. Second, an efficient symmetric block encryption scheme. Third, a secure video summarization framework. The implementation shows promising results making our proposal algorithm suitable candidate to be adopted in IoT applications.

1.2 Organization of the thesis and contributions

In this thesis, we focus on the security mechanisms to ensure the confidentiality of digital images. In this regard, our work is divided into two parts. We look for acquaint some terminologies of digital images along with their properties. Next, we illuminate the security mechanisms which would guarantee the digital images privacy. The first part presents the contexts of our work, while the second part presents our contributions. Herein, we propose three frameworks to deal with digital images security issues.

The first part is composed of two chapters. In the first chapter, we show a brief overview of the digital images basics terminology. In the second chapter, we present forward some mechanisms mainly based on cryptography tools, and particularly large classes of encryption techniques. While, the second part represents our contributions that have been published in peer reviewed journals.

In the first contribution, we have proposed a novel algorithm as a pseudo random number sequence generator based on the samples of Chen chaotic system. Here, a secure pseudo-random sequence generator is proposed based on a combination of three coordinates of Chen chaotic orbits. We overcome the weaknesses of the former PRNG based on Chen chaotic map (50, 88). Furthermore, our

pseudo random numbers' generator solves the problem of the non-uniform probability distribution of the sequence generated directly by Chen chaotic system.

The second contribution is a novel cipher algorithm to encrypt digital images which would guarantee the confidentiality of data. The cipher structure has been chosen based on permutation-diffusion processes. We have adopted the classic permutation substitution network, which ensures both confusion and diffusion properties for the encrypted image. Herein, we have employed Zaslavsky chaotic map as a pseudo-random number to produce the keys encryption for the proposed image cryptosystem. Conducted experiments demonstrated that the our cryptosystem approach can achieve excellent encryption performance, and confirms its efficiency against well-known attacks. The encryption algorithm can provide a high level of security with several features such as the sensitivity for the plain image and secret key. Also, the proposed cipher scheme possesses a large space of key keys and fast exhaustion time of encryption/decryption processes. Indeed, the proposed cipher algorithm ensures good confusion-diffusion properties of the encrypted data, additionally to eliminates the correlation coefficients of the plain image. The original image can be recovered completely only if the secret keys are exactly known.

The third contribution is a secure video summarization framework for outdoor patients going through WCE procedure. The proposed cryptosystem resolves the issues mentioned above by using video summarization technology combined with image encryption. The proposed system is two-fold. First, extracting keyframes using video summarization (frame per frame). Second, encrypting the extracted keyframes using our robust image encryption scheme. The proposed method can guarantee the secrecy of the keyframes with larger key space and can provide excellent confusion and diffusion properties with high level security. Moreover, it can be used for authentication of keyframes, preventing the possibility of injecting false keyframes. The proposed framework can facilitate healthcare centers in ensuring the privacy of patients, reducing the energy, processing and communication cost, helping the specialist to browse quickly for desired contents and fast

analysis, leading to improved diagnosis with personalization.

Finally, we present a general conclusion and some perspectives that can help in the improvement of the current systems in the future works.

Part I

State of the art

2

Digital image processing

They say "a picture is worth a thousand words", but i think they are wrong. When i looked at your picture, i was speechless...

Anonymous

Contents

2.1 Introduction 12

2.2 Digital image 12

2.3 Types of images 13

2.3.1 Vector graphics 14

2.3.2 Matrix graphics 15

2.4 Digital image characteristics 17

2.4.1 Pixels 17

2.4.2 Quantization and Sampling 17

2.4.3 Image size and resolution 18

2.4.4 Size file of an image 20

2.5 Digital images colours 20

2.5.1 Binary images 20

2.5.2 Gray images 20

2.5.3 Colours images 21

2.6 2D images & 3D images 24

2.7 Image processing operations 26

2.8 Medical images 28

2.9 Conclusion 29

2.1 Introduction

Digital images are everywhere. In fact, these data are considered an important source of information due to the fact that most of the data over the internet are generally provided in graphic forms. In this chapter, we mainly deal with basic terminology of the state of the art in image processing. The contents of this chapter are sum up in sections only subjects with direct relationship with our contributions in the second part. Herein, we define the scope of the field in our research. We discuss briefly the principal characteristics of a digital image. Finally, we present a practical example based on the digital images for the medical diagnostics.

2.2 Digital image

Our life is depend on the advancement of technology, and we completely rely on the internet to live. For instance, it has improved the techniques to obtain products, communicate, travel and learn!. Consequently, many devices have been developed, well-known examples of such devices are mobile devices and applications for health care professionals.

The images can convey the essence of a topic more effectively than words and description as the English idiom sentence says "*an image is worth a thousand words*". These data became an important part of human daily life especially with the exploiting the social media and growing the use of imaging technologies systems. The term "digital image" indicates to an image that has been acquired, processed and stored in a coded form that can be represented with numerical values. So, the digital image is an array of discrete samples reflected from or transmitted through objects. Processing image could be achieved through a machine or computer program.

Mathematically (14), a digital image I is a two-dimensional function of integer coordinates $\mathbb{N} \times \mathbb{N}$, these coordinates refers to an image elements values (pixels) $\mathbb{P}$, such that

$$I(u, v) \in \mathbb{P} \quad and \quad u, v \in \mathbb{N}. \tag{2.1}$$

Simply, digital images are represented as an array which contains a finite discrete range of pixel values. At this point, image is a two-dimensional matrix of integers number. So, it is no longer important to us how the image originated was before.

Digital Image processing refers to manipulation of the digital bitsteam (112), which also can be consist of applying mathematical transformations to images in order to improve the quality or extract information from these data. Generally, digitization is a process in which materials are converted from the hard copies to electronic copies (25). Here, the digitization contains the process that allows to switch from the optical image to digital image. The optical image is characterized by the continuous aspect of the signal that it represents (visually), while digital image is characterized by the discrete aspect. The intensity of digital images can take values in a finite number of distinct points (47).

2.3 Types of images

In this part, we classify images into two types, vector graphics and matrix graphics.

Figure 2.1: A zoom for a part of a vector image

2.3.1 Vector graphics

A vector image is composed of geometric shapes that can be mathematically described (straight lines, circles, points, ...). These images are very useful for large scale reproductions, computations which can be carried out each time, in order to obtain the exact image, whatever the size chosen. Vector file formats such as EPS, PDF are used in many applications web that frequently require resizing and creating graphics. For example, using application of writing by Latex with "eps" images for better view and reading.

Figure 2.1 shows a vector image with extension 'eps' (2).Here, a zoom part of image is elucidated. The show part did not lost its certainty with the zooming. In fact, the extracted part was very clear as Figure 2.1 shown.

2.3.1.1 Advantages

- The digital image must be calculated before it can be displayed by the device.
- All spatial image changes, such as translation, rotation ... etc., are easy and do not cause any loss of information.
- The vector image is particularly suitable for schematic and stylized representations consisting of geometric shapes, uniformly filled with colour plates or patterns.
- A vector file is much more compact than a bitmap file. Its size varies depending on the complexity of the image, but not according to the required resolution.

2.3.1.2 Disadvantages

- The work on graphic objects that must associate to the graphic designer or illustrator. It requires a certain habit and learning new procedures of creation.

- Some manipulations such as colour changes are not easy and difficult on an area of an object, on a single object, or on a group of objects.
- Since each vector file format has its own attributes, compatibility between formats is difficult.
- The slightest degradation of information in vector file is often irreparable. Thus, a vector file is more fragile than a bitmap file.

2.3.2 Matrix graphics

The main interest in this dissertation is with this specific type of image. A matrix image is composed of a set of points (pixels). Each of them has a precise position and colour. A matrix image called a Bitmap too. This type of images are the most common type used for many digital images such as photos and scanned documents. Different formats of bitmap are proposed, where you can find common Compressed bitmap formats such as "JPEG" format, and you can find common original formats such as "BMP" format. We listed 5 famous formats which are also the most used images formats over internet.

- BMP: Windows BitMap
- TIFF: Tagged Image File Format
- JPEG: Joint Photographic Expert Group
- GIF: Graphics Interchange Format
- PNG: Portable Network Graphic

Figure 2.2 shows a zoom part of a matrix image. The image is a frame extracted from a capsule endoscopy video. The extracted part has clearly lost its certainty with the zooming, not clear as Figure 2.2 shown.

2.3.2.1 Advantages

- The encoding mode of bitmap images (24 bits, RGB coding) makes them suitable for the operation of the main peripherals.
- They are very suitable for complex images.

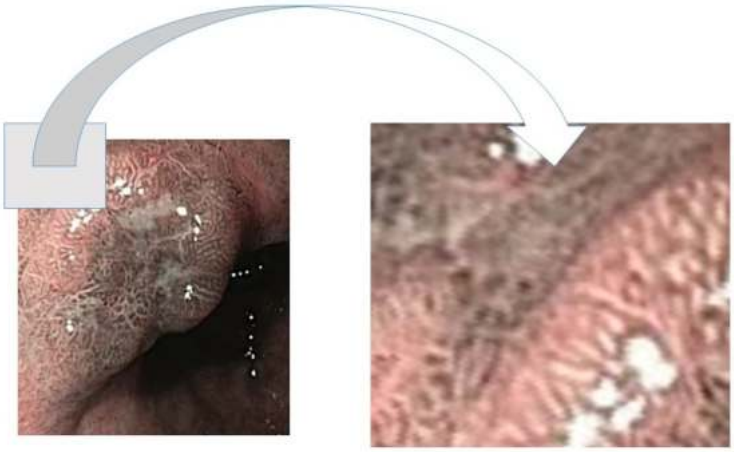


Figure 2.2: A zoom for a part of a matrix image

- Applications of digital images allow several operations such as image quality enhancement, local image changes (contrast, colourimetry, effects, filters, etc.).

- Since the point-by-point coding mode is relatively universal, the transcoding requires repetitive but relatively simple calculations. Compatibility is easy between the different formats.

- The degradation of the data does not necessarily make it unusable.

2.3.2.2 Disadvantages

- Bitmap images have a fixed resolution.

- They do not support resizing, reducing or enlarging operations, these operations could result in a loss of information.

- Bitmap images are heavy with huge sizes for a good quality image.

2.4 Digital image characteristics

In the following, we assume that an image is a raster image (image matrix), and exceptions do exist.

2.4.1 Pixels

Pixels are the numbers as the elements of columns in the image that multiplies its number of lines. For example, an image with 10 columns and 11 lines will have a size of 10x11. Basically, the pixel is a basic unit, of a Square or rectangular, which defines the measure of a matrix image. Thus, each pixel is indeed an image element. A digital image occupies a certain place from the storage device. This special data could be expressed in bytes, and pixels, where the value of the pixel is represented by bits. In RGB colour space, each pixel has a red (R), green (G) and blue (B) component.

- Bit depth

Bit depth is determined by the number of bits employed to define each pixel. Here, each pixel has a numerical value with bit depth which can refers to a colour or gray scale value. Therefore, digital images can be produced in black and white (Binary), grayscale, or colour. For example, when the pixel bit depth is eight bits, a pixel can refers to a grayscale image which contains 256 different values, each value represents a shades of gray. A binary image has 2 bit depth, while in grayscale image we will have 8 bits (one byte) for each pixel value. RGB image pixels could be in totals 24 bits.

2.4.2 Quantization and Sampling

In terminology science, quantization is opposite to sampling. However, digital image processing has another perspective where we cannot say they are opposite. A digital image is digitized with two-step procedures: sampling and quantization (113). The first step is sampling, which refers to a function f(x, y) representing a continuous image. This means that we sampled at points of an ordered array.

Simply, we can say that the image is divided into a set of image elements (pixels). The second step quantization refers to the density value at each pixel (113), and a digitized image could takes integer density values.

- Quantization of pixel values

The image pixel values are commonly converted to a range of integer values using the bit depth, for example, $256 = 2^8$ or $16777216 = 2^{24}$. Occasionally, a floating-point scale is used in professional applications such as medical imaging.

2.4.3 Image size and resolution

The size of an image is determined directly from the width M (number of columns) and the height N (number of rows) of the image matrix I (14).

Generally, resolution is the ability to distinguish accurate detail in digital images, while image resolution determines how many pixels the image shows (92). This mean that the resolution can be referred to the number of pixels, which leads us to the pixel density.

In this context, pixel density can be measured using pixels per inch (PPI), dots per inch (DPI), or pixels per centimeter (PPCM). Those are common terms used to express measurements of the resolution for digital images.

Figure 2.3: Different Pixel Resolutions for logo of university of Batna 2. (a) a block of [512,512] pixels, (b) have a block of [256, 256] pixels, (c) have a block of [128, 128] pixels, (c) have a block of [64, 64] pixels, (e) have a block of [32, 32] pixels.

Figure 2.4: (a) Binary image, (b) Gray image, (c) a colour image

Pixels size defines the resolution with respect to the original digital image so that the larger the grid, the more information is averaged and vice versa. For example, in a case that the number of pixels in the image decreases, the resolution will decreases. Consequently, the quality of the digital image deteriorates. Figure 2.3 illustrates how an image (logo of university of Batna 2) can be appeared at different pixel sampling. Here, pixel resolutions can be represented by the number of pixel columns (width) and the number of pixel rows (height). For example the resolution of the capsule endoscopy systems ranges between 256×256 and 1920×1080 pixels (54).

We sum up some important points regarding digital image resolution.

- PPI is a display resolution. PPI is NOT image resolution.

- DPI is a printer resolution. DPI is NOT image resolution.

- SPI (samples per inch) is a scanner resolution. SPI is NOT image resolution.

-The higher the resolution, the higher the SPI. DPI and PPI are often used instead, although they are actually different measures of resolution.

- In most cases, the resolution of an image is the same in the horizontal and vertical directions (14), which means that digital image resolution could refer to the pixel size of the image with x pixels by y pixels.

2.4.4 Size file of an image

File size is determined by the total number of pixels in an image. A simple equation can be denoted to find the size file of an image if the pixel dimensions are given, where we multiply them by each other and the bit depth to determine the number of bits in an image file as shown in Eq. 2.2 .

$$File\ Size\ (bytes) = \frac{(pixel\ dimensions \times bit\ depth)}{8} \tag{2.2}$$

For instance, if we take a 24-bit image with pixel dimensions of 1024×640, then the file size equals 1966080 bytes (See Eq 2.3).

$$Filesize\ (bytes) = \frac{1024 \times 640 \times 24}{8} \tag{2.3}$$

2.5 Digital images colours

In this section, we present the digital image colour analysis.

2.5.1 Binary images

A binary image is an image for which each pixel can have a value of 0 or 1. Indeed, this type of images is the simplest ones, where typically zero is taken to be black, and 1 is taken to be white. Figure 2.5 elucidate some bits extracted from a binary image.

2.5.2 Gray images

A grayscale image contains only shades of gray and no colour. Also, can be denoted as one matrix image. Here, the pixel value is a single number that represents the brightness of the pixel. The number of pixels is stored as an 8-bit integer giving a range of possible values from 0 to 255. Typically zero is taken to be black, and 255 is taken to be white, and the values of the pixels make up the different shades of gray.

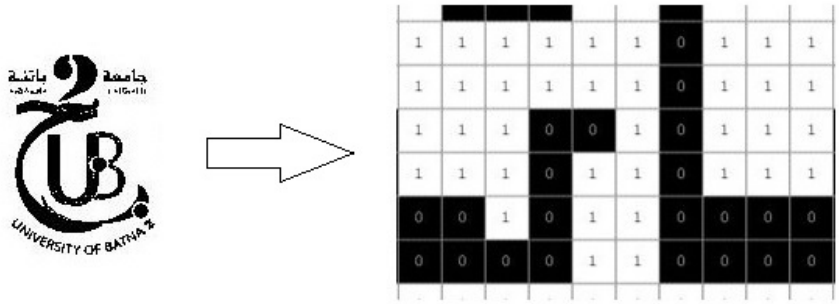


Figure 2.5: Binary image

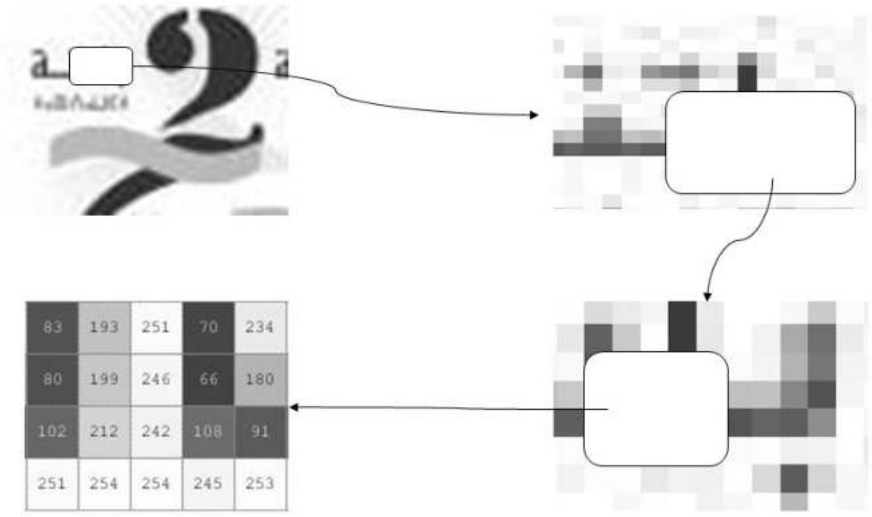


Figure 2.6: Pixels values for a gray image

2.5.3 Colours images

Thanks to a composition made from the space colours, we can obtain very precise colours. One of famous composition for space colours is called RGB mode, where it contains red, green, and blue channels. On the other hand, RGB can be represented by three matrices, each matrix determines the amount of red, green and blue that constitutes the image. For further illustration, Figure 2.7 represents the symbol of our university Batna 2 and its component R,G, and B channel. The pixels of these matrices are integers between 0 and 255 which determine the intensity of the colour of the matrix for the corresponding pixel. Thus, with the RGB colour space, it is possible to represent $256^3 = 2^{(8\times3)} = 16777216$ different

colours. However, RGB colour space is only one of many colour spaces. There

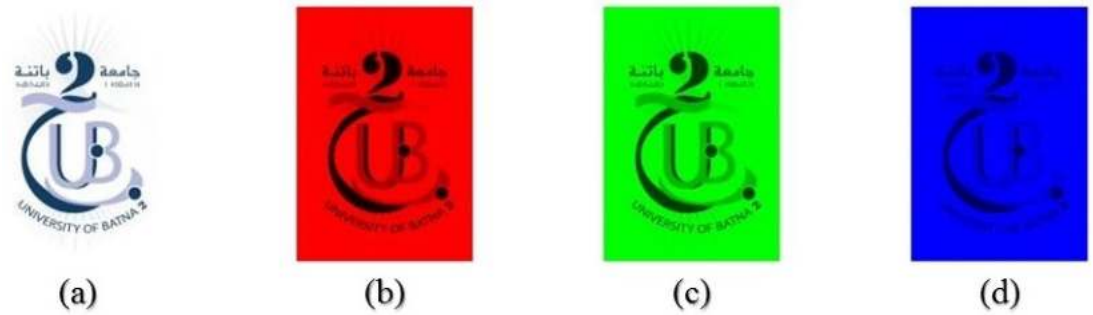


Figure 2.7: (a) Original image, (b), (c), and (d) components Red, Green and Blue, respectively.

are many other colour spaces, for various uses. For an example: Four-colour or CMYK used manually in print, Y'IQ for analog TV. In the next subsections, we

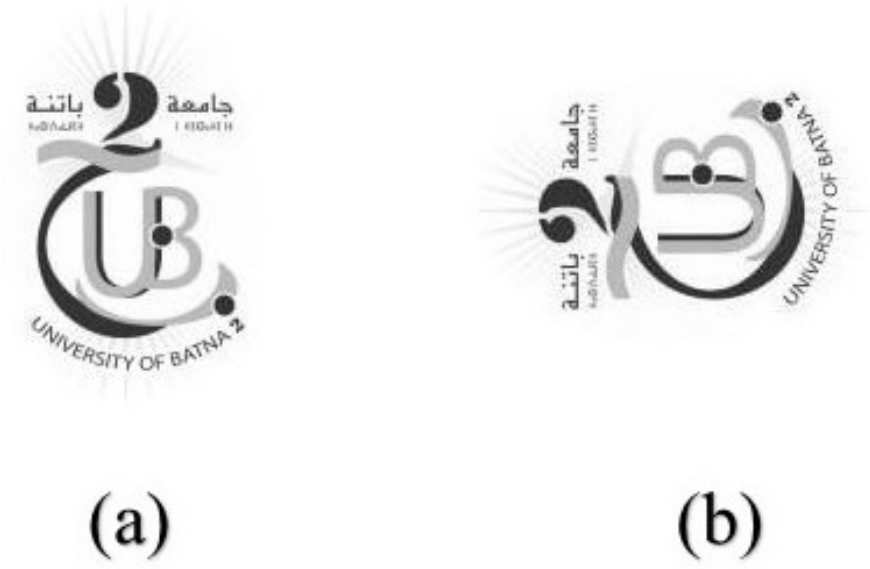


Figure 2.8: Matrix transformations effect on the visual show for a gray image.

will discuss the difference between true colour images, and indexed images.

2.5.3.1 True colour images

True colour images are appropriate when the image contains many colours (14). Here, true colour images utilize colours uniformly selected from the entire colour space. Note that this type consists of 24 *bits RGB* (14), with 16,777,216 (2^{24}) different possible colours. There are two methods of ordering the colour components in true colour images.

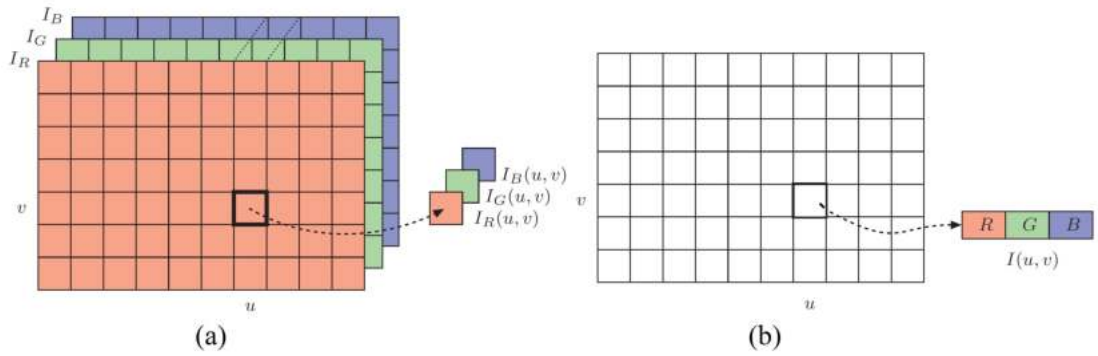


Figure 2.9: RGB image colour ordering. (a) RGB colour image in component ordering. (b) RGB-colour image using packed ordering.

The first is component ordering which referred to the colour components are laid out in the separate arrays. Figure 2.9 (a) shows an RGB component values of an colour image I at position (u, v).

The second method is the packed ordering. Here, a single element of the image array (a single pixel) contains a packing components that can represent the three components of the colour.

2.5.3.2 Indexed colour images

In indexed colour images, only a selected set of distinct colours are used. Mostly this type is used for illustrations and graphics that contain large regions of the same colour (14). Figure 2.9.(b) shows the RGB component values packed together into a single element of the image array.

Figure 2.10 shows RGB indexed for image $I_{index(u,v)}$. Readers are referred to Ref (14). Here, each pixel is listed in a vector index k. The colour value for each k

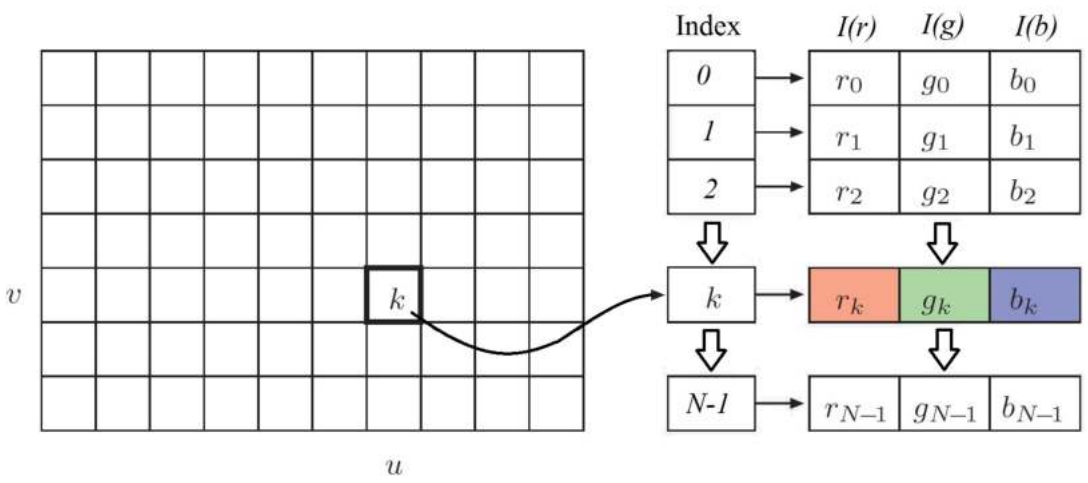


Figure 2.10: RGB indexed image.

is defined by an entry in the colour table (next to image matrix). Indexed images contents of the colour table are not intensity values (like in grayscale image) but RGB values.

2.6 2D images & 3D images

2D images are flat, and the scene can referred to visual imaging, while 3D images have depth. Herein, the brain processes the 3D images that can perceive the depth and distance in the image.

Basically, 2D image is a matrix with a set vectors which have (u, v) as indexes for elements of the matrix. Here, matrices have two dimensions only, the row and the column dimensions. Three dimensions image can be represented by N matrices which employs the depth for real representation. These dimensions include width, depth, and height. Figure 2.11 shows 3D reconstruction from multiple medical images (for a brain).

Figure 2.12 shows a 3D side-by-side images (left&right) which considered as a 3D technique. The figure shows a 3D-frame from 3D video of a surgery, which obtained from Dr. Thushara Hewage, university of Cardiff (48).

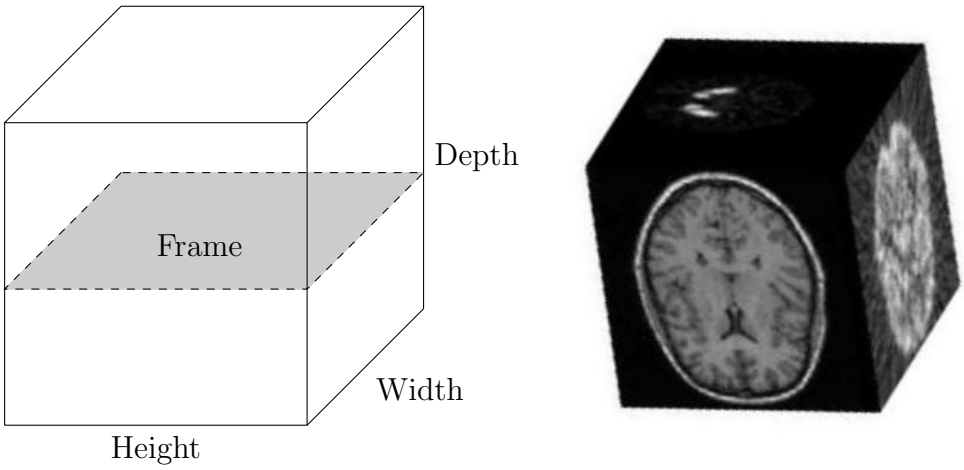


Figure 2.11: 3D reconstruction from multiple medical frames.

A 3D image is defined by a scalar function of three variables $f(x, y, z)$, where f represents a characteristic value at a point (x, y, z) in 3D orbits (see Figure 2.13).

Although RGB images contain three matrices, but they do not illuminated to any depth, only referred to the colour matrices.

Technological advances have allowed for convert of the two-dimensional image to three-dimensional. In this regard, 2D images can be converted to 3D images. In principle, 2D-to-3D conversion algorithms derive a depth map sequence from

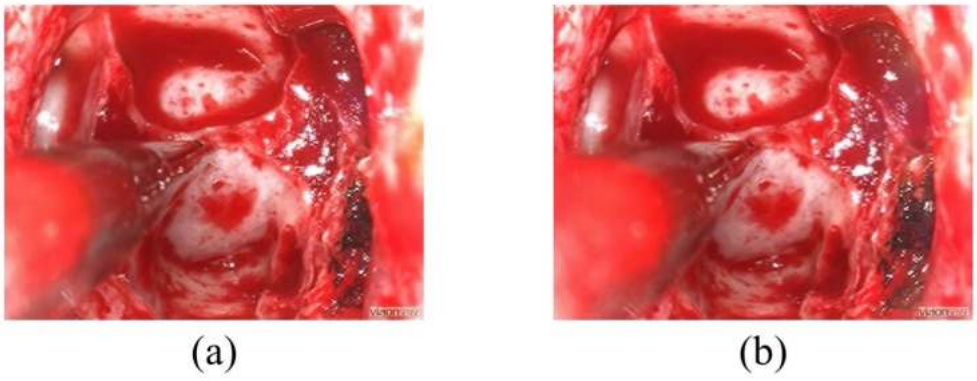


Figure 2.12: Left and right (Side-by-side) 3D image.

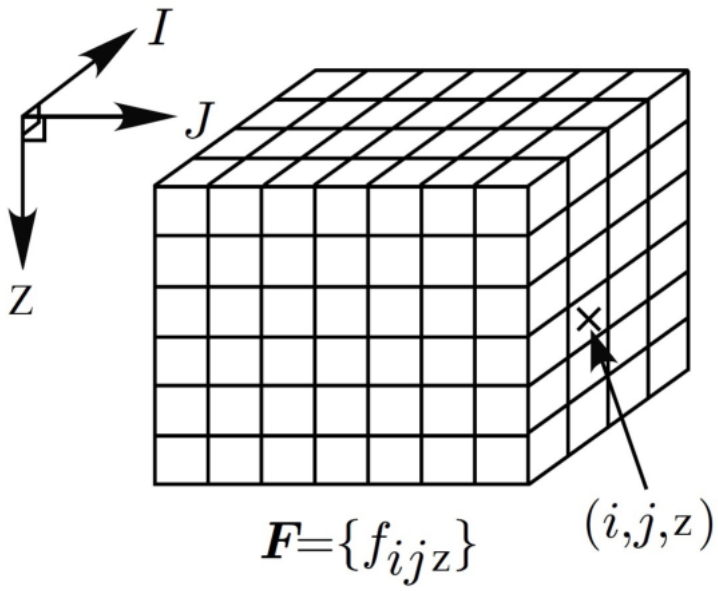


Figure 2.13: 3D image.

a 2-D still image sequence (48).

2.7 Image processing operations

As we have discussed previously, an image can be represented by a set of matrices. The number of this matrix can indicate if the image is a binary image (in a case of pixels are 0 or 1), a gray image (in a case of one matrix) or a colour image (in a case of Multi-matrices).

Image operation is the function $T[.]$ which transforms an input image I(x,y) into an output image C(x,y) according to the formula 2.4.

$$C(x, y) = T[I(x, y)] \tag{2.4}$$

Where x,y are pixels of the image, mainly are integers in $\{0, 1, .., 255\}$.

For example, considering the gray image A (See Figure 2.8 (a)) as a matrix $A = (a_{i,j})$, then the image B (See Figure 2.8 (b)) corresponds to the transposed matrix of $B = A^T$, where: $(b_{i,j}) = (a_{j,i})$.

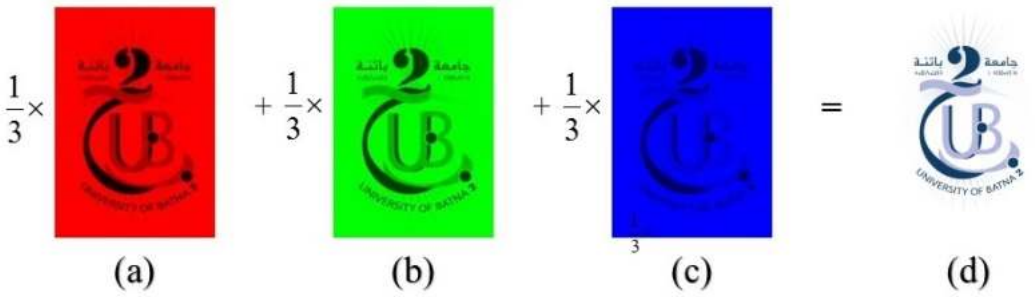


Figure 2.14: Arithmetic mean for the components of an RGB image

Another example with colour space, if the matrices R, G and B of the colour images are arithmetically arranged, a version of the gray level image is obtained (the values are rounded to the nearest integer):

Basically digital images are just matrices of pixels, that allow us to do multi-operations of manipulation across images for different purposes. The number of pixels also determines the complexity of the hardware used to manipulate these pixels (92).

Increasing the image's contrast by 50% can be accomplished using Eq 2.5.

$$\begin{cases} newR = R \times \alpha_R \\ newG = G \times \alpha_G \\ newB = B \times \alpha_B \end{cases} \tag{2.5}$$

Where α_R, α_G, and α_B specify how much changes required to scale the R, G, and B components of colours. Also, this could be employed to adjust the colour balance of an image.

Figure 2.15 illustrates brightness and contrast in detail using Eq 2.5. Here we take $\alpha_{(R)} = \alpha_{(G)} = \alpha_{(B)} = \alpha_{(R,\ G,\ B)}$. Where $\alpha_{(R,\ G,\ B)} = 0.25$ for Figure 2.15.(d) , $\alpha_{(R,\ G,\ B)} = 0.5$ for Figure 2.15.(b) , $\alpha_{(R,\ G,\ B)} = 1.25$ for Figure 2.15.(c) , and $\alpha_{(R,\ G,\ B)} = 2$ for Figure 2.15.(a).

The matrices manipulation can be employed with many applications in digital images processing. Security is one of critical applications for most of these manipulation. For example, image encryption is a manipulation from a plain image

Figure 2.15: Brightness and contrast tests.

to a random image or unclear image that cannot lead us visually to the original ones. Figure 2.16 shows encryption of a medical image. Herein, Figure 2.16(a) shows a keyframe extracted using our a video summarization scheme. Figure 2.16(b) shows the encrypted keyframe using our proposed scheme. Figure 2.16(c) shows the corresponding decrypted keyframe.

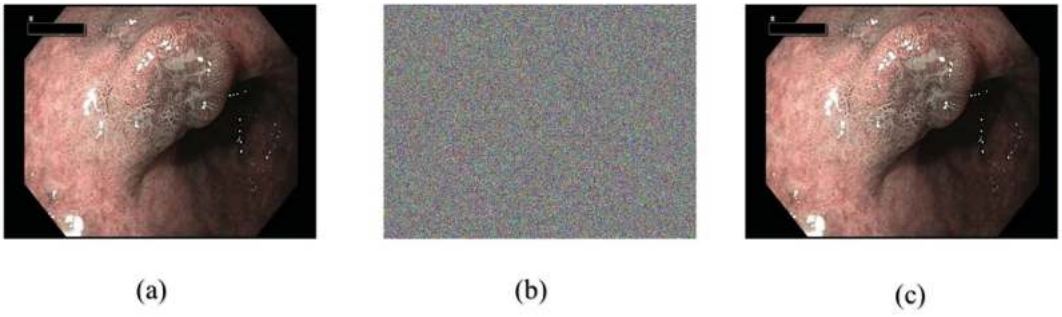


Figure 2.16: Encryption of a medical image.

2.8 Medical images

The purpose of medical imaging is to create an intelligible visual representation of a medical information (3). Medical imaging can be utilized with several different physical principles of imaging modalities. Here, medical images as an image that

is used for the diagnosis of diseases in addition to clinical examination and other investigations such as biological examinations (1). Thus, we can manifest that medical images is each image that is related to the medical body no matter its extension or its type.

In this regard, many critical problems in medical diagnosis await the development of novel approaches and new transducers (104). As results, many inventions have been proposed to improve the human being conditions. Hence, one of the most recent invention for the healthy human being is wireless capsule endoscopy device.

2.9 Conclusion

In this chapter, we have presented some notions on images in general manner, and processing digital images specifically. We have endeavoured to explain the underlying scientific principles of the major digital images techniques. In this pursuit, we have discussed some aspects of image processing, and the important related knowledge for our study. Evidently, the need to secure these digital data is paramount. Thus, cryptography mechanisms are required to ensure the digital images' security.

3

Security Mechanisms

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

Bruce Schneier

Contents

3.1 Introduction 31

3.2 Secure Digital Images 31

3.2.1 Cryptology 32

3.2.2 Security concepts 32

3.2.3 Cryptography 33

3.2.4 Cryptanalysis 34

3.3 Probabilistic approach 35

3.3.1 Randomized algorithms 35

3.3.2 Summarization algorithms 36

3.4 Encryption terminologies 37

3.5 Encryption types 39

3.5.1 Asymmetric encryption 39

3.5.2 Symmetric encryption 40

3.6 Ciphers modes 41

3.6.1 Cipher stream 41

3.6.2 Cipher block 41

3.6.3 Comparative study 41

3.7 Substitution-Permutation Network 42

3.7.1 Rijndael Advanced Encryption Standard (AES) 44

3.8 Chaos Theory 48

3.9 Requirements and metrics 50

3.9.1 Kerckhoffs principles 51

3.9.2 Encryption requirements 51

3.9.3 PRNG requirements 52

3.10 Semantic Security 53

3.11 Conclusion 55

3.1 Introduction

Digital images security has become an issue over the internet and network applications due their growing use. Here, cryptography can propose some reliable solutions to secure the digital images, cryptography can propose some reliable solutions to secure the digital images, where various mechanisms can present necessary protection against the intruders attacks. one of the solutions employed is the probabilistic approach. In this pursuit, we aim in this chapter to illustrate an overview of the probabilistic approaches and the cryptography encryptions.

In this chapter, we present general thoughts about security mechanisms for the digital images, particularly with encryption mechanism, their characteristics and the challenges that face applying to the digital images. Also, we present some probabilistic approaches that are employed in our works. The objective is to propose a survey about the research works that tried to meet the main requirement: digital images security.

3.2 Secure Digital Images

In this section, we listed the main mechanisms to guarantee digital images privacy. Security in cryptography is usually defined by the combination of a security goal and an adversarial model (27). The main objective is to ensure that the attacker cannot learn the message or the secret key. The word "Learn" here means that the attacker should not be able to analyse the cryptosystem and get the message or the secret keys. Using Probabilistic encryption can guarantee that no information will be available to attackers to build his cryptanalysis model. This means that the adversary should not learn parts of the message, e.g. a block of bits of the message. Adversary should not learn any predicate of the message, e.g. he cannot find a relationship between the encrypted data and the original data. Adversary should not be able to recognize any relations between encrypted messages, for instance, he should not know if a message was sent twice.

Digital images have unique merits such as the correlations among the pixels of the image, large volume and high redundancy (61). Thus, the traditional ciphers techniques may not provide good solutions to ensure digital images security. As

results, some alternatives security techniques are discovered. The strategy to perform and achieve digital images security can be mainly divided into two parts:

In the first part, Data hiding techniques allow hiding some information into a digital content like an image. The host data can be detected or extracted later by means of computing operations to make an assertion about the data (93)

In the second part, cryptology approaches include cryptography and cryptanalysis. The main study in this dissertation contains this part in the following sections and chapters.

3.2.1 Cryptology

Cryptology addresses the security studies of information with cryptography and cryptanalysis. It is the foundation of all information security (114).

Cryptology is the study of cryptosystems by all means. Mainly, cryptography and cryptanalysis are disciplines from cryptology (114). In this regard, cryptography studies the structures of cryptosystems, while cryptanalysis studies how to break of these cryptosystems.

3.2.2 Security concepts

Key concepts of information security based on cryptology are mainly divided into four aspects.

- Authentication

Authentication is a process of verifying users identity. The recipient of a message must be able to verify its origin. Here, an intruder must not be able to pretend to be someone else. Copyright is good example here to guarantee identity authentication, where protection of the property rights of a digital image is of paramount importance in emerging multimedia applications(94).

- Confidentiality

Confidentiality is a process to guarantee that only the authorized users with the right permission can access and use data. A good example to safeguarding data confidentiality is by using encryption schemes. The encrypted data must be readable only by the authorized recipients. Here, it must not be able to be read by an intruder (decryption is enabled only by the authorized recipients).

- Integrity

Integrity is a process of confirming the image pixels accuracy which safeguarding information data. Herein, the recipient of a data must be able to prove that it has not been adjusted. An intruder must not be able to pass a false data to the authorized recipient. Here, a hash function is a mechanism to ensure the integrity of a digital image.

- Non-repudiation

A recipient must not be able to erroneously deny sending a message. Here, a proof of data integrity and authentication are typically the easiest of these requirements to accomplish non-repudiation.

In the following part, we introduce cryptography and cryptanalysis for a better understanding to security mechanisms.

3.2.3 Cryptography

Cryptography is the art of mathematical theory, where maths equations are employed to confirm content security for information in communication. The means included various purposes such as cipher, hash, digital signature, key generation, and authentication (61). One of the main mechanism to secure the digital images based cryptography is the encryption. The cipher is a mechanism to transform the original information into an unintelligible form under the control of a secret keys. The encryption is considered as the main technique to protect confidentiality of the data.

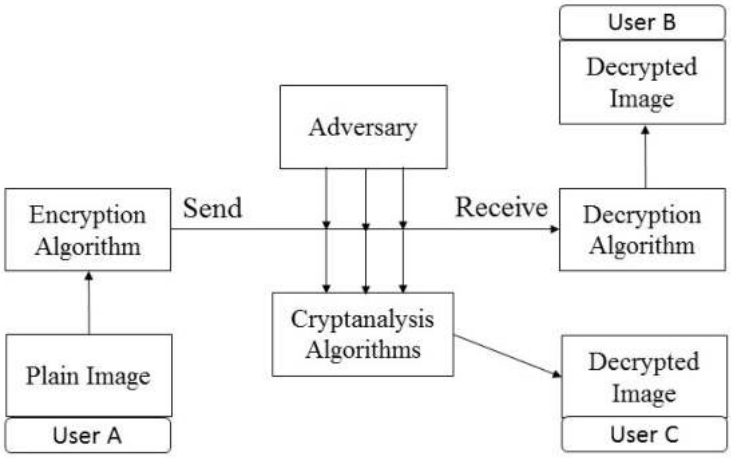


Figure 3.1: Scenarios of cryptosystem/cryptanalysis

3.2.4 Cryptanalysis

Cryptanalysis focuses on the methods to analyze or break cryptographic means. In Cryptanalysis image encryption, it means that it provides some special algorithms to analyse the security of cipher structure. Decrypting the encrypted image should be near to impossible without the authoritative users (have the secret keys).

Recently, some security issues have been presented with the encryption schemes (57, 59, 63, 122), mainly from three reasons: key space, the structures algorithmic and their combination. Figure 3.1 shows a framework of a cryptosystem (in a normal process) and an attacker trying to crack/analyse the encrypted images without the secret keys, where users A, and B are the authorized users, while user C is the Adversary (not authorized user). Here, and according to Kerckhoff's principle (15), the security of a cryptosystem should not depend on keeping the cryptographic algorithm secret (19). This means that the structure of a cryptosystem should be considered as known to an adversary. Herein, the attacker will proceed to break either the key or the cipher structures, and in some cases there are reported for breaking the cipher algorithms based on the weakness of both structures (59).

3.3 Probabilistic approach

A probabilistic approach is an approach where the result and/or the way the output is obtained depends on chance. Furthermore, it works for all practical purposes but has a theoretical chance of being wrong. Algorithms such as randomized encryption schemes and summarization algorithms are defined as probabilistic algorithms.

3.3.1 Randomized algorithms

Randomized algorithms are algorithms that make random choices during their execution (76). In encryption field, a probabilistic encryption scheme is a randomized cipher algorithm. The first probabilistic encryption scheme was introduced in 1982 by Goldwasser-Micali (39).

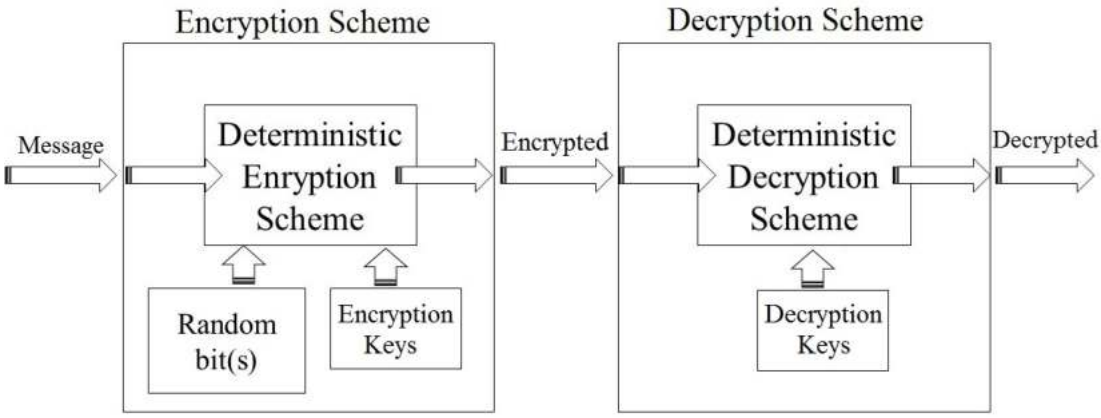


Figure 3.2: Block diagram of a randomized encryption procedure (39)

In randomized encryption, the generated ciphered images should be completely different from each other even under the same secret key of the encryption scheme and the plain image. Cryptographers often enhance the security of their codes and ciphers structure by using randomization in the encryption process (98). Moreover, randomized cipher attempts to obtain higher levels of security through increasing the entropy of the message (105). Randomized encryption schemes require a source of random bits (98). Figure 3.2 shows a randomized

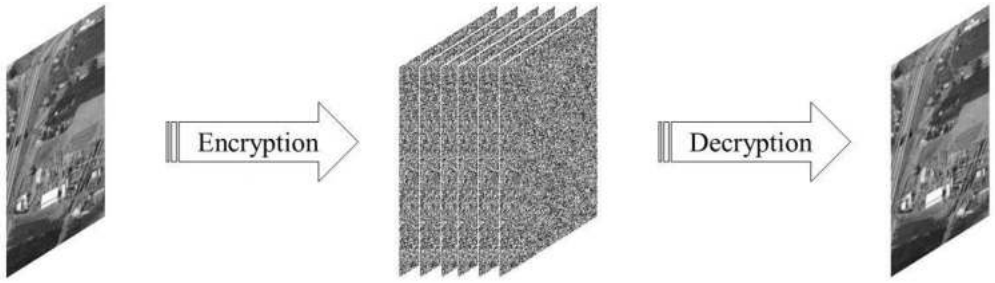


Figure 3.3: Probabilistic image Encryption/Decryption.

encryption procedure block diagram to secure transmission of data over an insecure communications. Here, we assume that an enemy cannot determine the intermediate results or the encryption and decryption computations, where the ciphered data is acting like a true random numbers.

A randomized encryption attempts to obtain higher levels of security (98). Figure 3.3 shows the ciphered images C_1 and C_2 produced by a randomized encryption twice for same plain image and secret keys. As shown, the ciphered images are different $C_1 \neq C_2$, and the decryption leads to the original image (at least visually).

One of the famous technique to randomize the ciphers structure is by adding random bits (98). A good example will be with our work (46). Herein, we employed the sensibility of any adjustment in plain-image pixels to produce a probabilistic ciphered images. Basically, we randomized the plain image by embedding only one bit in random position into image pixels. Although, the decrypted image will lose one bit in its accurate, but it will guarantee a cryptosystem that is semantically secure.

3.3.2 Summarization algorithms

A major problem associated with the new technology is with the huge amount of images that need to be manually examined by clinicians (33). Video synopsis technology is presented as solution for fast browsing a days worth of video in several minutes, especially with the explosive growth of video data (32) such as

in video capsule endoscopy with 8 hours of capturing around 50000 frames (65), and ofcourse there is the surveillance video data.

In summarization schemes, where a frame can be extracted as keyframe with possibility of being false keyframe. Generally, a video summary is a sequence of still or moving images, and could be with audio (38). So, a video summarization algorithm shall endeavored reducing the amount of data that must be examined (for example in a case of capsule video) in order to extract an important piece of information in a video. For more details, see chapter 6

3.4 Encryption terminologies

The following points show the meaning of famous terms in image encryption.

-Encryption algorithm

Encryption Algorithm contains the steps of encrypting the plain images (clear form) into encrypted image(unclear form). The encryption of an image cannot proceed without a secret key.

-Decryption algorithm

Decryption Algorithm is the steps of inverting the operations of encryption algorithm, which decrypt the encrypted image (unclear form) back into the plain images (clear form). The success of decryption of an encrypted image cannot be achieved without the secret key.

-Plain image

Plain image is the original image before proceeding to encryption processes. Also, the original images can be defined as a plainImages or clearImages, and unencrypted images.

-Ciphered image

Ciphered image is the encrypted image which is a result of transforming the plain image to ambiguous and unintelligible image.

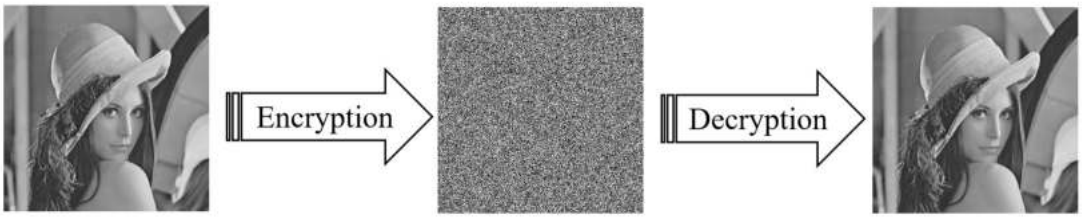


Figure 3.4: Encryption and Decryption of an image "Lenna".

-Decrypted image

Decrypted image is a result of transforming the encrypted image to plain image. The decryption can lead to a decrypted image appear as the plain image, but not with same accuracy the original ones. The original image can be restored from the encrypted image without any loss of its integrity and its accuracy, herein is the second type of decryption.

Figure 3.4 shows a plain image (Lenna) and its corresponding ciphered image, and finally the decrypted image based on our proposed image encryption scheme (46) (see chapter 5)).

-Secret keys

A Secret Key is an array of data that are employed to encrypt or decrypt the digital images using cryptographic functions. The Secret keys can be symmetric or asymmetric (see the next sections for more details). Generally, the secret keys are employed to produce appropriate keys for the digital images (Encryption Keys). Note that in most cases of chaos-based image encryption, the initial values (called seeds) of the chaotic maps considered as secret keys in many works (62, 91, 123, 130).

-Encryption keys

An Encryption key is a cryptographic algorithm that uses the secret key to generate appropriate keys for encrypt and decrypt the digital images. PRNG is well-known method to produce these encryption keys for the digital images. Figure 3.5 shows the steps of using the secret keys to manufacture PRNG, the generated keys will be employed either for encryption or decryption.

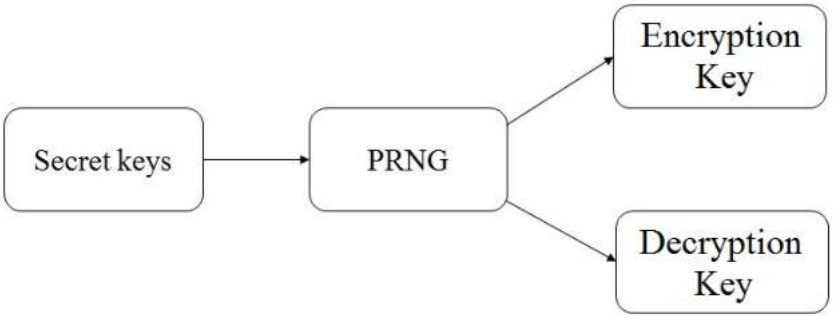


Figure 3.5: Framework of generating the cryptographic keys.

-Pseudo random numbers generator

A pseudo random numbers generator (PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers (50, 125). In most cases, the generated sequences are for image encryption algorithms (see chapter 4). A good example here is linear feedback shift register (LFSR) (61, 68) which can be used as a PRNG too. The initial secret keys is required to generate the random sequences which are keys employed in many cryptographic purposes.

3.5 Encryption types

In this section, we present the type of ciphers algorithms, which are categories in to two categories based on secret key structure.

3.5.1 Asymmetric encryption

Asymmetric encryption is called public ciphers too. Generally, the secret key is divert from the encryption to the decryption. This means that the cryptosystem could use two keys, one for encryption and the other for decryption.

The asymmetric cipher can be defined mathematically as follows:

$$\begin{cases} C = E(P, K_E) \\ P' = D(C, K_D) \end{cases} \tag{3.1}$$

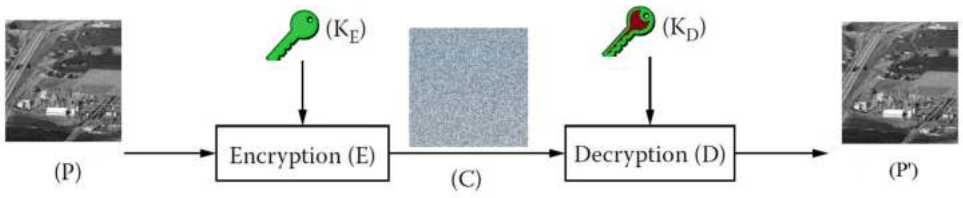


Figure 3.6: Architectures of asymmetric encryption.

Here, K_E and K_D are the encryption key and decryption key, respectively. Figure 3.6 shows the architectures of a asymmetric image encryption scheme based on Equations 3.1. while P, E(), D(), and P' are the original image, encryption algorithm, decryption algorithm, and decrypted image, respectively. Some public ciphers have been published based on mathematical difficulties such as the difficulty of factorization of large prime numbers in RSA (61, 71), and the difficulty of the discrete logarithm problem in Finite Fields for ElGamal (61, 71).

3.5.2 Symmetric encryption

In this architecture, the encryption key is the same as the decryption key. This means that the decryption operation is symmetric to the encryption operation. In this case, the symmetric cipher can be defined mathematically as Eq 3.2 shows.

$$\begin{cases} C = E(P, K) \\ P' = D(C, K) \end{cases} \tag{3.2}$$

Here, P, C , P', K, E(), and D() are the original image, encrypted image, Decrypted image, the secret keys, Encryption scheme, and Decryption scheme ,respectively. Figure 3.7 shows the architectures of a asymmetric image encryption scheme based on 3.2.

In the symmetric encryption, the key K is only known to the sender and receiver. Thus, it should be kept private and not be made known to a third party.

According to this property, a symmetric cipher is also called a private cipher. Well-known symmetric ciphers include Data Advanced Encryption Standard (AES) (20).

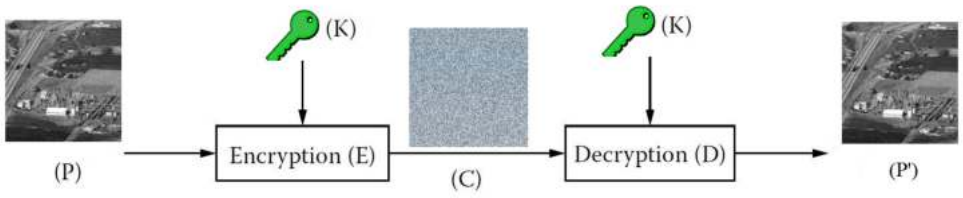


Figure 3.7: Architectures of symmetric encryption.

3.6 Ciphers modes

The cipher techniques can be also classified into two modes based on the cryptosystem structures.

3.6.1 Cipher stream

- A typical stream cipher encrypts the data one byte at a time, although a stream cipher may be designed to operate on one bit at a time or on units larger than a byte at a time (62, 109). Further details in stream cipher, the original image P can be modulated by the random key sequence K. The XOR operation often acts as the modulation operation (61, 71). Disadvantage of Stream Cipher

3.6.2 Cipher block

-In Block cipher, the encryption modes are operated on blocks of a certain length in the plain image (109). So, A block cipher operates on image blocks of a fixed size, instead of on individual pixels. The output changes almost completely when only one bit of the input is changed (115). Furthermore, this property of embedding one random bits into the original image makes the proposal encryption probabilistic algorithm.

3.6.3 Comparative study

In this part, we present a comparative study in short based on relevant works (21, 56, 107, 132). The following points shows the main results .

• Block ciphers typically works on larger chunks of data and often have proceed from previous blocks of the data. Herein, block ciphers require more memory than steam ciphers. While the stream cipher works with bits at a time, which they have low memory requirements relatively.

• As data is usually processed and transmitted in the form of "blocks", block cipher can be easily implemented comparing with stream process.

• The stream ciphers are typically faster than block ciphers, but some studies did not take into consideration the characteristics of digital images.

• PRNG has same strict requirements for both block image encryption and stream image encryption.

• Some block ciphers with excellent S-box (see substitution-permutation network section) required accuracy to have the decrypted image, where identical ciphertext blocks imply identical plaintext blocks (56). This can provide integrity protection, and authentication in addition to the confidentiality.

3.7 Substitution-Permutation Network

Over the last decades, permutation-substitution network is considered as the most common symmetric key cryptosystem. The network is comprised of a number of rounds of permutation, substitution (12). Substitution-permutation network is also a special type of iterated block cipher. This model has several attractive features such as the simplicity of the design along with its efficiency in hardware and software (110). The Permutation Box (P-box) and the substitution-box (S-box) are utilized to provide confusion and diffusion (131). Indeed, these boxes are used widely with almost all famous references of block ciphers schemes such as "DES" and "AES".

Shannon (105) in 1945 has proposed the most famous properties in encryption data: the confusion and diffusion properties. An algorithm with confusion-diffusion structure encrypts the images with a number of iterations, in each iteration shall be composed of a confusion operating as well as a diffusion operating (105). Herein, both confusion and diffusion properties can ensure the ciphered

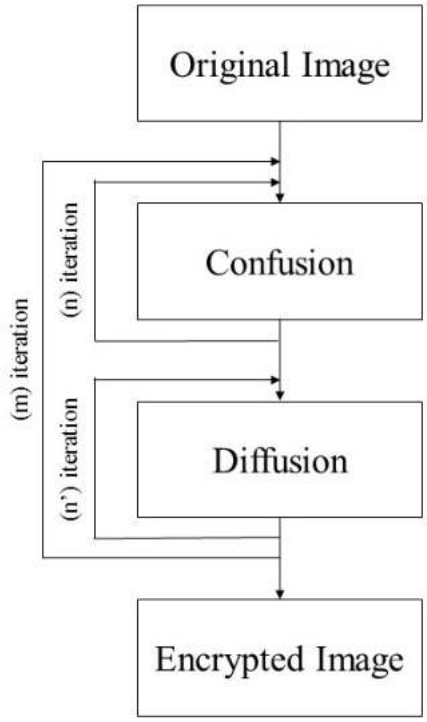


Figure 3.8: Confusion and diffusion algorithm

image security (137). Figure 3.8 shows the common steps of encrypting an image by a confusion and diffusion algorithm, where n, and n' iterations for each confusion and diffusion step, and m iteration for both steps.

• Confusion in encryption image means that the operation of changing the positions for the pixels from the plain image to ciphered image. For instance, Figure 3.9 shows the pixels matrix (with 5×5 pixels as its size) and the scrambled matrix.

• Diffusion in encryption image means that changing a single pixel of the plain image shall change many pixels of the ciphered image. For instance, Figure 3.9 shows that changing one pixel, from the plain matrix with 5×5 pixels as its size, led to change many pixels.

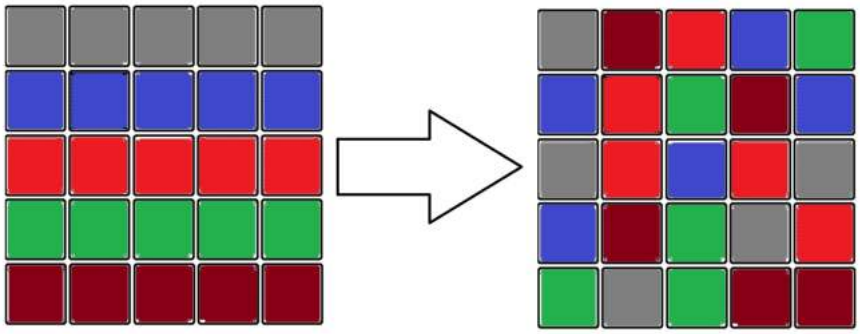


Figure 3.9: An instance of confusion algorithm of a pixels block.

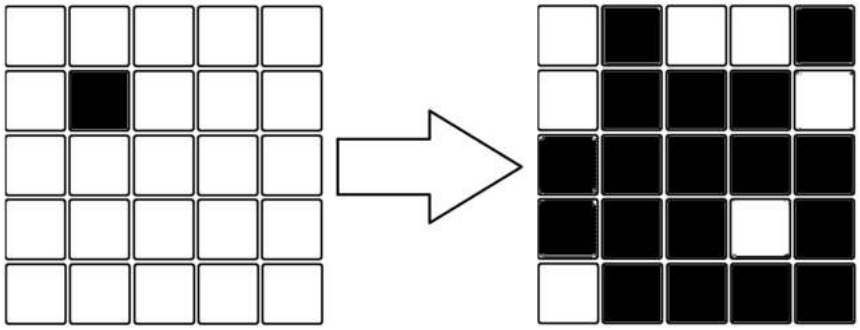


Figure 3.10: An instance of diffusion algorithm of a pixels block.

3.7.1 Rijndael Advanced Encryption Standard (AES)

Rijndael AES is a multi-iteration symmetric block encryption algorithm with a size of blocks and keys that are higher and variable, chosen between 128, 196 and 256 bits (20, 99) and recently improved to 512 bits (77) . Basically, AES was introduced to replace the DES (20). Upon to this day, exhaustive attacks are the only effective attacks known against this algorithm.

In the recent years, there were several implementations done for the original standard AES (20, 77). In this section, we study advanced encryption standard Rijndael, where more details about 128-AES structure are described in the coming points.

Finite Field

As known, a byte "A" is composed of 8 bits which can be represented as $A_7, A_6, A_5, A_4, A_3, A_2, A_1, A_0$. In Finite Field, this representative can be seen as a polynomial of degree less than or equal to 7 with coefficients {0,1}.

$$A_7\ x^7 + A_6\ x^6 + A_5\ x^5 + A_4\ x^4 + A_3\ x^3 + A_2\ x^2 + A_1\ x + A_0 \qquad (3.3)$$

The addition of two polynomials over the finite field is the same as the adding modulo 2 to the coefficients of each. Or, we can say that this addition corresponds to the exclusive OR $\oplus$.

The multiplication of two polynomials, it is a multiplication followed by a reduction modulo an irreducible polynomial of degree 8. Obviously, the result of this multiplication will be a polynomial of degree less than or equal to 7.

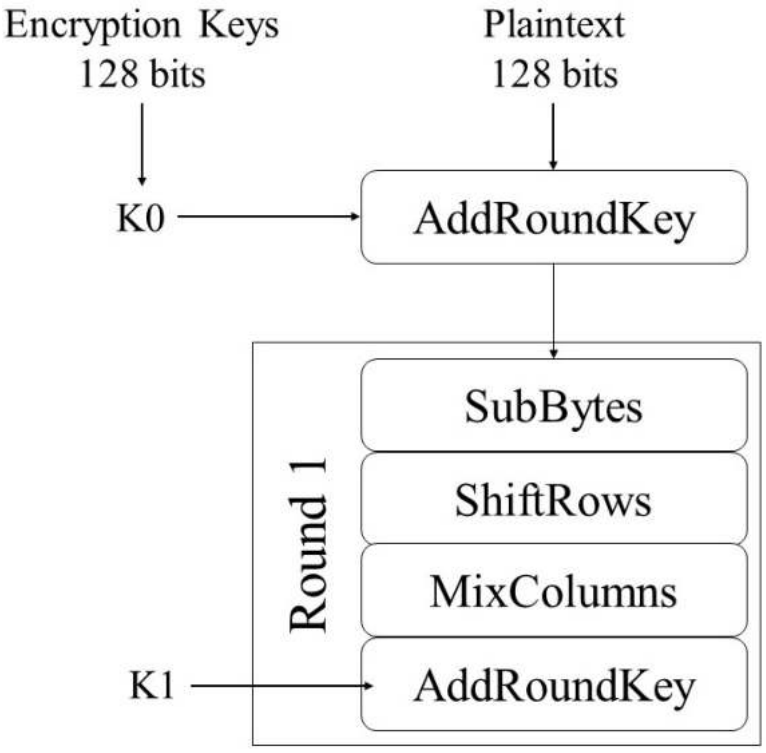


Figure 3.11: First round process in 128-AES

Overall Structure

Note that the following explanation only applies to 128-AES (with 128 -bit key). The structure is based on a block cipher with array of 4×4 bytes. AES breaks data into matrices of bytes (called states) and encrypt every state independently of each other. Here, a state is defined as a matrix referred to each element in the data (please see 3.4). In this point, digital image has high correlations among the pixels which requires encrypts the mentioned states to eliminate this correlation.

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,2} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \tag{3.4}$$

Rijndael uses fours main operations :

- `SubBytes` (S-box),
- `ShiftRows`,
- `MixColumns`,
- `AddRoundKey`.

1- In the step S-box, each byte is replaced with another byte using the equation affine: $Ax + B$ over the finite field $(GF_2)^8$. In a case of a byte is 0 which does not have an inverse in the finite field, the byte remains 0. Figure 3.12 depicts the first round process.

$$Ax + B = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{3.5}$$

Where $[x_7, ..., x_0]$ is the multiplicative inverse as a vector. And we denote the matrix A as a matrix 8×8 with coefficients in GF_2 and B a binary vector where $B \in (GF_2)^8$.

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

2- In the step of ShiftRows, we make a circular permutation to the left to the rows from the array, respectively of 0, 1, 2, 3 boxes:

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\longrightarrow$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

. Mainly, this process is an operation to scramble data.

3- In the step of MixColumns, we take each column in the state and perform linear transformation on it. MixColumns interprets as a matrix multiplication over the finite field $(GF_2)^8$:

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$\longrightarrow$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Where,

$$\begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,2} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix} = \begin{pmatrix} \alpha & \alpha+1 & 1 & 1 \\ 1 & \alpha & \alpha+1 & 1 \\ 1 & 1 & \alpha & \alpha+1 \\ \alpha+1 & 1 & 1 & \alpha \end{pmatrix} \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,2} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

4- AddRoundKey: Here, bitwise addition (XOR) of each round key K_i, cell by cell. This means that for each round, a subkey is derived from the main key. Indeed, this is the most important stage in AES as it provides inevitably a complex operation. The schematic of 128-AES structure is given in Figure 3.12.

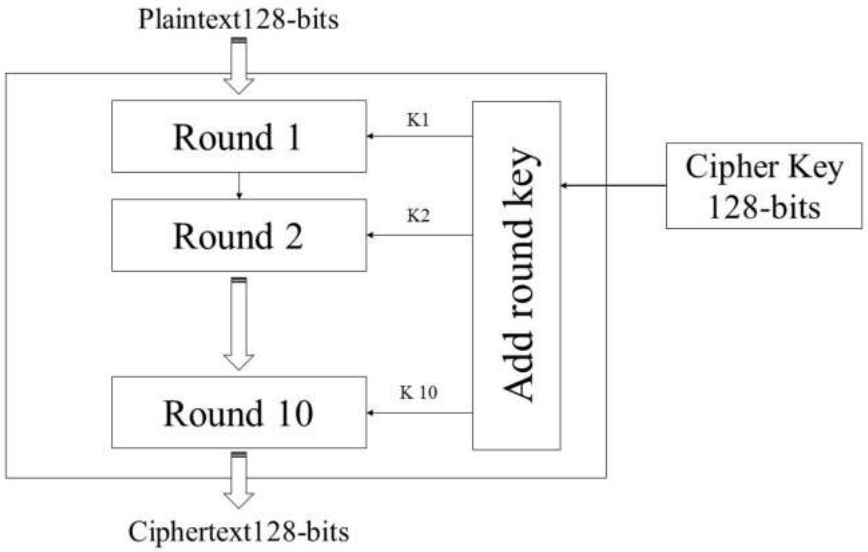


Figure 3.12: schematic of 128-AES structure

For more deep details regarding AES structure, see (11, 77, 95).

3.8 Chaos Theory

In this part, we examine the theory behind chaotic cryptosystems in order to ensure digital images security.

The chaotic maps can be distinguished by a discrete-time such as logistic map (26), or a continuous-time like chen chaotic system (60). Generally, the nonlinear systems have parameters controlling and initial seeds, whichever the nature of these maps (discrete or continuous). Here, the chaotic systems should be robust which means they remains chaotic in a continuous interval of the parameter space (75). The logistic map is one of the famous chaotic systems, considered as a prelude into the chaotic systems.

Generally, these maps proved their importance in several fields, and especially with cryptography applications including light-weight image encryption algorithms (70, 91), and watermark schemes (78, 133), true and pseudo random number generator (36, 116, 138).

Additionally, chaos-encryption algorithms have been proposed as a solution for digital images security (121, 129). In this regard, chaos-based algorithms are consisting of two steps: confusion shuffling and diffusion, based on substitution-permutation network. The advantages of employing the chaotic maps are related to their characteristics, which have many excellent intrinsic properties such as the high sensitivity to initial conditions and controlling parameter (72).

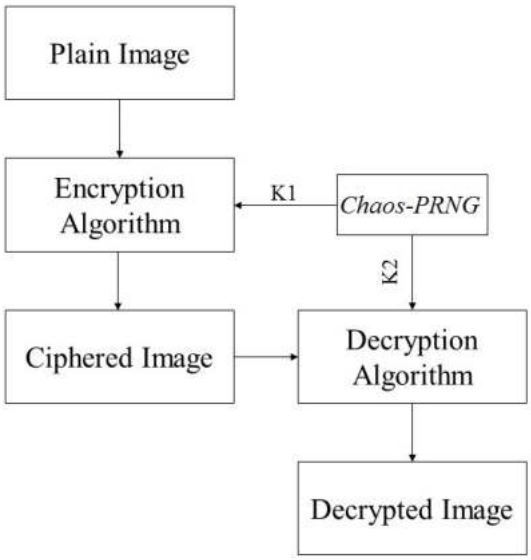


Figure 3.13: Mechanism of PRNG for image encryption.

PRNG is a good example of chaos-based cryptography applications, where the encryption keys are generated to encrypt digital images. Figure 3.13 shows the rule of PRNG for encrypting digital images. The PRNG generates two keys $K1$, and $K2$ employed for the structure of encryptions, where these keys can be the same ($K1 = K2$) in a case of a symmetric encryption algorithm.

However, using chaos systems for encryption purposes is not always secure. For an example, employing lower chaotic maps like logistic map is insecure and can not resist attacks such as brute-force, and the attackers are able to beat almost

all the one-dimensional chaotic maps (50). Furthermore, chaos-based algorithms have some problems such as problem of the compute finite precision, which can degrade the dynamical behaviour, and become less random or waste its chaotic behaviour. This means that the generated PRNG or the ciphered image will have a short cyclic length of its sequence, which basically will easier the work of the exhaustive attacks such us brute-force attacks (143). Thus, it is more preferred to use a high chaotic map for better security of PRNG (50), and avoid using lower chaotic maps like logistic map.

3.9 Requirements and metrics

In this part, we present some metrics and security requirements for strong and secure cryptographic-image schemes based on various researches notes (57, 58, 59, 61, 63, 91, 105, 122).

As known, cryptography applications should be resistant to different types of cryptanalysis attacks. Furthermore, the cryptographic keys have a very important role in cryptography applications. These keys should be infeasible to find or estimate without the exact secret keys due to the fact that the security depends only on keeping the secret keys secretly (58).

Although some techniques attempt to have high ability of withstanding various attacks, the cracked succeeded to break most of them (57, 59, 63, 122).

In this regard, the ciphers structures have been analysed based on three points.
- First, the structures of the cryptographic key. Herein, the weakness of the cryptographic keys can be in the space secret key, or can be in the pseudo random numbers generator.
- Second, the weakness in structures of the encryption algorithms. These schemes have low sensitivity to plain image change. As result, the presented cryptosystems could not resist against well-known analysis such as the differential attacks.
- Third, combination between the weakness in PRNG and ciphers structures. Herein, the hackers try to be more creative with they attempts. In this regard, the poor employing of the cryptographic keys among the encryption scheme eases the work of the cryptanalysis.

3.9.1 Kerckhoffs principles

Auguste Kerckhoffs is a cryptographer who published a scientific paper contains a set of requirements for the cryptographic applications in 1883. These principles become rules that should apply in order to design any cryptosystem. According to Kerckhoffs principle, an adversary knows the cryptosystem. This does not necessarily imply that the method should be made public (61). We quote the following: "*A cryptosystem should be secure even if everything about the system, except the key, is public knowledge*".We denoted these principles as follow.

• The Cryptosystem should be physically, if not mathematically indecipherable.

• The Cryptosystem should not require secrecy, and it should not be an issue if it falls into enemy hands. Any cryptosystem should depend only on keeping the key secret.

• The Cryptosystem should be possible to communicate and remember the key without using written notes, and be changed or modified at the option of the correspondents.

• It must be applicable to telegraphic correspondence.

• The Cryptosystem should be portable, and its usage and its operation does not require the cooperation of several people.

• Finally, it is necessary that the system should be an easy to use, given the circumstances in which control the application, and should be required neither mental strain nor the knowledge of a long series of rules to be observed.

Obviously, with the advancement of technologies, some of the Kerckhoff's principle are not applicable. However, the second hypothesis remains vitally important.

3.9.2 Encryption requirements

In the following points, we aim to present some encryption requirements which enhance the security for digital images.

Encryption can ensure digital images security. These digits data often have high redundancies, and have large sizes compared with texts or binary data (61).

These properties require that image encryption algorithms satisfy certain requirements such as eliminate the correlations among the pixels of the image. Thus, the traditional cipher techniques may not be secure enough for digital images (61, 91). In this context, a new encryption schemes is required. That lead to the questions regarding the encryption metrics requirements.

The main requirement of a good encryption scheme is to be able of resisting the exist attacks. any encryption technique to secure digital images is determined by the ability to resist the known cryptanalysis methods, including such attacks as differential analysis, related-key attack, and statistical attacks (67). Moreover, the encrypted image shall be acting like a random source according to information entropy of Shannon (105). Furthermore, ciphered image can be measured using a variety of methods, such as histogram analysis, global Shannon entropy measure, adjacent pixel correlations (137). The outputs of the probabilistic algorithm shall be merely independent of the input distribution using a random source (98), so that it will be impossible for an attacker to guess from which source the encrypted message originated. Indeed, the ciphered images should essentially uniform as well as the output of PRNG (98). In addition, and according to Lian et el. (61), the secret key and plain image sensitivity, and ciphered image randomness are the critical metrics to measure the cipher's resistance against the standard attacks. For further details about the encryption metrics requirements, see next chapters 5, and 6, sections of experimental results and discussion.

In the implementation of encryption schemes, efficiency is one of the most important factors. For a long time, attempts have been made to propose solutions for encryption schemes that are both efficient and safe. Unfortunately, strong security rarely goes hand in hand with practical implementation.

3.9.3 PRNG requirements

In this part, we take into consideration other researchers works in order to provide an appropriate techniques for digital images. Mainly, we study various researches notes regarding PRGN that generate a sequence of integers, or a stream of bits (7, 10, 37, 68, 89, 100, 124, 126, 138).

The main requirement of a cryptographic PRNG is that an adversary will be unable to determine the PRNG output without the seeds.

The cryptographic keys require numerous properties such as statistical randomness, and avoid the short periodic and predictable non-randomness keys. The pseudo random numbers algorithms can propose a good solution to produce these keys.

In this regard, the requirements for secrecy of the output of a PRNG leads mainly to specific requirements such as randomness, unpredictability of the output, and seed characteristics.

- In randomness term, the requirement for a secure PRNG is to produce key stream that appears like a random-source even though it is deterministic using the seed (initial values of a PRNG).

- In unpredictability term, one way to determine this point of output of PRNG is to look for its characteristics as random sequence of numbers including the distribution where PRNG should produce uniformly distributed of its output. There is very tricky to determine if a PRNG generates numbers that are unpredictable. But, if an attacker have a sequence bits (without seeds) from a PRNG, he should not be able to predict the next bits with probability greater than 0.5 (fifty-fifty game).

- In seed term, the seed that serves as input to launch a pseudo random number generator. Some researchers , mentioned above, require random seed as essential characteristic for PRNG's seed. The are no conditional specific characteristics for PRNG's seed. Here, there are only some recommendations such as employing random seed, preferly unpredictable, and avoid using same seed many times. Typically, the perfect seed for secure PRNG will be generated as true random, must be unpredictable, and seed itself must be a random.

3.10 Semantic Security

In open networks, we often should assume that there are adversaries everywhere in the network. Here, an adversary could controls on large number of network devices that are linked in the open network, often using a set of techniques may

include eavesdrop, manupulate, inject, alter, duplicate,,etc. Based on this, semantic security is a good solution to make the attacker "blind" where he could not sniff any associated information which could employed to build his/her attacks model.

Over the recent years, many researchers referred to a probabilistic encryption scheme as a semantically secure cryptosystem (22, 28, 34, 39). Herein, an intruder is infeasible to collection any information regarding the original data from the ciphered data.

In this part, we present one of the most interesting point of view for the definition of a semantically secure cryptosystem with some intuitive notions (34).

– Let M be the set of all possible messages ($m \in M$).

– Let p_m be the probability that m is sent.

– Let $f : M \rightarrow V$ be a function defined on M that represents such information about messages.

– Let V_m be a value for $f(m)$, here the adversary has a probability $P_(M)$ to occur when m is chosen at random (maximal probability).

Now, lets consider the following two points:

Point 1. Randomly chose a message (m), and ask the adversary to guess the value of the ciphered message V_m without telling him m. The probability of adversary guess being right should be the maximal value P_M.

Point 2. Let the adversary employs the function f. Randomly chose a message (m). Compute the encryption of m and send m to the adversary. Now, ask the adversary to guess $f(m)$.

A cryptosystem achieves the semantic security if an attacker could not win in Point 2 with higher probability than in Point 1 (34), it should be 50/50 game.

In a cryptosystem which is a semantically secure, even if the adversary knows the encryption algorithm, it must be hard for him to extract any information about messages from their encryption.

3.11 Conclusion

In this chapter, we have conducted a study about security mechanisms related to our studies. In this regard, we have described some patterns in cryptography which can be used in order to enhance the digital image security. Here, some specific modern cryptography techniques are introduced. Finally, we presented a practical requirements and metrics to improve pseudo random numbers generators, and encryptions schemes properties. Indeed, this chapter has attempted to provide a taxonomy of the available techniques to secure the digital images.

In the following part, we present our contributions in this dissertation. The solutions are proposed in order to improve the security of digital image.

Part II

New approaches to secure digital images

Chapter 4, in full, is a reprint of the material as it appears in (41) A novel pseudo random sequence generator for image-cryptographic applications" By Rafik Hamza, published in Journal of Information Security and Applications, volume 35, page 119-127, 2017. The dissertation author was the primary investigator and author of this manuscript.

Chapter 5, in full, is a reprint of the material as it appears in (46) "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map" By Rafik Hamza and Faiza Titouna. Published in Information Security Journal: A Global Perspective, Volume 25(4-6), pages 162-179, 2016. The dissertation author was the primary investigator and author of this manuscript.

Chapter 6, in parts, is a reprint of the material as it appears in (42) "Secure video summarization framework for personalized wireless capsule endoscopy" By Rafik Hamza, Khan Muhammad, Zhihan Lv, and Faiza Titouna. Published in Pervasive and Mobile Computing Journal, Pages 436-450, Volume 41, 2017. The dissertation author was the primary investigator and author of this manuscript.

4

Pseudo random numbers generator

Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.

John von Neumann

Contents

4.1 Introduction 60

4.2 Proposed System 62

4.2.1 Chen chaotic system 62

4.2.2 Proposed algorithm structure 64

4.3 Experimental Results 66

4.3.1 Security Analysis 67

4.3.2 Randomness tests 69

4.3.3 Encryption image simulation 71

4.3.4 Security Properties comparison 76

4.4 Conclusion 77

4.1 Introduction

Recently, some security issues have been presented with the encryption schemes based on chaos (57, 59, 63, 122), mainly from three reasons: key space, the structures algorithmic and their combination. For example, Lambić et al. (57) showed some issues on the image encryption algorithm presented in (129) using the weakness of the cryptographic keys. Authors in (59, 63) established equivalent keys for most ciphers using some arithmetic operations such as XOR, and modulo Addition. In Özkaynak et al. (88), authors analyzed a security weaknesses of the pseudo sequence generator above-mentioned (50), with total break and exposure the security problems to retrieve the sequence generated with a complexity lower than a brute force attack. The authors in (88) relied on the subordination of output values of a chaotic system that yield a smaller key space, which exploited with a complexity lower than a brute force attack.

The chaotic maps can be distinguished by a discrete-time such as the logistic map (26), or a continuous-time like Chen chaotic system (60). The logistic map is one of the famous chaotic systems, considered as a prelude into the chaotic systems. This map proved its importance in several fields, especially with cryptography applications including light-weight image encryption algorithms (70, 91), and watermarking algorithms (64, 78, 133), and true or pseudo random number generator (36, 116, 120, 138). For example, in our previous work (46), we presented a novel encryption scheme that employed 2D Zaslavsky chaotic map only with the P-box processes, where we permute the pixels based on the indexes sort of the chaotic map directly. García-Martínez et al. (36) proposed a pseudo-random bit generator based on lag time series of the logistic map. Authors used the positive and negative values of this logistic map in the bifurcation parameter with some of a delay in the generation of time series. Franois et al. (29) proposed a novel algorithm to produce a random sequence that consists of mixing three chaotic maps produced from an input initial vector and the generator can resist some attacks such as differential attack and exhaustive attacks. Hu et al. (50) presented a pseudo random sequence generator based on Chen's chaotic system with highly capable of withstanding attacks. Öztürk et al. (89) presented a novel

method based on the differential equation from chaotic systems to produce a new pseudo random numbers generator.

The most important problem in chaos-based cryptography is the selection of the chaotic system to generate the pseudo random bits (6, 57). The chaotic maps are defined on real numbers, while almost all cryptographic applications are defined on finite numbers. These defects import some difficulties for the chaos-based image encryption methods, due to round-off errors in real number quantization, which may lead to irreversible functions for encryption and make the decryption process impossible (136). In addition, chaotic maps in low dimension (eg., 1D or 2D) may lose its chaotic nature completely and become periodic with dynamical degradation when it is discretized in finite precision computation (136). One dimension logistic map has periodic windows (145), and also with other low dimensional chaotic maps such as the piecewise linear chaotic map (125, 126). The lower chaotic maps along with some low spatiotemporal maps are more exposed to the problem of degradation during the finite precision computations. Indeed, the complexity of a chaotic map with high-dimensions is more secure than any lower chaotic map, and can improve the security of the pseudo random number generator. Thus, it is adequate to construct PRNG by high-dimensional chaotic systems to produce digital stream keys.

In this chapter, we propose a new effective and secure pseudo-random sequence generator based on Chen chaotic system. We propose a secure pseudo-random sequence generator based on a combination of the three coordinates of the Chen chaotic orbits. We overcome the weaknesses of the former PRNG based on Chen chaotic map (50, 88). The proposed PRNG solves the problem of non-uniform distribution of the sequences generated directly by Chen chaotic system. The properties of the high-dimensional Chen chaotic map have been used with the average function of the samples by multiplication and applying arithmetic modular. Herein, we have avoided the problem of degradation during the finite precision computations by using a high-dimension map with cascading and mixing the orbit samples. The proposed algorithm provides various advantages such as the large key space and a complex dynamic of the generated binary sequence. Moreover, the PRNG sequences are verified with two famous statistical packages (NIST, and DIEHARD tests) using several sequences up to 8 million bits,

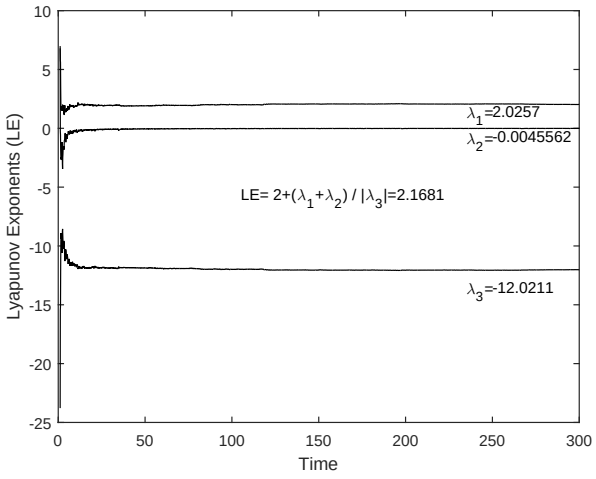


Figure 4.1: Lyapunov exponents of Chen's chaotic system

to demonstrate that the proposed system is highly secure and can provide good statistical characteristics.

The rest of the chapter is organized as the follows. We introduce the nonlinear dynamic "Chen" in section 2. Overall architecture of the proposed algorithm is presented in section 3. The experimental results and the security performance are well discussed in section 4. Finally, the conclusion is presented in the last section.

4.2 Proposed System

4.2.1 Chen chaotic system

Chen chaotic system was introduced by Chen (18) with an extension of the three-dimensional orbit. This map is also called Lorenz-like systems, which means it is similar as the chaotic system Lorenz (60, 66). These systems have been well studied and applied in several areas (50, 60, 88).

The complex dynamical behaviors of Chen chaotic system can be elaborated in Figure 4.2. Chen's chaotic system can be represented mathematically by the

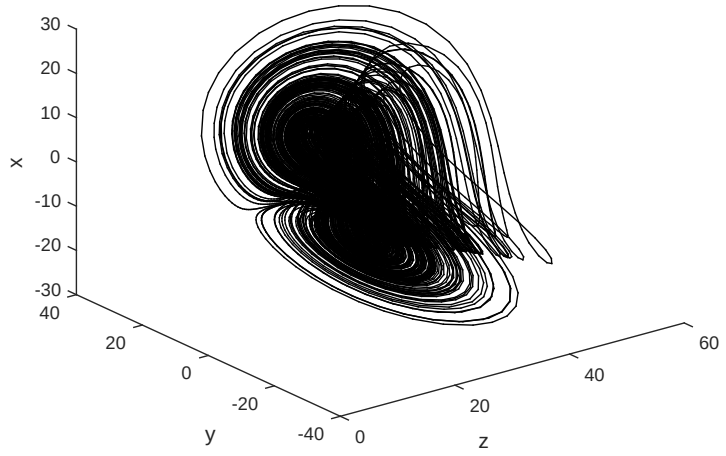


Figure 4.2: Chaotic behavior of Chen's system.

following equations:

$$\begin{cases} \dot{x} = ay - ax \\ \dot{y} = cx - ax + cy - xz \\ \dot{z} = xy - bz \end{cases} \tag{4.1}$$

where x, y and z are the samples of this system while a, b, and c are the control parameters.

Lyapunov exponents of system 4.1 are found to be $\lambda_1 = 2.02$, $\lambda_2 = -0.004$, $\lambda_3 = -12.02$. The complex dynamical behaviors of Chen chaotic system can be elaborated in Figure 4.2. Figure 4.1 shows dynamics of Lyapunov exponents of system chaotic Chen. The Lyapunov exponents dimension of Chen chaotic system is 2.1681 (50), which is large and not the most widely used compared to the rest of chaotic systems.

Figures 5.4, 4.4, and Figure 4.5 show the forms of the distributions for the orbits (x, y, z) sequentially using different seeds (initial values). The first line of figures shows the plot of distributions with number of iteration, while the second line of figures shows the histogram of distribution. These figures illuminate the

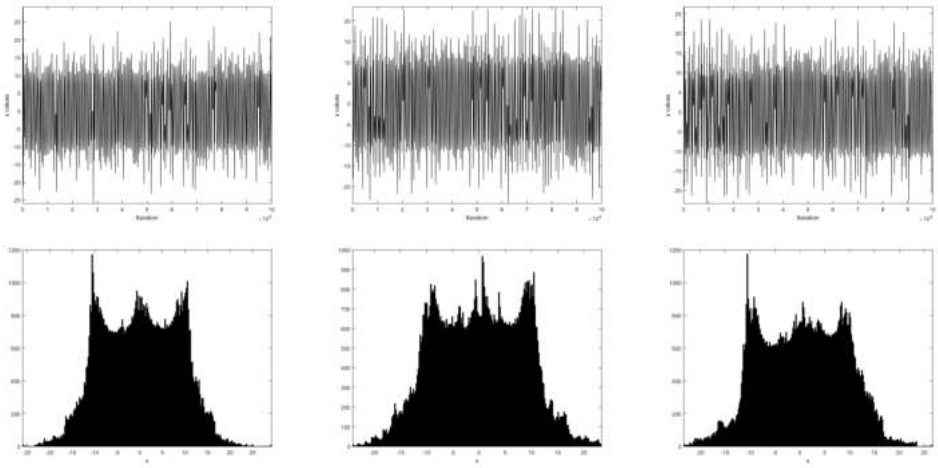


Figure 4.3: The distribution of values x using different seeds.

problem of non-uniformly distributed with the generated sequences directly by Chen chaotic system . Figure 4.2 shows the plot of Chen attractor obtained using Runge-Kutta methods with step size 0.01. All the figures were generated using the control parameters: $a = 35,\ b = 3$, and $c = 28$, and the initial values $(x_0, y_0, z_0) = (-1.5,\ 0.6,\ 17)$.

The range of the sequences that the sequence generated directly by the Chen chaotic system does not fit the requirement of most applications with images, which demands a range in the finite field $\{0, 1, ..., 255\}$, or in binary range $\{0, 1\}$.

4.2.2 Proposed algorithm structure

To generate the pseudo random sequence, we use Runge-kutta step size 0.01, with iterating the chaotic system for $1+\frac{n}{3}$ times to obtain the real values x_i, y_i, and z_i. The size of each sequence is $1 + \frac{n}{3}$. To get rid of initial values effect, we discard the first number of each sequence. Consequently, the three sequences x_i, y_i, and z_i will be generated with length of each sequence is $k = \frac{n}{3}$.

Based on a large number of experiments, we propose the following coding Algorithm (4.2). The generated sequences are uniformly distributed and it have randomness statistical properties, and solves the problems that have discussed

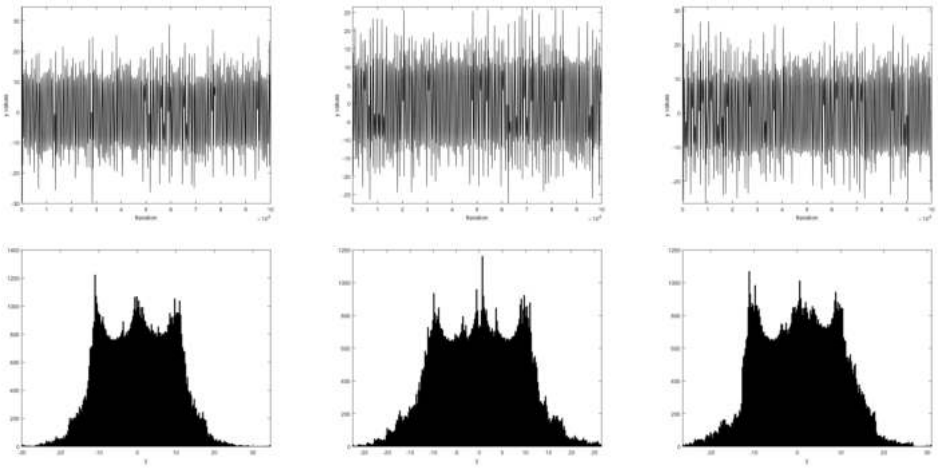


Figure 4.4: The distribution of values y using different seeds.

previously.

$$\begin{cases} P(3 \cdot i) & = \alpha \cdot m \cdot x \\ P(3 \cdot i + 1) & = \beta \cdot m \cdot y \\ P(3 \cdot i + 2) & = \gamma \cdot m \cdot z \\ i & = 0, 1, 2, 3, ..., k. \end{cases} \tag{4.2}$$

Where:

$$\begin{cases} \alpha = \dfrac{\sum |x(i)|}{n} \\ \beta = \dfrac{\sum |y(i)|}{n} \\ \gamma = \dfrac{\sum |z(i)|}{n} \\ m = 251 \cdot \alpha \cdot \beta \cdot \gamma \end{cases} \tag{4.3}$$

x(i), y(i), z(i) are the samples from Chen chaotic system, α, β, γ are the averages of absolute sample values, and k is length of one of the orbits x, y, z. This means that k is one-third of the length sequence n. In Eq 4.1, we generate a one-dimensional sequence P_i in the set of real numbers ($\mathbb{R}$). Then, we can generate the sequence S using Eq (4) .

$$S = round|P| \ mod \ l \tag{4.4}$$

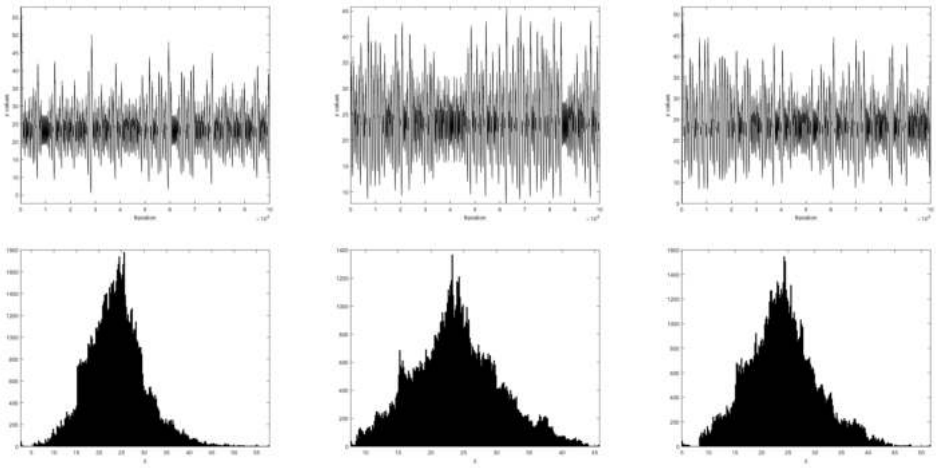


Figure 4.5: The distribution of values z using different seeds.

Herein, l is 2 for binary output $\{0, 1\}$, or 256 for a sequence of numbers in the finite field $\{0, 1, ..., 255\}$, and S is a one-dimensional sequence of proposed algorithm.

Figure 4.6 represents the structure of the proposed algorithm that generate binary or numbers sequence, depending on the l value. Figure 4.7 shows flowcharts of the proposed pseudo random number generator algorithm.

So basically, the proposed algorithm founded on a combination of the three coordinates of the chaotic orbit with some perturbations which ensure a secure PRNG. Figure 4.6 shows the frame of the proposed algorithm to generate numbers $l = 256$ or binary sequence $l = 2$ with randomness properties, where the input is the secret keys, which are the initial values and control parameters, and n is length of the sequence. Figure 4.8 shows the plot of generated sequence by the proposed algorithm, and describes the uniform distribution of the values.

4.3 Experimental Results

In this section, we present the security and performance analysis for the proposed algorithm. The experiments include analysis of secret key size and its sensitivity, linear complexity, randomness tests, encryption simulation, histogram analysis,

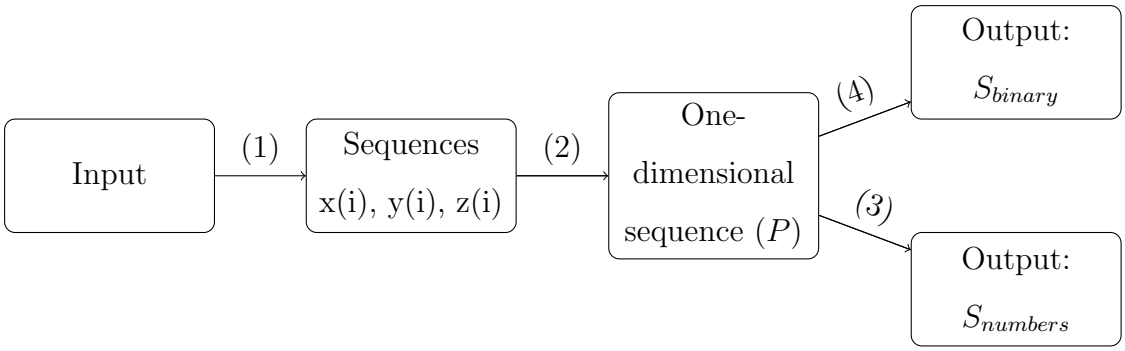


Figure 4.6: The structure of the proposed algorithm: The input: Secret-Keys, n, and l. (1) generate the Sequences $x(i)$, $y(i)$, $z(i)$ using equations 4.1 of chaotic Chen equations. (2) generate the sequence P using the equations 4.2. (3) generate a binary sequence using the equation 4.4 with $l = 2$. (4) generate numbers sequence using the equation 4.4 with $l = 256$.

and comparison with recent PRNGs (124, 126, 139). The main secret keys is selected as ($x_0 = -1.5,\ y_0 = 0.6,\ z_0 = 17$, $a = 35, b = 3$, and $c = 28$). The simulation and tests have been done using database images (sipi.usc.edu/database/) along with some standard testing images such as Cameraman image.

4.3.1 Security Analysis

4.3.1.1 Key sensitivity

In this test, we analysed the sensitivity of the secret keys in the proposed algorithm. We changed slightly the secret keys in the proposed algorithm, to show that the produced sequence changed completely compared to the original sequence.

Figure 4.9a shows the difference plot between two sequences S_1 and S_2 produced by our pseudo-random algorithm. The first random sequence S_1 is generated using the secret keys while the second sequence S_2 is generated after a single slight changing ($+10^{14}$) with one of the original secret keys. The experiments show that the variance ratio between the two sequences S_1 and S_2 can be

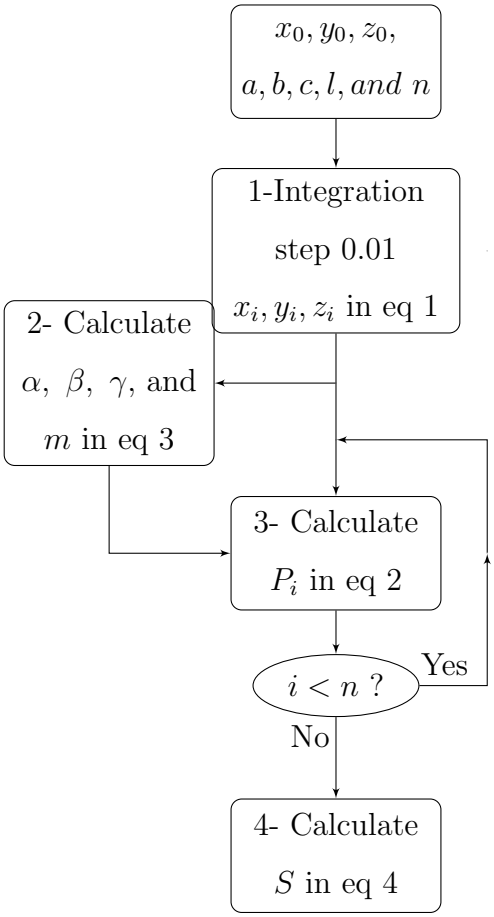


Figure 4.7: Flowchart of the proposed PRNG algorithm

approximated to 99% for at least 4×10^4 iterations, even with extremely small changing in the secret keys. So, our proposed algorithm requires producing at least 4×10^4 to start. Also, the auto-correlation of these sequences is presented in Figure 4.9b. As results show, the two sequences are completely unrelated and separate from each other, which prove that our proposed algorithm is extremely sensitive to the secret keys.

4.3.1.2 Key Space

All the initial values and controlling parameters in Chen chaotic system are selected as secret keys in our proposed pseudo-random sequence generator. There-

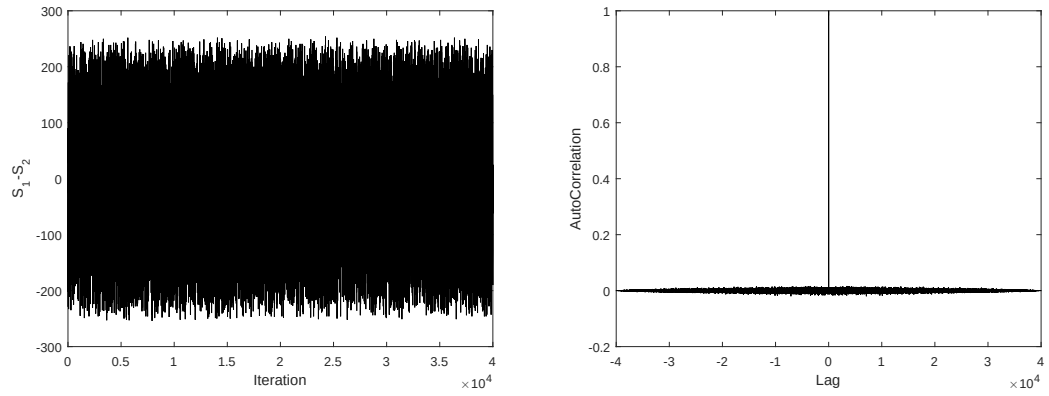
Figure 4.8: Histogram of the pseudo random numbers

fore, the key space can be calculated using the sensibility to both initial values and controlling parameters of the Chen chaotic system. The keys are sensitive to any differences equal to or large than 10^{-14}. Therefore, the key space for the proposed pseudo random sequence generator is more than $10^{84} \simeq 2^{279}$. According to Alvarez et al. (7), the size of the key space should not be smaller than 2^{128}. Therefore, the key space size in our proposed algorithm is larger enough to withstand various attacks and there is no significant for the exhaustive attacks.

4.3.2 Randomness tests

The NIST suite test (100) requires a binary sequence with at least 10^6 bits to find potential defects in the pseudo random sequence generator structure. The result of this test appears with the values P_{values}, which must come bigger than 0.01 to pass the tests. We employ the default values that comes with the $NIST$ tests (100).

The binary sequences generated by our proposed algorithm passed successfully all the tests of SP 800-22. The results are listed in Table 4.1 and Table 4.2. Since our proposed algorithm can produce two sequences S_{bin} and S_{dig}, we generated two sequences S_{bin} with length 10^6 bits, and S_{dig} with length (8×10^6) bits for the numerical experiments to prove the randomness of the generated sequences. According to the numerical results from tables 4.1 and 4.2, the proposed pseudo



(a) (b)

Figure 4.9: **(a)** The difference Plot $(S_1 - S_2)$, **(b)** Auto-correlation of these sequences

random fails only in the non-overlapping template matching test for length of sequence 8×10^6 bits. Since other well-known pseudorandom sequence generator's failed in the same test for the same size 8×10^6 bits (89), this means it is not a defect in the proposed pseudo random sequence generator. Thus, both generators S_{bin} and S_{dig} passed with success the NIST SP 800-22 tests.

Diehard battery statistical test is also represented in our experimental tests. The package of Diehard Battery includes several statistical tests. Herein, we used the default parameters which come with this package. The results of tests return P_{values}, which should be uniform within $[0, 1)$ to pass the tests. This is a contrast with the condition to pass the $NIST$ tests, where a bigger P_{values} indicates better randomness. Unlike $NIST$ test suite, Diehard tests do not provide specific criteria for success or failure, just the P_{values} which should be uniform on $[0.025, 0.975]$, based on the significance level 0.05. This does not necessarily indicate the that the proposed algorithm has failed the test at 0.05 level when they are isolated in a single case. In our experiment, we tested 100 different number sequences, each sequence have a length of 16×10^7 bits, about $20Mb$ file size. The results are listed in table 4.3. Herein, we counted the number of P_{values} that are in acceptable range $[0.025, 0.975]$ in "Ratio" column, and compute the average value

Table 4.1: Results of the NIST SP 800-22 randomness tests for 1000000 *bits*

Name of Tests	P_{values}	Results
Frequency (monobit)	0.9203	Passed
Frequency (block)	0.7615	Passed
Runs test	0.8103	Passed
Longest run of ones in a block	0.7994	Passed
Binary matrix rank	0.6866	Passed
Discrete Fourier transform (spectral)	0.5945	Passed
Non-overlapping template matching	0.6890	Passed
Overlapping template matching	0.9629	Passed
Maurer's universal statistical	0.8360	Passed
Linear complexity	0.4906	Passed
Serial 1	0.9539	Passed
Serial 2	0.7220	Passed
Approximate entropy	0.9262	Passed
Cumulative sums	0.9275	Passed
Random excursions (x = -4)	0.5509	Passed
Random excursions variants (x = -9)	0.3308	Passed

for P_{values} in "Average" column. The results lead us to the conclusion that the number sequences generated by our scheme have good statistical properties and have passed all the tests suite.

4.3.3 Encryption image simulation

The simulation of encryption image based on our proposed algorithm is presented in this subsection. Our purpose is to illustrate that our PRNG can resist against the differential attacks. This attack refers to an adversary that tries to make a slight change in the initial secret key and then observes the effect on encrypted

Table 4.2: Results of the NIST SP 800-22 randomness tests for 8000000 bits

Name of Tests	P_{values}	Results
Frequency (monobit)	0.1428	Passed
Frequency (block)	0.2028	Passed
Runs test	0.2859	Passed
Longest run of ones in a block	0.8303	Passed
Binary matrix rank	0.8813	Passed
Discrete Fourier transform (spectral)	0.1729	Passed
Non-overlapping template matching	0.00001	Failed
Overlapping template matching	0.5782	Passed
Maurer's universal statistical	0.6342	Passed
Linear complexity	0.9511	Passed
Serial 1	0.3608	Passed
Serial 2	0.4480	Passed
Approximate entropy	0.0216	Passed
Cumulative sums	0.2666	Passed
Random excursions (x = -4)	0.7147	Passed
Random excursions variants (x = -9)	0.5142	Passed

images(145). The encryption has been established as follows. First, we produce a matrix K from our proposed algorithm with the same dimension of the plain image. The plain image is diffused with the bitwise Exclusive-OR operation using the matrix K. Next, we shuffle the position of the image pixels (pixel position permutation) using sort-index of the generated matrix K.

Figure 4.10 shows the related results. Herein, (a) shows the plain-image, (b) the encrypted image C_1 using the correct keys, (c) the decryption image with the correct keys, (d) the decryption using the wrong keys, while (e) shows the encrypted image C_2 with the wrong keys, and finally (f) refer to difference between images $C_1,\ C_2$. We denoted the correct keys by $x_0 = -1.5,\ y_0 = 0.6,\ z_0 = 17,$

Table 4.3: DIEHARD statistical test results

Tests DIEHARD	Ratio	Average
Birthday Spacings	99/100	0.56
Overlapping Permutations	99/100	0.72
Ranks of 31x31 matrices	99/100	0.34
Ranks of 32x32 matrices	98/100	0.56
Ranks of 6x8 Matrices	97/100	0.55
Monkey tests on 20-bit Words	98/100	0.11
OPSO	97/100	0.33
OQSO	100/100	0.23
DNA	99/100	0.59
Count the ones in a Stream of Bytes	100/100	0.67
Count the ones in Specific Bytes	100/100	0.61
Parking Lot	99/100	0.25
Minimum Distance	96/100	0.47
Random Spheres	100/100	0.85
The Sqeeze	98/100	0.91
Overlapping sums test	100/100	0.60
Runs up	100/100	0.18
Runs down	99/100	0.35
Craps	98/100	0.61

while the wrong keys : $x_0 = -1.5,\ y_0 = 0.6 + 10^{-14},\ z_0 = 17$, which means there is a tiny difference between the correct key and the wrong key. Figure 4.10 (a) shows the original image (cameraman). Figure 4.10 (b) shows the encrypted image denoted by C_1. Figure 4.10 (c) shows the successful decryption using the right keys. Figure 4.10 (d) shows the decryption using a wrong keys, while Figure 4.10 (e) shows the encrypted image C_2 using a wrong keys. Finally, Figure 4.10 (f) shows the absolute difference between the images C_1 and C_2. The results show

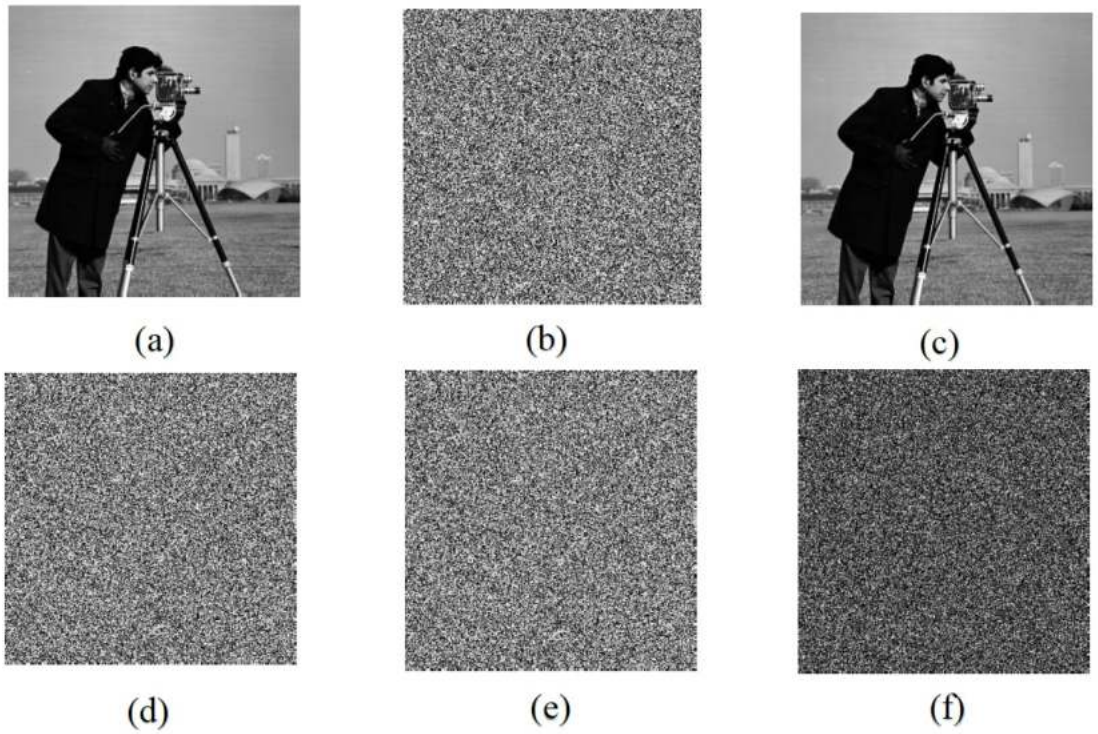


Figure 4.10: Basic tests of image encryption using transposition pixels position based on our proposed algorithm.

that the proposed algorithm can be used as a part of image encryption scheme with high sensitivity to its stream keys. The results indicate that our algorithm is not exposed to the differential attacks among other attacks. The simulation test shows that the proposed PRNG has good harmony with the image encryption.

We use the variances of histograms to evaluate the uniformity of pixels distributions accurately. According to (144), variances of histograms can be used for quantity analyses of each key and to evaluate uniformity of ciphered images. The closest of the two values of variances indicates the higher uniformity of ciphered images when the secret keys are varying. We computed two variances of ciphered images that are encrypted by two secret keys on the same plain image.

The variance of histogram is presented mathematically as follows:

$$\begin{cases} var(Z) = \dfrac{1}{256}\displaystyle\sum_{i=0}^{255}(z_i - \upsilon)^2 \\ \upsilon = \dfrac{1}{256}\displaystyle\sum_{i=0}^{255} z_i \end{cases} \tag{4.5}$$

Where Z is the vector of the histogram values and z_i is the number of pixels which pixel value is equal to i.

Table 4.4: Variances of histograms compared among all secret keys in the proposed algorithm.

Ciphered image	SC1	x_0	y_0	z_0	A	B	C
5.1.11	5456	5461	5425	5483	5473	5475	5469
5.1.12	5466	5457	5459	5452	5467	5476	5459
5.1.13	5.470	5431	5436	5475	5458	5453	5472
5.1.14	5438	5449	5456	5452	5469	5461	5463
lenna	5450	5506	5440	5464	5427	5 478	5449
cameraman	5446	5470	5474	5481	5437	5446	5459

We employed this test as follows. First, we encrypted the same plain image with two different secret keys. These keys differ only in one parameter with a tiny change. Then, we computed two variances of histograms of two ciphered images. The results of these tests are listed in Table 4.4. We changed one parameter before encryption so that each column in Table 4.4 has the result the variance of histogram for the two ciphered images. The results tends to be average as Table 4.4 shows, where the variances values are very close to 5460. Moreover, Table 4.5 shows the percentage of variances difference of histograms. The simulation results shows that the proposed scheme can resist the statistical attacks.

Table 4.5: Percentage of variances difference of histograms compared among all secret keys in the proposed algorithm.

Ciphered image	x_0	y_0	z_0	A	B	C
5.1.11	0.100	0.568	0.503	0.325	0.358	0.238
5.1.12	0.166	0.124	0.249	0.031	0.194	0.131
5.1.13	0.718	0.616	0.100	0.216	0.301	0.033
5.1.14	0.210	0.326	0.262	0.569	0.415	0.466
lenna	1.027	0.178	0.260	0.409	0.524	0.018
cameraman	0.427	0.505	0.637	0.161	0.003	0.238

4.3.4 Security Properties comparison

We compare security properties of our proposed scheme with some chaos-based algorithms (124, 126, 139). We listed the main properties of our proposed algorithm and other related schemes (124, 126, 139). Table 4.6 shows that our proposed scheme has more good characteristics due to the fact that the cryptosystem employs a high-dimensional chaotic system. This map has very chaotic behavior with high complexity and positive Lyapunov value. Also, Chen chaotic map known for its high sensitivity to the initial values. This means that our PRNG provides a higher level of security and it is more complex compared with other PRNG based on low dimensions chaotic system such as in (124, 126), even with some true random numbers generator such as in (139). Furthermore, the key space in our scheme is large enough to withstand attacks most of which depend on low chaotic map such as in (124, 126). In the statistical tests, all these proposed schemes seem to have good statistical properties, which can meet the requirements of cryptographic keys while our PRBG proved its harmony with the digital images as pseudo cryptography keys and passed various statistical tests and security analysis. Therefore, our scheme is more secure and competitive than other schemes (124, 126, 139).

Table 4.6: Security Properties comparison

References	Chaos	Type	Statistical tests
Proposed algorithm	Three Dimensional Chaotic Map	PRNG	Yes (Passed)
(139)	One Dimensional Chaotic Map	TRNG	Yes (Passed)
(124)	One Dimensional Chaotic Map-CML	PRNG	Yes (Passed)
(126)	Dual one-dimensional chaotic maps	PRNG	Yes (Passed)

4.4 Conclusion

This chapter presented a new pseudo-random sequence generator algorithm based on a combination of the three coordinates of the Chen chaotic orbits. The proposed PRNG solves the problem of non-uniform distribution of the sequences generated directly by Chen chaotic system. Our PRNG algorithm was validated with several randomness tests such as NIST SP 800-22 test and DIEHARD package. Analysis and statistical tests proved that our PRNG has several properties such as high pseudo-randomness, good statistical characteristics, good speed, and excellent effectiveness. The proposed algorithm is comparatively more convenient for encryption of images and meets different security aspects such as large key space, key sensitivity, robustness against differential attacks, and capability of withstand against attacks. In addition, the proposed scheme can be successfully employed in numerous applications that require a secure PRNG such as in electronic payment, industry, and military fields. The proposed algorithm requires producing at least $[64 \times 64]$ bits to start, which is its limitation. This property does not cause any issue with digital data, given that the images have a large number of pixels.

5

Chaos-based cryptosystem

Encryption...is a powerful defensive weapon for free people. It offers a technical guarantee of privacy.. It's hard to think of a more powerful, less dangerous tool for liberty.

Esther Dyson

Contents

5.1 Introduction 80

5.2 Proposed encryption scheme 81

5.2.1 Generating encryption keys 81

5.2.2 Encryption algorithm 83

5.2.3 Decryption algorithm 85

5.2.4 RGB image encryption 87

5.3 Experimental results and discussion 88

5.3.1 Histogram analysis 89

5.3.2 Information entropy 90

5.3.3 Correlation of two adjacent pixels 90

5.3.4 Randomness tests 93

5.3.5 Key Sensibility 94

5.3.6 Key Space 96

5.3.7 NPCR and UACI tests 97

5.3.8 Known/Chosen attack 99

5.3.9 Comparative analysis 101

5.4 Conclusion 103

5.1 Introduction

Many images encryption schemes have been analysed and became insecure against the hackers. Basically, the hackers used many types of attacks aiming to get sensitive information. One common attack is chosen/known plain-image attack using special images like a black-image (all pixels equal to zero) (117). The attackers build their cryptanalysis on the weakness of low sensitivity in plainimage change, along with other reasons such as the bad ciphering scheme regardless of the generators keys or the pseudo keys itself. Wang et al. (122) presented a security analysis with totally break for the work in Huang et al. (52), based on the chosen-plain-text attack, which demonstrated. The algorithm presented has low sensitivity to any tiny changing of the plain-image, and also proved the existing of equivalent keys for encryption schemes. Rhouma et al. (97) presented a Cryptanalysis and an improvement of a new image encryption algorithm based on hyper-chaos Gao et al. (35). Furthermore, Jeng et al. (53) found that modified image cryptosystem of Rhouma et al. (97) still exists a security weakness, especially the problem of low security-sensitivity to plain-image change. The main issue that allows cryptanalysis to break many encryption schemes is the problem of low security-sensitivity to plain-image change Akhavan et al. (117). Therefore, any adjustment in plain-image pixels should change completely the corresponding ciphered image.

In this chapter, we introduce a novel image encryption scheme based on Zaslavsky chaotic map. In particular, the proposed algorithm has a high level of security and high sensitivity, which ensures the good property of confusion, and eliminate the correlation coefficients of the original image. Along with possessing large-sized of keyspace, and very sensitive to plainimage and the secret key. Moreover, the proposed algorithm has good speed of encryption/decryption. The original image can be recovered completely if the secret keys are exactly known. These features make our proposed algorithm secure against many types of attacks such as the brute-force attack. Conducted experiments show that the proposed cryptosystem approach can achieve excellent encryption performance, and confirms its efficiency against cryptographic attacks. Our work also indicates that

the two-dimensional map of Zaslavsky chaotic system is suitable for image encryption, due to the wide range of the initial conditions and control parameters and high sensitivity. We avoided the problem of degradation caused by finite precision computation with the proposed chaotic system, where we employ directly the generated sequence from the coupled map of the chaotic map. Furthermore, this map is very chaotic (largest Lyapunov exponent 3.65), producing very chaotic sequences, and can lead us to increase the resistance of our cryptosystem against attacks. In order to get high sensitivity to plain image, we use matrix multiplication over the finite field $Gf(2^8)$, where we used the matrix K with its invertible L. The square matrix K is self-invertible, which means that the equation $K.L = Id$ has a unique solution L, where Id is the identity matrix. And the invertible matrix L can be found by $L = K^{-1}$.

5.2 Proposed encryption scheme

5.2.1 Generating encryption keys

In order to produce appropriate keys to our proposing scheme. We iterate the equation 5.1 for k time to produce the one dimensional vector Vec, which means that the produced vector Vec has $2 \times k$ length, while $k = ceil(\frac{n}{2})$ and n is length of the generated sequence Vec. The pseudo random number generator is defined by following equation:

$$\begin{cases} Vec_{\ 2k} = x_{k+1} \\ Vec_{\ 2k+1} = y_{k+1} \\ k = 0, 1, 2, ... \end{cases} \tag{5.1}$$

The proposed image encryption image uses the pseudo random of Zaslavsky chaotic map by mixing and cascading its samples. That ensure a highly chaotic for the pseudo random number generator. To get rid of initial values effect, we discard the first teen numbers of the generated sequence Vec.

The Algorithm 1 illustrates the steps to compute keys for our image encryption method. $\sum(:)$ referring to the sum of all numbers, and $\lfloor\ \rfloor$ means round to the nearest number.

$$\begin{bmatrix}
0 & 0 & 1 & 0 & 2 & 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 \\
0 & 1 & 0 & 2 & 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 \\
1 & 0 & 2 & 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 \\
0 & 2 & 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 \\
2 & 0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 \\
0 & 3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 \\
3 & 0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 \\
0 & 4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 \\
4 & 0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 \\
0 & 5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 \\
5 & 0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 \\
0 & 6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 \\
6 & 0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 \\
0 & 7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 \\
7 & 0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 \\
0 & 8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 \\
8 & 0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 \\
0 & 9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 \\
9 & 0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 \\
0 & 10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 \\
10 & 0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 \\
0 & 11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 \\
11 & 0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 \\
0 & 12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 \\
12 & 0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 \\
0 & 13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 \\
13 & 0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 & 0 \\
0 & 14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 & 0 & 29 \\
14 & 0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 & 0 & 29 & 0 \\
0 & 15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 & 0 & 29 & 0 & 30 \\
15 & 0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 & 0 & 29 & 0 & 30 & 0 \\
0 & 16 & 0 & 17 & 0 & 18 & 0 & 19 & 0 & 20 & 0 & 21 & 0 & 22 & 0 & 23 & 0 & 24 & 0 & 25 & 0 & 26 & 0 & 27 & 0 & 28 & 0 & 29 & 0 & 30 & 0 & 0
\end{bmatrix}$$

Figure 5.1: The initial matrix K_{init}

The chaotic map generates the matrix R_{init}, and the vectors V_{init}, V'_{init} using the secrets keys $(x_0, y_0, \varepsilon, \tau, \nu)$. Then, we sort these generated keys in ascending order and returning the index array of each key. Followed by computing α, K and L.

The generated keys from algorithm 1 are:

• The random matrix R_{init}, and vectors V_{init}, V'_{init}.

• The index matrix R, and indexes vectors V, V'.

• α is a non-null value, computed using the random sequences V_{init}, V'_{init} and the random matrix R_{init} as it shown in algorithm 1

• The matrix K and L are defined over $Gf(2^8)$.

These generated keys denote encryption keys, while the initial keys of the 2-D

chaotic map are the secret keys for our proposed scheme.

The matrix R contains indexes sorts the elements in each columns of the matrix generated R_{init}, which means that R is a collection of columns index vectors obtained by sorting the generated matrix R_{init}. V and V' are two vectors representing the index sorts of V_{init} and V'_{init}. The two initial vectors (V_{init}, V'_{init}) are related to the height (h) and width (w) of the plain image I.

Based on a large number of experiments to find a suitable matrix for our proposed algorithm, we propose the $[32 \times 32]$ constant symmetric matrix denoted by K_{init}. Figure 5.1 shows the values numerical of the proposed matrix K_{init}. We use this matrix to compute and produce the encryption keys K and L as it shown in algorithm 1.

The rows of K_{init} are linearly independent over $GF(2^8)$ (rank(K_{init})=32), which means that K_{init} is an invertible matrix. Therefore K is an invertible matrix, and K_{init} is proved as an invertible matrix, and we already stated that $\alpha \neq 0$.

In our work, we select the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$ as default polynomial. Where the arithmetic matrix multiplication over Galois Fields $GF(2^8)$ is applied for each sub-block $[32 \times 32]$ of the data matrix image. The image appears distorted so that the image is completely incomprehensible.

5.2.2 Encryption algorithm

The proposed encryption algorithm is a two-step process. The first is to produce encryption keys using algorithm 1 based on the 2-D Zaslavsky map. The second step is to dismantle and distribute pixels of the plainimage using permutation and diffusion processes. The plainimage I should have one matrix with size $(h \times w)$.

Figure 5.2 shows the plain image lena of dimension 512×512 pixels along with its corresponding encrypted and decrypted images using our proposed algorithm.

The detailed encryption process includes the following steps:

Step 0. Read the 8-bit gray image I and get its size $h \times w$.

Step 1. Apply the algorithm1 using the secret keys, which produces the indexes: (R), (V) , and (V'), alongside α, K, L.

Algorithm 1 Compute the encryption keys

INPUT: $x_0, y_0, \varepsilon, \tau, \nu, K_{init}, I$

OUTPUT: R, V, $V^{'}$, α, K, L.

[h,w] $\longleftarrow$ size(I)

Apply equation 5.1, Which generate Vec.

$R_{init} \longleftarrow reshape(Vec(1:1024), 32, 32)$

$V_{init} \longleftarrow Vec(1:h)$.

$V^{'}_{init} \longleftarrow Vec(1:w)$.

R $\longleftarrow$ indexsort(R_{init})

V $\longleftarrow$ indexsort(V_{init})

V' $\longleftarrow$ indexsort(V'_{init})

$\alpha = \lfloor \sum R_{init}(:) + \sum V_{init}(:) + \sum V'_{init}(:) \rfloor \ mod\ 256$

if $\alpha = 0$ **then**

$\alpha = \lfloor \sum R_{init}(:) + \sum V_{init}(:) + \sum V'_{init}(:) \rfloor \ mod\ 255$

end if

$K \longleftarrow \alpha \cdot K_{init}$.

$L \longleftarrow K^{-1}$.

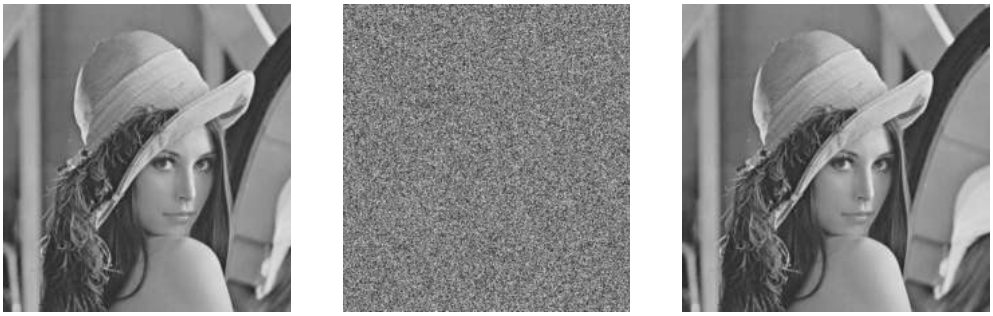
Step 2. Shift the rows and columns of the plainimage matrix using the sorts elements V and V' and then apply the following equation.:

$$I_2 : I \oplus \alpha \tag{5.2}$$

Where $\oplus$ is the bit-wise operation, and I_2 represent the obtained matrix.

Step 3. In order to distort the image, we permute the obtained image pixels using the indexes in matrix R, we split I_2 into $[32 \times 32]$ blocks denoted by B. We permute the rows and columns for each block B of I_2 using the column of matrix R as indexes. The obtained matrix is denoted by I_3.

Step 4. The following equation shows the diffusion processes, where we diffuse each $[32 \times 32]$ block B within the obtained image I_3 over the finite field



(a) **(b)** **(c)**

Figure 5.2: Test image encryption by our encryption scheme. (a) The plainimage, (b) The encrypted image , (c) The decrypted image

$GF(2^8)$ using the matrix K and L.

$$I_4 : L \cdot B \cdot K \tag{5.3}$$

Where I_4 represent the obtained matrix.

Step 5. Shift each row and column from the obtained matrix I_4 using the sorts elements V and V'. Note that the vector V is defined with (h) length , while $V^{'}$ has (w) length. So that shifting the columns can be using the vector V', and shifting the rows can be using the vector V. The obtained matrix is denoted by I_5.

Step 6. Repeat the previous steps $3-5$, sequentially four rounds. The matrix results from these possessing steps are denoted by (C) the ciphered image for the plainimage.

5.2.3 Decryption algorithm

The decryption involves reconstructing the original image from the encrypted image with an inverse process of the proposed encryption algorithm.

The indexes sorted of the matrix R_{init}, V_{init} and V'_{init} are unique, which means that the original pixels should recovered successfully using the inverse operations of step 3 and step 5 in the encryption steps.

Furthermore, since K is invertible matrix and $L \times K = Id$ over the finite field $GF(2^8)$, L can computed by $L = K^{-1}$, where Id is a $[32 \times 32]$ identical matrix.

The decryption method can be performed by applying the following steps :

Step 0. Read the ciphered image C and get its size $h \times w$

Step 1. Generate the encryption keys (R), (V) , and (V'), alongside α, K, L using the correct initial values (the secret keys) based on algorithm 1.

Step 2. Apply an operation inverse of step 5 in the encryption algorithm, within the matrix C, using the unique indexes sorted V and V'. The obtained matrix is denoted by C_2.

Step 3. Similar to the encryption step, we apply the equation 5.4 for each $[32 \times 32]$ block B over the finite field $GF(2^8)$ within the image data C_2.

$$C_3 : \ K \cdot B \cdot L \tag{5.4}$$

Where C_3 represent the obtained matrix.

Step 4. Apply an operation inverse of step 3 in the encryption algorithm using the index column in R for each $[32 \times 32]$ Block of C_3. The obtained matrix is denoted by C_4.

Step 5. Repeat the previous steps 2 to 4, sequentially four rounds. The result matrix is denoted by C_5

Step 6. Finally, apply the following equation 5.5. Then, we apply the inverse shifting by the indexes in V and V'.

$$D : \ C_5 \oplus \alpha \tag{5.5}$$

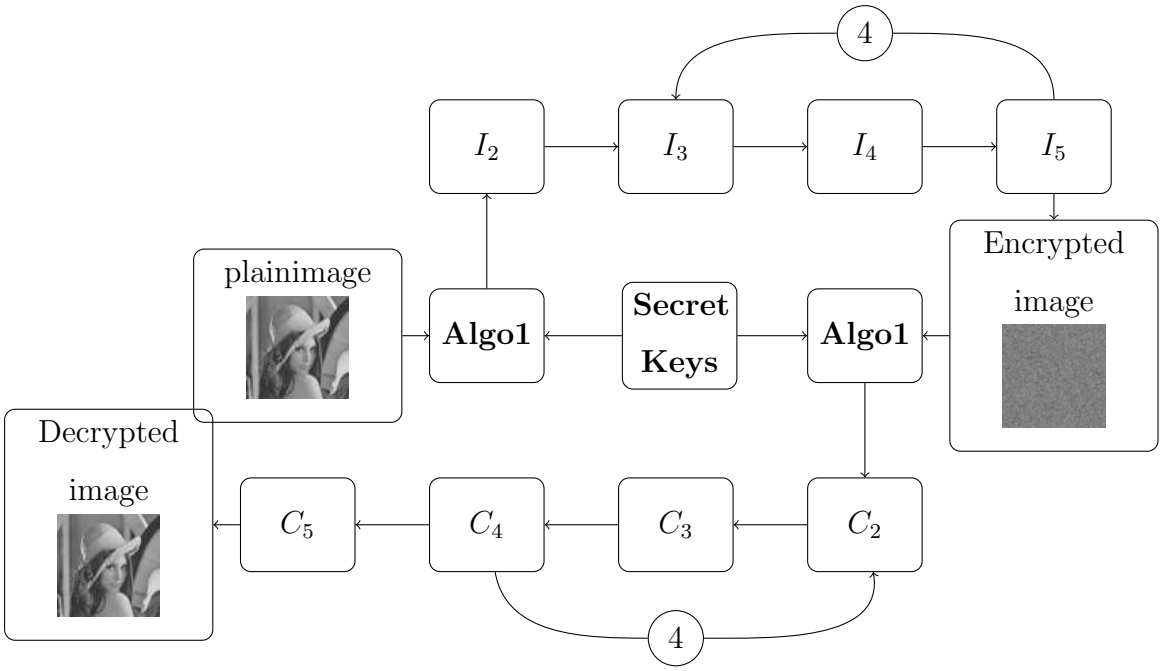


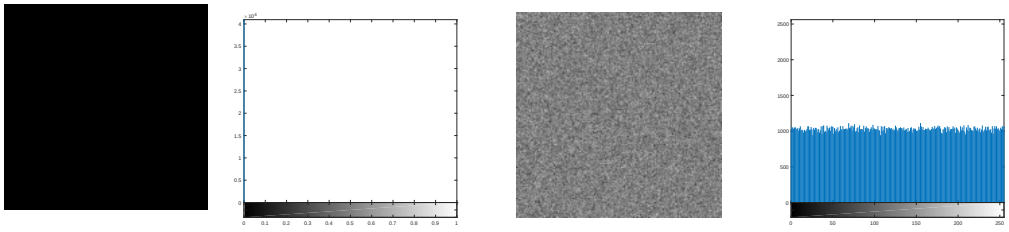
Figure 5.3: Illustration the encryption / decryption algorithm for gray image (the girl *lenna*)

Where D is the decrypting image of the ciphered image C after applying the inverse shifting.

Figure 5.3 shows the steps of pursuing encryption and the decryption for image of girl *lena* 512×512, where I_1, I_2, I_3, I_4, and I_5 represent the obtained matrix from the corresponding encryption step, while C_1, C_2, C_3, C_4, and C_5 represent the obtained matrix from the corresponding decryption step.

5.2.4 RGB image encryption

As we know, the grey scale image is stored in a matrix (2D array), where each position of the matrix represents a pixel value. While the color images such us *RGB* image, stored in three matrices that represent the corresponding RGB color. So, the proposed scheme can encrypt one matrix at a time, which means that the proposed image encryption method can encrypt each matrix separately.



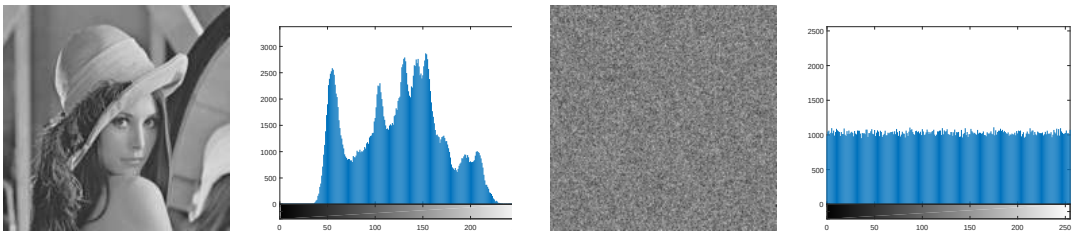
(a) (b) (c) (d)

Figure 5.4: Test the histogram of zeros image, and its corresponding encrypted image. (a) The zeros image. (b) Histogram for the zeros image. (c) The corresponding encrypted image. (d) Histogram for the encrypted image.

Alternatively, the color image with three $[h, w]$ matrices can be transformed to one matrix with $[3 \times h, w]$. The obtained matrix is encrypted similar to the encryption of a grey level image. Therefore, our proposed scheme would be capable of encrypting the color images.

5.3 Experimental results and discussion

Any proposed encryption method must give good performance and results comparing to the existing algorithms. We run various tests using MATLAB Version: 8.3.0.532 (R2014a) under the Windows 7 environment (64 bit) in a personal laptop with Intel Pentium CPU 2020M 2.4 GHz and 4 GB memory. The secret keys are selected as $(x_0 = 0.14, y_0 = 0.17, \varepsilon = 6.66, \tau = 5.55, \nu = 7.77)$ for the following tests. The performances of encryption and decryption of our proposed cryptosystem are analysed and well discussed. The tests and simulation have been done using database images (sipi.usc.edu/database/) along with standard testing images such as Lena, Cameraman, and Black images. Starting with the analysis of the histogram, the original image and its encrypted image along with the mathematical quantitative analysis using the variance, which evaluates the uniformity of distributions of pixels. The correlation coefficient analysis of pixels in the cipher image in the three directions: vertical, horizontal, and diagonal one.



(a) **(b)** **(c)** **(d)**

Figure 5.5: Test the histogram of plain image, and its corresponding encrypted image. (a) The plain image *girl 'Lena'*. (b) Histogram for the plain image. (d) The corresponding encrypted image. (d) Histogram for the encrypted image.

The test of NIST suite is presented to prove the randomness statistical properties of the ciphered image. We also present the criterion of difference between the original image with its corresponding encrypted image, using the number of pixel change rate ($NPCR$) test, and the test of unified average changing intensity ($UACI$). Also, key space analysis and key sensitivity have been presented. We show the efficiency of our proposed algorithm against known/chosen attacks, even with some typical data images. Ultimately, we have been able to compare the performance achieved by our proposed image encryption, based on several criteria, with the performance of other recent chaotic algorithms.

5.3.1 Histogram analysis

The histogram of the image represents the distribution of intensity levels for its pixels. A histogram shows pixels distribution values. Therefore, the histogram of encrypted image should be uniformly distributed, which prevent any type of the statistical attacks.

Figure 5.5, and Figure 5.4 shows the histogram for different images with their corresponding ciphering image. The pixels in ciphering images are uniformly well distributed, which is closer to equivalent probability of occurrence for each intensity level. The tests prove that the encrypted images are visually indistinguishable, even with special image e.g Black image (see Figure 5.4). The proposed

encryption algorithm possesses good confusion properties.

5.3.2 Information entropy

The entropy of information expresses the uniform distribution of the pixel value (105). For a random image with 8 bits intensity levels, the ideal entropy should be 8, that means it's a truly random image. Therefore, an ideal Information entropy of an encrypted image should be equal 8, Which prove that the information is completely random, and confirm the robustness of the proposed encryption algorithm. The information entropy H(X) of a message source X can be computed as:

$$H(X) = -\sum_{i=1}^{z} \mathrm{P}(x_i) \log_2 \mathrm{P}(x_i) \tag{5.6}$$

Where Z is the total number of symbols, and $x_i \in X$ and $P(x_i)$ represents the probability of the symbol x_i . Assuming that we have an 8-bit grey image, the entropy of encrypted image should ideally be H (X) =8. Therefore, an effective encryption method should achieve an entropy close to 8 for the ciphered image.

Table 5.1 shows the information entropy scores for a set of sample images from the chosen database. The average entropy of the cipher images, with 512×512 pixels, is computed to be 7.9993. Indeed, the entropies of all the images encrypted by our algorithm are very close to the ideal value, and prove that the ciphered images from the proposed encryption algorithm are almost close to a random source.

5.3.3 Correlation of two adjacent pixels

An efficient image encryption algorithm should eliminate the correlation of pixels. In this part of the analysis, the correlations between two adjacent pixels along the horizontal, vertical and diagonal directions in the original image and its corresponding ciphering image has been analysed. The correlation through two adjacent pixels is a very important perspective in security analysis, because the high correlation between adjacent pixels of the plainimage. Thus, The value absolute of the correlation coefficient of two adjacent pixels in ciphered images

Table 5.1: Entropy of the plain and cipher image of different size images

Name	Original image	Encrypted image
Black	0	7.9973
lenna	7.5954	7.9978
cameraman	7.0097	7.9973
5.1.14	7.3424	7.9977
7.1.03	5.4957	7.9993
7.1.09	6.1898	7.9994
numbers	7.7292	7.9994
gray21	4.3923	7.9993
ruler	0.5000	7.9994
testpat.1k	4.4077	7.9998
5.3.01	7.5237	7.9998

should be as low as possible (equal to zero), and achieves the ideal result of this test. Firstly, we select randomly 2048 pairs of two-adjacent pixels in diagonal, vertical and horizontal directions from the two images: the original image and its corresponding ciphered image. Then, we calculate the correlation coefficient of each pair by using the following formulas:

$$corr(x, y) = \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \tag{5.7}$$

Where:

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{5.8}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{5.9}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \tag{5.10}$$

In Table 5.2, the correlation between pixels of ciphered image is listed. The correlation coefficient of two adjacent pixels in ciphered images is almost zero, and archive the ideal value, which means that our approach can effectively remove correlations among the adjacent pixels. In addition, Figure 5.6 shows the histograms for an image with its corresponding ciphering image in the three direction diagonal, vertical and horizontal. Therefore, the proposed algorithm is robust against different statistical attacks.

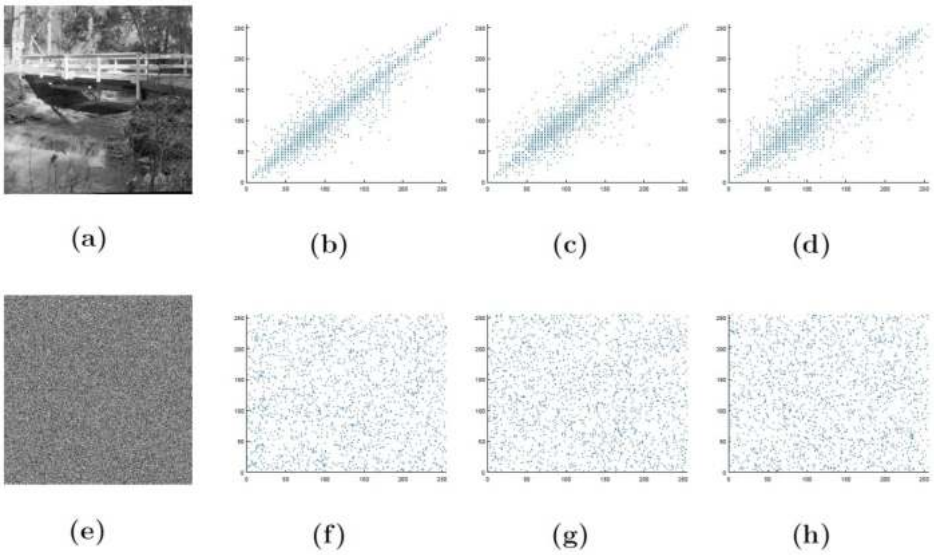


Figure 5.6: Correlation analysis of two adjacent pixels in an image and its corresponding encrypted image. (a) The plain image. (b) Distributions of two horizontally adjacent pixels in the plain image. (c) Distributions of two vertically adjacent pixels in the plain image. (d) Distributions of two diagonally adjacent pixels in the plain image. (e) The encrypted image. (f) Distributions of two horizontally adjacent pixels in the encrypted image. (g) Distributions of two vertically adjacent pixels in the encrypted image. (h) Distributions of two diagonally adjacent pixels in the encrypted image.

Table 5.2: Correlation coefficients of two adjacent pixels in the Plain and cipher images

Filename	Original			Cipher		
	horizontal	vertical	diagonal	horizontal	vertical	diagonal
Black	0	0	0	8.9950e-04	0.0038	0.0080
Lena	0.9201	0.9560	0.8986	0.0023	0.0049	0.0054
cameraman	0.9335	0.9592	0.9087	6.9973e-04	5.09e-04	0.0023
5.1.09	0.9020	0.9390	0.9037	-0.0049	-0.0015	-4.00e-04
5.1.14	0.9466	0.8984	0.8529	0.0057	-0.0018	-9.52e-04
7.1.03	0.9456	0.9321	0.9017	-0.0025	-0.0030	0.0055
7.1.09	0.9657	0.9304	0.9168	0.0023	8.7995e-04	0.0031
numbers.512	0.7386	0.7159	0.6253	-0.0044	0.0012	0.0017
gray21.512	0.9965	0.9998	0.9964	-3.5805e-04	0.0029	0.0016
ruler.512	0.4542	0.4648	-0.0290	0.0021	0.0019	-0.0014
testpat.1k	0.7593	0.7992	0.6978	5.5709e-04	-3.07e-05	0.0012
5.3.01	0.9774	0.9813	0.9671	3.4210e-04	8.37e-04	2.79e-04

5.3.4 Randomness tests

To have confirmation that the ciphered image is act like true random. We employ the $NIST$ suits tests (100). This test has 15 statistical, which requires a binary sequence with at least: 10^6 bits to find potential defects. The result of this test comes with the values P_{values}, and must come bigger than 0.01 to pass the tests. Also, e set B=000010011 in Non-overlapping template matching test. Otherwise, we use the default values that come with the $NIST$ suits tests (100).

First, we encrypted the "*elaine*.512" image that has $[512 \times 512]$ pixels. The ciphered data has been converted to binary data and passed into the suits tests of NIST. The results of statistical tests $NIST$ are listed in Table 5.3. The cipher image passed all the tests of NIST.

Table 5.3: Results of the NIST SP 800-22 randomness test on encrypted image

STATISTICAL TEST	P_{values}	Results
Frequency (monobit)	0.8697	Passed
Frequency (block)	0.7657	Passed
Runs test	0.6484	Passed
Random excursions(x=-3)	0.2921	Passed
Random excursions variants(x=-5)	0.9032	Passed
Longest run of ones in a block	0.9523	Passed
Binary matrix rank	0.0776	Passed
Discrete Fourier transform (spectral)	0.6729	Passed
Cumulative sums	0.9861	Passed
Non-overlapping template matching (B= 000010011)	0.6558	Passed
Overlapping template matching	0.1401	Passed
Universal	0.5945	Passed
Linear complexity	0.6511	Passed
Serial	0.5493, 0.7315	Passed
Approximate entropy	0.2683	Passed

5.3.5 Key Sensibility

The secret Keys in our proposed image encryption algorithm are very sensitive to its slightest modifications. Table 5.4 represents the tests of $NPCR$ and $UACI$ between two images C_1, C_2. We choose to produce the keys $R, V, V^{'}$ with different secret keys :

- $(x_R(0), y_R(0), \varepsilon_R, \tau_R, \nu_R)$=$(0.12, 0.13, 2.3, 5, 4)$.
- $(x_V(0), y_V(0), \varepsilon_V, \tau_V, \nu_V)$=$(0.14, 0.15, 5.6, 8, 7)$.
- $(x_{V'}(0), y_{V'}(0), \varepsilon_{V'}, \tau_{V'}, \nu_{V'})$=$(0.16, 0.17, 10.11, 12, 9)$.

In this test, we cipher the same plainimage with two different secret keys SC_1 and SC_2. The first secret key SC_1 is different from the second secret key SC_2 by a slight modification $(+10^{-15})$ in one of the initial values. The corresponding

ciphering is tested using the NPCR and UACI tests. Table 5.4 shows that all initial values are very sensitive for every single tiny change : $(x_0 : 10^{-15}, y_0 : 10^{-15}, \varepsilon : 10^{-15}, \tau : 10^{-15}, \nu : 10^{-15})$ for each encryption key produced. Table 4 shows the high sensitivity of our proposed scheme depended to the secret keys.

Table 5.4: NPCR and UACI between cipher images with slightly different keys $+10^{-15}$.

The initial value change	NPCR	UACI
$x(0)_R + 10^{-15}$	99.6323	33.5473
$y(0)_R + 10^{-15}$	99.6185	33.5836
$\varepsilon_R + 10^{-15}$	99.5926	33.3232
$\tau_R + 10^{-15}$	99.6201	33.3345
$\nu_R + 10^{-15}$	99.5987	33.6546
$x(0)_V + 10^{-15}$	99.6109	33.3711
$y(0)_V + 10^{-15}$	99.6155	33.4464
$\varepsilon_V + 10^{-15}$	99.5804	33.3092
$\tau_V + 10^{-15}$	99.5560	33.6771
$\nu_V + 10^{-15}$	99.6109	33.5089
$x(0)_{V'} + 10^{-15}$	99.6155	33.6750
$y(0)_{V'} + 10^{-15}$	99.6109	33.5089
$\varepsilon_{V'} + 10^{-15}$	99.5804	33.4856
$\tau_{V'} + 10^{-15}$	99.6033	33.3522
$\nu_{V'} + 10^{-15}$	99.6155	33.5106

Figure 5.7 shows tests of key sensitivity results in both encryption and decryption processes. We encrypt the same plainimage using three different secret keys SC_1, SC_2 and SC_3. The first secret key SC_1 is different from the second secret key SC_2 by a slight modification ($+10^{-15}$), and the second key SC_2 is also different from the third secret key SC_2 by a slight modification ($+10^{-15}$). The dif-

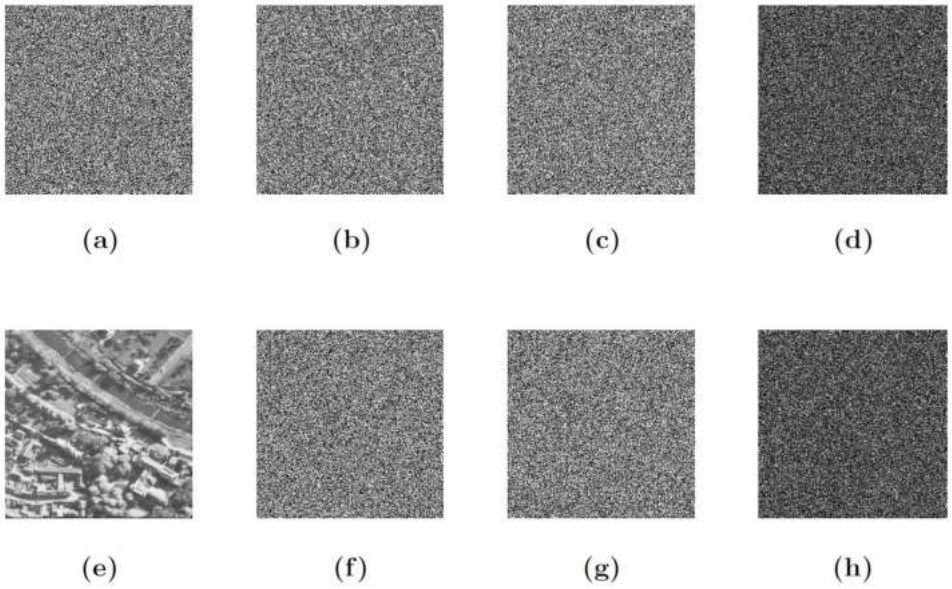


Figure 5.7: Key sensitivity results. (a) The encrypted image C using the secret key SC_1, (b) the encrypted image C_1 using the secret key SC_2, (c) the encrypted image C_2 using the secret key SC_3, (d) the image difference $|C_1 - C_2|$ (e) the decrypted image using the secret key SC_1, (f) the decrypted image D_1 using the secret key SC_2, (g) the decrypted image D_3 using the secret key SC_3, (h) the image difference $|D_1 - D_2|$.

ference between each pair of keys is only in one of the initial values $(x_0, y_0, \varepsilon, \tau, \nu)$. The results show that the reconstructed image is not possible without the exact secret keys that has been encrypted with it. Indeed, all results show that our proposed algorithm is highly sensitive to its secret keys for both encryption and decryption algorithm.

5.3.6 Key Space

A reliable ciphering algorithm should have large key space to resist the exhaustive search attacks. The space of keys in any encryption scheme should not be smaller than 2^{128} to make brute-force attacks infeasible (Alvarez et al. (7)). In our

proposed algorithm, all the initial values and controlling parameters are selected as secret keys. These keys are double-precision numbers, and according to the IEEE floating point standard (Bailey et al. (8)), the computational precision of the 64-bit double-precision numbers is about 10^{-15}. Indeed, all initial values are very sensible for every single modification as shown in Table 5.4. Therefore, the space key in the pseudo random number generator can compute approximately with more than $(10^{15})^5 = 10^{75}$. Indeed, if we consider that we can generate the vectors V, V', and (R) from different keys (see Table 5.4). This makes the space key more than $10^{225} \simeq 2^{711}$ for our proposed image encryption algorithm. And with such large space of the key is nearly impossible to estimate the selected secret keys, and there is no significant for the exhaustive attacks (Wang et al. (127)).

5.3.7 NPCR and UACI tests

The differential attacks are considered as the most common way to break any image encryption algorithm. Usually, the attacker seeks to find a relationship between the pixels from plainImage pairs that can affect the results of the difference at the ciphering image pair. So, any change in the initial image even with one-bit should change completely the ciphering image, so that the attacker cannot find any information related to the differential attacks.

The tests of $NPCR$ (Wu et al. (134)) and $UACI$ (Wu et al. (134)) are proposed in this subsection. $NPCR$ analysis shows the behavior of all pixels between two paired cipher images, while $UACI$ measures the average intensity of differences between the two paired cipher images (Wu et al. (134)). Both $NPCR$ and $UACI$ use two paired cipher images with one-pixel changing of the plainimage, which can prove the high resisting of any algorithm against the differential attacks.

The mathematical representation of the tests $NPCR$ and $UACI$ are presented as follows:

$$NPCR = \frac{\sum C(i,j)}{N \times M} \tag{5.11}$$

$$UACI = \sum \frac{\mid C_1(i,j) - C_2(i,j) \mid}{255 \times N \times M} \tag{5.12}$$

Where C_1 and C_2 are the ciphering images produced from two images that differ just in one pixel with a bit. The C size $N \times M$, and C is defined by following equation:

$$C(l,m) = \begin{cases} 1, if\ C_1(i,j) = C_2(i,j) \\ 0, otherwise. \end{cases} \tag{5.13}$$

For Block ciphering that is deterministic cipher which preserves the length, the notion of semantic security has recently been studied by padding noises bits into the plain image, this will produce a randomized ciphered image.

In our work, we consider the notion of indistinguishabe for block ciphering. Note that the decryption of a ciphered image lead to lossless original image, thanks to the determinism of block ciphers. The lose will be only among the effected bits during the randomized process.

Figure 5.8a, and Figure 5.8b show the scores of NPCR and UACI tests for the $[256 \times 256]$ Lena image. These tests are performed over 1000 times to evaluate plainimage sensitivity in our proposed encryption algorithm. Proceeding with these tests was carried out as follows. Fisrt, cloning the Plain Image $J = I$, where I is the plainimage, and J is the cloned image. Then, randomly selecting the position of one pixel. Finally, we applied equation 5.14.

Here, our proposed algorithm can have randomized proprieties like the probabilistic ones if we embeds one bit into the plain image. Herein, we randomly selecting the position of one pixel. Finally, we applied the following equation:

$$J(x,y) = I(x,y) \oplus 1 \tag{5.14}$$

Where J is the modified image, and (x,y) is the index of the selected pixel. Next, we carry out on the encryption algorithm as the above steps illustrated.

Both images (I, and J) are encrypted using the same secret keys. Finally, the pair ciphered images are tested using the $NPCR$ and $UACI$ over 1000 times. That should ensure the approximate average results.

Table 5.5 provides the experimental results with different images grey scalars with the above test. These tests are performed 1,000 times for each sample

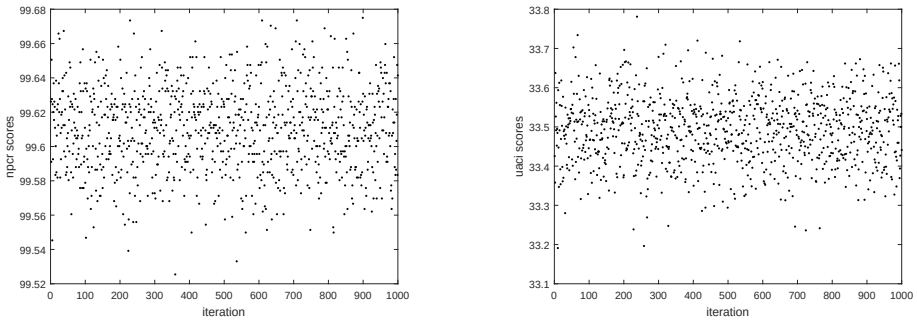
image. As shown in Table 5.5, the values of NPCR and UACI of our method are exceeding the ideal one which is 99.60% for NPCR and 33.46% for UACI (Sun et al. (111)). Indeed, the score of NPCR is around 99.61%, and the score of UACI is about 33.47% for our proposed image encryption algorithm. The results of these tests indicate the high sensitivity to plainimage change even with tiny change can completely change the corresponding ciphered image. Therefore, the proposed algorithm can provide a high security against the differential attacks.

Table 5.5: NPCR & UACI tests

Name	size	UACI %	NPCR %
Black	256×256	33.4819	99.6121
lenna	256×256	33.5124	99.6101
cameraman	256×256	33.4524	99.6068
5.1.13	256×256	33.4817	99.6080
5.1.14	256×256	33.4217	99.6112
7.1.03	512×512	33.4668	99.6085
7.1.09	512×512	33.4981	99.6108
numbers	512×512	33.4533	99.6084
gray21	512×512	33.4525	99.6098
ruler	512×512	33.4613	99.6077

5.3.8 Known/Chosen attack

The attacker should not obtain any useful information by encrypting some special images such as Black image (zero pixels). Figures 5.9 shows the resistance against chosen/known attack based on black image. This test is organized as follows. First, we generate $[256 \times 256]$ zero pixel image denoted by I. The image J is also $[256 \times 256]$ zero pixels with one bit different, where we randomly select and change the bit in one pixel. CI, CJ represent the ciphered images corespondent



(a) **(b)**

Figure 5.8: $NPCR$ and $UACI$ tests. (a) NPRC test for 1000 modified plain-images in one bit with a single pixel. (b) UACI test for 1000 modified plain-images in one bit with a single pixel.

to I, J images. Finally, we show the mean absolute of the pair images $|I - J|$, and $|CI - CJ|$. The tests confirm that the attacker cannot find or get any useful information to build his attack. The results come with no observe of black zone, and express the previous result of the high security against the attacks differential even with the chosen/known image.

According to the Kerckhoff's principle, the security of a cryptosystem must not depend upon keeping it secret. The security depends only on keeping the secret of keys (58). The hacker can access or/and knows exactly the design and working of the cryptosystem, and remain with him the secret keys and the original image. Therefore, assuming that the attacker has obtained the access for the encryption algorithm, even for a temporary time. There's four classical types of attacks.

1-Known Ciphertext attack. The attacker possesses a string of ciphers image.

2-Known Plaintext attack. The attacker possesses a string of original image, and obviously the corresponding ciphered image.

3-Chosen Plaintext attack. The attacker chooses an original image string and constructs the corresponding ciphered image string using the encryption algorithm.

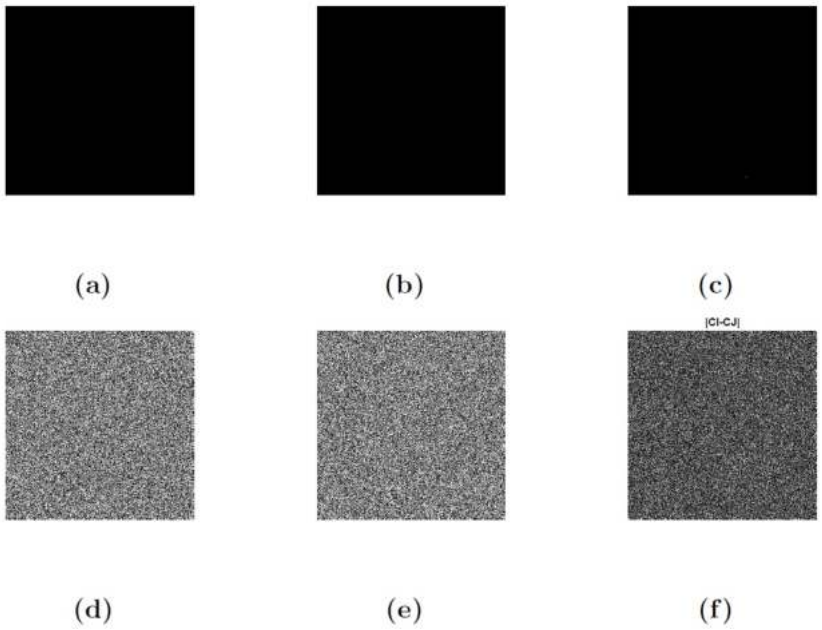


Figure 5.9: plainimage sensitivity results. (a) The plain image I. (b) The modified image J. (c) The image difference $|I - J|$. (d) The encrypted image CI. (e) The encrypted image CJ. (f) The image difference $|CI - CJ|$

4-Chosen Ciphertext attack. The attacker chooses a ciphered image string and constructs the corresponding decrypted image string.

If a cryptosystem can resist the attack of chosen plaintext, it can resist other types of attack due to the fact that chosen plaintext attack is the most powerful/effective attack (123). Therefore, and according to the previous tests, the proposed algorithm can resist these classical types of attacks.

5.3.9 Comparative analysis

Our cryptosystem algorithm is divided into two stages: initialization and processing operations. In the first stage, we produce keys for the encryption/decryption processes. This initialization stage will take around 0.06 seconds for a $[256 \times 256]$ image. In the second processing stage, the approximate time can take about 0.26 seconds (encryption and decryption have the same speed) for a $[256 \times 256]$ image.

The encryption speed is highly dependent on the CPU/GPU performance, RAM size, and the programming environment (C/C++, Java, Python...) (85). Therefore, the comparison of speed encryption is an approximate test due to various system characteristics and the platform that has been used in each study.

The complexity performance of the proposed algorithm is shown in Table 5.6. The algorithms have also been reported the encryption time of their algorithm as shown in Table 5.6 for the same $[256 \times 256]$ Lena image. The test speed demonstrates that our algorithm can achieve good speed, and shows that it is faster and better than the methods presented in Table 5.6. Therefore, our proposed image encryption algorithm is faster than state-of-the-art image encryption schemes, validating its better performance.

Table 5.6: The speed analysis between our proposed method and the other chaotic-cryptosystems

Algorithm	Encryption time (s)	Platform & System characteristics
Our proposed algorithm	0.32 s	MATLAB 8.3, CPU 2.4 GHz
Norouzi et al. algorithm (85)	0.4 s	MATLAB 7.6, CPU 2.4 GHz
Norouzi et al. algorithm (86)	0.41 s	MATLAB 7.6, CPU 2.4 GHz
Huang et al. algorithm (52)	0.55 s	MATLAB 6.5, CPU 2.00 GHz
XU et al. algorithm (140)	1.32 s	MATLAB 7.8, CPU 2.5 GHz

In addition, we compared the performances of our algorithm to several typical image encryption chaos-based algorithms. To compare the correlation coefficient values for the encrypted $[256 \times 256]$ Lena image, we use the following equation:

$$CC = \frac{|C_h| + |C_v| + |C_d|}{3} \tag{5.15}$$

Where the correlation coefficient value is denoted by CC, and the correlation in three directions (horizontal, vertical, and diagonal) are denoted by C_h, C_v, and C_d.

Table 5.7 shows the comparison of various efficiencies for different image encryption algorithms using the standard Lena image with dimension $[256 \times 256]$

pixels. Indeed, Table 5.7 confirm that our algorithm has larger space key, good performances, and exceeded the ideal scores for an encryption algorithm.

Table 5.7: Comparison between our proposed method and the other cryptosystems

Algorithm	CC	NPCR	UACI	Entropy	Space key
Ideal Values	$\simeq 0$	> 99.60	$\simeq 33.46$	$\simeq 8$	$> 2^{100}$
Proposed Algorithm	0.0031	99.61	33.50	7.9978	2^{711}
Akhshani et al. algorithm (5)	0.0058	0.39	0.33	7.9989	2^{225}
Akhavan et al. algorithm (4)	0.0031	39.45	33.28	7.9978	2^{180}
Huang et al. algorithm (51)	0.0027	99.54	28.27	7.9967	2^{152}
Wu et al. algorithm (135)	0.002	99.59	33.58	7.9972	2^{256}
Wang et al. algorithm (128)	0.0013	99.65	33.48	7.9970	2^{173}
Norouzi et al. algorithm (86)	0.0001	99.61	33.45	7.9979	2^{512}
XU et al. algorithm (140)	0.0094	99.62	33.51	7.9974	2^{210}
Norouzi et al. algorithm (87)	0.0078	99.61	33.45	7.9980	2^{256}

5.4 Conclusion

This chapter presented a novel image encryption algorithm based on the two-dimensional Zaslavsky map using the permutation and diffusion structure. Our proposed image encryption algorithm consists of two stages. In the first stage, the proposed cryptosystem employed the 2D Zaslavsky chaotic map to produce encryption keys for our proposed algorithm. These keys are applied to shuffle and diffuse the pixels of the plain image in the second stage using the permutation-diffusion processes. The simulations tests and security analysis were carried out carefully and well discussed. These tests including the statistical, histogram, sensibility and space keys, differential, quality and speed analysis, prove the high-

security level and sensitivity in plainimage with its secret key of the proposed scheme. The proposed image encryption algorithm has good ability to resist differential attack and withstand the known-plainimage, chosen-plainimage attack, and highly capable of withstanding the various attacks. The comparison with recent several chaos-based image encryption algorithms shown that our proposed encryption image algorithm is fast with excellent performance, making it more appropriate for reliable and practical cryptographic applications.

6

Secure framework for wireless capsule endoscopy

A smartphone links patients bodies and doctors computers, which in turn are connected to the Internet, which in turn is connected to any smartphone anywhere. The new devices could put the management of an individual's internal organs in the hands of every hacker, online scammer, and digital vandal on Earth.

Charles C. Mann

Contents

6.1 Introduction 107

6.2 Proposed framework 108

6.2.1 Summarization of video data captured during WCE . 109

6.2.2 ZCM-based image encryption algorithm 115

6.3 Experimental results and discussion 117

6.3.1 Histogram analysis 118

6.3.2 Differential attack analysis 120

6.3.3 Chosen/Known attack analysis 122

6.3.4 Sensibility analysis 122

6.3.5 Space Key analysis 125

6.3.6 Entropy analysis 125

6.3.7 Correlation coefficient analysis 125

6.4 Analysis and evaluation results 127

6.4.1 Summarization scheme 127

6.4.2 Encryption scheme 128

6.5 Conclusion 131

6.1 Introduction

Recently, the problem of secure dissemination of secret information over the Internet is growing fast. Ensuring the confidentiality and privacy of medical images is becoming one of the challenging problem as they contain sensitive data with distinguishing visual representations of the interior of a body (83, 103). One of the popular methods to record images of the digestive tract is wireless capsule endoscopy(WCE). During WCE procedure, the patient swallows a pill-sized capsule, which captures the images of gasterointestianl (GI) track while passing throught it. The captured images are recorded in an image recording unit (IRU), which is fitted in a belt worn by patient (119). The capsule is expelled from the body naturelly after 72 hours, however, the frames captured in the initial 8 hours are important for visualization of GI track (9). During this eight hours period, a large sequence of images (around 50000) are generated, out of which only a limited number of frames are important for diagnosis by gasteroentrologists. The collected video data contains a significant amount of redundant and non-informative frames due to capsules explosion to turbid fluids and food particles (73, 82). In this regard, it becomes inherently difficult and time consuming for gasteroentrologists to find the desired contents from this huge amount of collected video data. Thus, it is important to exploit a mechanism for automatic extraction of diagnostically important frames from the collected enormous amount of video data. Video summarization (VS) techniques can be used to solve this problem, where the informative frames can be extracted authomatically and can be sent to the remote pateint monitering centres and gasteroentrologists. As the overall diagnosis is mainly based on the extracted keyframes, it is necessary to send these frames securely as they can be exposed to various attacks such as spoofing or injection attacks. Hence, the problem of security and authentication arises for which we have devised a new framework.

In this work, we propose an efficient and secure video summarization framework for overcoming the drawbacks of existing systems. Our main contributions are summarized as follows:

1. An efficient and privacy-preserving video summarization framework is proposed for extraction of diagnostically important frames from WCE videos and its

secure dissemination to gastroenterologists and remote healthcare centers.

2. The proposed video summarization method uses the concept of integral image in features computation, increasing its suitability in real-time applications such as WCE.

3. A robust Zaslavsky chaotic map (ZCM) based image encryption scheme is proposed for security of keyframes. The proposed method can guarantee the secrecy of the keyframes with larger key space and can provide excellent confusion and diffusion properties with high level security. Moreover, it can be used for authentication of keyframes, preventing the possibility of injecting false keyframes.

4. The proposed framework can facilitate healthcare centers in ensuring the privacy of patients, reducing the energy, processing and communication cost, helping gastroenterologists to quickly browse for desired contents and fast analysis, leading to improved diagnosis with personalization.

The remaining of this chapter is organized as follows. The proposed system is explained in Section 2. Experimental results and discussion are presented in Section 3. The comparison tests are given in Section 4, followed by conclusion in Section 5.

6.2 Proposed framework

Medical data has become very interesting especially in remote health monitoring applications due to rapid advancement in smart sensor technologies. The current sensor technology is facilitating remote patient monitoring centers to produce different bio-signals and images from the outdoor patients body and monitor them remotely (69, 141). For example, during gait analysis, wearable sensors are used to measure numerous gait parameters including step length, cadence, swing-stance radio, stride length, and stride width, which are useful for diagnosis of several diseases such as Parkinsons disease, Huntington, and stroke (13). Another interesting application of medical sensors is WCE, where a capsule swollen by patient visualizes the entire GI track by capturing its images for several hours, producing a large amount of video data which is stored in IRU. Using smart phones, this video data can be transferred remotely to healthcare centers but it requires more

transmission cost, bandwidth, and energy and wastes the time of gastroenterologists in searching for diagnostically desired frames. In addition, ensuring the security of large amount of data is also comparatively challenging. Our proposed framework resolves these issues by using video summarization technology combined with image encryption. Our proposed system is two-fold: 1) extracting keyframes using video summarization and 2) encrypting the extracted keyframes using a robust image encryption scheme (46). Figure 6.1 highlights the proposed framework for secure dissemination of keyframes to remote health monitoring centers during WCE. The technical detail of the framework is provided in the sub-sequent sections.

In this section, the process of summarization of WCE video data is presented. During WCE, a large amount of redundant and non-informative video data is generated due to explosion of wireless capsule to food substances while passing through GI track (9). Considering the limited resources of smart phones and long duration of WCE process, it is usually assumed that sending all the WCE data to healthcare centers and gastroenterologists is impractical (73, 101). Therefore, it is important to devise a mechanism, which can allow only the informative frames for transmission and discard the redundant and non-informative frames. This goal can be achieved using video summarization methods. Keeping in view the constraints of WCE, we have used our recent video summarization scheme (74) for extraction of diagnostically important frames. Our recent VS method is computationally inexpensive, which is the main motivational reason for using it in the proposed framework. The reason is the utilization of integral image, which is a light-weight process with time complexity of 2WH (H: height, W: width of the frame), making this method more suitable for real-time processing of WCE video data.

6.2.1 Summarization of video data captured during WCE

Suppose the sequence of WCE frames coming from wireless capsule is with where NT indicates the total number of frames. Here, we aim to eliminate the redundant frames and classify the remaining WCE frames into informative and non-informative, thereby sending the informative frames to healthcare centers

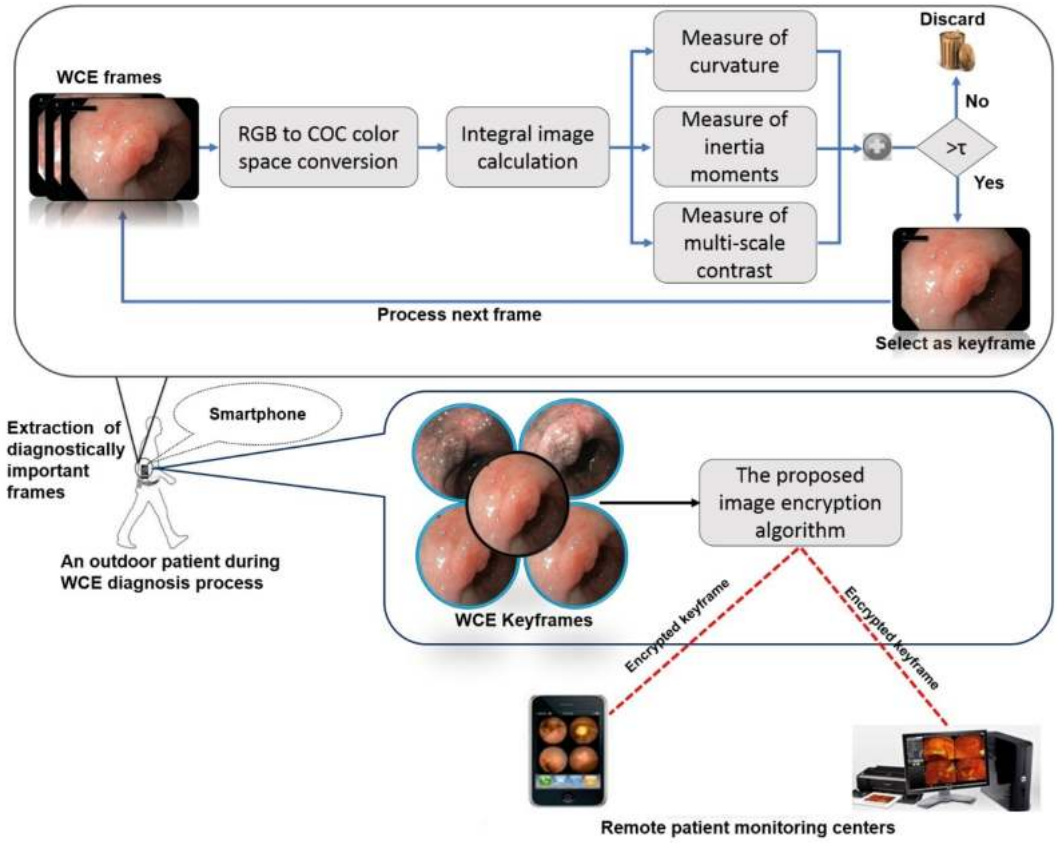


Figure 6.1: Framework of the proposed system.

and discarding the non-informative. To this end, each frame is converted from RGB to COC color model based on which the integral image is computed. Next, three features including moments of inertia, multi-scale contrast, and curvature map are computed. The saliency scores of these features are then normalized in the range 0-1. The normalized values of individual saliencies are then fused to form an aggregated attention curve based on which the keyframes can be extracted. Overall, this scheme provides several advantages such as reduction in the transmission cost, storage, and battery and saving the analysis time of gastroenterologists by avoiding large amount of redundant and non-informative frames. Figure 6.1 summarizes the overall process of the proposed framework by combining the video summarization module with encryption module during WCE. While Figure 6.2 shows the experimental test of encryption a keyframe, where (a) is a

sample of keyframe extracted using our recent video summarization scheme. The encrypted keyframe using our proposed scheme is shown in (b). and (c) shown the decrypted keyframe.

Figure 6.2: Experimental test of ciphering the extracted keyframe

Wireless Capsule Endoscopy video contains frame sequence f_t, where $t = 1, 2, 3, N_t$ and N_t is the total number of frames.Each frame captured and digitized in RGB color space. By using video summarization, extracted keyframe from the underlying video are transmit to the corresponding specialist doctor (74). The following steps explain the techniques of extracting the keyframes.

6.2.1.1 Color space conversion: RGB to COC

COC is a color space introduced based on the RGB model, and it has improved color perception (24, 74). RGB color channel is converted into four broadly-tuned color channels as follows.

$$R' = R - \frac{G + B}{2} \tag{6.1}$$

$$B' = B - \frac{R + G}{2} \tag{6.2}$$

$$G' = G - \frac{R + B}{2} \tag{6.3}$$

$$Y' = \frac{R + G}{2} - \frac{|R - G|}{2} - B \tag{6.4}$$

Now, by using these four channels (R', B', G', Y'), two opponent color pairs red-green and blue-yellow are computed as follows:

$$RG' = R' - G' \tag{6.5}$$

$$BY' = B' - Y' \tag{6.6}$$

The intensity channel is computed. Followed by fusing with red-green (RG') and blue-yellow (BY') channels that have been computed using Egs. 6.6 , and 6.5.

Eqs. 6.7 , and 6.8 show how to compute the final aggregated image F_t. Finally, saliency map is holistically computed only for this aggregated image F_t.

$$I_t = \frac{R' + B' + G'}{3} \tag{6.7}$$

$$F_t = RG' + BY' + I_t. \tag{6.8}$$

6.2.1.2 Integral image computation

Integral image is a summed array by cumulative addition of intensities on subsequent pixels in both columns and lines. Basically, the integral image can constructed by replacing each image pixel with a value equal to sum of all pixels above and to the left of the current pixel (74). In this step, we compute the Integral image for the aggregated image F_t using Eq 6.9.

$$F(x, y) = \sum_{x' \leq x, y' \leq y} F_t(x', y'). \tag{6.9}$$

6.2.1.3 Visual saliency computation

The human visual attention model consists of high-level cognitive processes which lead to saliency maps (74). The Saliency Map is a topographically arranged map that represents visual saliency of a corresponding visual scene (65). The saliency map reduces the complexity of scene analysis and focuses on the most relevant objects. In this context, the visual attention model can be used to

efficiently summarize the contents of WCE videos (74). In this work, the proposed saliency model is based on three features: image moment, multi-scales contrast, and curvature.

- Image moments

In this step, VS algorithm employs the four moments of inertia: mean, standard deviation, skewness, and kurtosis. These statistical moments qualitatively describe the structural shape of a region, its boundaries, texture etc. Here, these techniques are computed from the aggregated image F_t.

$$E_t = \frac{\sum_{x=1}^{W}\sum_{y=1}^{H} F_t(x,y)}{W \times H} \tag{6.10}$$

$$\sigma_t = \sqrt{\frac{\sum_{x=1}^{W}\sum_{y=1}^{H}(F_t(x,y) - E_t)^2}{W \times H}} \tag{6.11}$$

$$S_t = \frac{\frac{1}{\sigma_t^3}\sum_{x=1}^{W}\sum_{y=1}^{H}(F_t(x,y) - E_t)^3}{W \times H} \tag{6.12}$$

$$K_t = \frac{\frac{1}{\sigma_t^4}\sum_{x=1}^{W}\sum_{y=1}^{H}(F_t(x,y) - E_t)^4}{W \times H} \tag{6.13}$$

Herein, E_t, σ_t, S_t, and K_t are the mean, standard deviation, skewness, and kurtosis values of the aggregated image F_t, respectively.

Here, the sum of pixels within any rectangular region can be determined with only four array-references using the aggregated image F_t. Next, an algorithm of distance between two integral image F_t and F_{t+1} can be defined as:

$$d_{mom}(F_t, F_{t+1}) = \sqrt{(E_t - E_{t+1})^2 + (\sigma_t - \sigma_{t+1})^2 + (S_t - S_{t+1})^2 + (K_t - K_{t+1})^2} \tag{6.14}$$

The result value of d_{moment} is employed for removing redundancy in the sequences images from WCE.

- Multi-scale contrast

Multi-scale contrast is used in this work to deal with varying size anomalies in WCE extracted frames. For each image, multi-scale contrast at pixel (x, y) is computed on aggregated image F_t as:

$$MC^S = \|F(x, y) - \mu\| \tag{6.15}$$

Where

$$\mu = \frac{F(x+N, y+N) + F(x-N, y-N) - F(x-N, y) - F(x, y-N)}{N \times N} \tag{6.16}$$

where $s \in [1, 3]$ is the image Gaussian pyramid scale and N=5 is the neighborhood around pixel (x,y). While, μ is computed in constant time that requires operation on only four indexes of integral-image (74). Final step here by adding the contrast at three levels of Gaussian pyramid. This step produces a gray scale saliency image.

$$MC(x, y) = \sum_{S=1}^{3} MC^3(x, y) \tag{6.17}$$

- Gaussian filter

In this step of work, a Gaussian filter is applied for the gray scale saliency image extracted from Multi-scale contrast. The gaussian filter efficiently reduces noise by smoothing the overall image.

$$G_t = F_t(x, y) \times \frac{1}{2\pi\sigma^2} \cdot e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{6.18}$$

Where, σ is the standard deviation of the Gaussian distribution (using Eq 6.14).

- Curvature feature

After computing gaussian filter in Eq 6.18, first order derivative of G_t is computed that produces a two dimensional column vector as mentioned in equation 6.19, and 6.20. The computed vector C has an important geometric characteristic feature that highlights curvature of G_t.

$$C = \nabla(G_t) \tag{6.19}$$

Where,

$$\nabla(G_t) = [G_t^x, G_t^y] = [\frac{\partial G_t}{\partial x}, \frac{\partial G_t}{\partial y}] \tag{6.20}$$

Next, magnitude of curvature vector C is computed using Eq 6.21.

$$C_{mag} = \sqrt{(G_t^x)^2 + (G_t^y)^2} \tag{6.21}$$

These measures are normalized in the range $[0, 1]$ and are fused to get a final saliency map. Where the average of non-zero pixel values is considered as a saliency value, which computed for each frame in the video. Basically, the keyframe extraction is based on the comparison of frames saliency values computed using the above subsections. Herein, the selection of a new keyframe is based on the significant change between the saliency values of the current frame and the previous keyframe. The specialist (mainly will be a the gastroenterologists and the technique) which can adjust the significant change according to the level of details they require in summaries (74).

6.2.2 ZCM-based image encryption algorithm

In this sub-section, we describe our image encryption algorithm (46), for ciphering the keyframes in detail. The proposed cryptosystem is divided into two steps: initialization and processing steps. In the first step, the algorithm for generating the encryption keys for the cryptosystem process is described. In the second part, the proposed encryption/decryption algorithms are explained, which are based on permutation-diffusion processes, achieving a high level of security. All the initial values of the ZCM are taken as secret keys in our encryption method. The upcoming sub-sections explain the key generation procedure, followed by encryption/decryption of keyframes. For detailed information about our image encryption, the readers are referred to chapter 5 (46).

Algorithm 6.3 shows the steps of encryption for the extracted keyframe from WCE video data using our recent video summarization scheme. Firstly, we pack the matrices of the keyframe, which represent the corresponding RGB color (three matrices), into one matrix with size $[h, e \times w]$, followed by dismantling and distribution of pixels for the obtained data matrix. The symbol $\oplus$ indicates the

Algorithm **6.3:** Encryption algorithm.

Input: *Secret keys*, $I(Keyframe)$.

0: Read the plain frame, and generate the cryptographic keys

1: Transform the frame matrices into one matrix with [h, 3×w]

2: $I_2 \leftarrow$ Permutation using the matrix $V, and\ V'$

3: $I_3 \leftarrow I_2 \oplus \alpha$

4: $I_4 \leftarrow$ Permutation using the matrix R

5: $I_5 \leftarrow L \cdot B_{I_4} \cdot K$

6: $I_6 \leftarrow$ Permutation using the matrix $V, and\ V'$

7: Repeat the previous steps 4-6 four rounds, sequentially

8: $C \leftarrow$ Reshape the obtained matrix intro three matrices with size [h, w]

Output: C: Encrypted keyframe.

bitwise XOR operator. The term permutation in Algorithm 2 means that each pixel is permuted using the given element sort. We use the matrix R as indexes for shifting each block B. Similarly, we use the indexes vector V and V' to shift each column and row of the image. We use the arithmetic matrix multiplication for each B block using the matrices K,L, where L is the invertible matrix of K such that $L \cdot K = Id_{32}$ is an [32,32] identical matrix. The symbol $'\cdot'$ in Algorithm 2 is the operator of the multiplication over Galois Fields $GF(2^8)$.

By padding noises bits into the plain image, the proposed cryptosystem will produces a randomized ciphered image (probabilistic encryption). Decrypted image will be almost the same as the original image (different only in amended bits).

Algorithm 6.4 shows the decryption steps for our proposed scheme. The inverse steps for the encryption processes can recover the original pixels completely only by using the exact secret keys. Since the sorted indexes are unique, the original pixels can be recovered successfully from the permutation steps. Figure 6.1 Overall procedure of the proposed framework, illustrating the extraction of keyframes and flow of the proposed encryption/decryption algorithms for secure WCE in remote healthcare. Figure 6.5 summarizes the overall process of the pro-

posed framework by combining the video summarization module with encryption module during WCE.

Algorithm **6.4:** Decryption algorithm.

Input: *Secret keys*, I(*Encrypted_Keyframe*).

0: Read the encrypted frame, and generate the cryptographic keys.

1: Transform the frame matrices to one matrix with [h, 3×w]

2: $C_2 \leftarrow$ Permutation inverse using the matrix V, and V'

3: $C_3 \leftarrow K \cdot B \cdot L$

4: $C_4 \leftarrow$ Permutation inverse using the matrix R

5: $C_5 \leftarrow$ Repeat the previous steps 2-4 four rounds, sequentially

6: $C_6 \leftarrow C_5 \oplus \alpha$

7: $C_7 \leftarrow$ Permutation inverse using the matrix V, and V'

8: $D \leftarrow$ Reshape the obtained matrix intro three matrices with size[h, w]

Output: D: the decrypted keyframe

6.3 Experimental results and discussion

In this section, the proposed system is evaluated through different experiments from security and statistical analysis point of view. First, we evaluated the proposed method through histogram analysis, key space, and sensibility analysis. Next, we analyzed the performance of the secret key and showed its resistance to common security attacks. Next, we exposed our proposed method to different attacks such as chosen/known attacks, and resisting differential attack, followed by its analysis using different tests such as randomness tests, and test of correlation analysis for two adjacent pixels in a ciphered keyframe. Finally, we showed the advantages of our proposed image encryption scheme by comparing its performance results with several recent state-of-the-art image encryption methods (135, 146, 147, 148). Due to special nature of WCE images, we directly used their

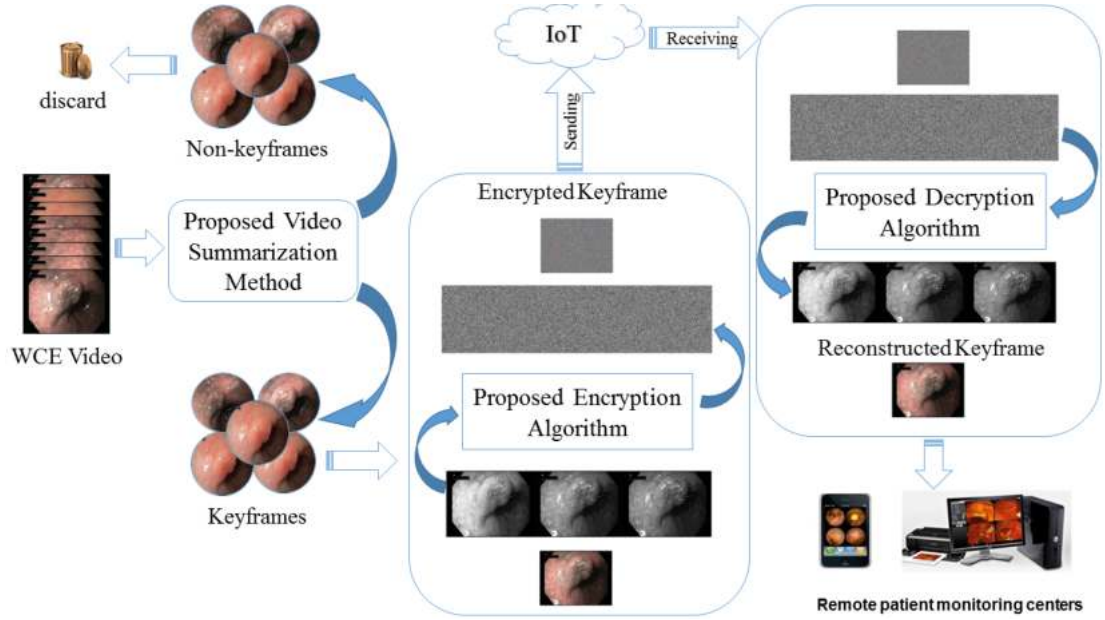


Figure 6.5: Overall procedure of the proposed framework.

source codes for the frames extracted by our recent VS method for comparison of results using the same platform and configurations, making the comparative analysis more fair and unbiased. A set of test keyframes and non-keyframes from a sample WCE video along with frame number are shown in Figure 6.6 and Figure 6.7.

6.3.1 Histogram analysis

The histogram of a frame illustrates the distribution of its gray levels. Figure 6.8 shows the uniform probability distribution of ciphered keyframe without any statistical similarity, while the original keyframe appears significantly different from the ciphered keyframe. Here, (a) represent keyframe 0065, (e) the encrypted keyframe, histogram of the original keyframe in (b) Red, (c) Green, and (d) Blue components. While Histogram of the encrypted keyframe in the (f) Red, (g) Green, and (h) Blue components. The histogram of encrypted frame is obviously uniform and the visual view is impossible to redirect to the original one as shown in Figure 6.8. Consequently, our proposed scheme does not provide any informa-

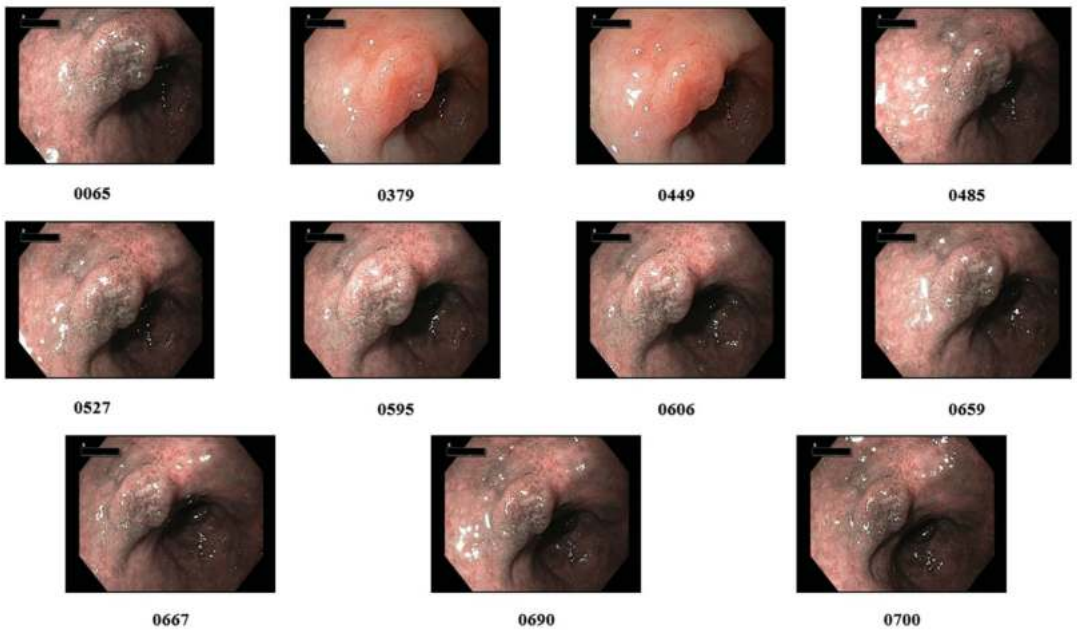


Figure 6.6: Selected test keyframes with frame numbers from our proposed scheme.

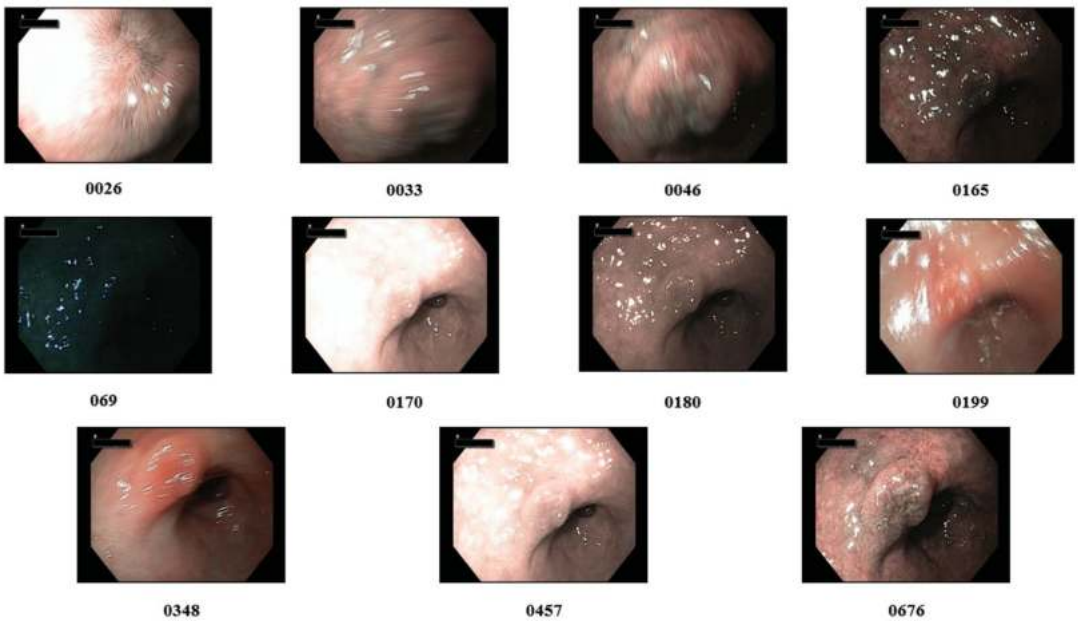


Figure 6.7: Sample non-keyframes with frame numbers from our proposed scheme.

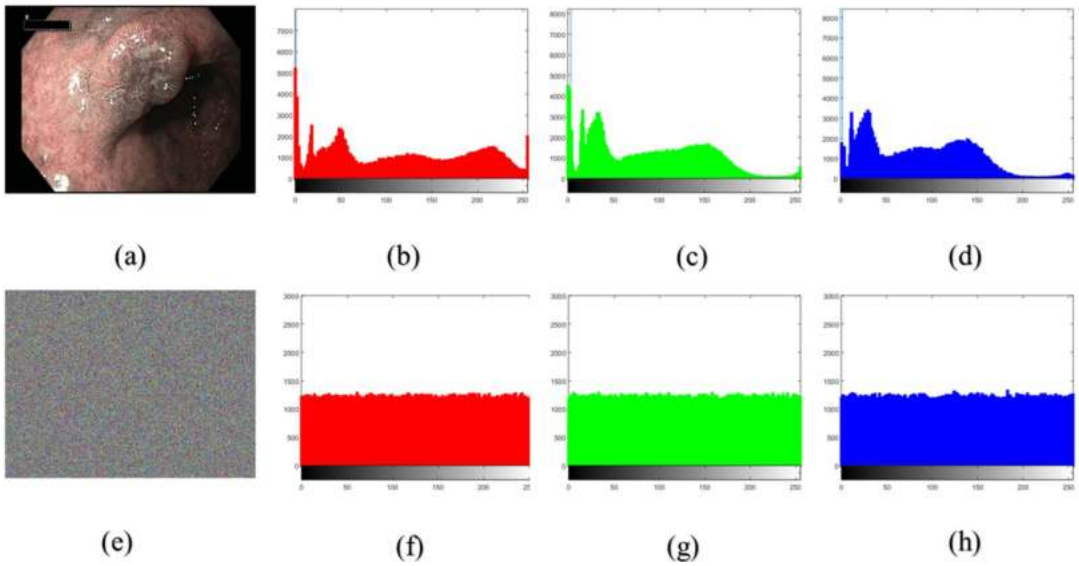


Figure 6.8: Histogram of a frame 0065.

tion for attackers to be used in statistical attacks, which makes it more suitable for securing transmission of keyframes during wireless capsule endoscopy.

6.3.2 Differential attack analysis

Differential attack refers to investigating the difference in inputs and its corresponding effects on outputs (147). Basically, an attacker investigates how a small change in any frame can affect the ciphered image so that he/she can proceed with his/her attacks. The ability to resist the differential attack can reveal the security level of any image encryption technique. This resistance of the differential attack can be measured using the number of pixel changing rate (NPCR) test (142) and unified average changed intensity (UACI) test (142), which are computed using Eq. 6.22 and Eq. 6.23 as follows:

$$NPCR(C_1, C_2) = \frac{\sum_{i,,j} S(i,j)}{D} \times 100\% \tag{6.22}$$

$$UACI(C_1, C_2) = \sum_{i,,j} \frac{\mid C_1(i,j) - C_2(i,j) \mid}{255 \times D} \times 100\% \tag{6.23}$$

Table 6.1: NPCR and UACI tests results for each channel of RGB frame.

Frames	0065		0606		0667		0690	
Test	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
R	99.6126	33.4412	99.6247	33.4923	99.6139	33.4750	99.6090	33.4698
G	99.6117	33.4361	99.6245	33.3929	99.6234	33.4864	99.6051	33.4480
B	99.6071	33.4371	99.6058	33.4985	99.5964	33.4861	99.6276	33.5088

Table 6.2: NPCR and UACI tests results for a set of keyframes.

Frames	0065	0379	0449	0485	0527	0595	0606
NPCR	99.6104	99.6085	99.6172	99.6164	99.6161	99.6235	99.6112
UACI	33.4381	33.4575	33.4784	33.5177	33.4456	33.4614	33.4825

Herein, D denotes the number of pixels and S is represented by Eq. 6.24.

$$S(i,j) = \begin{cases} 1, \ If \ C_1(i,j) = C_2(i,j) \\ 0, otherwise. \end{cases} \tag{6.24}$$

In this test, we randomly change one bit of a pixel from a keyframe I. The obtained keyframe is denoted by J. We use the same secret key in our proposed scheme to encrypt both keyframes. C_1 and C_2 are the two ciphered keyframes corresponding to I and J, respectively. Finally, we apply the tests of NPCR and UACI using both C_1 and C_2. The results of this analysis for a complete set of test keyframes and non-keyframes are listed in Tables 6.1, and 6.2. The obtained results show the high level security presented by our approach. The scores exceeded the ideal score for an encryption algorithm 99.61 % and 33.44% for NPCR and UACI (30), respectively.

Figure 6.9 shows the NPCR and UACI tests repeated 100 times for one keyframe randomized (randomly we change one bit) . The results confirm that any minor change of the plain keyframe can change the corresponding ciphered keyframe completely. Therefore, the proposed image encryption demonstrated good ability to resist the differential attack and can provide high-level security to the keyframe extracted using VS during WCE.

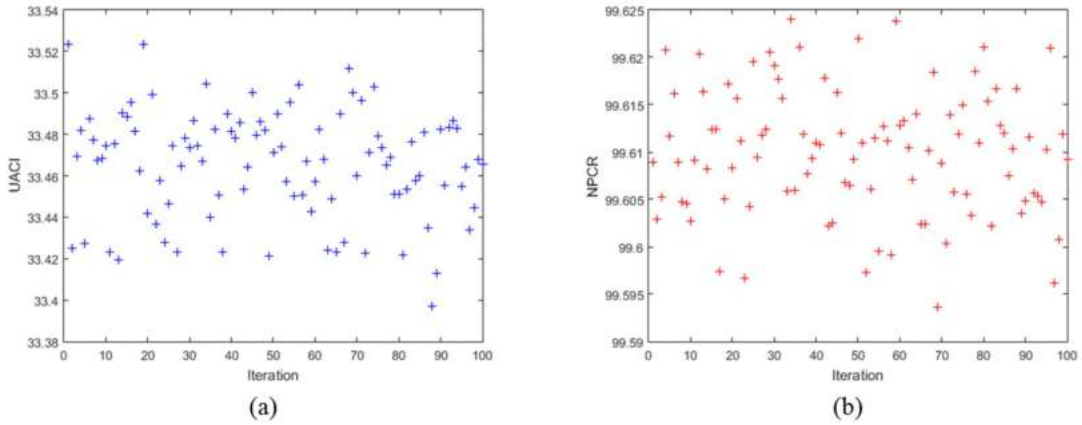


Figure 6.9: NPRC tests (a) and UACI tests (b) for 100 plain-images (randomized)

6.3.3 Chosen/Known attack analysis

In previous sections, we explained that our proposed algorithm has high sensitivity to any tiny modification in the plain frame as well as in its secret keys. Furthermore, no information can be obtained by cryptanalysis regardless of the attack type by malicious users because each encryption is related completely to the plain frames and the secret keys. Moreover, according to the previous tests, our proposed scheme is immune to the chosen attacks. It is a well-known fact that any cipher resistant to the chosen-plaintext attacks is considered as immune to other chosen/known attacks (123). This confirms the better ability of the proposed method to resist chosen/known attacks.

6.3.4 Sensibility analysis

The proposed algorithm is based on a chaotic map, which is known by its sensibility for any tiny change in the initial values and controlling parameters. Therefore, all these initial values and controlling parameters are selected as secret keys in our method. To confirm that our image encryption technique has a high security level, we change one initial value or parameter of the chaotic systems slightly to analyze the effect of the ciphered image.

Table 6.3 shows the NPRC and UACI test results for pair ciphered images. The encrypted images are obtained with the same plain keyframe using a single

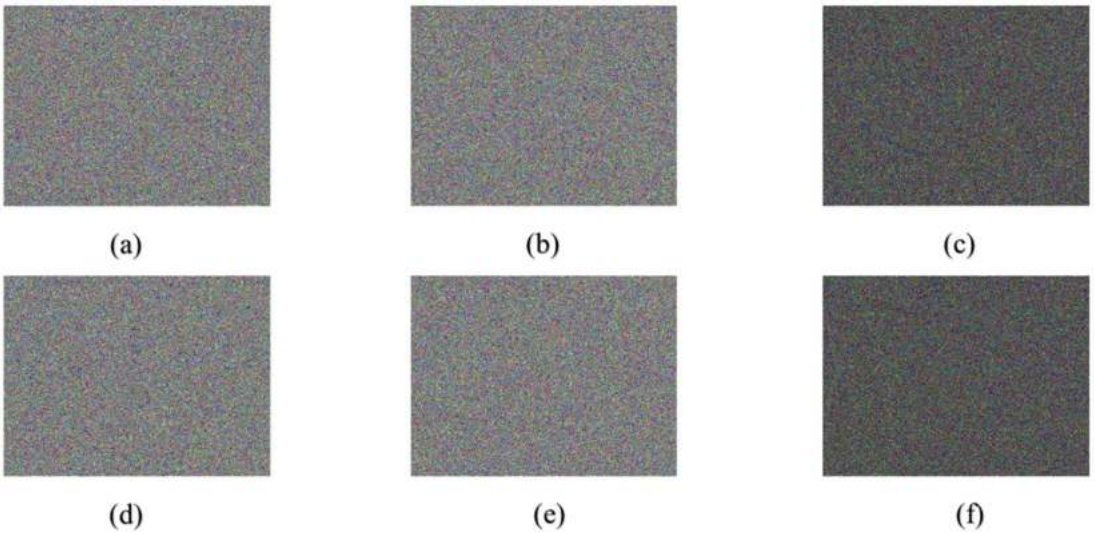


Figure 6.10: Key sensitivity analysis at the encrypted/decryption stage.

Table 6.3: Tests of secret keys sensibility.

Key Change	x_0	y_0	v	ε	τ
NPRC	99.6105	99.6082	99.6112	99.5966	99.6125
UACI	33.4365	33.4794	33.4825	33.4665	33.4525

slight change $+10^{-15}$ in one of the secret key. Figure 6.10 shows some tests of sensibility on the secret keys. In order to test the encryption/decryption sensibility, we use two secret keys. Each secret Key differs only in one tiny change in one of the initial values with $+10^{-15}$. Figure 6.10 (a) shows the encrypted keyframe using the first secret key. Figure 6.10 (b) shows the encrypted keyframe using the second secret key. Figure 6.10 (d) shows the decrypted version of the keyframe in Figure 6.10 (b) using the first secret key. Figure 6.10 (e) shows the decrypted of the keyframe in Figure 6.10 (a) using the second secret key. Figure 6.10 (c) shows the abs mean difference between the encrypted images in Figure 6.10 (a), and (b). Figure 6.10 (f) shows the abs mean difference between the decrypted images in Figure 6.10 (d), and (e). The obtained image in Figure 6.10 (c) and Figure 6.10 (f) are without any black-zone (zero pixels), indicating no

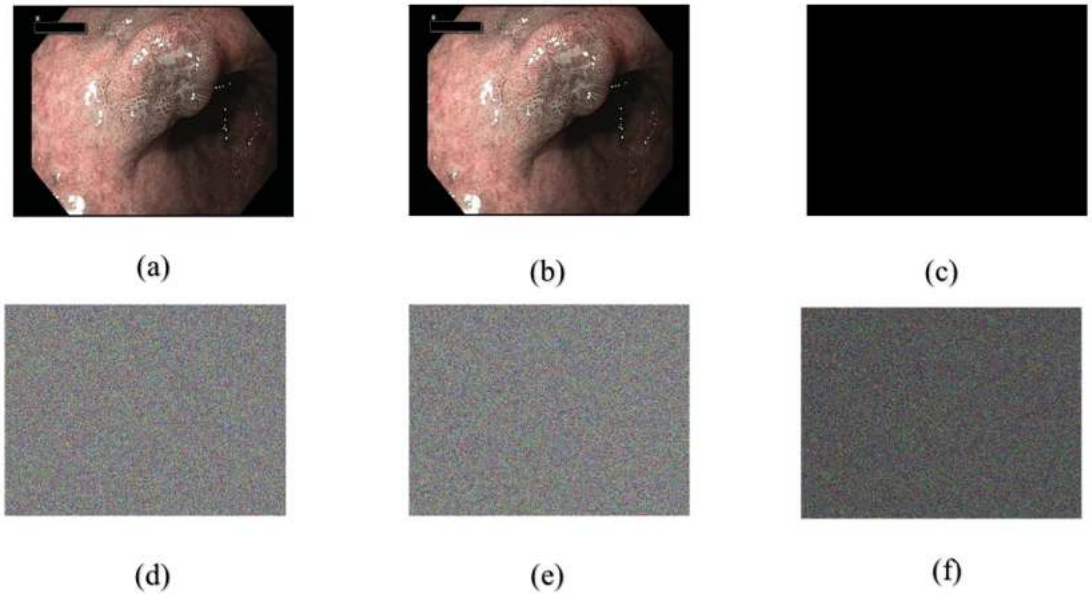


Figure 6.11: Tests of the keyframe sensitivity.

observation to any equal block between the ciphered/decrypted data. Therefore, any tiny adjustment of the secret keys can produce completely different cipher data and the only possible way to recover the original data is using the exact secret key.

In addition to the secret key sensitivity, we test the plain keyframe sensitivity in Figure 6.11. Firstly, we encrypt the original keyframe as shown in Figure 6.11 (a). The ciphered keyframe is denoted by CI (Figure 6.11 (d)). Secondly, we randomly select one pixel and we change the least significant bit. The modified keyframe is denoted by J (Figure 6.11 (b)). Finally, Figure 6.11 (f) shows the abs mean image difference $|CI - CJ|$, where CJ is the corresponding encrypted image for J (Figure 6.11 (e)). The obtained image in Figure 6.11 (f), has no observation for a black zone, indicating the existence of non-equal blocks on the ciphered data. Therefore, the attackers cannot obtain any useful information, even with using some special attacks. The tests confirm that our proposed method is very sensitive to any tiny alteration to its secret keys as well as pixels of plain-keyframe.

Table 6.4: The Entropy tests for a set of data keyframe.

Frame/Entropy	0065	0379	0449	0485	0527	0595	0606	0659	0667
Original	7.3656	7.4360	7.4328	7.4028	7.3647	7.3674	7.3208	7.3700	7.1773
Ciphered	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998

6.3.5 Space Key analysis

In this work, all the initial values and controlling parameters of ZCM are selected as secret keys, making the space keys for the proposed pseudo random sequence generator more than $10^{5*15} = 2^{237}$. Indeed, we can generate each key encryption with other secret keys as we have three main encryption keys ($K, V, and\ V'$). This leads to a key space of around 2^{711} for the proposed algorithm, making it larger enough to withstand exhaustive attacks.

6.3.6 Entropy analysis

The pixel values of a ciphered image are expected to be uniformly distributed to achieve a high security level. Shannons entropy (106) can measure the randomness of the ciphered data. To achieve high-level security, the local Shannon entropy score should be equal to 8 for a random frame with 256 gray levels (111). The local Shannon entropy is calculated to check the level of randomness between the input image and its ciphered version. Therefore, the entropy score of an encrypted image generated by any effective encryption method should be close to 8. Table 6.4 shows the information related to local Shannon entropy for various ciphered keyframes. All the results demonstrate that the ciphered keyframes are almost close to a random source, validating the effectiveness of our proposed framework.

6.3.7 Correlation coefficient analysis

In this sub-section, we investigate the correlation coefficient effect on the ciphered frames. The relationship between correlation and security is described as follows. The lesser the correlation of two adjacent pixels is, the safer the ciphered frame is.

Therefore, we randomly select 2048 pairs of adjacent pixels for testing the correlations between two adjacent pixels in the three directions: vertically, horizontally, and diagonally, respectively.

Table 6.5: The correlation coefficient of adjacent pixels tests.

Keyframe#	Component	Keyframe			Ciphered		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
0065	R	0.9931	0.9907	0.9856	0.0028	-0.0016	8.609e-04
	G	0.9886	0.9847	0.9764	-3.991e-04	1.833e-04	-0.0019
	B	0.9872	0.9828	0.9735	0.0017	0.0047	0.0013
0379	R	0.9963	0.9944	0.9919	-8.509e-04	-7.219e-04	-7.116e-04
	G	0.9929	0.9900	0.9853	0.0013	-7.229e-04	-0.0034
	B	0.9913	0.9881	0.9824	-0.0040	0.0013	6.472e-04
0527	R	0.9917	0.9914	0.9849	-0.0042	-0.0022	9.524e-04
	G	0.9860	0.9862	0.9754	-7.046e-05	-0.0019	-6.470e-04
	B	0.9843	0.9846	0.9726	-0.0021	-0.0025	0.0030

The test results of the plain frames and ciphered frames for each component are listed in Table 6.5. The correlation coefficients are all greater than 0.98 in the original frames, indicating strong correlation between adjacent pixels of each direction in plain frames. On the other hand, the correlation coefficients are all almost 0.001 in the ciphered frames, representing negligible correlation and nearby to the ideal value (CC=0) for an encrypted frame (85). Figure 6.12 illustrates the plot of the correlation distribution for the plain frame and its corresponding ciphered frame. The test has been handled using pixels values in the range [0, 1], we converted the pixels from uint8 to double precision. Here, Figure 6.12(a) shows the original Keyframe, Figures 6.12(b), (c), and (d) show correlation distribution for keyframe in diagonal, vertical, and horizontal direction, respectively. Figure 6.12(e) shows the ciphered keyframe, and Figures 6.12 (f), (g), and (h) are referred to correlation distribution for ciphered keyframe in diagonal, vertical, and horizontal direction, respectively. Here, the strong correlation between adjacent pixels is obvious with agglomeration of the dots for the plot of the plain frame. However, in case of ciphered frame, the dots are scattered over the entire plot.

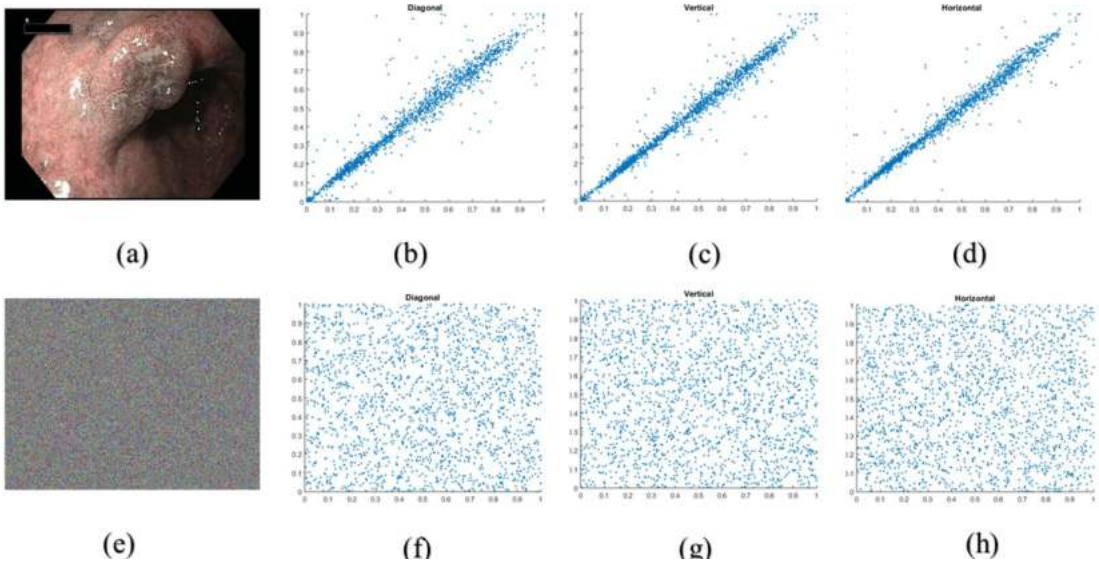


Figure 6.12: Correlation coefficient diagrams (blue channel).

Therefore, our proposed method can efficiently minimize the strong correlation between adjacent pixels of the plain frames.

6.4 Analysis and evaluation results

6.4.1 Summarization scheme

In this subsection, we evaluate the summarization algorithm performances and the significance of the chosen framework. For this purpose, two gastroenterologists were requested for Evaluate the keyframes, and to select significant frames in each video.

Basically, there are three matrices are computed to evaluation and compare the results of the summarization scheme (74).

1- A true positive (TP) which represent a frame selected as keyframe from both the gastroenterologists and the technique.

2- A False negative (FN) which represent a frame chosen as keyframe by the gastroenterologist but not by the technique.

3- A False positive (FP) which represent a frame selected as keyframe by the technique but not by the gastroenterologist.

The frames selected by the particular summarization scheme were then compared with the ground truth to find Recall, Precision Eqs 6.26, and 6.27.

$$Recall_{initial} = \frac{TP}{TP + FN} \tag{6.25}$$

$$Precision = \frac{TP}{TP + FP} \tag{6.26}$$

$$Recall = 2 \times \frac{Recall_{initial} \times Precision}{Recall_{initial} + Precision} \tag{6.27}$$

A value of F-measure close to 1 indicates high values of both Recall and Precision and vice versa (74). The presented summarization technique resulted by Recall (R), Precision (P), and F-measure (F) are listed in Table 6.6. Comparison to other algorithms (23, 90), using the averages of R, P, and F as points of comparison, show that the proposed technique outperformed other mentioned techniques by yielding higher values of Recall, Precision, and F-measure as Table 6.7 shows.

The results show that the proposed vs model to extract the informative frames from WCE was very effective in detecting various medical abnormalities. This techniques has three advantages: 1) reduction in the size of extracted frames to be encrypted, 2) saving the resources of WCE and health care systems (especially regarding time), and 3) comparatively high keyframes quality.

6.4.2 Encryption scheme

In this section, we evaluate the performance of our proposed method by conducting several tests based on image quality and other evaluation metrics. The metrics for comparative study include mean square error (MSE) (40), structural

Table 6.6: Summarization Scheme Evaluation.

Video No.	1	2	3	4	5	6	7	8	9	10	Average
R	0.75	0.83	0.91	0.8	0.85	0.84	0.89	0.89	0.86	0.84	0.84
P	0.8	0.91	0.88	0.82	0.83	0.87	0.92	0.91	0.81	0.82	0.85
F	0.77	0.87	.089	.081	0.84	0.85	0.90	0.90	0.83	0.83	0.85

Table 6.7: Recall (R), Precision (P), and F-measure (F) results compared with different summarization techniques.

	Pan et al. (90)	Ejaz et al. (23)	Proposed algorithm
R	0.68	0.78	0.84
P	0.70	0.79	0.85
F	0.69	0.785	0.85

similarity index metric (SSIM) (79), NCC (80), NPCR, UACI, entropy, and correlation coefficient (111, 137). The mathematical equations for the last three metrics are already given in previous sub-sections. The remaining three metrics (MSE, SSIM, and NCC) can be computed using Eqs. 6.28, 6.29, and 6.30 as follows:

$$MSE = \frac{1}{m\,n}\sum_{x=1}^{m}\sum_{y=1}^{n}[I(x,y) - E(x,y)]^2 \tag{6.28}$$

$$NCC = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}[I(x,y) \times E(x,y)]^2}{\sum_{x=1}^{m}\sum_{y=1}^{n}[E(x,y)]^2} \tag{6.29}$$

$$\text{SSIM} = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{6.30}$$

Herein, I is the input frame, E is encrypted frame, x and y are loop counters, m and n show frame dimension, and c_1 and c_2 avoid division by zero exception.

Table 6.8: Comparison of the proposed image encryption method with recent state-of-the-art encryption algorithms based on multiple performance evaluation metrics.

Method Name	Space Keys	Time Encrypt (s)	Time Decrypt (s)	MSE	SSIM	NCC	NPCR	UACI	Entropy	Correlation Coefficient
Our	2^{711}	2.58	2.65	≅0	≅1	≅1	99.609	33.450	7.9998	0.0019
Wu et al.[135]	2^{256}	180.60	180.97	0	1	1	99.613	33.409	7.9998	0.0014
Zhou et al.[146]	2^{215}	1.3831	1.6248	0	1	1	99.609	33.434	7.9998	0.0013
Zhou et al.[147]	2^{265}	8.642	5.3614	97.2274	0.9770	1	99.686	33.246	7.9998	0.0008
Zhou et al.[148]	2^{256}	41.0262	41.5787	0.0763	0.9999	1	99.605	33.490	7.9998	0.0026

MSE should be as minimum as possible for better performance. Conversely, the value of NCC and SSIM should be as closer to 1 as possible (64, 81)

In the comparison tests, initialization steps were introducted by packing the corresponding matrices of RGB frames into one matrix. The Matlab source code for other papers was obtained and the tests were performed on the same data keyframe using the same configurations for fair evaluation and comparison. Table 6.8 tabulates the performance values of the cipher-keyframe encrypted by different image encdryption schemes (135, 146, 147, 148). All the presented image encryption schemes in Table 6.8 have good confusion and diffusion properties. Each scheme has the same entropy and NCC score. The correlation coefficient values are approximately zero for all reviewed schemes. However, there is some variation in the MSE and SSIM tests, where the performance of our proposed scheme is better than Zhou et al. (148) and Zhou et al. (147). The authors in (147) have used a random pixel insertion in the beginning of each row in the original image, which led to the highest score of MSE among the methods under consideration.

The recent existing schemes (135, 147, 148) are computationally complex in terms of encryption and decryption compared to our proposed method for keyframes encryption. The proposed framework of WCE is a real-time procedure, requiring real-time fast response in terms of encryption. Therefore, these methods cannot be used in the proposed framework. The method introduced in (146) has lower execution time compared to our method, however, its key space is

too short, making its security limited for the proposed sensitive WCE framework according to Kirchhoff's principle (please refer to chapter 3, last section). Moreover, our key space is also better than the other methods mentioned in Table 6.8 . This validates the suitability of the proposed encryption method for integration with the proposed video summarization assisted WCE procedure for healthcare centers.

6.5 Conclusion

In this chapter, we formulated the problem of effective management of wireless capsules data and its secure dissemination to remote health monitoring centers for personalized WCE. Considering the limited resources during WCE such as smartphones battery, processing, and transmission cost, an energy-efficient video summarization algorithm is devised to automatically extract the keyframes from the sequence of WCE frames. The proposed VS scheme is based on integral-image, which is a light-weight process, making it more suitable for real-time application such as WCE. Next, we proposed a cryptosystem for secure dissemination of the keyframes extracted using our VS scheme to gastroenterologists and healthcare centers. We used 2D chaotic map to generate the permutation keys, which shift the position of the plain keyframe pixels, followed by diffusion per block using the arithmetic matrix multiplication over finite field. The proposed method has a larger key space with high sensitivity to any tiny modification. Any minor bit adjustment on the original keyframe can produce completely different ciphered keyframe. Moreover, the proposed cryptosystem scheme has a higher ability to resist chosen/known attacks and differential attacks. The proposed encryption method is fast and provides a high level of security with large space keys compared to other state-of-the-art encryption schemes. These characteristics verify the suitability of our framework for secure dissemination of the keyframes to healthcare centers and remote gastroenterologists, facilitating them with correct real-time decisions, leading to improved healthcare facilities.

Conclusion and future work

In the last decades, many security techniques have been proposed to guarantee digital images security. Yet, existing mechanisms still need to fitful the security requirements of digital images to withstand the growing threat of hackers. Mainly, most of the traditional cryptographic techniques did not take into account the characteristics of digital images in general and medical images in particular.

Medical images is a very promising field which can establish many practical applications in order to save lives and helping doctors making critical decisions. In fact, medical data can be exploited to be beneficial for better life and improve health and well-being. However, information security risk exposures are always present and show privacy issues. Furthermore, new technologies introduced some security problems such as ensuring the confidentiality of the extracted keyframe from WCE, where the lack of protection is present.

In this pursuit, ciphers techniques are proposed to embed secret information in digital images domain. Accordingly, we succeeded to find some solutions to secure the digital images using chaotic maps and probabilistic approaches. We also managed to combine between a summarization technique and an encryption scheme into a secure framework for personalized wireless capsule endoscopy. The proposed structure secures the transmission of informative data that are extracted from wireless capsule endoscopy videos.

The main purpose of this thesis is to provide some solutions to the problems related to digital image security with different cryptography techniques and mechanisms. In this regard, we have investigated to get a better understanding of the behavior and the specifics for different kinds of digital images as well as the various problems associated with security in this field of work. We have studied the

security of digital images issues, where we considered both generating the cryptographic keys for digital images and encryption as points of view for our works. Mainly, we have discussed digital image security with a randomized algorithm and probabilistic techniques. As a matter of fact, we have proposed different solutions to achieve our goal (41, 42, 43, 44, 45, 46). However, I sincerely believe that the field of information security will be always an open research due to the unconventional thoughts which can lead to break any cryptographic techniques.

In the first contribution, we have proposed a novel pseudo-random numbers generator based on a high dimensional chaotic map samples. The proposed algorithm is designed to generate cryptographic keys for the digital images. Indeed, we have dealt with the problem of a non uniform probability of the generated sequences from Chen chaotic map, where the previous works used this map directly and as result have been analyzed due to the mentioned problem.

In the second contribution, we have proposed a novel image encryption algorithm based on 2D Zaslavsky chaotic map. The ciphering structures have been chosen based on permutation-diffusion processes, which adopted from the classic permutation substitution network. The proposed scheme is very sensitive for any adjustment for the original image. So, embedding noises bits to the image pixels can lead to adjusting the mechanism of producing an encrypted image to become a randomized ciphered image. The proposed image encryption algorithm can withstand several well-known attacks and have good confusion and diffusion properties which guarantee high-security level for the digital images.

In the third contribution, we have proposed a new approach to secure the keyframes extracted from wireless capsule endoscopy data. In our proposed framework, a keyframe is extracted from WCE using a light-weight video summarization scheme. Later, we employed our second contribution (image cipher) to encrypt the extracted keyframe. An efficient and privacy-preserving video summarization framework is proposed for extraction of diagnostically important frames from WCE videos and its secure dissemination to gastroenterologists and remote healthcare centers.

Finally, we believe that the solutions are certainly not complete solutions for digital images security issues. Indeed, some points in the digital images security still need to be addressed. I hope, of course, that we have succeeded in covering

most discerned issues in this research. In addition, the current studies shall unfold some new subjects to studies in future to develop or make more improvements to the presented solutions. Despite the obvious success of publishing numerous solutions in this dissertation, I consider there will always be opportunities to do better improvements.So, we look to the future by reflecting in order to achieve better protection for digital images.

Hopefully, future works on this topic will extend the current works to secure the rest of files data and not just the digital images. Also, we intend to explore the hash functions to improve the encryption structure scheme as well as using cellular automaton to generate the cryptographic keys. In addition, detection anomalies among digital images using a set of cryptographic techniques could be a very interesting direction in future work. Finally, we will explore the cryptanalysis techniques.

References

[1] Cea: Medical imaging. http://www.cea.fr/comprendre/Pages/sante-sciences-du-vivant/essentiel-sur-imagerie-medicale.aspx. Accessed: 2017-06-23. 29

[2] Vectorfresh: Sample pack of imaging eps. https://www.vectorfresh.com/freeimages-SamplePack1.html. Accessed: 2017-06-25. 14

[3] wikipedia: Medical imaging. https://en.wikipedia.org/wiki/Medical_imaging. Accessed: 2017-06-23. 28

[4] Akhavan, A., Samsudin, A., and Akhshani, A. A symmetric image encryption scheme based on combination of nonlinear chaotic maps. *Journal of the Franklin Institute 348*, 8 (2011), 1797–1813. 104

[5] Akhshani, A., Behnia, S., Akhavan, A., Hassan, H. A., and Hassan, Z. A novel scheme for image encryption based on 2d piecewise chaotic maps. *Optics Communications 283*, 17 (2010), 3259–3266. 104

[6] Alvarez, G., Amigó, J. M., Arroyo, D., and Li, S. Lessons learnt from the cryptanalysis of chaos-based ciphers. In *Chaos-Based Cryptography*. Springer, 2011, pp. 257–295. 62

[7] Alvarez, G., and Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos 16*, 08 (2006), 2129–2151. 53, 70, 97

[8] Bailey, D. H. High-precision floating-point arithmetic in scientific computation. *Computing in science & engineering 7*, 3 (2005), 54–61. 98

[9] Basar, M. R., Malek, F., Juni, K. M., Idris, M. S., and Saleh, M. I. M. Ingestible wireless capsule technology: A review of development and future indication. *International Journal of Antennas and Propagation 2012* (2012). 108, 110

[10] Behnia, S., Akhavan, A., Akhshani, A., and Samsudin, A. A novel dynamic model of pseudo random number generator. *Journal of Computational and Applied Mathematics 235*, 12 (2011), 3455–3463. 53

[11] Benvenuto, C. J. Galois field in cryptography. *University of Washington* (2012). 49

[12] Brown, J. A., Houghten, S., and Ombuki-Berman, B. Genetic algorithm cryptanalysis of a substitution permutation network. In *Computational Intelligence in Cyber Security, 2009. CICS'09. IEEE Symposium on* (2009), IEEE, pp. 115–121. 43

[13] Buke, A., Gaoli, F., Yongcai, W., Lei, S., and Zhiqi, Y. Healthcare algorithms by wearable inertial sensors: a survey. *Communications, China 12*, 4 (2015), 1–12. 109

[14] Burger, W., and Burge, M. J. *Principles of digital image processing: fundamental techniques*, vol. 1. Springer Science & Business Media, 2010. 12, 18, 19, 23

[15] Cayre, F., Fontaine, C., and Furon, T. Watermarking security part i: Theory. In *Security, Steganography, and Watermarking of Multimedia Contents VII* (2005), vol. 5681, SPIE, pp. 746–757. 35

[16] Chen, G., Mao, Y., and Chui, C. K. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals 21*, 3 (2004), 749–761. 2

[17] Chen, G., Mao, Y., and Chui, C. K. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals 21*, 3 (2004), 749 – 761. 4

[18] Chen, G., and Ueta, T. Yet another chaotic attractor. *International Journal of Bifurcation and Chaos 9*, 07 (1999), 1465–1466. 63

[19] Chen, T.-H., Chang, C.-C., Wu, C.-S., and Lou, D.-C. On the security of a copyright protection scheme based on visual cryptography. *Computer Standards & Interfaces 31*, 1 (2009), 1–5. 35

[20] Daemen, J., and Rijmen, V. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013. 41, 45

[21] De Canniere, C. T. A stream cipher construction inspired by block cipher design principles. *Information Security* (2006), 171–186. 42

[22] Delfs, H., and Knebl, H. *Probabilistic Algorithms*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2002, pp. 111–121. 2, 55

[23] Ejaz, N., Mehmood, I., and Baik, S. W. Efficient visual attention based framework for extracting key frames from videos. *Signal Processing: Image Communication 28*, 1 (2013), 34–44. 129, 130

[24] Engel, S., Zhang, X., and Wandell, B. Colour tuning in human visual cortex measured with functional magnetic resonance imaging. *Nature 388*, 6637 (1997), 68–71. 112

[25] Fabunmi, B. A., Paris, M., and Fabunmi, M. Digitization of library resources:

Challenges and implications for policy and planning. *International Journal of African & African-American Studies 5*, 2 (2009). 13

[26] Farmer, J. D., and Sidorowich, J. J. Predicting chaotic time series. *Physical review letters 59*, 8 (1987), 845. 49, 61

[27] Fouque, P.-A., Martinet, G., and Poupard, G. Practical symmetric on-line encryption. In *FSE* (2003), vol. 2887, Springer, pp. 362–375. 32

[28] Fousse, L., Lafourcade, P., and Alnuaimi, M. Benalohs dense probabilistic encryption revisited. In *International Conference on Cryptology in Africa* (2011), Springer, pp. 348–362. 55

[29] Franois, M., Grosges, T., Barchiesi, D., and Erra, R. Pseudo-random number generator based on mixing of three chaotic maps. *Communications in Nonlinear Science and Numerical Simulation 19*, 4 (2014), 887 – 895. 61

[30] Fu, C., Chen, J.-j., Zou, H., Meng, W.-h., Zhan, Y.-f., and Yu, Y.-w. A chaos-based digital image encryption scheme with an improved diffusion strategy. *Optics Express 20*, 3 (2012), 2363–2378. 122

[31] Fu, C., Zhang, Z.-C., and yu Cao, Y. An improved image encryption algorithm based on chaotic maps. In *Natural Computation, 2007. ICNC 2007. Third International Conference on* (Aug 2007), vol. 3, pp. 189–193. 4

[32] Fu, W., Wang, J., Gui, L., Lu, H., and Ma, S. Online video synopsis of structured motion. *Neurocomputing 135* (2014), 155 – 162. 37

[33] Fu, Y., Zhang, W., Mandal, M., and Meng, M. Q.-H. Computer-aided bleeding detection in wce video. *IEEE journal of biomedical and health informatics 18*, 2 (2014), 636–642. 4, 37

[34] Fuchsbauer, G. J. An introduction to probabilistic encryption. *Osječki matematički list 6*, 1 (2006), 37–44. 55

[35] Gao, T., and Chen, Z. A new image encryption algorithm based on hyper-chaos. *Physics Letters A 372*, 4 (2008), 394–400. 81

[36] García-Martínez, M., and Campos-Cantón, E. Pseudo-random bit generator based on lag time series. *International Journal of Modern Physics C 25*, 04 (2014), 1350105. 3, 50, 61

[37] Gentle, J. E. *Random number generation and Monte Carlo methods*. Springer Science & Business Media, 2006. 53

[38] Gianluigi, C., and Raimondo, S. An innovative algorithm for key frame extraction in video summarization. *Journal of Real-Time Image Processing 1*, 1 (2006), 69–88. 38

[39] Goldwasser, S., and Micali, S. Probabilistic encryption. *Journal of computer and system sciences 28*, 2 (1984), 270–299. xvii, 36, 55

[40] Gutub, A. A.-A. Pixel indicator technique for rgb image steganography. *Journal of Emerging Technologies in Web Intelligence 2*, 1 (2010), 56–64. 129

[41] Hamza, R. A novel pseudo random sequence generator for image-cryptographic applications. *Journal of Information Security and Applications 35* (2017), 119 – 127. x, 134

[42] Hamza, R., Muhammad, K., Lv, Z., and Titouna, F. Secure video summarization framework for personalized wireless capsule endoscopy. *Pervasive and Mobile Computing* (2017), –. x, 134

[43] Hamza, R., Muhammad, K., Nachiappan, A., and González, G. R. Hash based encryption for keyframes of diagnostic hysteroscopy. *IEEE Access* (2017). x, 134

[44] Hamza, R., and Titouna, F. A study on chaotic maps to produce randomness

numbers. *Journes nationales sur les mathmatiques appliques: Skikda JNMA'15* (2015). xi, 134

[45] Hamza, R., and Titouna, F. A new pseudo random sequence generator based on chen chaotic map. *International Conference on Cryptography and its Applications, Oran - IWCA'16* (2016). xi, 134

[46] Hamza, R., and Titouna, F. A novel sensitive image encryption algorithm based on the zaslavsky chaotic map. *Information Security Journal: A Global Perspective 25*, 4-6 (2016), 162–179. x, 37, 39, 61, 110, 116, 134

[47] Hassouna, H. *Gaussian Process for Image Classification*. PhD thesis, Université Mohamed Khider-Biskra, 2016. 13

[48] Hewage, C. T. *Perceptual quality driven 3-D video over networks*. PhD thesis, University of Surrey, 2008. 24, 26

[49] Howard, R. Data encryption standard. *Information age 9*, 4 (1987), 204–210. 2

[50] Hu, H., Liu, L., and Ding, N. Pseudorandom sequence generator based on the chen chaotic system. *Computer Physics Communications 184*, 3 (2013), 765–768. 5, 40, 51, 61, 62, 63, 64

[51] Huang, C., Liao, C.-W., Hsu, S., and Jeng, Y. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. *Telecommunication Systems 52*, 2 (2013), 563–571. 104

[52] Huang, X. Image encryption algorithm using chaotic chebyshev generator. *Nonlinear Dynamics 67*, 4 (2012), 2411–2417. 81, 103

[53] Jeng, F.-G., Huang, W.-L., and Chen, T.-H. Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes. *Signal Processing: Image Communication 34* (2015), 45–51. 81

[54] Keuchel, M., Hagenmüller, F., and Tajiri, H. *Video capsule endoscopy: a reference guide and atlas.* Springer, 2015. 19

[55] Khan Muhammad, Rafik Hamza, J. A. J. L. H. W., and Baik, S. W. Secure surveillance framework for iot systems using probabilistic image encryption. *IEEE Transactions on Industrial Informatics* (2018). x

[56] Lai, X. *On the design and security of block ciphers.* PhD thesis, 1992. 42, 43

[57] Lambić, D. Security analysis and improvement of a block cipher with dynamic s-boxes based on tent map. *Nonlinear Dynamics 79*, 4 (2015), 2531–2539. 2, 35, 51, 61, 62

[58] Lee, W.-B., and Chen, T.-H. A public verifiable copy protection technique for still images. *Journal of Systems and Software 62*, 3 (2002), 195–204. 3, 51, 101

[59] Li, C., Liu, Y., Zhang, L. Y., and Chen, M. Z. Breaking a chaotic image encryption algorithm based on modulo addition and xor operation. *International Journal of Bifurcation and Chaos 23*, 04 (2013), 1350075. 2, 35, 51, 61

[60] Li, Y., Tang, W. K., and Chen, G. Generating hyperchaos via state feedback control. *International Journal of Bifurcation and Chaos 15*, 10 (2005), 3367–3375. 49, 61, 63

[61] Lian, S. *Multimedia content encryption: techniques and applications.* CRC press, 2008. 2, 32, 34, 40, 41, 42, 51, 52, 53

[62] liang Zhu, Z., Zhang, W., wo Wong, K., and Yu, H. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences 181*, 6 (2011), 1171 – 1186. 4, 39, 42

[63] Liu, Y., Zhang, L. Y., Wang, J., Zhang, Y., and Wong, K.-w. Chosen-plaintext attack of an image encryption scheme based on modified permutation–

diffusion structure. *Nonlinear Dynamics 84*, 4 (2016), 2241–2250. 2, 35, 51, 61

[64] Liu, Z., Zhang, F., Wang, J., Wang, H., and Huang, J. Authentication and recovery algorithm for speech signal based on digital watermarking. *Signal Processing 123* (2016), 157–166. 61, 131

[65] Loo, C., Siah, Y., Wong, K., Jin, A., and Huang, K. *Neural Information Processing: 21st International Conference, ICONIP 2014, Kuching, Malaysia, November 3-6, 2014. Proceedings.* No. ptie. 3 in Lecture Notes in Computer Science. Springer International Publishing, 2014. 4, 38, 113

[66] Lorenz, E. N. Deterministic nonperiodic flow. *Journal of the atmospheric sciences 20*, 2 (1963), 130–141. 63

[67] Loukhaoukha, K., Chouinard, J.-Y., and Berdai, A. A secure image encryption algorithm based on rubik's cube principle. *Journal of Electrical and Computer Engineering 2012* (2012), 7. 53

[68] Luby, M. G., and Luby, M. *Pseudorandomness and cryptographic applications.* Princeton University Press, 1996. 40, 53

[69] Lv, Z., Chirivella, J., and Gagliardo, P. Bigdata oriented multimedia mobile health applications. *Journal of medical systems 40*, 5 (2016), 1–10. 109

[70] Mandal, M. K., Banik, G. D., Chattopadhyay, D., and Nandi, D. An image encryption process based on chaotic logistic map. *IETE Technical Review 29*, 5 (2012), 395–404. 50, 61

[71] Manifavas, C., Hatzivasilis, G., Fysarakis, K., and Rantos, K. Lightweight cryptography for embedded systems–a comparative analysis. In *Data Privacy Management and Autonomous Spontaneous Security.* Springer, 2014, pp. 333–349. 41, 42

[72] Mao, Y., and Chen, G. Chaos-based image encryption. *Handbook of Geometric Computing* (2005), 231–265. 50

[73] Mehmood, I., Sajjad, M., and Baik, S. W. Mobile-cloud assisted video summarization framework for efficient management of remote sensing data generated by wireless capsule sensors. *Sensors 14*, 9 (2014), 17112–17145. 108, 110

[74] Mehmood, I., Sajjad, M., and Baik, S. W. Video summarization based tele-endoscopy: a service to efficiently manage visual data generated during wireless capsule endoscopy procedure. *Journal of medical systems 38*, 9 (2014), 109. 110, 112, 113, 114, 115, 116, 128, 129

[75] Mishkovski, I., and Kocarev, L. Chaos-based public-key cryptography. In *Chaos-Based Cryptography*. Springer, 2011, pp. 27–65. 49

[76] Mitzenmacher, M., and Upfal, E. *Probability and Computing: Randomization and Probabilistic Techniques in Algorithms and Data Analysis*. Cambridge university press, 2017. 2, 36

[77] Moh'd, A., Jararweh, Y., and Tawalbeh, L. Aes-512: 512-bit advanced encryption standard algorithm design and evaluation. In *Information Assurance and Security (IAS), 2011 7th International Conference on* (2011), IEEE, pp. 292–297. 45, 49

[78] Mooney, A., Keating, J. G., and Heffernan, D. M. A detailed study of the generation of optically detectable watermarks using the logistic map. *Chaos, Solitons & Fractals 30*, 5 (2006), 1088–1097. 50, 61

[79] Mstafa, R. J., and Elleithy, K. M. A video steganography algorithm based on kanade-lucas-tomasi tracking algorithm and error correcting codes. *Multimedia Tools and Applications* (2015), 1–23. 130

[80] Muhammad, K., Ahmad, J., Farman, H., Jan, Z., Sajjad, M., and Baik, S. W. A secure method for color image steganography using gray-level modifica-

tion and multi-level encryption. *KSII Transactions on Internet and Information Systems (TIIS) 9* (2015), 1938–1962. 130

[81] Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., and Sajjad, M. Cisska-lsb: color image steganography using stego key-directed adaptive lsb substitution method. *Multimedia Tools and Applications* (2016), 1–30. 131

[82] Muhammad, K., Ahmad, J., Sajjad, M., and Baik, S. W. Visual saliency models for summarization of diagnostic hysteroscopy videos in healthcare systems. *SpringerPlus 5*, 1 (2016), 1495. 108

[83] Muhammad, K., Sajjad, M., and Baik, S. W. Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy. *Journal of Medical Systems 40*, 5 (2016), 1–16. 4, 108

[84] Nakamura, T., and Terano, A. Capsule endoscopy: past, present, and future. *Journal of Gastroenterology 43*, 2 (2008), 93–99. 4

[85] Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S. M., and Mosavi, M. R. A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia tools and applications 71*, 3 (2014), 1469–1497. 2, 103, 127

[86] Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., and Mosavi, M. R. A novel image encryption based on hash function with only two-round diffusion process. *Multimedia systems 20*, 1 (2014), 45–64. 103, 104

[87] Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., and Mosavi, M. R. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. *Multimedia Tools and Applications 74*, 3 (2015), 781–811. 104

[88] Özkaynak, F., and Yavuz, S. Security problems for a pseudorandom sequence generator based on the chen chaotic system. *Computer Physics Communications 184*, 9 (2013), 2178–2181. 5, 61, 62, 63

[89] Öztürk, İ., and Kiliç, R. A novel method for producing pseudo random numbers from differential equation-based chaotic systems. *Nonlinear Dynamics 80*, 3 (2015), 1147–1157. 53, 61, 71

[90] Pan, G., Yan, G., Qiu, X., and Cui, J. Bleeding detection in wireless capsule endoscopy based on probabilistic neural network. *Journal of medical systems 35*, 6 (2011), 1477–1484. 129, 130

[91] Pareek, N., Patidar, V., and Sud, K. Image encryption using chaotic logistic map. *Image and Vision Computing 24*, 9 (2006), 926 – 934. 2, 39, 50, 51, 53, 61

[92] Parker, M., and Dhanani, S. *Digital video processing for engineers: A foundation for embedded systems design*. Newnes, 2013. 18, 27

[93] Piva, A. Cryptography and data hiding for media security. *Multimedia Services in Intelligent Environments* (2008), 227–255. 33

[94] Plataniotis, K., and Venetsanopoulos, A. N. *Color image processing and applications*. Springer Science & Business Media, 2013. 33

[95] Pub, N. F. 197: Advanced encryption standard (aes). *Federal Information Processing Standards Publication 197* (2001), 441–0311. 2, 49

[96] Rafik Hamza, F. T., and Hewage, C. Investigation of 3d-images security based on improved image randomized encryption method. *NED University Journal of Research - An International Journal* (2018). x

[97] Rhouma, R., and Belghith, S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos. *Physics Letters A 372*, 38 (2008), 5973–5978. 81

[98] Rivest, R. L., and Sherman, A. T. *Randomized Encryption Techniques*. Springer US, Boston, MA, 1983, pp. 145–163. 2, 36, 37, 53

[99] Rudra, A., Dubey, P., Jutla, C., Kumar, V., Rao, J., and Rohatgi, P. Efficient rijndael encryption implementation with composite field arithmetic. In *Cryptographic Hardware and Embedded SystemsCHES 2001* (2001), Springer, pp. 171–184. 45

[100] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., and Barker, E. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Tech. rep., DTIC Document, 2001. 53, 70, 94

[101] Sajjad, M., Mehmood, I., and Baik, S. W. Sparse representations-based super-resolution of key-frames extracted from frames-sequences generated by a visual sensor network. *Sensors 14*, 2 (2014), 3652–3674. 110

[102] Sajjad, M., Muhammad, K., Baik, S. W., Rho, S., Jan, Z., Yeo, S.-S., and Mehmood, I. Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. *Multimedia Tools and Applications* (2016), 1–18. 4

[103] Sajjad, M., Muhammad, K., Baik, S. W., Rho, S., Jan, Z., Yeo, S.-S., and Mehmood, I. Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. *Multimedia Tools and Applications* (2016), 1–18. 108

[104] Semmlow, J. L., and Griffel, B. *Biosignal and medical image processing*. CRC press, 2014. 29

[105] Shannon, C. E. Communication theory of secrecy systems*. *Bell system technical journal 28*, 4 (1949), 656–715. 36, 43, 51, 53, 91

[106] Shannon, C. E. A mathematical theory of communication. *ACM SIGMOBILE Mobile Computing and Communications Review 5*, 1 (2001), 3–55. 126

[107] Sharif, S. O., and Mansoor, S. Performance analysis of stream and block cipher algorithms. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on* (2010), vol. 1, IEEE, pp. V1–522. 42

[108] Shujun, L., Xuanqin, M., and Yuanlong, C. Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In *International Conference on Cryptology in India* (2001), Springer, pp. 316–329. 3

[109] Stallings, W. *Cryptography and network security: principles and practices*. Pearson Education India, 2006. 42

[110] Stinson, D. R. *Cryptography: theory and practice*. CRC press, 2005. 43

[111] Sun, F., Lü, Z., and Liu, S. A new cryptosystem based on spatial chaotic system. *Optics Communications 283*, 10 (2010), 2066–2073. 100, 126, 130

[112] Tekalp, A. M. *Digital video processing*. Prentice Hall Press, 2015. 13

[113] Toriwaki, J., and Yoshida, H. *Fundamentals of three-dimensional digital image processing*. Springer Science & Business Media, 2009. 17, 18

[114] Van Tilborg, H. C. *Fundamentals of cryptology: a professional reference and interactive tutorial*, vol. 528. Springer Science & Business Media, 2006. 33

[115] Verdult, R. *The (in) security of proprietary cryptography*. Sl: sn, 2015. 42

[116] Volos, C. K., Kyprianidis, I. M., and Stouboulos, I. N. Fingerprint images encryption process based on a chaotic true random bits generator. *International Journal of Multimedia Intelligence and Security 1*, 4 (2010), 320–335. 50, 61

[117] Akhavan, A., Samsudin, A., and Akhshani, A. Cryptanalysis of an improvement over an image encryption method based on total shuffling. *Optics Communications 350* (2015), 77–82. 3, 81

[118] Wang, A., Banerjee, S., Barth, B. A., Bhat, Y. M., Chauhan, S., Gottlieb, K. T., Konda, V., Maple, J. T., Murad, F., Pfau, P. R., et al. Wireless capsule endoscopy. *Gastrointestinal endoscopy 78*, 6 (2013), 805–815. 4

[119] Wang, A., Banerjee, S., Barth, B. A., Bhat, Y. M., Chauhan, S., Gottlieb, K. T., Konda, V., Maple, J. T., Murad, F., Pfau, P. R., Pleskow, D. K., Siddiqui, U. D., Tokar, J. L., and Rodriguez, S. A. Wireless capsule endoscopy. *Gastrointestinal Endoscopy 78*, 6 (2013), 805–815. 108

[120] Wang, Q., Yu, S., Li, C., Lü, J., Fang, X., Guyeux, C., and Bahi, J. M. Theoretical design and fpga-based implementation of higher-dimensional digital chaotic systems. *IEEE Transactions on Circuits and Systems I: Regular Papers 63*, 3 (2016), 401–412. 61

[121] Wang, X., and Luan, D. A novel image encryption algorithm using chaos and reversible cellular automata. *Communications in Nonlinear Science and Numerical Simulation 18*, 11 (2013), 3075–3085. 50

[122] Wang, X., Luan, D., and Bao, X. Cryptanalysis of an image encryption algorithm using chebyshev generator. *Digital Signal Processing 25* (2014), 244–247. 2, 35, 51, 61, 81

[123] Wang, X., Teng, L., and Qin, X. A novel colour image encryption algorithm based on chaos. *Signal Processing 92*, 4 (2012), 1101–1108. 39, 102, 123

[124] Wang, X.-y., and Qin, X. A new pseudo-random number generator based on cml and chaotic iteration. *Nonlinear Dynamics 70*, 2 (2012), 1589–1592. 53, 68, 77, 78

[125] Wang, X.-Y., and Wang, X.-J. Design of chaotic pseudo-random bit generator and its applications in stream-cipher cryptography. *International Journal of Modern Physics C 19*, 05 (2008), 813–820. 40, 62

[126] Wang, X.-Y., and Yang, L. Design of pseudo-random bit generator based on chaotic maps. *International Journal of Modern Physics B 26*, 32 (2012), 1250208. 53, 62, 68, 77, 78

[127] Wang, X.-Y., Yang, L., Liu, R., and Kadir, A. A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics 62*, 3 (2010), 615–621. 98

[128] Wang, X.-Y., Zhang, Y.-Q., and Bao, X.-M. A novel chaotic image encryption scheme using dna sequence operations. *Optics and Lasers in Engineering 73* (2015), 53–61. 104

[129] Wang, Y., Wong, K.-W., Liao, X., and Xiang, T. A block cipher with dynamic s-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation 14*, 7 (2009), 3089–3099. 50, 61

[130] Wang, Y., Wong, K.-W., Liao, X., Xiang, T., and Chen, G. A chaos-based image encryption algorithm with variable control parameters. *Chaos, Solitons and Fractals 41*, 4 (2009), 1773 – 1783. 39

[131] Wong, K.-W., Kwok, B. S.-H., and Yuen, C.-H. An efficient diffusion approach for chaos-based image encryption. *Chaos, Solitons & Fractals 41*, 5 (2009), 2652–2663. 43

[132] Wu, W., and Zhang, L. Lblock: a lightweight block cipher. In *Applied Cryptography and Network Security* (2011), Springer, pp. 327–344. 42

[133] Wu, X., and Guan, Z.-H. A novel digital watermark algorithm based on chaotic maps. *Physics Letters A 365*, 5 (2007), 403–406. 50, 61

[134] Wu, Y., Noonan, J. P., and Agaian, S. Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)* (2011), 31–38. 98

[135] Wu, Y., Yang, G., Jin, H., and Noonan, J. P. Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging 21*, 1 (2012), 013014–1. 104, 118, 131

[136] Wu, Y., Zhou, Y., Noonan, J. P., and Agaian, S. Design of image cipher using latin squares. *Information Sciences 264* (2014), 317–339. 62

[137] Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J. P., and Natarajan, P. Local shannon entropy measure with statistical tests for image randomness. *Information Sciences 222* (2013), 323–342. 44, 53, 130

[138] Xing-Yuan, W., Xue, Q., and Yi-Xin, X. Pseudo-random sequences generated by a class of one-dimensional smooth map. *Chinese Physics Letters 28*, 8 (2011), 080501. 50, 53, 61

[139] Xingyuan, W., Xue, Q., and Lin, T. A novel true random number generator based on mouse movement and a one-dimensional chaotic map. *Mathematical Problems in Engineering 2012*, 931802 (2012), 9 pages. 68, 77, 78

[140] Xu, L., Li, Z., Li, J., and Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering 78* (2016), 17–25. 103, 104

[141] Yang, J.-J., Li, J., Mulder, J., Wang, Y., Chen, S., Wu, H., Wang, Q., and Pan, H. Emerging information technologies for enhanced healthcare. *Computers in Industry 69* (2015), 3–11. 109

[142] Zhang, G., and Liu, Q. A novel image encryption method based on total shuffling scheme. *Optics Communications 284*, 12 (2011), 2775–2780. 121

[143] Zhang, Q., Guo, L., and Wei, X. A novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system. *Optik-International Journal for Light and Electron Optics 124*, 18 (2013), 3596–3600. 51

[144] Zhang, Y.-Q., and Wang, X.-Y. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Information Sciences 273* (2014), 329–351. 75

[145] Zhang, Y.-Q., and Wang, X.-Y. A new image encryption algorithm based on non-adjacent coupled map lattices. *Applied Soft Computing 26* (2015), 10–20. 62, 73

[146] Zhou, Y., Bao, L., and Chen, C. P. Image encryption using a new parametric switching chaotic system. *Signal processing 93*, 11 (2013), 3039–3052. 118, 131

[147] Zhou, Y., Bao, L., and Chen, C. P. A new 1d chaotic system for image encryption. *Signal processing 97* (2014), 172–182. 118, 121, 131

[148] Zhou, Y., Hua, Z., Pun, C.-M., and Chen, C. P. Cascade chaotic system with applications. *IEEE transactions on cybernetics 45*, 9 (2015), 2001–2012. 118, 131