State of the Art of Image Ciphering: A Review

Ali Shakir Mahmood[1, 3] and Mohd Shafry Mohd Rahim[1, 2]

[1]Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia

[2]Iskandar Regional Development Authority (IRDA) Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia

[3]Department of Computer Science, Faculty of Education, Al- Mustansiriya University, Baghdad, Iraq

Abstract

The different methods for encryption and decryption in digital images have received growing attention recently. This is due to the availability of new editing software, sophisticated digital cameras, and in addition to tremendous development in communication networks including the Internet, which used by many people to send and receive various types of data including digital images, Although this use on a large scale of this network, but it remains unsafe environment because there are a lot of hackers who are trying to spy on various data sent over the Internet, for this reason has been the development of a range of ways that maintain the security of data including the digital images. In this paper, described the working process of digital color image encryption, where the different schemes are illustrated in this work. This paper highlights current issues in the image encryption approaches and all their comparative analysis.

Keyword: *Image Encryption, Traditional Algorithms, Chaotic Schemes, Transformation Schemes.*

1. Introduction

The cryptography or encryption has known since ancient times and used for secret communication in military as well as civilian sectors [1]. The first encryption processes for messaging between sectors of the military have been introduced by Pharaohs, Chinese and Arabs have used cryptography to transmit messages during wars [2], to secure messages. The most popular method was used in the antiquity Czar Julius, one of the roman emperors [3].

The advent of personal computers and the Internet has made it possible for anyone to distribute worldwide digital information easily and economically. Several applications like military image databases, confidential video conferencing, medical imaging system and online personal photograph album need dependable, fast and strong security system to store and exchange digital images [4]. In the present time there is an urgent need of science, "encryption" and linked the world via open networks, where these networks are used to transmit information electronically, either among ordinary people or between private and public organizations, by keeping the information confidential. It has made great efforts from all over the world to develop the systems or networks in which they can exchange data with out the possibility of disclosing information [5].

The primary purpose of encryption is to provide services to the people and to maintain the security of their information. There are four main objectives behind the use of cryptography which are confidentiality, data integrity, proof of identity and lack of ingratitude [6]. There is several security obstacles associated with the processing and transmission of digital images over an open network [7-8].

Images encryption is different from text encryption due to some essential characteristics like, redundancy of data, less sensitive, correlation between adjacent pixels and huge capacity of data. To overcome these challenges a many of cryptographic protocols have been appeared [9]. Several traditional encryption algorithms like Data Encryption Standard (DES), Triple Data Encryption Algorithm (TDEA), Advanced Encryption Standard (AES) and Rivest, Shamir and Adleman (RSA) have been developed [10], these schemes have some weakness in the encryption of digital images, so these not suitable for image encryption and suffer from low level efficiency when the image is large [11].

In this paper the different techniques of image encryption have been reviewed. This paper is organized as follows: section 1, general introduction of encryption and image encryption, section 2, general classification of encryption schemes, section 3, general image encryption schemes and the conclusion is written in section 4.

2. Types of Encryption Schemes

The encryption schemes can be classified into two main categories first traditional encryption schemes like Caesar and Vignere, second the modern encryption schemes like RSA and DES [12-14]. Figure - 1 illustrates the general classification of different encryption type.

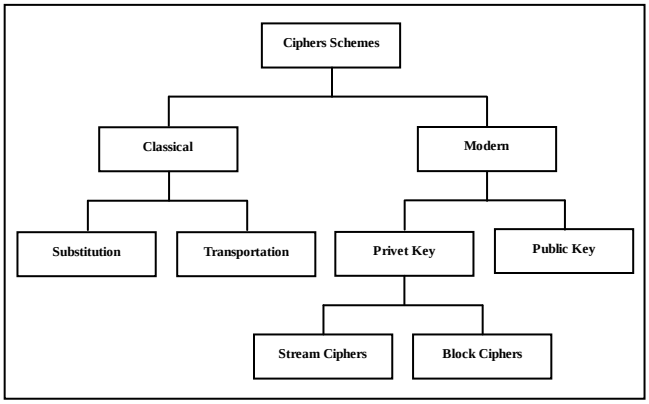

Fig.1 General Classification of Encryption Types

3. General Types of Image Encryption Schemes

Image encryption is broadly classified into three groups according to the encryption schemes used in cryptosystem, the Ordinary Algorithms, Transformations and Chaotic. The first branch is the modified traditional encryption algorithm, actually these algorithms are design for text encryption and then modified to encrypt image. In the visual transformation algorithm, the mathematical equations are used to compress image and developed equation is used in the encryption process. In the chaotic methods the image pixels are scrambled. The researchers are usually combined two or more of these encryption types to get more secure encryption system [15-18]. Figure - 2 illustrates the general image encryption types.

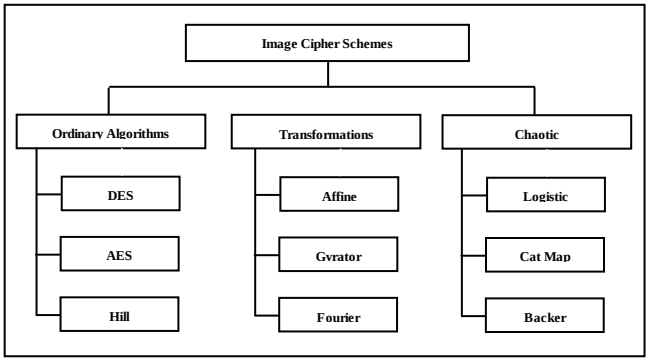

Fig.2 General Image Encryption Types

3.1 Traditional Encryption Algorithm

The traditional algorithms were designed for text data. Due to large data size and real time constrains, the traditional algorithms that are good for text data but do not suitable for multimedia data (image and video). Some of those techniques used in image encryption process are discussed in this section.

Nithin et al. have used Fast Encryption Algorithm (FEAL), also called Japanese Encryption algorithm to encrypt the image data. The encryption algorithm is almost similar to DES algorithm, but it is faster than DES. According to FEAL, the input image is split into 16x16 blocks of information to encrypt the images. Encryption/Decryption is carried out using 12 keys, each of length 16-bits [19-21].

Ismail et al. have introduced a simple Multi-Layer Perception (MLP) network for image encryption. The back-propagation algorithm is used for adjustment of the weight coefficients of the neural network. The bias between the input layer and the hidden layer works as the first key, while the bias between the hidden layer and the output layer represents a second key. The training method uses both keys. The MLP network has been tested using different images and video images [22-23].

Weyori et al. have modeled a Secured Digital Image Encryption Scheme Using a Three Set. The encryption process of image data passes through coding system which consists of an encoder and a decoder. The encoder is built by R/B converter, which requires a Residue Number System (RNS) image processor of small word length. The decoder is used to recover the encrypted bit stream according to the module set. The modified RNS to Binary conversion method does not require the computation of a multiplicative inverse and also reduces the problem of the large modulo as a compared to the conversion using in the traditional cathode ray tube (CRT) [24-25].

An improved image encryption method based on permutation diffusion architecture and total shuffling scheme has proposed by Shen et al. In the permutation process every image shuffle the position of pixels by its own P-box, where in the diffusion process, the key stream is related to the plain image directly and a more secure feedback is employed to change the number of iterations of the chaotic map. Moreover, a reverse diffusion process is added to protect the final cipher image [26].

A new approach towards the key generation for encryption algorithms, Genetic Algorithm (GA), has been introduced by Sandeep et al. to generate encryption key. A hybridized

technique called BlowGA is also proposed which is a combination of Blowfish and GA. Blowfish Algorithm is a conventional method of encryption [27-28].

Mohamed et al. have implemented and analyzed the RC5 block cipher algorithm for digital images encryption. They have also used RC5 and RC6 block cipher to digital images encryption. Bajaj et al. discussed and analyzed the weaknesses of RC5 for image encryption and made an improvement in RC5 algorithm [29-31].

Indrakanti et al. used permutation based image encryption technique contains all the three types of classifications like position permutation, value and visual transformation. The first phase is the image encryption where the image is split into blocks and these blocks are permutated. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver to decrypt the image [11].

Color image encryption has been done by Rohit et al. using novel blackjack based Scrambling Scheme Henon map is used for generating pseudo random numbers from original pixel values and also its exhibits chaotic behavior which maps image pixels into pseudorandom values. These values are shuffled and confused using blackjack based scrambling scheme using logistic map, since scrambling increases sustainability to differential attacks [32].

Rasul et al. have proposed a method for image security via genetic algorithm in which a chaotic function Logistic Map and a key extracted from the plain image are used to encrypt the image. The method is employed to produce a number of encrypted images using the plain image. These encrypted images are considered as the initial population for the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher image is chosen as the final encryption image [33].

A novel image encryption algorithm based on hash function has proposed by Seyedzade et al. The main idea of the presented work is to use one half of image data for encryption of the other half of the image reciprocally. The algorithm consists of two main sections. The first does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask for substituting pixel values using recursive cellular automata permutation based on a CBC-like mode. The mask is then XORed with the other part of the image which is going to be encrypted. This method can be applied for encryption of gray-level and color images [34-35].

Kamali et al. have used a new modified version of advanced encryption standard (AES) based algorithm for image encryption. The new method mainly focused on Shift Row Transformations, where modification is done by adjusting the Shift Row Transformation. In the Shift Row Transformation, if the value in the first row and first column is even, the first and fourth rows are unchanged and each byte in the second and third rows of the state are cyclically shifted right over different number. The first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes [36-37].

Zhu et al. have proposed ZGW-1 digital encryption algorithm based on three levels and multilayer scramble. The proposed scheme can be divided into primary, intermediate and advanced levels, with gradually increasing security. The key parameters of different levels are encrypted by Elliptic Curve Cryptography (ECC).The core parameters of different levels are encrypted by ECC. ZGW-1 algorithm adopts mature technology, possesses large enough key space and has the attribute of the time needed to decipher toward long interval time [38].

Zhou et al. have used DNA Self-Assembly Technology for image encryption. A complete design scheme of DNA self-assembly that is suitable for the image encryption with suitable properties is discussed. This algorithm still has some immature places, however it is feasible to encrypt the image and it can enhance the image information security and be implemented in DNA computer in theory [39].

A method for image encryption based on a combination of image scrambling and well known encryption and decryption algorithms has presented by Abdulsattar. The original image can be viewed as an arrangement of pixels, which are rearranged into a scrambled image using a pseudo random index generator, and then the generated image is encrypted using one of encryption algorithm [40].

Panigrahy et al. have carried out the image encryption using self-invertible key matrix of hill cipher algorithm. The generating process of self invertible key matrix can be used in Hill Block cipher algorithm. The decryption process cannot be complete if the key matrix is not invertible. This proposed method for generating self invertible matrix can also be used in other algorithms where matrix inversion is required and can be widely applied in other information security fields such as video encryption [41].

Muttoo et al. have done some, modification where rendering the image content completely scrambled using multiple self-invertible keys, block shuffling and a pel transformation [42].

Acharya et al. have used a novel advanced Hill (AdvHill) cipher algorithm to encrypt the image, where an involuntary key matrix for encryption is used. The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where may not be able to decrypt the encrypted message, if the key matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption. The proposed algorithm can encrypt gray scale as well as color images [43].

A new approach based on the combination of the image permutation and a Rijn Dael encryption algorithm has been proposed by Younes et al. to encrypt image. The transformation process is used to divide the original image into a number of blocks then shuffled their positions within the image. The new shuffled image is then fed to the Rijn Dael encryption algorithm. The process of dividing and replacing the image pixels into blocks reduce the correlation between image elements and confuse the relationship between the original image and the generated one [44].

A new method of key stream generator to the AES has proposed by Zeghid et al. to design a secure symmetric image encryption technique and to ensure improvement in the encryption performance, mainly for images characterization with reduced entropy. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms. The new scheme offers high security and can be realized easily in both hardware and software. The key stream generator has an important influence on the encryption performance [45].

Khamy et al. have proposed a new color image encryption technique utilizing fuzzy pseudo random bit generator. The pseudo random binary sequences are generated by fuzzy logic. According to these sequences each pixel color byte value is rotated as bits in right or left direction for some bits, after rotation process the pixel color is XOR by one of binary sequences [46].

Maniccam et al. proposed a new method for multimedia encryption based on the SCAN methodology. It is a formal language based on two dimensional spatial accessing methodologies which can generate a very large number of scanning paths or space filling curves. These rearrange the pixels of the image and change the pixel values. The pixel values are changed by a simple substitution mechanism which adds confusion and diffusion properties of the encryption method [47].

Chang et al. proposed encryption algorithm for image cryptosystem based on vector quantization. This method is used to design high security image cryptosystem and to reduce computational complexity of the encryption and decryption algorithm. Vector quantization transforms the image into the combination of the codebook and a set of indices, two data items need to be transmitted. There are two ways to encrypt these items; first one is directly encrypt the set of indices on the codebook by using any encryption algorithm. Where as, in the other method to encrypt the codebook, the set of indices on the codebook is transmitted in plaintext form [48].

Dang et al. proposed an image encryption for secure internet multimedia applications based on the packetization encryption and wavelet embedded zero tree coding technique. In the proposed scheme Discrete Wavelet Transform (DWT) for image compression and DES for image encryption are employed. These algorithms compress images with high compression ratio and enhance the security of transmission process [49].

3.2 Transformation Methods

The transformation obscures the statistical dependence between the plaintext and the cipher text in a sense that the possibility of key discovery is frustrated. The statistical structure of the plaintext is dissipated by spreading it out over the cipher text. Transformation is achieved by using complex substitution algorithms.

Zhou et al. introduced an image encryption scheme based on fractional Mellin transform (FrMT) and phase retrieval technique. The annular domain is chosen in advance for FrMT which is carried out in annular domain. Different annular domains can be chosen from the selected cipher text to achieve multiple image encryptions, and the annular domain of cipher text is first transformed by FrMT. With transformed result and original image, phase key is generated in the phase retrieval process [50].

Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains has proposed by Liu et al. The proposed scheme consists of two stages, image encryption using random

pixel exchanging as a scrambling method and random phase encoding in gyrator domains. Two original images are dignified as the real part and imaginary part of complex function during the first stage of the encryption process. Then, the complex function is encrypted by the two operations [51].

A color image encryption based on the affine transform and gyrator transform has proposed by Chen et al. The proposed system uses the gyrator transform and affine transform as a base to design image encryption system. An original color image is divided into red, green and blue components. A 3x3 matrix defined by a random angle is used to exchange the pixel value of RGB components of the color image. Subsequently the exchanged image is transformed by gyrator transform [52].

Rajput et al. proposed color image encryption using polarized light. This work describes a color image encryption scheme using dual polarization encoding. A color image is segregated into three primary color components and each component is encrypted using Stokes-Mueller formalism in which two independent optical plane waves are used. In most of the image encryption schemes, images are encrypted by using monochromatic light so color information is not preserved by during decryption [53].

Secure Image encryption through key hashing and wavelet transform techniques has done by Bandyo pad hyay et al. Asymmetric key for image encryption is used in this system. The hash value of the key file is generated randomly. The key hash value is expanded to match with the image dimension. To create confusion the image is encrypted into wavelet transform which is first calculated and then converted into binary string. The hash of the secret key value is finally bit XORed to create the encrypted image [54].

Color image system using double random structured phase encoding in gyrator transform domain has proposed by Abuturab et al. A color image is first segmented into three basic color red, green, and blue and each one encrypted independently into a first random phase mask placed at input plane and transmitted through a structured phase mask, and then performed gyrator transform [55].

Zhou et al. proposed novel color image encryption algorithm based on the reality preserving fractional mellin transform. The color image encryption algorithm is based on reality preserving fractional Mellin transform (RPFrMT). The encrypted data contains real values which are convenient for display, transmission and storage. The whole encryption process mainly includes three steps, namely color space rotation, RPFrMT and three dimensional scrambling. The main step of the proposed encryption scheme is employed to transform the three components of the output of color space rotation, after that realized by multiplication of permutation matrices then the encrypted image is obtained [56].

The nonlinear image encryption algorithm based on the fractional Mellin transform (FrMT) is proposed by Zhou et al. The FrMT is a nonlinear transform which helps to make the encryption system nonlinear. In accordance with the characteristics of the FrMT, different annular parts of the original image with center at the geometric center of the original image are transformed by the FrMTs of different orders. The outputs are several complex-valued images with the same sizes. The main keys of the proposed algorithm with different phases are generated in the encryption process, which are relevant to the original image [57].

The modified nonlinear image encryption algorithm (MODFrMT) is derived by transforming the image in log polar coordinates, where the MODFrFT is based on the closed form expression of the FrFT. Kaplan Yorke map is involved in the log polar transformation process [58].

The use of orthogonal polynomials based transformation for image encryption has proposed by Parthasarathy et al. to analyze the image formation system. Where a linear 2D image formation system is considered around a Cartesian coordinate separable, blurring, point spread operator in which the image results in the superposition of the point source of impulse weighted by the value of the object. The proposed encryption algorithm security lies on the secret key [59].

The encryption technique using the fractional wavelet transforms (FWT) and random phase masks (RPMs) has proposed by Vilardyet al. The digital image is first transformed with the FWT, after that the coefficients resulting from the FWT (Horizontal, vertical and diagonal) are multiplied each one by different RPMs (statistically independent) and these latest results are applied an Inverse Wavelet Transform (IWT), obtaining the encrypted digital image. The decryption technique is the same encryption technique in reverse sense [60].

Nag et al. proposed a system based on scramble the image pixels using affine transform and the transformed image is divided into (2 x 2) pixels blocks and each block is encrypted using XOR operation. The length of used key is 64-bit which is quite good for practical purposes [61].

Research and implementation of image encryption algorithm based on zigzag transformation and inner product polarization vector has carried out by Xiaolin et al. Zigzag transformation is a kind of scrambling algorithm with low time complexity and good accuracy. The inner polarization vector algorithm is a new encryption algorithm and deduced from polarization vector and decomposition of inner product of a constant based on polarization identity of Attribute Theory. Integration with Zigzag scrambling algorithm can change both positions and values of pixels. The image pixels are encrypted twice to produce final encrypted image [62].

According to the fact of achieving higher levels of security, one solution is to change image pixel values while scrambling the positions of image pixels or blocks using different techniques. Zhou et al. introduces new image encryption algorithms using a new concept "key-image" which is a binary image with the same size as the original image to be encrypted. One algorithm is called the Bit plane Crypt, which generates the key-image by extracting a binary bit plane from another new or existing image. The key image of the other algorithm, called Edge map Crypt, is an edge map obtained from a new or existing image using a specific edge detector with a specified threshold. The original image is decomposed into binary bit planes. The bit planes are encrypted by performing an XOR operation with the key-image one by one [63].

A selective encryption approach using DCT and stream cipher is proposed by Krikor et al., where the DC coefficients and some selective AC coefficients are encrypted to image. The DC coefficients carry important visual information and it's difficult to predict the selective AC coefficients. The algorithm is not encrypted bit by bit the whole image but only selective DCT coefficients are encrypted, and extra security is added to the resulted encrypted blocks by using Block Shuffling method depending on two preferred prime numbers [64].

A new approach for image encryption based on the chaotic Baker map (a chaotic map) has proposed by Naeem et al., which randomizes a unit square using 2D map. During operation, it is cut into two halves, stacked on one another, but in the different transform domains. The encryption can be performed in the spatial domain or any transform domain. Chaotic spatial domain schemes are mainly related to the positions of the pixels in the image. In the discrete wavelet transform (DWT), the image after wavelet decomposition is divided into four bands; a low frequency band LL, and three high frequency bands LH, HL and HH [65].

Joshi et al. proposed color image encryption and decryption using fractional Fourier transform .In this technique, each of the color channels (R, G, and B) are encrypted independently using double random phase encoding. For this purpose, each channel requires effectively one random phase mask in the fractional Fourier domain and four different fractional orders. Collectively this requires three different random phase masks and 12 different fractional orders for the three different color channels [66].

Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms has proposed by Chen et al. According to the proposed system, each pixel is represented by three RGB values of its color. The real color is the composition of three RGB values with certain proportions. Therefore, all image pixels can be decomposed into three color matrix. Both the optical and optoelectronic architectures are realized based on lensless Fresnel transform holograms [67].

Alexopoulos et al. presented a cryptographic scheme for encrypting 2D gray scale images by using a large family of fractals. This scheme is based on a transposition of the image elements implemented by a generator of 2D hierarchical scanning patterns producing a large subset of the possible orders defined on 2D image elements. Each pattern defines a distinct order of pixels and can be described by an expression, which is considered as the key of the transposition. This cryptographic scheme called SCAN encryption scheme for 2D image encryption, which is based on the family of SCAN patterns [68].

3.3 Chaotic Encryption Schemes

This section explains the use of chaos theory in the filed of image encryption. The chaos theory deals with systems that evolve in time to a particular kind of dynamical behavior. In general, these systems obey a certain set of laws of evolution, and so, they are deterministic. It has to be said, that chaos occurs only in some deterministic non-linear systems. Explicitly, chaos appears when there is a sustained and disorderly looking long term evaluate that satisfies certain mathematical criteria.

Zhou et al. has introduced a new parametric switching chaotic system (PSCS) by embedding three existing chaotic maps Logistic, Sine and Tent maps. The output of the Logistic map controls a switch to select either the Sine map or the Tent map as a generator to produce the output sequence [69].

A new scheme with variable control parameters, has proposed by Zhang et al., where a spatiotemporal chaotic system and time varying delay are utilized in the presented scheme. This cryptosystem is based on confusion and diffusion architecture which can make a high secure level, confusion and diffusion performance [70].

Jolfaei et al. used a Chaotic baker's map for shuffling and improving AES efficiency through S-box design (Baker's map is used to generate a permutation matrix, which is in turn used to generate S-box in the AES algorithm). Chaos is used to expand diffusion and confusion in the image. Due to sensitivity to initial conditions, chaotic baker's map has a good potential for designing dynamic permutation map and S-box [71].

Mingming et al. introduced a multiple chaotic encryption scheme for image. The encryption algorithm includes two parts, in the first part the positions of the original image pixels are permuted by using Arnold cat map, and then the values of the permuted pixels are encrypted by multiple-chaotic map as a second step, also there are a new image encryption scheme has introduced using the Ikeda map by Jia et al. A parametric discrete Ikeda map is utilized to generate random sequences. These sequences are used for shuffling the image pixels' positions and change the image pixels' values [72].

Min et al. designed and analyzed a novel chaotic image encryption. A relation between the plain image and the generated pseudo random numbers is created, which are consequently used in pixel position shuffled process and pixel value confusion process. Two chaotic maps are used to generate complicated pseudo random sequences (Henon Map and Logistic Map) to shuffle the pixel position and confuse the pixel value. At the same time, layer rotation, circle shift and pseudo random sequences are employed to diffuse and confuse image pixels [73].

A Coupled Nonlinear Chaotic Map (CNCM) and a novel chaos-based image encryption algorithm to encrypt color images have been proposed by Mazloom et al. The nonlinear chaotic algorithm uses the power function and the tangent function instead of linear function. The CNCM map uses these functions to give nonlinearity property to CNCM. In order to increase the security of the proposed algorithm, 240 bit-long secret key is used to generate the initial conditions and parameters of the chaotic map by making some algebraic transformations to the key [74].

A chaotic image encryption design using tompkins-paige algorithm has introduced by Borujeni et al. The proposed chaotic image encryption system includes two major units, chaotic pixel permutation of rows and columns simultaneously and chaotic pixel substitution unit. Two different dynamical systems, which are, logistic and tent maps, are also considered to generate a more complicated key. The logistic map is used as a pseudorandom bit generator while tent map is utilized to generate a pseudorandom image generator. Pixels of a plain image are rearranged by the permutation unit. The permutation unit uses a chaotic bit generator and Tompkins-Paige algorithm, to implement an image permutation [75].

A new approach based on improving 3D cat map has suggested by Liu et al. for secure image encryption. In the scheme, Henon map and improved two-dimensional Logistic map are combined into 3D cat map, while shuffling the positions and changing the gray values of image pixels are performed simultaneously to achieve the purpose of confusion and diffusion in cryptography [76].

In order to design an effective digital image encryption and decryption system, Dinghui et al. has used a 2D discrete Chebyshev chaotic sequence for row and column scrambling of the pixels on original image for decryption process [77].

A fast image encryption scheme based on chaotic standard map has proposed by Wong et al. The new image pixel values are obtained by (XOR). The current pixel value of the permuted image with a sequence is obtained from the logistic map taking the previous diffused pixel value as input. The diffused pixel affects the current one, a tiny change in the plain image is reflected in more than one pixel in the cipher image and so the diffusion effect is introduced in this stage. To generate the distinct substitution, diffusion keys are used in different rounds, a key generator is composed of skewed tent maps [78].

Fu et al. described an improved chaos-based image encryption scheme, in which the grayscale substitution is done by a circular bit shift method. The grayscale substitution is implemented by circular bit shift operation, which is used for deciding the shift direction [79].

An alternative chaotic image encryption based on Baker's map has proposed by Salleh et al. This enhanced symmetric key algorithm can support a variable size image as opposed to the algorithm which is mainly based on Baker's map that requires only square image for encryption, where the algorithm also includes other functions such as password binding and pixel shifting to further strengthen the security of the cipher image [80].

Scharinger introduced a new encryption system which encrypts large blocks of plaintext by repeated convoluted application of substitution and permutation operations. The introduced scheme involves key permutations on large data blocks (whole images) induced by Kolmogorov flows, which represents a class of extraordinary unstable chaotic systems where each element of the class is characterized by the parameter. By combining these highly unstable dynamics with an adaptation of a very fast shift register based pseudo-random number generator, fast encryption of image data can be achieved [81].

4. Conclusion

The rapid progress of communication networks technology, where used to exchange the various kinds of data spicily image called for the need to develop ways to keep this data secure agents unauthorized people, this filed still is an interesting research topic in image encryption.

A large variety of image encryption techniques are currently available and illustrate in this work, some of these techniques can be fairly successful in achieving the desired properties. However, these image encryption techniques are not perfect, and require more modifications to get high level of accuracy in encryption process.

Reference

1. Silberglitt, R., et al., *The global technology revolution 2020, in-depth analyses: Bio/nano/materials/information trends, drivers, barriers, and social implications*. 2002: Rand Corporation.
2. Furht, B., E. Muharemagic, and D. Socek, *Multimedia encryption and watermarking*. Vol. 1. 2005: Springer Heidelberg.
3. Bhattacharyya, D., et al., *Text steganography: a novel approach.* International Journal of Advanced Science and Technology, 2009. **3**: p. 79-86.
4. Rieback, M.R., B. Crispo, and A.S. Tanenbaum, *The evolution of RFID security*. IEEE Pervasive Computing, 2006. **5**(1): p. 62-69.
5. Abelson, H., et al., *The risks of key recovery, key escrow, and trusted third-party encryption.* 1997.
6. Pearson, S. and B. Balacheff, *Trusted computing platforms: TCPA technology in context*. 2003: Prentice Hall Professional.
7. Liepins, P., et al., *A browser based image bank, useful tool or expensive toy?* Informatics for Health and Social Care, 1998. **23**(3): p. 199-206.
8. Kuppusamy, K. and K. Thamodaran, *OPTIMIZED HYBRID SECURITY MECHANISM FOR IMAGE AUTHENTICATION AND SECRECY USING PSO.* International Journal of Network Security & Its Applications, 2013. **5**(5).
9. Grossi, M., *Homeland security technology challenges: from sensing and encrypting to mining and modeling*. 2008: Artech House.
10. Abomhara, M., O. Zakaria, and O.O. Khalifa, *An overview of video encryption techniques.* Int. J. Comput. Theory Eng, 2010. **2**(1): p. 103-110.
11. Mazloom, S. and A.M. Eftekhari-Moghadam, *Color image encryption based on coupled nonlinear chaotic map.* Chaos, Solitons & Fractals, 2009. **42**(3): p. 1745-1754.
12. Burnett, S. and S. Paine, *The RSA Security's Official Guide to Cryptography*. 2001: McGraw-Hill, Inc.
13. Dang, P.P. and P.M. Chau, *Image encryption for secure internet multimedia applications.* Consumer Electronics, IEEE Transactions on, 2000. **46**(3): p. 395-403.
14. Duggan, D. *Cryptographic types*. in *Computer Security Foundations Workshop, 2002. Proceedings. 15th IEEE*. 2002: IEEE.
15. Liao, X., S. Lai, and Q. Zhou, *A novel image encryption algorithm based on self-adaptive wave transmission.* Signal Processing, 2010. **90**(9): p. 2714-2722.
16. Bigdeli, N., Y. Farid, and K. Afshar, *A robust hybrid method for image encryption based on Hopfield neural network.* Computers & Electrical Engineering, 2012. **38**(2): p. 356-369.
17. Zhou, S., et al., *A Summarization on Image Encryption.* IETE Technical Review, 2010. **27**(6): p. 503.
18. GUPTA, K., *DIFFERENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES AND KA IMAGE CRYPTOGRAPHY.*
19. Salleh, M., S. Ibrahim, and I.F. Isnin, *Image encryption algorithm based on chaotic mapping.* Jurnal Teknologi, 2012. **39**(1): p. 1–12.
20. Dong, Y., et al. *Image encryption algorithm based on chaotic mapping*. in *Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on*. 2010: IEEE.
21. Hui-bin, L. and X. Xia, *Image Encryption Algorithm Based on Chaotic Mappings.* Computer Engineering, 2011. **24**: p. 038.
22. Maniccam, S.S. and N.G. Bourbakis, *Image and video encryption using SCAN patterns.* Pattern Recognition, 2004. **37**(4): p. 725-737.
23. Maniccam, S. and N.G. Bourbakis, *Lossless image compression and encryption using SCAN.* Pattern Recognition, 2001. **34**(6): p. 1229-1245.
24. Liu, Z., et al., *Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains.* Optics & Laser Technology, 2013. **47**: p. 152-158.
25. Liu, Z., et al., *Double image encryption by using iterative random binary encoding in gyrator domains.* Opt. Express, 2010. **18**(11): p. 12033-12043.
26. Ahmed, H.E.-d.H., H.M. Kalash, and O.S.F. Allah, *An efficient chaos-based feedback stream cipher (ECBFSC)*

for image encryption and decryption. Informatica (Slovenia), 2007. **31**(1): p. 121-129.
27. Scharinger, J., *Fast encryption of image data using chaotic Kolmogorov flows*. Journal of Electronic Imaging, 1998. **7**(2): p. 318-325.
28. Pareek, N.K., V. Patidar, and K.K. Sud, *Image encryption using chaotic logistic map*. Image and Vision Computing, 2006. **24**(9): p. 926-934.
29. Zou, J., R.K. Ward, and D. Qi. *A new digital image scrambling method based on Fibonacci numbers*. in *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*. 2004: IEEE.
30. Gao, H., et al., *A new chaotic algorithm for image encryption*. Chaos, Solitons & Fractals, 2006. **29**(2): p. 393-399.
31. Etemadi Borujeni, S. and M. Eshghi, *Chaotic image encryption design using Tompkins-Paige algorithm*. Mathematical Problems in Engineering, 2009. **2009**.
32. Li, C., et al., *Cryptanalysis of an image encryption scheme based on a compound chaotic sequence*. Image and Vision Computing, 2009. **27**(8): p. 1035-1039.
33. Salleh, M., S. Ibrahim, and I.F. Isnin. *Enhanced chaotic image encryption algorithm based on Baker's map*. in *Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on*. 2003: IEEE.
34. Liu, H., et al. *A novel image encryption algorithm based on improved 3D chaotic cat map*. in *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*. 2008: IEEE.
35. Mao, Y., G. Chen, and S. Lian, *A novel fast image encryption scheme based on 3D chaotic Baker maps*. International Journal of Bifurcation and Chaos, 2004. **14**(10): p. 3613-3624.
36. Gao, F. and X.-h. LI, *Bitmap Encryption Study Based on Chaotic Sequences [J]*. Journal of Beijing Institute of Technology, 2005. **5**: p. 018.
37. Furht, B. and D. Kirovski, *Multimedia security handbook*. Vol. 158. 2005: CRC press New York.
38. He, J., et al. *Color image cryptography using multiple one-dimensional chaotic maps and OCML*. in *Information Engineering and Electronic Commerce, 2009. IEEC'09. International Symposium on*. 2009: IEEE.
39. Zhu, G., et al. *ZGW-1 digital image encryption algorithm based on three levels and multilayer scramble*. in *Network Infrastructure and Digital Content, 2010 2nd IEEE International Conference on*. 2010: IEEE.
40. Joshi, R., S. Joshi, and H. Chaudhari. *Color Image Encryption Using Novel Blackjack Based Scrambling Scheme*. in *Computer Modeling and Simulation (EMS), 2011 Fifth UKSim European Symposium on*. 2011: IEEE.
41. Fu, C. and Z. Zhu. *A chaotic image encryption scheme based on circular bit shift method*. in *Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for*. 2008: IEEE.
42. Zhu, Z.-l., et al. *A Chaotic Image Encryption Scheme Based on Magic Cube Transformation*. in *Chaos-Fractals Theories and Applications (IWCFTA), 2011 Fourth International Workshop on*. 2011: IEEE.
43. Min, L. and H. Lu. *Design and analysis of a novel chaotic image encryption*. in *Computer Modeling and Simulation, 2010. ICCMS'10. Second International Conference on*. 2010: IEEE.
44. He, C., et al. *Scrambling Chaotic Image Encryption Algorithm Based on Contourlet*. in *Chaos-Fractals Theories and Applications (IWCFTA), 2011 Fourth International Workshop on*. 2011: IEEE.
45. Srividya, G. and P. Nandakumar. *A Triple-Key chaotic image encryption method*. in *Communications and Signal Processing (ICCSP), 2011 International Conference on*. 2011: IEEE.
46. Al Haj Hassan, H., et al. *New chaotic image encryption technique*. in *Broadband Networks and Fast Internet (RELABIRA), 2012 Symposium on*. 2012: IEEE.
47. Naeem, E.A., M. Abd Elnaby, and M.M. Hadhoud. *Chaotic image encryption in transform domains*. in *Computer Engineering & Systems, 2009. ICCES 2009. International Conference on*. 2009: IEEE.
48. Yu, C., B. Zhang, and X. Ruan. *The chaotic feature of trigonometric function and its use for image encryption*. in *Fuzzy Systems and Knowledge Discovery (FSKD), 2011 Eighth International Conference on*. 2011: IEEE.
49. Dinghui, Z., et al. *Discrete chaotic encryption and decryption of digital images*. in *Computer Science and Software Engineering, 2008 International Conference on*. 2008: IEEE.
50. Enzeng, D., et al. *A Chaotic Images Encryption Algorithm with the Key Mixing Proportion Factor*. in *Information Management, Innovation Management and Industrial Engineering, 2008. ICIII'08. International Conference on*. 2008: IEEE.
51. Zhang, Y., et al., *A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations*. Signal Processing: Image Communication, 2013. **28**(3): p. 292-300.
52. Yoon, J.W. and H. Kim, *An image encryption scheme with a pseudorandom permutation based on chaotic maps*. Communications in Nonlinear Science and Numerical Simulation, 2010. **15**(12): p. 3998-4006.
53. Zhang, Q. and X. Wei, *A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system*. Optik-International Journal for Light and Electron Optics, 2013. **124**(23): p. 6276-6281.
54. Zhou, Y., L. Bao, and C. Philip Chen, *Image encryption using a new parametric switching chaotic system*. Signal Processing, 2013.
55. Liu, H. and X. Wang, *Color image encryption based on one-time keys and robust chaotic maps*. Computers & Mathematics with Applications, 2010. **59**(10): p. 3320-3327.
56. Abd El-Latif, A.A., et al., *A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces*. Signal Processing, 2013.
57. Zhu, A., L. Li, and M. Chen. *An improved BMP image encryption algorithm based on logistic map*. in *Computer and Communication Technologies in Agriculture*

Engineering (CCTAE), 2010 International Conference On. 2010: IEEE.
58. He, X. and Q. Zhang. *Image Encryption Based on Chaotic Modulation of Wavelet Coefficients*. in *Image and Signal Processing, 2008. CISP'08. Congress on*. 2008: IEEE.
59. Lin, R., Y. Mao, and Z. Wang. *Chaotic secure image coding based on spiht*. in *Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on*. 2008: IEEE.
60. Jolfaei, A. and A. Mirghadri, *Image encryption using chaos and block cipher.* Computer and Information Science, 2010. **4**(1): p. p172.
61. Xiaolin, X. and F. Jiali. *Research and Implementation of Image Encryption Algorithm Based on Zigzag Transformation and Inner Product Polarization Vector*. in *Granular Computing (GrC), 2010 IEEE International Conference on*. 2010: IEEE.
62. Aihong, Z., L. Lian, and Z. Shuai. *Research on method of color image protective transmission based on Logistic map*. in *Computer Application and System Modeling (ICCASM), 2010 International Conference on*. 2010: IEEE.
63. Zhou, S., Q. Zhang, and X. Wei. *An image encryption algorithm based on DNA self-assembly technology*. in *Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on*. 2010: IEEE.
64. Nag, A., et al. *Image encryption using affine transform and XOR operation*. in *Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on*. 2011: IEEE.
65. Wong, K.-W., B.S.-H. Kwok, and W.-S. Law, *A fast image encryption scheme based on chaotic standard map.* Physics Letters A, 2008. **372**(15): p. 2645-2652.
66. El-Khamy, S., M. Lotfy, and A. Ali. *A new color image encryption. technique utilizing fuzzy pseudo-random bit generator*. in *Radio Science Conference, 2005. NRSC 2005. Proceedings of the Twenty-Second National*. 2005: IEEE.
67. Shen, Y., et al., *An Improved Image Encryption Method Based on Total Shuffling Scheme*, in *Advances in Computer Science and Information Engineering*. 2012, Springer. p. 643-650.
68. Fridrich, J. *Image encryption based on chaotic maps*. in *Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on*. 1997: IEEE.
69. Abuturab, M.R., *Color image security system using double random-structured phase encoding in gyrator transform domain.* Applied Optics, 2012. **51**(15): p. 3006-3016.
70. Chen, H., et al., *Color image encryption based on the affine transform and gyrator transform.* Optics and Lasers in Engineering, 2013.
71. Joshi, M. and K. Singh, *Color image encryption and decryption using fractional Fourier transform.* Optics communications, 2007. **279**(1): p. 35-42.
72. Zhou, N., Y. Wang, and J. Wu, *Image encryption algorithm based on the multi-order discrete fractional Mellin transform.* Optics communications, 2011. **284**(24): p. 5588-5597.
73. Zhou, N., Y. Wang, and L. Gong, *Novel optical image encryption scheme based on fractional Mellin transform.* Optics communications, 2011. **284**(13): p. 3234-3242.
74. Zhou, N., et al., *Image encryption scheme based on fractional Mellin transform and phase retrieval technique in fractional Fourier domain.* Optics & Laser Technology, 2013. **47**: p. 341-346.
75. Zhou, N., et al., *Novel color image encryption algorithm based on the reality preserving fractional Mellin transform.* Optics & Laser Technology, 2012. **44**(7): p. 2270-2281.
76. Bandyopadhyay, T., B. Bandyopadhyay, and B. Chatterji, *Secure Image encryption through key hashing and wavelet transform techniques.* International Journal of emerging technology and Advanced engineering, 2012. **2**: p. 26-31.
77. Chen, L. and D. Zhao, *Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms.* Optics Express, 2006. **14**(19): p. 8552-8560.
78. Vilardy, J.M., et al. *Image encryption using the fractional wavelet transform*. in *Journal of Physics: Conference Series*. 2011: IOP Publishing.
79. Krikor, L., et al., *Image encryption using DCT and stream cipher.* European Journal of Scientific Research, 2009. **32**(1): p. 47-57.
80. Alsultanny, Y.A., *Developing a High Level of Image Encryption Using Wavelet and Cipher Block Chaining (CBC).* Journal of Engineering and Applied Sciences, 2006. **1**(4): p. 316-322.
81. Nithin, N., A.M. Bongale, and G. Hegde, *Image Encryption based on FEAL Algorithm.* International Journal of Advances in Computer Science and Technology, 2013. **2**(3): p. 14-20.

Ali Shakir Mahmood received the BSc Degree in Software Engineering from Al-Rafidain University College, Baghdad, Iraq, in 2003 and the MSc Degree in Computer Science from Iraqi Commission for Computers and Informatics, Baghdad, Iraq, in 2006. Currently a PhD student at University Technology Malaysia, Johor Bahru, Malaysia.

Mohd Shafry Mohd Rahim born in 19 January 1976 Malaysia. Received the BSc in Computer Science in 1999, MSc in Computer Science in 2002 and PhD in Spatial Information System in 2008, all degrees from University Technology Malaysia, Malaysia, Currently Fellow Researcher of IRDA (Iskandar Regional Development Authority) in University Technology Malaysia. His research interest includes image processing and computer graphics, also he also editor in chief in International Journal of Interactive Digital Media, publish in more than 50 journal also he have 5 PhD and 10 MSc students.