Security and Performance Analysis of Chaos-based Image Encryption Schemes

Abdul-Gabbar. T. Al-Tamimi
Department of Computer Science
Faculty of Applied Sciences
University of Taiz, Yemen

Bushra Abduh Mohammed Aljafary
Department of Computer Science
Faculty of Applied Sciences
University of Taiz, Yemen

ABSTRACT

The widespread of images and their massive daily transmission in cyber society have created excess demand for encryption of image assets to guarantee confidentiality, integrity, and availability. Many researchers have applied chaotic encryption methods due to image cryptography's high efficiency and quality. This paper is an in-depth performance analysis and comparative study on three recent chaos-based image encryption schemes. The three schemes implement the *multiple chaotification method*, *hybrid chaotification method*, and *hyper chaotification method*, with a single-round design to improve the random behaviors. This research evaluates the schemes' strengths, weaknesses, vulnerabilities, performance, and robustness. In addition, it assesses the schemes' performance using a common analytical standard to measure their security. It also explores that choosing the appropriate chaotification method with high security and reasonable computational cost in encryption schemes is insufficient to ensure the security and efficiency of encryption schemes. However, the general structure of the scheme is an essential complement and plays a crucial role in the security and efficiency of the encryption system. Finally, this research explores that several statistical tests are insufficient metrics for security analysis measures for detecting weaknesses even though they pass all tests. Statistical tests can only provide a necessary but not sufficient condition, and cryptanalysis is the only proof of cryptographic schemes' security. These facts highlight the need for principles for designing robust chaotic ciphers.

General Terms

Cryptography, Computer Security

Keywords

Chaotic Cryptography, Chaotic maps, Fridrich's Strcture, Image encryption schemes

1. INTRODUCTION

Information security has become a key challenge for protecting secret information during transmission in practical applications in the digital age. Images must be secured since they contain sensitive information and maintain their authenticity, confidentiality, and integrity. The security of these images can be attained by employing different techniques, and one of the frequently applied techniques is encryption. It is the procedure in which an plain-image is converted into a cryptic image with the help of any encryption algorithm. Besides, the plain-image can be retrieved by applying decryption to the cipher image. There are many applications for image encryption algorithms, such as medical imaging, multimedia applications, intellectual properties, biometric images, satellite images, and military applications [40]. Hence, developing secure image encryption algorithms has become an important research issue. Image data have special features such as bulky capacity, containing much redundant information, and exhibiting high correlation among pixels. Therefore, traditional cryptographic algorithms, such as DES, IDEA, and RSA [43] can not be applied directly to an image. Also, the image occupies more memory space and bandwidth, making applying traditional encryption methods difficult and slow to process. This, in turn, affects the cost of computation and speed of the encryption algorithm, and hence traditional encryption algorithms offer less sensitivity to initial values of key or image, which results in slight resistance to the differential attacks on images. Since the 1990s, many researchers have noticed a relationship between chaos and cryptography [5]. Chaos theory has attracted the cryptography field due to its characteristics, such as deterministic nature, sensitivity to parameters and initial values, ergodicity, unpredictability, and complex structure [15, 47].

Chaotic dynamical systems are Non-Linear Dynamic Systems (NLDS). They can be used to implement the idea of confusion and diffusion developed by Shannon in 1949. NLDS are applied in digital image cryptography through chaotic maps, studied in a dynamic environment as they exhibit chaotic behavior. Chaotic maps are iterated functions that exhibit chaotic behavior. Small changes in initial conditions can produce drastic outputs [3]. In a nutshell, chaotic maps should have desirable properties, including a large phase space, high ergodicity, and great sensitivity to small changes in initial conditions and/or control parameters. Indeed, chaos-based ciphers generally use chaotic maps to combine security and relatively low complexity. These features are similar to what encryption algorithms require [15, 47]. The connection between chaos and cryptography introduced a new regime in modern information security. Therefore, several cryptographic schemes based on chaotic systems have been proposed recently [34, 7, 19, 32, 52, 26, 56]. In [34], the authors reviewed different techniques for image encryption based on chaotic maps within the period (2011-2019). Every scheme is unrivaled in its method, which may be appropriate for various applications.

Providing high security and good performance in chaotic cryptography is very important, and these mainly depend on selecting an excellent chaotic system, the algorithm's internal structure, and/or secret key. This paper analyzes three recent symmetric chaos-based image encryption schemes in the spatial domain. These schemes implemented some of the most chaotification methods recently applied in chaos-based image cryptography, such as *multiple chaotification methods*, *hybrid chaotification methods*, and *hyper chaotification methods* with a single-round [17]. Our assessment of these chaos schemes' security is based on their structure and performance by examining the adequacy of specific chaotification methods in chosen schemes. The selected schemes have almost the same structure but differ only in the chaotification methods employed. We're assessing their security to see if they're suitable for protecting image confidentiality or providing safer and more reliable performance on insecure networks. In this paper, we introduce an in-depth performance analysis and a comparative study on the three recent chaos-based image encryption schemes. We explore the most important current issues facing the quality and efficiency of chaotic cryptography using a common analytical standard by examining many experimental security analyses for the three schemes.

The remaining part of the paper is ordered as follows. Section 2 presents preliminaries. Section 3 presents brief details about chaos-based image cryptosystems. Section 4 presents an in-depth analysis of the selected schemes' efficiency and security. Finally, section 5 concludes the paper.

2. PRELIMINARIES

Several image encryption techniques based on chaotic systems were developed based on spatial and frequency domains. The term spatial domain refers to the image plane itself. Spatial domain-based techniques are those techniques that directly manipulate pixels. The various spatial domain-based techniques like Meta-heuristics, Chaotic maps, Elliptic curve, Cellular Automata, DNA and Fuzzy have been discussed in [22]. Transform-based image encryption techniques have been extensively used in image encryption. The given image is transformed from spatial to the frequency domain by using suitable transform models such as discrete cosine and sine transform, fast Fourier transform, and wavelets transform [28]. In this paper the emphasis is on the encryption category of advanced digital images focused around the *Spatial Domain-based Image Encryption schemes* due to encryption in the spatial domain is faster and cheaper to implement [45].

In general image cryptography is classified into asymmetric-key cryptosystem and symmetric-key cryptosystem [37]. Several image encryption techniques based on chaotic systems were developed based on chaotic asymmetric-key cryptosystem and symmetric-key cryptosystem. In the asymmetric-key cryptosystem, two different keys are used, i.e. first key is the private key, and the second is the public key for both encryption and decryption. The symmetric-key cryptosystem uses the same key for encryption and decryption, which is considered secret and must be securely shared between parties. Although asymmetric-key cipher uses two keys to increase security, symmetric key ciphers are typically faster and cheaper to implement. Symmetric-key cryptosystems are typically used for relatively bulk data encryption to satisfy high-speed transmission in unsecured communication. Due to the inherent image characteristics such as large size, in this paper the emphasis is on the encryption schemes of advanced digital images focused around the *symmetric key ciphers* due to their intrinsic properties such as speed transmission of bulk data.

2.1 Chaotic maps in chaos-based image cryptography

Chaos-based cryptosystems use chaotic maps in two categories which are one-dimensional (1D) and Multi-dimensional (MD) chaotic maps [31]. 1D chaotic maps are highly efficient, speedy, and simple in structure [27], but 1D chaotic maps consist of variable and limited parameters such as Gaussian, Sine, Tent, and Logistic maps [47]. Their chaotic orbits and design are simple but suffer from the problem of smaller keyspace [57], non-uniform data distribution, and weaker security [2]. With the enhancement of chaotic signals, if even small data is obtained, the orbits of chaotic maps can be evaluated, and their initial values can be identified. These limitations affect their applications in various security areas [61]. MD chaotic maps model the evolutions of at least two variables. Examples are the Henon map which has two dimensions (2D) [42], Lorenz system, which has four dimensions [8], Chen and Lee system, which has three dimensions [9], and hyperchaotic systems, which has at least four dimensions (4D) or more [49]. MD chaotic maps are more secure than 1D counterparts due to their large keyspace, highly dynamic system behavior, complex attractor, and high ergodicity [12]. However, the high computational complexity of MD chaotic maps makes them costly to implement on hardware and software [54]. As a result, identifying and selecting suitable chaotic maps or chaotification methods for the encryption process requires extensive analysis and understanding of the nature of chaos systems [4]. For that, any chaos cryptosystem's security is assessed based on chaos mapping performance or chaotification methods [20, 21].

Chaotic maps with excellent chaotic behaviors have security benefits to data encryption and the efficiency of chaos theory in cryptography is based on the implementation of chaotic maps. Therefore, one of the most important issues that should be considered in chaotic cryptography is selection of a suitable chaotic maps. Identifying and selecting the suitable chaotic maps for the encryption process involves massive analysis and understanding of the chaos systems' nature, and examining the adequacy of a specific chaotic map for an encryption architecture is a very complex problem.

Recently, many chaotic map schemes with improved properties have been proposed. Many proposed solutions improve chaos mapping performance, include more complex chaotic behavior, more comprehensive chaotic ranges, and low computational cost by producing other suitable chaotification methods such as *multiple chaotification methods* [24, 64], *hybrid chaotification methods* [41, 10] and *hyper chaotification methods* with fewer rounds [44]. These types of chaotification methods improvements fall under the elimination of the defects of one-dimensional maps and defects of multi-dimensional maps to balance the performance of these maps without degrading the security. These improvements provide a good balance of security and efficiency, making them the best candidate for designing chaos-based image algorithms.

2.2 Architectures of digital chaotic image cryptosystems

The first chaotic-based encryption algorithm was proposed by Matthews [35]. A secure encryption algorithm must possess the confusion and diffusion functions in its algorithm [48]. Confusion can be attained by obscuring the relationship between the cipher image and the secret key. In other words, as many as possible, every pixel of the cipher image should be affected by the secret key. Besides, diffusion can reduce the redundancy of the plain-image by spreading it over the cipher image. It also means that changing a pixel of plain-image will change many pixels of a cipher image. To achieve good confusion and diffusion properties, the architectures of the chaotic-based image encryption scheme can be designed based on:

—Permutation-only structure [29].

—Diffusion-only structure [63].

—Diffusion-permutation structure [53].

—Permutation-diffusion structure [13].

The first three structures are considered poor designs because it is not secure to have only the confusion phase or diffusion phase in the encryption process as they are prone to most attacks. Some previous studies based on the three structures were analyzed, and it was proven that they are poor design structures, due to their weak against differential cryptanalysis and vulnerability to attacks [58].
The *Permutation-diffusion structure* [13] is the distinctive structural design of prevailing chaos-based image cryptosystems and it has been considered the optimum design. It is also known as *Fridrich's strcture* because it was firstly proposed by Fridrich [13]. Fridrich was the first cryptographer who used a chaotic map in digital security in 1998 [13]. Since the first appearance of Fridrich's structure that is depicted in Fig. 1, the usage of permutation-diffusion structure for designing digital image cryptosystem has been receiving increasing research attention in the field of chaos-based cryptography, and it is the most typical structure that fulfills confusion and diffusion, and other researchers in their ciphers have widely used it [24, 64, 30, 44, 26, 17, 7].
Chaos-based encryption architecture consists of two phases: confusion and diffusion. The permutation-diffusion operations are performed multiple times to achieve the high security of encryption implementation. In the confusion phase, permutations of image pixels are done in secret without changing their values. The diffusion phase's goal is to change pixel values sequentially so that a slight difference in one pixel is spread across several pixels in the whole image. The confusion phase is repeated n times, where n is usually greater than 1, to decorrelate the affiliation between adjacent pixels, followed by the diffusion phase with m times. To provide an adequate level of security, the whole n round confusion and single round diffusion are repeated many times, with m usually more significant than 1.

3. DETAILS OF THE SELECTED CRYPTOSYSTEMS

This section is a detailed presentation of the three selected recent cryptosystems, namely, S. Yousif et al. scheme [64], N. Khalil et al. schemel [23], and Z. Li et al. scheme [30]. The three selected schemes are chaotic symmetric-key cryptosystems based on Fridrich's structure in the spatial domain. These schemes, in their design, implemented chaotification methods with high random behavior that provide a good balance of security and efficiency, such as *multiple chaotification* methods [24, 64], *hybrid chaotification method* [1, 23], and *hyper chaotification method* with a single-round [44], these chaotification methods are considered the most chaotification methods recently applied by many researchers in chaos-based cryptography that satisfy efficiency and security in the design of chaos-based cryptography.

3.1 S. Yousif et al. scheme

S. Yousif et al. in [64] proposed a scheme that depends mainly on Fridrich's structure with a single-round. This scheme applies one of the most chaotification methods recently used, the *"multiple chaotification method"* as a chaotification method to create massive confusion and diffusion [17]. This chaotification method overcomes the limitation of low control parameters in 1D chaotic maps [61], which in turn leads to a limited chaotic range then to small keyspace, where, if the key is poorly chosen or the keyspace is too tiny, the cryptosystem will be easily broken [61]. S. Yousif et al. scheme employs a variety of 1D maps, namely "Quadratic" and "Chebyshev" maps, and 2D chaotic maps, namely "Ikeda" and "Cross" maps. These four chaotic maps increase the key's complexity, security, and efficiency determined by brute force attacks. Where using several chaotic maps in one scheme increases the number of control parameters, leading to a large keyspace in the scheme. The scheme's encryption algorithm firstly divides the plain image into four blocks, and each block is rotated with 90° in the clockwise direction. Then, each block was encrypted by using a different map. Each map is used to shuffle the image pixel position. A diffusion process follows the confusion process to increase the security level. Finally, the four encrypted blocks are combined to get the cipher image. This image encryption scheme introduces a scheme with reasonable computational complexity without compromising the security level, especially for constrained environments and lightweight applications; the decrease in the number of rounds minimizes the computational cost, and the large keyspace resists brute-force attack. The authors tested the suggested scheme against different encryption quality measures to gauge the encryption scheme's strength; the performance results suggested that the proposed scheme shows better resistance against different attacks.

3.2 N. Khalil et al. scheme

N. Khalil et al. in [23] proposed an efficient scheme that depends mainly on Fridrich's structure with a single-round. This scheme applies one of the most chaotification methods recently used, the *"hybridization method"* or *"cascade system"* to create massive diffusion while maintaining a high level of security at a reasonable computing cost [17]. In other words, the limitations of 1D and HD chaotic maps have been solved using this kind of chaotification methods [67], which is a vital qualification for image encryption, and attackers find it difficult to predict the secret key [67].
Authors in [23] proposed a hybrid 2D composite chaotic map combined with a sine-cosine cross-chaotic map proposed in [38] for the transformation required to scramble the image as a confusion phase. Then, the hybrid chaotic map "Logistic-Tent" proposed in [55] generates a chaotic matrix required to diffuse the scrambled image as a diffusion phase to produce the final cipher image. The hybrid chaotic map "Logistic-Tent" is employed significantly to provide different chaotic properties, with far more sophisticated chaotic behaviors, parameter settings, and random output sequences. Authors indicated that their encryption system is durable and versatile, with a simple structure, simple implementation, and excellent chaotic properties that make chaotic

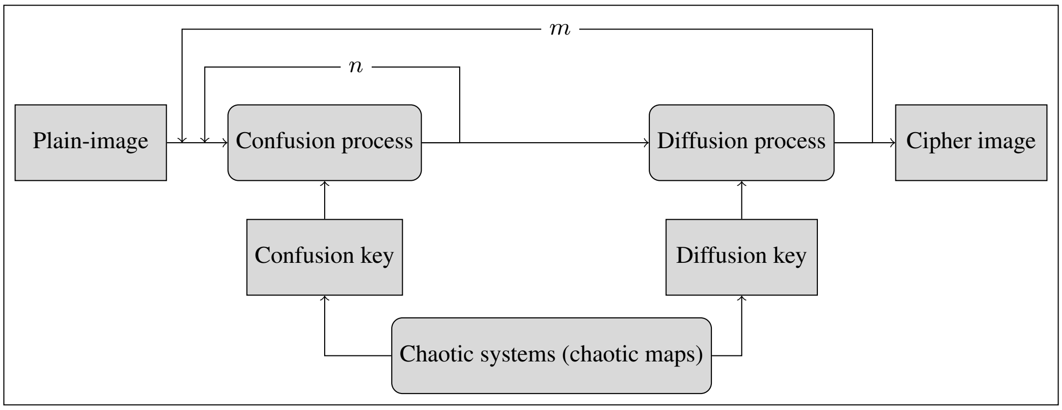


Fig. 1: Fridrich's structure.

orbits more unpredictable, which resulting in increasing the scheme's security. The simulations and analyses showed that the scheme has a promising security performance and strongly resists statistical and differential attacks, which can be expanded to other multimedia contents such as video and audio.

3.3 Z. Li et al. scheme

Z. Li et al. in [30] proposed an efficient scheme that depends mainly on Fridrich's structure with a single-round. The proposed scheme applies one of the most chaotification methods recently used, the *"hyper chaotification method"*, as a chaotification method to create massive confusion and diffusion [17]. The use of hyperchaotic systems for encrypting images will surely increase the security of a cryptosystem by introducing complex and unpredictable nonlinear behavior. However, the high computational complexity of hyperchaotic systems makes them costly to implement on hardware and software [54]. Thus, the authors decreased the computational cost of the cryptosystem by implementing image encryption with a single-round encryption. The authors declared that such a design could improve encryption efficiency while preserving a satisfactory security level.

Authors in [30] utilized a hyperchaotic Lorenz system and hash function to achieve confusion and diffusion capabilities. The permutation process presented a novel, strong plaintext-related permutation algorithm designed for a novel plain-image-related keystream generation algorithm. The plain-image and initial key information are used to construct the initial conditions of the hyperchaotic Lorenz system used in permutation and keystream generation algorithms. The encryption process strongly relates to the plain-image. The authors indicated that the scheme resists the known-plain-image and chosen-plain-image attacks. In addition, the results of many widely used security analyses and comparisons with other works showed that the proposed scheme had outstanding security performance for digital image communication.

4. EXPERIMENTAL RESULTS

This section is devoted to measuring and analyzing the security of the selected image encryption/decryption schemes mentioned in section 3. Statistical, differential, and key exhaustive search analyses are used to investigate the proposed schemes' viability and effectiveness of selected schemes. Here, the researchers would like to point out that the schemes specified in section 3 have been implemented by encrypting grayscale images only to standardize the evaluation and comparison of the security and efficiency of those algorithms. Experiments were performed using MATLAB (R2014a) and conducted on a 8-bit grayscale "Lena" image with a size of 256×256.

4.1 Statistical analysis

Encryption schemes can be broken using the statistical analysis of the ciphered image [11], and to check the robustness of the mentioned schemes in the face of statistical attacks. In this section, the histogram analysis and the correlation coefficient for the three selected schemes will be analyzed.

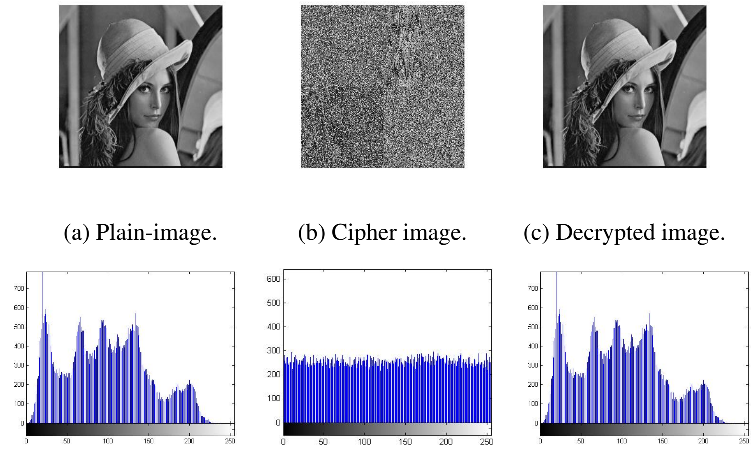
4.1.1 Histogram analysis. An image histogram is a diagram that shows the distribution of image pixels at various grey levels of intensity. Good encryption should give a flat and uniform histogram [62] to avoid statistical attacks. Figs. 2, 3 and 4 show the histograms of the plain and their cipher version from S. Yousif et al. scheme, N. Khalil et al.scheme, and Z. Li et al. scheme, respectively. It can be noticed from Figs. 2.d, 3.d and 4.d that the histograms of the plain-images contain many peaks, whereas the histograms of the cipher images in Figs. 2.e, 3.e and 4.e show a uniform scattering in the intensity of the ciphered image. Therefore, information leakage via statistical attack is challenging for attackers in the three selected schemes. As a result, the three selected schemes can effectively thwart such an assault.

4.1.2 Correlation coefficient. The adjacent pixels of plain images have a high correlation. Therefore, the cipher image should be highly de-correlated to prevent statistical attacks, and a good image encryption scheme reduces this relationship between the adjacent pixels in the cipher image. Let x and y represent gray values of two nearby pixels in an image. The correlations coefficients between x and y are calculated as follows [39]:

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \qquad (1)$$

where,

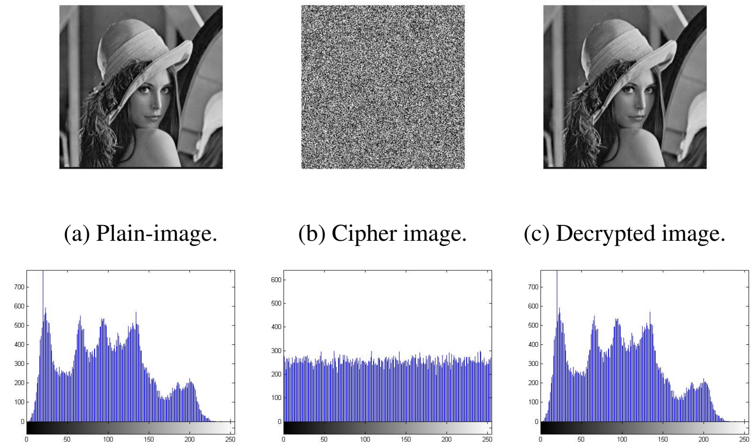
$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(y))}{K} \qquad (2)$$



(a) Plain-image. (b) Cipher image. (c) Decrypted image.

(d) Histogram of plain-image. (e) Histogram of cipher image. (f) Histogram of decrypted image.

Fig. 2: Histogram diagram of S. Yousif et al. scheme [64].



(a) Plain-image. (b) Cipher image. (c) Decrypted image.

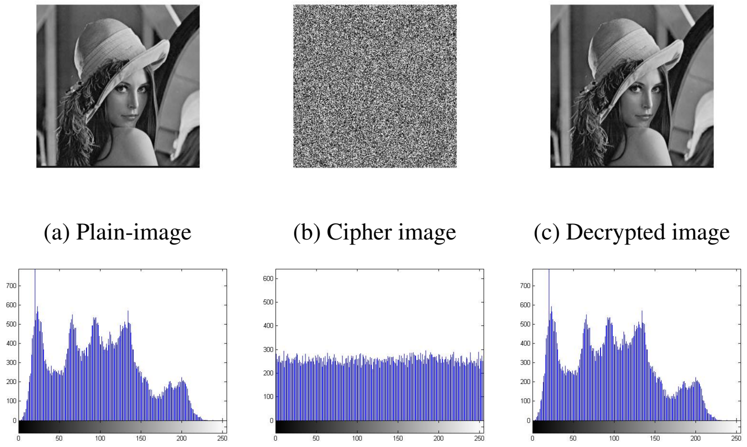
(d) Histogram of plain-image. (e) Histogram of cipher image. (f) Histogram of decrypted image.

Fig. 3: Histogram diagram of N. Khalil et al. scheme [23].

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}((x_i - E(x))^2 \tag{3}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}((y_i - E(y))^2 \tag{4}$$

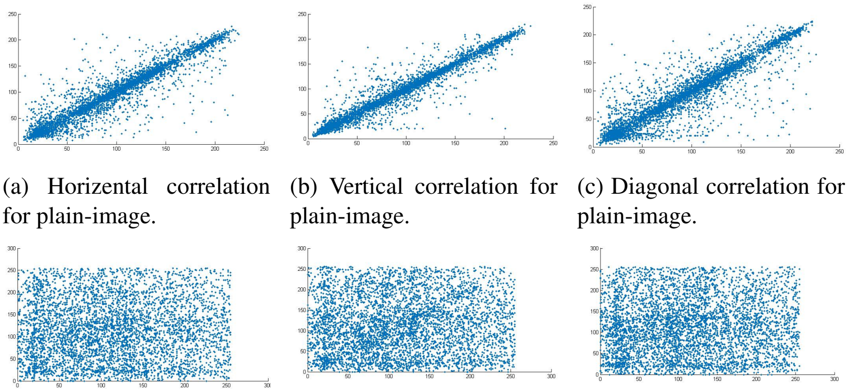
Where $C(x,y)$ is the covariance between samples x and y. K is the number of pixel pairs (x_i, y_i). $D(x)$ and $D(y)$ are the standard deviation of x and y, respectively. $E(x)$ is the mean of x_i pixel values. The range of $r_{x,y} \in [-1, 1]$. The $r_{x,y}$ value of cipher images should be near 0. We selected 5000 contiguous pixels from the plain-image and their cipher version. Then, the correlation coefficient for the plain-image and their cipher version in the three selected schemes is calculated. Tab. 1 shows the results of the correlation coefficients of the plain-image and their cipher version in horizontal, vertical, and diagonal directions for the three selected schemes. It can be noted that the values are very low for cipher images which confirms that the three selected scheme correlations are immune. The correlation coefficient plots are shown in Figs. 5, 6 and 7. It can be noted that the plots for the cipher images in the three selected schemes are uniformly distributed. They signify a good level of correlation immunity.



(a) Plain-image (b) Cipher image (c) Decrypted image

(d) Histogram ofplain-image (e) Histogram of cipher image. (f) Histogram of decrypted image.

Fig. 4: Histogram diagram of Z. Li et al. scheme [30]



(a) Horizontal correlation for plain-image. (b) Vertical correlation for plain-image. (c) Diagonal correlation for plain-image.

(d) Horizontal correlation for cipher image. (e) Vertical correlation for cipher image. (f) Diagonal correlation for cipher image.

Fig. 5: Correlation analysis of S. Yousif et al. scheme [64].

4.2 Quality of encryption

There are many measurements to measure the quality of encryption called, “Image entropy analysis (IE)”, “Mean Squared Error (MSE)”, “Peak Signal to Noise Ratio (PSNR)”, and “Signal Noise Ratio (SNR)”. Tab. 2 shows the results of the quality of the measurements between the plain and cipher images for the three selected schemes.

4.2.1 Image entropy analysis. It is an important measure to test image randomness. It contains the possible information available in the given image. Each pixel has a different value. Therefore, the entropy of a cipher image means each pixel has equal probability with uniform distribution [65]. Test of image randomness can be calculated as in Eq. 5.

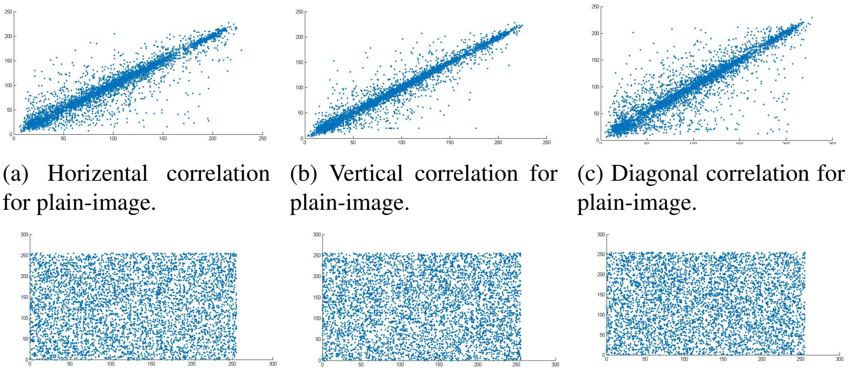
$$IE(C) = -\sum_{s=0}^{255}(P(s_i) \times \log_2 P(s_i)), \qquad (5)$$

where IE(C) represents the entropy of the message source(C). $P(s_i)$ denotes the probability of occurrence of s_i. The value of $IE \in [0, 8]$. It should be close to 8 for an 8-bit image(gray level). Tab. 2 shows the entropies of all the cipher images for the the three selected schemes are close to 8, which demonstrates that the three selected schemes produce random output images, making them resistant to entropy analysis.

4.2.2 Mean squared error (MSE)). MSE helps compare the “true” pixel values of the plain-image to the cipher image. The error is the amount by which the values of the plain-image differ from the cipher image [36]. MSE can be defined as in Eq. 6.

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[P(x, y) - E(x, y)]^2, \qquad (6)$$

where x and y are the pixel coordinates of images with the size of $M \times N$ pixels. P and E are the plain-image and cipher image,



(a) Horizontal correlation for plain-image.

(b) Vertical correlation for plain-image.

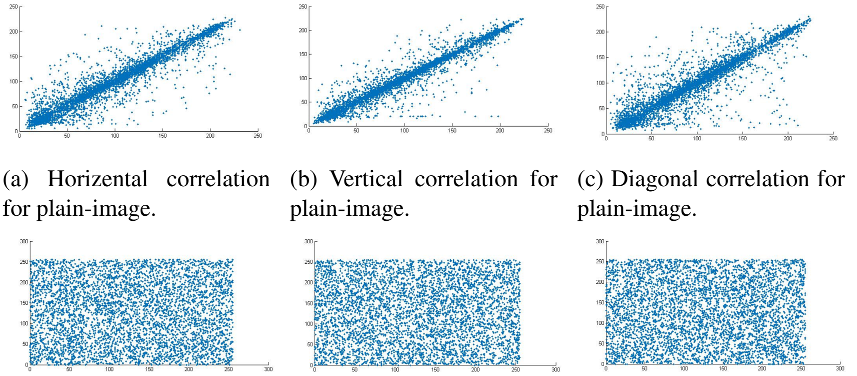
(c) Diagonal correlation for plain-image.

(d) Horizental correlation for cipher image.

(e) Vertical correlation for cipher image.

(f) Diagonal correlation for cipher image.

Fig. 6: Correlation analysis of N. Khalil et al.scheme [23].



(a) Horizontal correlation for plain-image.

(b) Vertical correlation for plain-image.

(c) Diagonal correlation for plain-image.

(d) Horizental correlation for cipher image.

(e) Vertical correlation for cipher image.

(f) Diagonal correlation for cipher image.

Fig. 7: Correlation analysis of Z. Li et al. scheme [30].

respectively. The value of the MSE $\in [0, \infty[$. The value of the MSE between the plain-image and the cipher image should be maximum. As shown in Tab. 2 all values of MSEs are high for the three selected schemes.

4.2.3 Peak signal to noise ratio (PSNR). PSNR is used to compare the quality of the plain and cipher images with the size of $M \times N$ [46]. PSNR can be mathematically computed as in Eq. 7.

$$PSNR = 10 \log_{10} \left[\frac{P_{max}^2}{MSE} \right] dB, \tag{7}$$

where P_{max} represents the maximum possible pixel value of the plain-image. For a good encryption scheme, the $PSNR$ should be as low as possible between the plain and cipher image. As shown in Tab. 2, all values of the PSNRs are low for the three selected schemes.

4.2.4 Signal to noise ratio (SNR). Signal to noise ratio (SNR) evaluates the results of an encryption algorithm quantitatively [25]. It can be computed as in Eq. 8.

$$SNR = 10 \log_{10} \left[\frac{\sum_{M,N} P(M,N)^2}{\sum_{M,N} (P(M,N) - E(M,N))^2} \right] \tag{8}$$

where $P(M, N)$ and $E(M, N)$ represent the plain-image and cipher image, respectively, with pixel coordinates M and N. The range of SNR $\in [0, \infty[$. The value of SNR should be low between the plain and cipher images. As shown in Tab. 2 all values of SNR are low for the three selected schemes.

4.3 Differential analysis

The differential attack is used to test the sensitivity of the encryption scheme toward the slightest changes in a plain-image. Attackers often make a slight change in the plain-image. Then, an encryption scheme is implemented on both images by employing the same keys. Afterward, they try to find the relationship between cipher images of plain and modified images. The relation between the plain and cipher images may be a helpful way to determine the secret keys. Two quantitative measures are put forward to analyze differential attacks, "Number of Pixel Change Rate (NPCR)" and

Table 1. : Results of the correlation coefficients.

Scheme	Horizontal		Vertical		Diagonal	
	Plain	Cipher	Plain	Cipher	Plain	Cipher
S. Yousif et al. scheme [64]	0.9433	-0.0195	0.9668	-0.0195	0.9160	0.0089
N. Khalil et al. scheme [23]	0.9432	0.0143	0.9625	-0.0091	0.9126	0.0075
Z. Li et al. scheme [30]	0.9467	-0.0179	0.9637	-0.0053	0.9204	0.0085

Table 2. : Results of the quality of measurements between the plain and cipher images.

Scheme	Plain Entropy	Cipher Entropy	MSE	PSNR	SNR
S. Yousif et al. scheme [64]	7.5534	7.9970	9.1668e+03	8.5426	3.7415
N. Khalil et al. scheme [23]	7.5534	7.9974	9.1646e+03	8.5436	1.2937
Z. Li et al. scheme [30]	7.5534	7.9969	9.1556e+03	8.5479	3.7640

“Unified Average Changing Intensity (UACI)” [14, 6]. NPCR is the percentage of different pixel numbers between two cipher images whose plain-images have only a one-pixel difference and can be computed by Eq. 9. UACI measures the average difference intensity between two cipher images, corresponding to plain-images with a one-pixel difference, and can be computed by Eq. 10. Most studies determine the values of NPCRs and UACIs are ideally 99.6 and 33.4, respectively [18].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad (9)$$

$$UACI = \frac{\sum_{i,j} \mid E(i,j) - E'(i,j) \mid}{255 \times M \times N} \times 100\% \qquad (10)$$

$$D(i,j) = \begin{cases} 0 & \text{if } E(i,j) = E'(i,j) \\ 1 & \text{if } E(i,j) \neq E'(i,j) \end{cases}$$

where M and N denote the width and height of the image, respectively. E and E' are the two cipher-images whose corresponding plain-images have one pixel difference, the gray-scale values of the pixels at point (i,j) of E and E' are denoted as $E(i,j)$ and $E'(i,j)$, respectively; $D(i,j)$ is determined by $E(i,j)$ and $E'(i,j)$.

Table 3. : Measurements sensitivity toward the slightest changes in the plain-image.

Scheme	NPCR(%)	UACI(%)
S. Yousif et al. scheme [64]	0.0015	0.0010
N. Khalil et al. scheme [23]	0.0015	0.0010
Z. Li et al. scheme [30]	99.6170	33.6286

As seen from Tab. 3, NPCR and UACI values for the S. Yousif et al. scheme [64] and N. Khalil et al. scheme [23] are not near their optimum values, they are at their minimal values. This means these schemes have low sensitivity to the change in plain-image due to linear transformations as XOR operations are implemented in the diffusion process without a cumulative manner; this violates the design rules of nonlinearity of cryptography. Thus, the S. Yousif et al. scheme and N. Khalil et al. scheme are vulnerable to differential attacks. While the Z. Li et al. scheme [30] has a high sensitivity to change in the plain-image better than the previous two schemes because of the cumulative diffusion process using XOR operation and plain-image related to the encryption process. Z. Li et al. scheme is close to the ideal values for NPCR and UACI. Thus it is not vulnerable to differential attacks.

4.4 Key analysis

Secure keys are the core of any encryption scheme whose strength depends on them. The secret keys should be able to withstand any form of attack. Desirable properties of vital secret keys are large keyspace and high sensitivity [16]. The keyspace depends on the size of the secret key. If the size is large, it is harder for an attacker to estimate the same key. On the other hand, key sensitivity indicates that even if the attacker changes a single pixel in the original key, the plain-image is unrecoverable.

4.4.1 Key space analysis. Keyspace is the total number of combinations of keys used in the encryption operation [51]. A good encryption scheme should possess considerable keyspace to possess enough security to resist brute-force attacks. The keyspace size should be greater than 2^{100} [33].
In S. Yousif et al. scheme [64] Keyspace is the total initial conditions, and the control parameters of the four chaotic maps used in the scheme are nine real values. The precision of calculation for the three schemes is (10^{-14}). Hence, keyspace in S. Yousif et al. scheme is $(10^{(14)})^9$. In N. Khalil et al. scheme [23] the total keyspace can be counted roughly as $10^{79} \approx 2^{262}$. In Z. Li et al. scheme [30] the substitution sequence and the key sequence is generated by the hyperchaotic Lorenz system. The chaotic initial conditions generation method is not only related to the initial key but also associated with pixels values of the plain-image. There are 8 initial values, and the changing step of each initial condition is 10^{-14}, therefore, the total keyspace is calculated as $S = (2.56 \times 10^{64})^2 \approx 2^{428}$. Tab. 4 shows the keyspace comparison of the three selected schemes. It indicates that the three selected schemes have large keyspace, making brute-force attacks infeasible.

Table 4. : Keyspace for the three selected schemes.

Scheme	Keyspace
S. Yousif et al. scheme [64]	2^{419}
N. Khalil et al. scheme [23]	2^{262}
Z. Li et al. scheme [30]	2^{428}

4.4.2 Key sensitivity analysis. The key sensitivity is an indicator to show the diffusion property of the scheme. Key sensitivity analysis guarantees that no information can be uncovered about a plain-image if there is a tenuous modification in the secret keys. This implies that a minor variation in the encryption and/or decryption keys should yield a large deformity in the cipher and plain- images [60]. We implement the key sensitivity analysis by employing slightly modified keys to encrypt the same input image in the three selected schemes. Figs. 8.c, 9.c and 10.c show the decrypted image for plain-image with slightly modified keys. The decrypted images cannot be recognized, indicating that the three selected schemes' secret keys are susceptible. Therefore, the encryption process of the three selected schemes is very sensitive to the small alteration in keys, and the attacker cannot obtain the plain-image without knowing the original secret key. It can be proved that the immunity of the three selected schemes to attacks on the key by observing the difference between the plain-image and the wrong decrypted image in terms of the UACI, NPCR, MSE, and PSNR, as shown in Tab. 5. The UACIs and NPCRs values are extremely large and near their ideal or critical values, which indicates that the difference between plain and decrypted images is more than 99%. Moreover, we evaluate the difference between two cipher images by encrypting the same plain-image using two keys with a tiny difference. When two cipher images significantly differ, the image cryptosystem would have a robust key sensitivity. The correlation between the original cipher image and the wrong cipher images is tabulated in Tab. 5. The UACIs and NPCRs values in each case of Tab. 5 are large, demonstrating that the cipher images are highly different.

4.5 Immunity to attacks analysis

This subsection explains immunity of the selected schemes to specific kinds of significant attacks such as Occlusion attacks, Noise attacks, and Chosen plain-image and Known plain-image attacks.

4.5.1 Immunity to occlusion attacks analysis. Occlusion is the first attack on the images, which greatly affects the decrypted image at the recipient [50]. Different sized blocks are removed from the cipher image by the three selected schemes. For testing their robustness against occlusion attack, the data loss or cutting in our experiment is performed at different positions at the ratio of 30 rows from the cipher image, 30 columns from the cipher image, $1/4$ the cipher image, and $1/2$ the cipher image, and the cut cipher image is utilized for decryption, as exemplified in Figs. 11.a-11.c, 12.a-12.c, 13.a-13.c, and 14.a-14.c. Then, these attacked images are decrypted to obtain plain-images as represented Figs. 11.d-11.f, 12.d-12.f, 13.d-13.f, and 14.d-14.f. As shown in Figs. 11, 12, 13 and 14, the N. Khalil et al. scheme [23] and Z. Li et al. scheme [30] have good resistance against the Occlusion attacks even when the data loss ratio is $1/2$; the main content of the image is still viewable. However, the S. Yousif et al. scheme [64] cannot recover the image if the size of the occlusion increases to $1/4$ or $1/2$. Inaddition, the relation between the occlusion size and the quality of the decrypted image is monotonically decreasing. It means that if the occlusion size increased, the quality of the decrypted image decreased.

4.5.2 Immunity to noise attacks analysis. Noise is the most influential attack on cipher images. Examples of these noises are Salt and Pepper, Poisson, and Gaussian noises which severely affect the security of digital images [66]. If the information of a cipher image is distorted by noise, then retrieving the decrypted image is notably tricky. In our experiments, "Gaussian" and "Salt and Pepper" noises are added to the cipher image with various densities to analyze the three selected schemes' capability to resist the noise attacks. The decrypted noisy results shown in Figs. 15, 16 and 17. Furthermore, Tab. 6 shows the MSEs, PSNRs, and correlations(r) values between the reconstructed and plain-images. These results show that the visual quality of the noisy decrypted images gradually increases as the noise intensity in the encrypted image decreases. The results show that the three selected schemes can keep the basic information in the recovered image distinguishable in several kinds of noise with different intensities.

4.5.3 Immunity to chosen plain-image and known plain-image attacks. Chosen plain-image (CPA) and known-plain-image (KPA) attacks are serious attacks in cryptography. Usually, the opponent in these attacks chooses a special plain-image, for instance, a white image or black image, to attack the image security schemes by eliminating confusion and diffusion functions to obtain the secret keys [55, 68]. Those two attacks are applied on a black and white input images to the three selected schemes for testing their robustness against CPA and KPA attacks, as shown in Figs. 18.a, 18.d, 19.a, 19.d, 20.a, and 20.d. Additionally, the corresponding encrypted versions with their histograms are illustrated in Figs. 18.b, 18.e, 18.c, 18.f, 19.b, 19.e, 19.c, 19.f, 20.b, 20.e, 20.c and 20.f respectively. In addition, Table.7 is used to present the entropy, MSEs, PSNRs, UACIs, NPCRs, and correlation coefficients scores for the cipher black and white images. It can be noticed from Figs. 18, 19 and 20 and Tab. 7 the obtained cipher images are noisy, and the distributions of their histograms are reasonably uniform. The metric values in Tab. 7 prove that the three selected schemes can successfully resist these two attacks.

4.6 Performance analysis

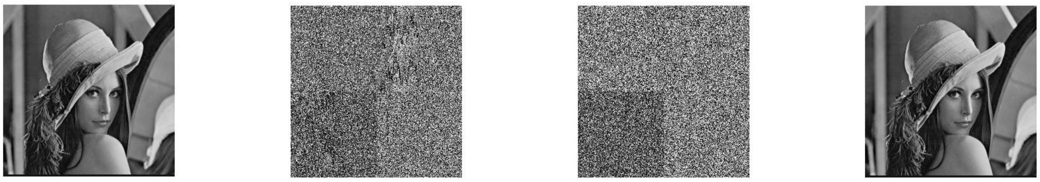
Measuring speed depends on many factors, such as the number of rounds of encryption processes, type of operations, and computer performance. As mentioned in section 4, the schemes are implemented in MATLAB R2014a. Our tests were worked on a Pc with Intel(R) Core i3, CPU 2.60 GHz, and 4GB memory, and the software running system is Windows 10 Pro. Tab. 8 shows simulation results for the encryption time and the decryption time for the test image.

Table 8. : Simulation results for the encrytion time and the decryption time for the three selected schemes.

Scheme	Encryption Time	Decryption Time
S. Yousif et al. scheme [64]	0.3215	0.2167
N. Khalil et al. scheme [23]	1.7866	0.0178
Z. Li et al. scheme [30]	3.2277	0.8524

4.7 Discussion

It can be noticed from the experimental analysis subsections 4.1- 4.6, all schemes fulfill most of the security requirements, and each of the three selected schemes has strengths and weaknesses from the other scheme. This section compares the three selected schemes and identifies strengths and weaknesses in each of the three schemes. Tab. 9 shows each scheme's strengths and weaknesses.



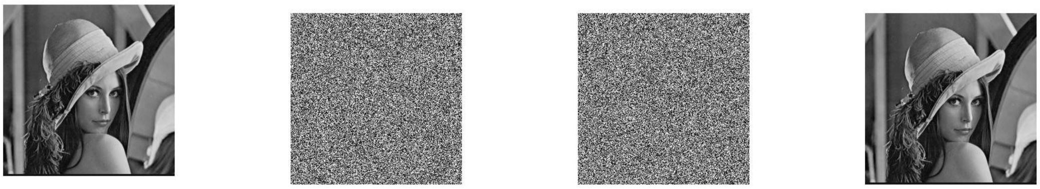
(a) Plain-image.

(b) Cipher image by the original key.

(c) Decrypted image by the modified key.

(d) Decrypted image by the original key.

Fig. 8: Key sensitivity analysis in encryption process for S. Yousif et al. scheme [64].



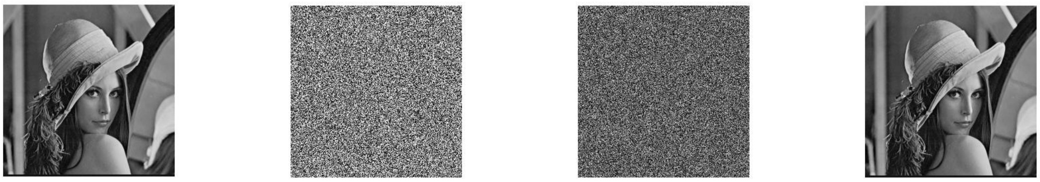
(a) Plain-image.

(b) Cipher image by the original key.

(c) Decrypted image by the modified key.

(d) Decrypted image by the original key.

Fig. 9: Key sensitivity analysis in encryption process for N. Khalil et al. scheme [23].



(a) Plain-image.

(b) Cipher image by the original key.

(c) Decrypted image by the modified key.

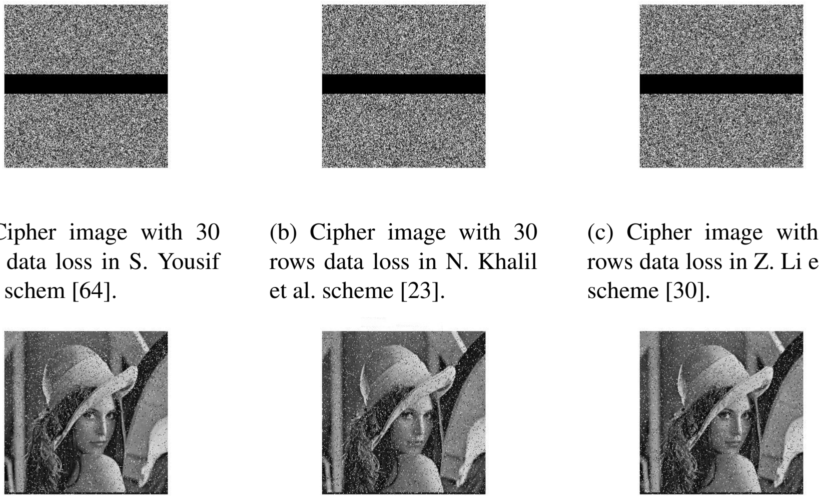
(d) Decrypted image by the original key.

Fig. 10: Key sensitivity analysis in encryption process for Z. Li et al. scheme [30].

Table 5. : Measurements of sensitivity toward the slightest changes in encryption keys for decryption processes.

Scheme	NPCR(%)	UACI(%)	MSE	PSNR
S. Yousif et al. scheme [64]	99.4598	29.0312	8.2818e+03	8.9835
N. Khalil et al. scheme [23]	99.6368	30.7588	9.1503e+03	8.5504
Z. Li et al. scheme [30]	99.6460	30.8170	9.1580e+03	8.5468

From subsections 4.1- 4.6, the three selected schemes passed all the statistical tests except for two tests where NPCR and UACI in the S. Yousif et al. scheme and the N. Khalil et al. scheme did not pass due to these schemes' insensitivity to changes in plain-image, poor diffusion mechanism due to linear transformations implemented in the encryption process, such as XORing operation only, and the low number of rounds of encryption processes that contributed by reducing the effect of avalanche effects resulting in weak resistance differential attacks. Although they passed statistical tests with each scheme has slightly higher or lower scores than the other in some statistical tests, it does not mean that this scheme is more secure than the other because their test scores are not statistically different. For example, in Tab. 2, N. Khalil et al. scheme [23] gives a relatively high encryption quality better than S. Yousif et al. scheme [64] and Z. Li et al. scheme [30] by simply comparing test scores. However, test results of S. Yousif et al. scheme [64] and Z. Li et al. scheme [30] show that they do not have a significant difference. This implies that both schemes



(a) Cipher image with 30 rows data loss in S. Yousif et al. schem [64].

(b) Cipher image with 30 rows data loss in N. Khalil et al. scheme [23].

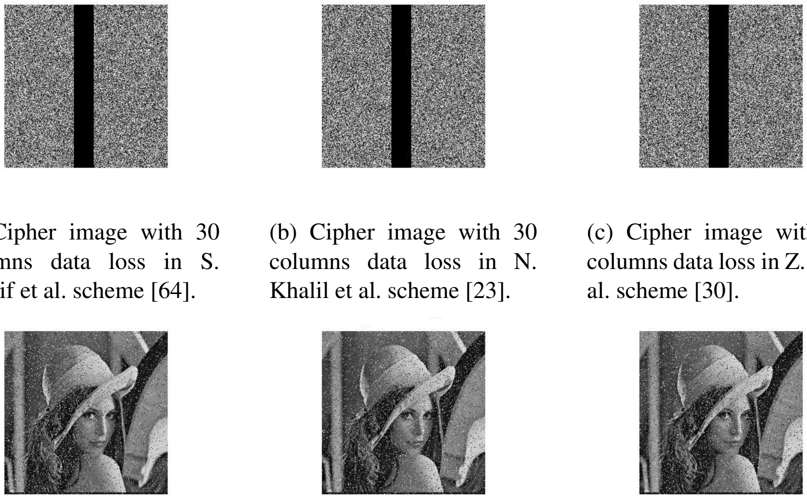
(c) Cipher image with 30 rows data loss in Z. Li et al. scheme [30].

(d) Restored image of (a).

(e) Restored image of (b).

(f) Restored image of (c)

Fig. 11: Results of data loss 30 rows (robustness against Occlusion attack) for the three selected schemes.



(a) Cipher image with 30 columns data loss in S. Yousif et al. scheme [64].

(b) Cipher image with 30 columns data loss in N. Khalil et al. scheme [23].

(c) Cipher image with 30 columns data loss in Z. Li et al. scheme [30].

(d) Restored image of (a).

(e) Restored image of (b).

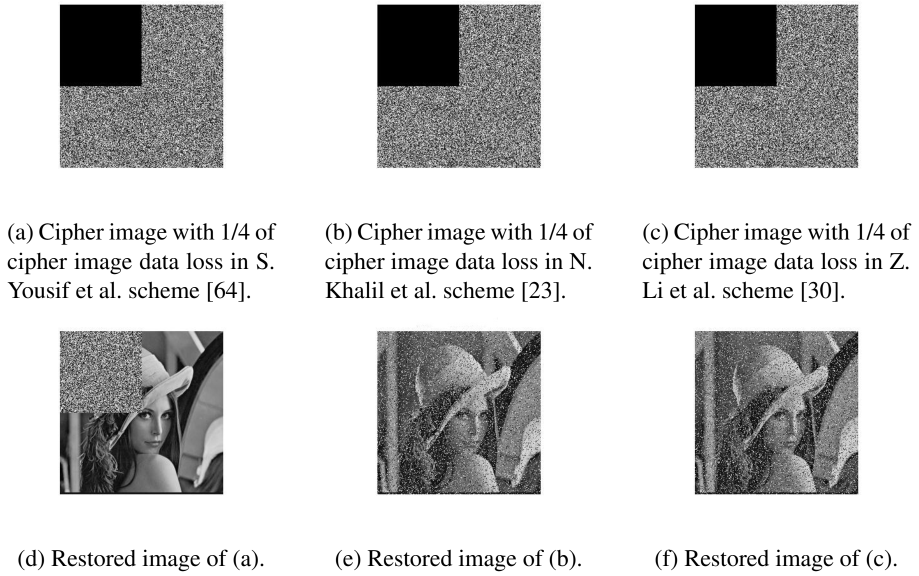
(f) Restored image of (c).

Fig. 12: Results of data loss 30 columns (robustness against Occlusion attacks) for the three selected schemes.

can generate random-like cipher-image. On the other hand, judging two encryption schemes quantifiable by comparing their test scores is also questionable [59]. Even in case experiments demonstrate that a cipher passes some security tests, several schemes have been broken through attacks that exploit inherent weaknesses of the encryption algorithms, which did not manifest themselves in the statistical properties of the ciphertexts. But, focusing on different cryptanalysis techniques can help identification of the strengths and weaknesses in the encryption techniques more than statistical tests, and this leads to the development of secure encryption algorithms to suit different process scenarios and the ability to judge encryption schemes to determine whether or not a method is good and how good it is. Tab. 9 shows the strengths and weaknesses of the three selected schemes.

5. COCLUSIONS

This paper is an in-depth performance analysis and a comparative study on three recent chaos-based image encryption schemes, through which we explore the most important current issues facing the quality and efficiency of chaotic cryptography. The three selected schemes apply the essential chaotification methods



(a) Cipher image with 1/4 of cipher image data loss in S. Yousif et al. scheme [64].

(b) Cipher image with 1/4 of cipher image data loss in N. Khalil et al. scheme [23].

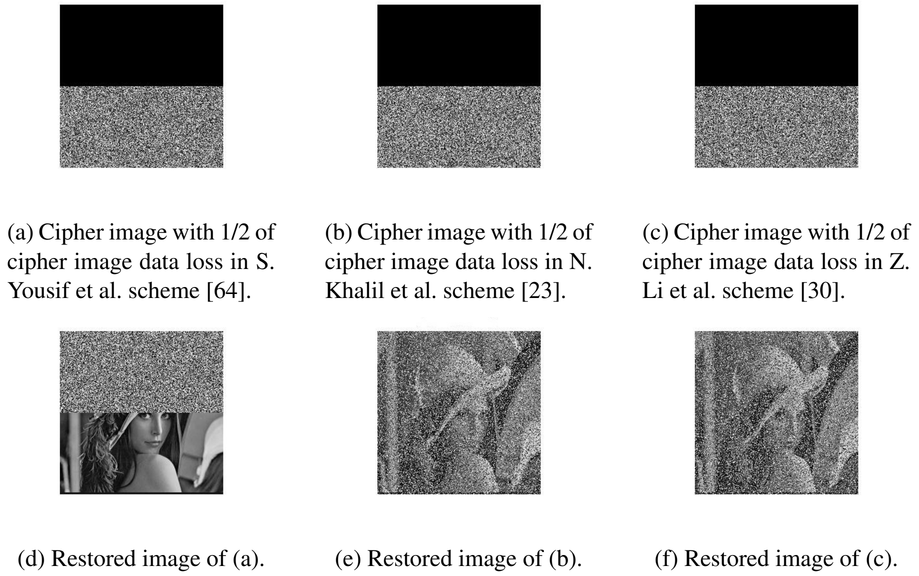
(c) Cipher image with 1/4 of cipher image data loss in Z. Li et al. scheme [30].

(d) Restored image of (a).

(e) Restored image of (b).

(f) Restored image of (c).

Fig. 13: Results of data loss 1/4 of cipher image (robustness against Occlusion attacks) for the three selected schemes.



(a) Cipher image with 1/2 of cipher image data loss in S. Yousif et al. scheme [64].

(b) Cipher image with 1/2 of cipher image data loss in N. Khalil et al. scheme [23].

(c) Cipher image with 1/2 of cipher image data loss in Z. Li et al. scheme [30].

(d) Restored image of (a).

(e) Restored image of (b).

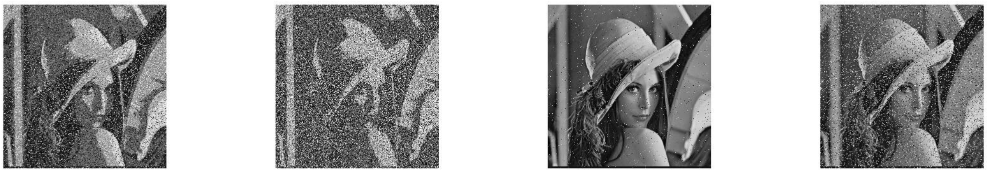
(f) Restored image of (c).

Fig. 14: Results of data loss 1/2 of cipher image (robustness against Occlusion attacks) for the three selected schemes.

that achieve high security and efficiency in the design of encryption algorithms, namely the *hyper chaotification method*, the *multiple chaotification method* and the *hybrid chaotification method*. Security analysis of the selected schemes shows that although they have some strengths, they suffer from weakness in implementation and security, fragile diffusion, reduced effect of avalanche, non-dependency of confusion and diffusion on the plain-image which all make them vulnerable to attacks. Choosing the appropriate chaotic maps with high security and reasonable computational cost in encryption schemes is insufficient to ensure the security and efficiency of these encryption schemes but besides the design structure of the scheme which plays a great role in its security. Developing a new image cryptosystem, with a good design structure, based on cryptanalysis techniques is our future work.

Table 6. : Results of the MSEs, PSNRs, and correlations between restored and plain-images under “Gaussian”, and “Salt and Pepper” noises attacks.

Gaussian noise				
Scheme	Noise density	MSE	PSNR	$r_{X,Y}$
S. Yousif et al. scheme [64]	0.02	2.4313e+03	14.3063	0.6615
	0.2	4.9912e+03	11.1827	0.3917
N. Khalil et al. scheme [23]	0.02	2.4465e+03	14.2794	0.6606
	0.2	4.9465e+03	11.2218	0.3939
Z. Li et al. scheme [30]	0.02	3.8040e+03	12.3624	0.5095
	0.2	6.6889e+03	9.9113	0.2364
Salt and pepper noise				
Scheme	Noise density	MSE	PSNR	$r_{x,y}$
S. Yousif et al. scheme [64]	0.02	183.1087	25.5377	0.9677
	0.2	1.7765e+03	15.6691	0.7244
N. Khalil et al. scheme [23]	0.02	184.8203	25.4973	0.9674
	0.2	1.8066e+03	15.5962	0.7211
Z. Li et al. scheme [30]	0.02	354.4449	22.6693	0.9383
	0.2	3.3076e+03	12.9697	0.5347



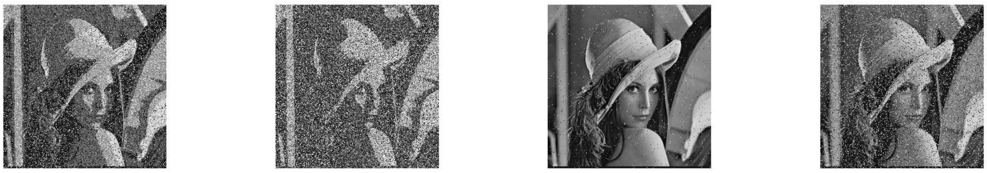
(a) Restored image withe “Gaussian” noise=0.02.

(b) Restored image withe “Gaussian” noise=0.2.

(c) Restored image withe “Salt and Papper” noise=0.02.

(d) Restored image withe “Salt and Papper” noise=0.2.

Fig. 15: Restored images under “Gaussian” and “Salt and Pepper” noises attacks of different levels by S. Yousif et al. scheme [64].



(a) Restored image withe “ Gaussian” noise=0.02.

(b) Restored image withe “Gaussian” noise=0.2.

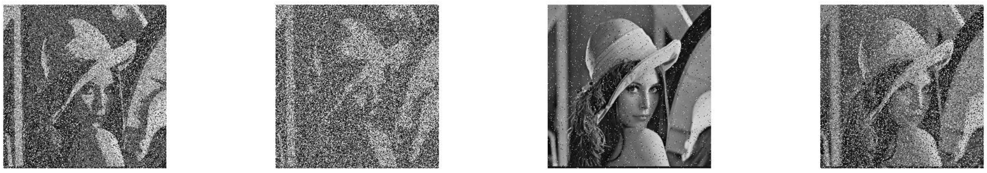
(c) Restored image withe “Salt and Papper” noise=0.02.

(d) Restored image withe “Salt and Papper” noise=0.2.

Fig. 16: Restored images under “Gaussian” and “Salt and Pepper” noises attacks of different levels by by N. Khalil et al. scheme [23].

Table 7. : Results of the quality metrics for cipher black and white images.

Scheme	Image	Entropy	PSNRs	MSE	NPCR	UACI	Correlation coefficient		
							H	V	D
S. Yousif et al. [64]	Black	7.9960	4.7791	2.1805e+04	99.8077	50.1576	-0.0213	-0.0070	-0.0298
	White	7.9960	4.7791	2.1805e+04	99.8077	50.1576	0.0101	0.0143	-0.0041
N. Khalil et al. [23]	Black	7.9960	4.7651	2.1876e+04	99.8093	50.2470	0.0045	0.0008	-0.0010
	White	7.9960	4.7651	2.1876e+04	99.8093	50.2470	-0.0045	-0.0017	0.0049
Z. Li et al. [30]	Black	7.9970	4.8124	2.1639e+04	99.5636	49.8608	-0.0183	-0.0166	0.0155
	White	7.9973	4.7872	2.1765e+04	99.6140	50.0892	-0.0104	0.0234	-0.0130



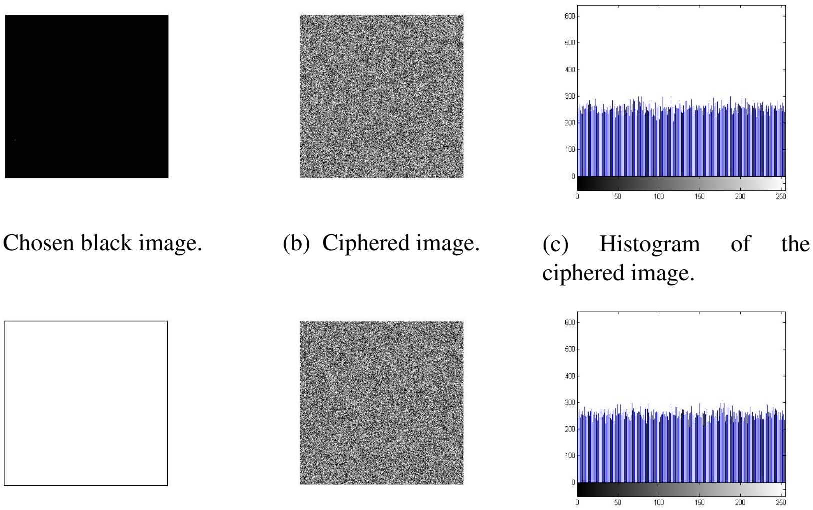
(a) Restored image withe “Gaussian” noise=0.02.

(b) Decrypted image withe “Gaussian” noise=0.2.

(c) Restored image withe “Salt and Papper” noise=0.02.

(d) Restored image withe “Salt and Papper” noise=0.2.

Fig. 17: Restored images under “Gaussian” and “Salt and Pepper” noises attacks of different levels by Z. Li et al. scheme [30].



(a) Chosen black image.

(b) Ciphered image.

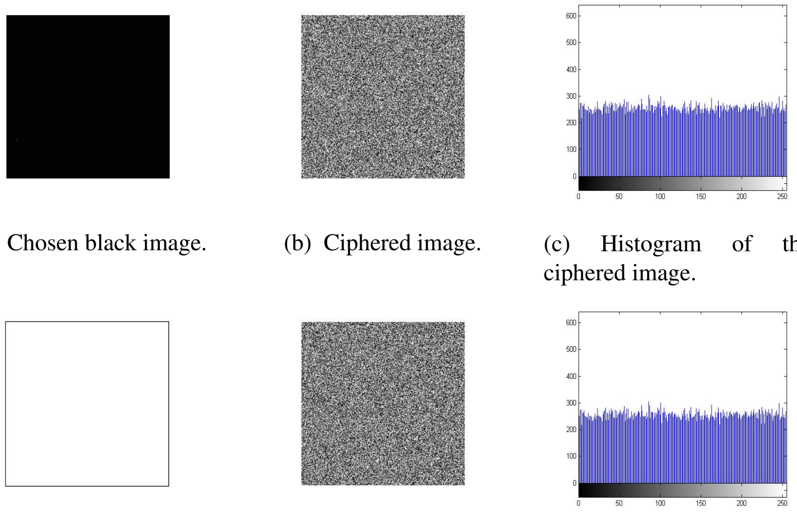
(c) Histogram of the ciphered image.

(d) Chosen white image.

(e) Ciphered image.

(f) Histogram of the ciphered image.

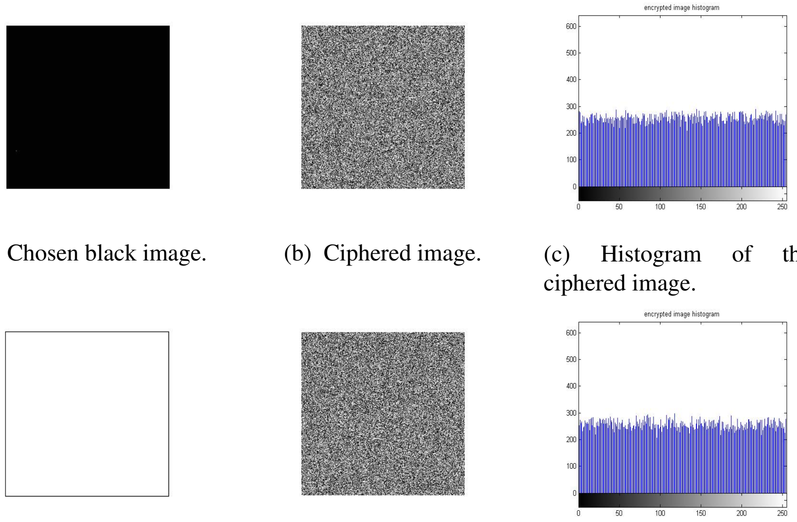
Fig. 18: Results of Chosen/Known plain-image attacks of S. Yousif et al. scheme [64].



(a) Chosen black image. (b) Ciphered image. (c) Histogram of the ciphered image.

(d) Chosen white image. (e) Ciphered image. (f) Histogram of the ciphered image.

Fig. 19: Results of Chosen/Known plain-image attacks of N. khalil et al scheme [23].



(a) Chosen black image. (b) Ciphered image. (c) Histogram of the ciphered image.

(d) Chosen white image. (e) Cipher white imag.e (f) Histogram of the ciphered image.

Fig. 20: Results of Chosen/Known plain-image attacks of Z. Li et al. scheme [30].

Table 9. : Strengths and weaknesses in the three selected schemes.

Scheme	Strengths	Weaknesses
S. Yousif et al. scheme [64]	(1) Simple maps implementation. (2) Large keyspace. (3) Encryption & decryption execution time is less than the N. Khalil et al. scheme [23] and the Z. Li et al. scheme [30]. (4) Better noise attacks resistance than Z. Li et al. scheme [30] and very close to the N. Khalil et al. scheme [23] noise attacks resistance. (5) Good sensitivity in key stream generation.	(1) Weak design structure. (2) Key streams of the algorithm generated by a chaotic system are independent of the plain-image. Therefore, it cannot withstand the differential attacks. (3) Insensitivity to changes in plain-image, poor diffusion mechanism, and the low number of rounds of encryption processes resulted in weak resistance to differential attacks. (4) Don't resistance to Occlusion attacks if it is large in size of cipher image. (5) Unchanged key stream, identical elements will be produced for multiple plain-images in case that the secret key remains unchanged.
N. Khalil et al. [23]	(1) Simple chaotic maps implementation than the Z. Li et al scheme [30]. (2) Gives a relatively high encryption quality better than the S. Yousif et al. scheme [64] and the Z. Li et al scheme [30]. (3) Better noise attacks resistance than the Z. Li et al. scheme [30] and very close to the S. Yousif et al. scheme [64]. (4) Better chosen/known plain-image attacks resistance than the Z. Li et al. scheme [30] and very close to the N. Khalil et al. scheme [23]. (5) Better resist against Occlusion attacks than the Z. Li et al. scheme [30] and the S. Yousif et al. scheme [64]. (6) Good sensitivity in key stream generation.	(1) Weak design structure. (2) Relatively complex chaotic maps implementation led to a high execution time and hardware implementation difficulty than the S. Yousif et al. scheme [64]. (3) Key streams of the algorithm generated by a chaotic system are independent of the plain-image. Therefore, it cannot withstand the differential attacks. (4) Insensitivity to changes in plain-image, poor diffusion mechanism, and the low number of rounds of encryption processes resulted in weak resistance to differential attacks. (5) Unchanged key stream, identical elements will be produced for multiple plain-images in case that the secret key remains unchanged. (6) Small Keyspace compared to the Z. Li et al. scheme [30] and the S. Yousif et al. scheme [64].
Z. Li et al. scheme [30]	(1) Good design structure. (2) Good sensitivity in key stream generation. (3) Large keypace. (4) Good resistance to Occlusion attacks. (5) High sensitivity in plain-image and key better than the S. Yousif et al. scheme [64] and the N. Khalil et al. scheme [23]. (6) Acceptable encryption and decryption execution time.	(1) Relatively complex in terms of computational cost due to continuous maps that take more time to implement than the S. Yousif et al. scheme and N. Khalil et al. scheme, which affects the scheme's efficiency. (2) There is an additional burden in the exchange of keys between the sender and receiver because the key depends on the plain-image. Where each image has a different encryption key.

6. REFERENCES

[1] Hikmat N Abdullah and Hamsa A Abdullah. Image encryption using hybrid chaotic map. In *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, pages 121–125. IEEE, 2017.

[2] Shafali Agarwal. A review of image scrambling technique using chaotic maps. *International Journal of Engineering and Technology Innovation*, 8(2):77, 2018.

[3] S Alam and Payer Ahmed. Several chaotic analysis of lorenz system. *Eur Sci J*, 13(9):438–455, 2017.

[4] Gonzalo Alvarez, José María Amigó, David Arroyo, and Shujun Li. Lessons learnt from the cryptanalysis of chaos-based ciphers. In *Chaos-Based Cryptography*, pages 257–295. Springer, 2011.

[5] Gonzalo Alvarez and Shujun Li. Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, 16(08):2129–2151, 2006.

[6] Xiuli Chai, Yiran Chen, and Lucie Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in engineering*, 88:197–213, 2017.

[7] Xiuli Chai, Xiaoyu Zheng, Zhihua Gan, and Yiran Chen. Exploiting plaintext-related mechanism for secure color image encryption. *Neural Computing and Applications*, 32(12):8065–8088, 2020.

[8] Guanrong Chen and Xinghuo Yu. *Chaos control: theory and applications*, volume 292. Springer Science & Business Media, 2003.

[9] Hsien-Keng Chen and Ching-I Lee. Anti-control of chaos in rigid body motion. *Chaos, Solitons & Fractals*, 21(4):957–965, 2004.

[10] Yashuang Deng, Hanping Hu, Naixue Xiong, Wei Xiong, and Lingfeng Liu. A general hybrid model for chaos robust synchronization and degradation reduction. *Information Sciences*, 305:146–164, 2015.

[11] NF Elabady, HM Abdalkader, MI Moussa, and So F Sabbeh. Image encryption based on new one-dimensional chaotic map. In *2014 international conference on engineering and technology (ICET)*, pages 1–6. IEEE, 2014.

[12] Michael François, Thomas Grosges, Dominique Barchiesi, and Robert Erra. Image encryption algorithm based on a chaotic iterative process. 2012.

[13] Jiri Fridrich. Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(06):1259–1284, 1998.

[14] Chong Fu, Gao-yuan Zhang, Mai Zhu, Zhe Chen, and Wei-min Lei. A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy. *Security and Communication Networks*, 2018, 2018.

[15] S Geetha, P Punithavathi, A Magnus Infanteena, and S Siva Sivatha Sindhu. A literature review on image encryption techniques. *International Journal of Information Security and Privacy (IJISP)*, 12(3):42–83, 2018.

[16] Mohammad Ghebleh, Ali Kanso, and Hassan Noura. An image encryption scheme based on irregularly decimated chaotic maps. *Signal Processing: Image Communication*, 29(5):618–627, 2014.

[17] T Gopalakrishnan and S Ramakrishnan. Performance analysis of image encryption methods using chaotic, multiple chaotic and hyper-chaotic maps. In *Handbook of Multimedia Information Security: Techniques and Applications*, pages 233–265. Springer, 2019.

[18] Gururaj Hanchinamani and Linganagouda Kulakarni. Image encryption based on 2-d zaslavskii chaotic map and pseudo hadmard transform. *International Journal of Hybrid Information Technology*, 7(4):185–200, 2014.

[19] Noha A Hikal and Marwa M Eid. A new approach for palmprint image encryption based on hybrid chaotic maps. *Journal of King Saud University-Computer and Information Sciences*, 32(7):870–882, 2020.

[20] Zhongyun Hua, Fan Jin, Binxuan Xu, and Hejiao Huang. 2d logistic-sine-coupling map for image encryption. *Signal Processing*, 149:148–161, 2018.

[21] Zhongyun Hua and Yicong Zhou. Design of image cipher using block-based scrambling and image filtering. *Information sciences*, 396:97–113, 2017.

[22] Manjit Kaur and Vijay Kumar. A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, 27(1):15–43, 2020.

[23] Noura Khalil, Amany Sarhan, and Mahmoud AM Alshewimy. An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology*, 143:107326, 2021.

[24] Majid Khan and Fawad Masood. A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, 78(18):26203–26222, 2019.

[25] Majid Khan and Tariq Shah. A novel statistical analysis of chaotic s-box in image encryption. *3D Research*, 5(3):16, 2014.

[26] Krishna Kumar, Satyabrata Roy, Umashankar Rawat, and Shashwat Malhotra. Iehc: An efficient image encryption technique using hybrid chaotic map. *Chaos, Solitons & Fractals*, 158:111994, 2022.

[27] Rushi Lan, Jinwen He, Shouhua Wang, Tianlong Gu, and Xiaonan Luo. Integrated chaotic systems for image encryption. *Signal Processing*, 147:133–145, 2018.

[28] Jun Lang. Image encryption based on the reality-preserving multiple-parameter fractional fourier transform and chaos permutation. *Optics and Lasers in Engineering*, 50(7):929–937, 2012.

[29] Shujun Li, Chengqing Li, Guanrong Chen, Nikolaos G Bourbakis, and Kwok-Tung Lo. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Processing: Image Communication*, 23(3):212–223, 2008.

[30] Zhen Li, Changgen Peng, Liangrong Li, and Xiaoyan Zhu. A novel plaintext-related image encryption scheme using hyper-chaotic system. *Nonlinear Dynamics*, 94(2):1319–1333, 2018.

[31] Wenhao Liu, Kehui Sun, and Congxu Zhu. A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 84:26–36, 2016.

[32] Noura Louzzani, Abdelkrim Boukabou, Halima Bahi, and Ali Boussayoud. A novel chaos based generating function of the chebyshev polynomials and its applications in image encryption. *Chaos, Solitons & Fractals*, 151:111315, 2021.

[33] Yaobin Mao, Guanrong Chen, and Shiguo Lian. A novel fast image encryption scheme based on 3d chaotic baker maps. *International Journal of Bifurcation and chaos*, 14(10):3613–3624, 2004.

[34] Amal Abdulbaqi Maryoosh, Raniah Ali Mustafa, and Zahraa Salah Dhaief. Image encryption techniques based on chaotic map. *Int. J. Eng. Res. Adv. Technol IJERAT (ISSN: 2454-6135)*, 5(9):01–05, 2019.

[35] Robert Matthews. On the derivation of a chaotic encryption algorithm. *Cryptologia*, 13(1):29–42, 1989.

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

[37] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2018.

[38] Bhaskar Mondal, Pratap Kumar Behera, and Sugata Gangopadhyay. A secure image encryption scheme based on a novel 2d sine–cosine cross-chaotic (sc3) map. *Journal of Real-Time Image Processing*, 18(1):1–18, 2021.

[39] MA Murillo-Escobar, MO Meranza-Castillón, RM López-Gutiérrez, and C Cruz-Hernández. A chaotic encryption algorithm for image privacy based on two pseudorandomly enhanced logistic. *Multimedia Security Using Chaotic Maps: Principles and Methodologies*, 884:111, 2020.

[40] Fatih Özkaynak. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, 92(2):305–313, 2018.

[41] Chanil Pak and Lilian Huang. A new color image encryption using combination of the 1d chaotic map. *Signal Processing*, 138:129–137, 2017.

[42] R Parvaz and Mohammad Zarebnia. A combination chaotic system and application in color image encryption. *Optics & Laser Technology*, 101:30–41, 2018.

[43] Priyadarshini Patil, Prashant Narayankar, DG Narayan, and S Md Meena. A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish. *Procedia Computer Science*, 78:617–624, 2016.

[44] K Abhimanyu Kumar Patro, Bibhudendra Acharya, and Vijay Nath. Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps. *Microsystem Technologies*, 25(12):4593–4607, 2019.

[45] Noha Ramadan, HossamEldin H Ahmed, Said E El-khamy, Abd El-Samie, and E Fathi. Permutation-substitution image encryption scheme based on a modified chaotic map in transform domain. *Journal of Central South University*, 24(9):2049–2057, 2017.

[46] Nitin Rawat, Byoungho Kim, and Rajesh Kumar. Fast digital image encryption based on compressive sensing using structurally random matrices and arnold transform technique. *Optik*, 127(4):2282–2286, 2016.

[47] Jai Ganesh Sekar and C Arun. Comparative performance analysis of chaos based image encryption techniques. *J. Crit. Rev*, 7(9):1138–1143, 2020.

[48] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[49] Chaowen Shen, Simin Yu, Jinhu Lü, and Guanrong Chen. A systematic methodology for constructing hyperchaotic systems with multiple positive lyapunov exponents and circuit implementation. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 61(3):854–864, 2013.

[50] Shuliang Sun, Yongning Guo, and Ruikun Wu. A novel plaintext-related image encryption algorithm based on stochastic signal insertion and block swapping. *IEEE Access*, 7:123049–123060, 2019.

[51] Yohan Suryanto, MT Suryadi, and Kalamullah Ramli. A secure and robust image encryption based on chaotic permutation multiple circular shrinking and expanding. *J. Inf. Hiding Multim. Signal Process.*, 7(4):697–713, 2016.

[52] DA Trujillo-Toledo, OR López-Bonilla, EE García-Guerrero, E Tlelo-Cuautle, D López-Mancilla, O Guillén-Fernández, and E Inzunza-González. Real-time rgb image encryption for iot applications using enhanced sequences from chaotic maps. *Chaos, Solitons & Fractals*, 153:111506, 2021.

[53] Bin Wang, Yingjie Xie, Changjun Zhou, Shihua Zhou, and Xuedong Zheng. Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps. *Optik*, 127(7):3541–3545, 2016.

[54] Hui Wang, Di Xiao, Xin Chen, and Hongyu Huang. Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map. *Signal processing*, 144:444–452, 2018.

[55] Xing-Yuan Wang and Zhi-Ming Li. A color image encryption algorithm based on hopfield chaotic neural network. *Optics and Lasers in Engineering*, 115:107–118, 2019.

[56] Xingyuan Wang and Xiaohui Du. Pixel-level and bit-level image encryption method based on logistic-chebyshev dynamic coupled map lattices. *Chaos, Solitons & Fractals*, 155:111629, 2022.

[57] Xingyuan Wang and Hui-li Zhang. A color image encryption with heterogeneous bit-permutation and correlated chaos. *Optics Communications*, 342:51–60, 2015.

[58] KW Wong, WS Yap, BM Goi, and Denis CK Wong. Differential cryptanalysis on chaotic based image encryption scheme. In *IOP conference series: materials science and engineering*, volume 495, page 012041. IOP Publishing, 2019.

[59] Yue Wu, Joseph P Noonan, Sos Agaian, et al. Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, 1(2):31–38, 2011.

[60] Lu Xu, Xu Gou, Zhi Li, and Jian Li. A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. *Optics and Lasers in Engineering*, 91:41–52, 2017.

[61] Erdem Yavuz, Rifat Yazıcı, Mustafa Cem Kasapbaşı, and Ezgi Yamaç. A chaos-based image encryption algorithm with simple logical functions. *Computers & Electrical Engineering*, 54:471–483, 2016.

[62] Guodong Ye, Chen Pan, Xiaoling Huang, and Qixiang Mei. An efficient pixel-level chaotic image encryption algorithm. *Nonlinear Dynamics*, 94(1):745–756, 2018.

[63] Guodong Ye and Junwei Zhou. A block chaotic image encryption scheme based on self-adaptive modelling. *Applied Soft Computing*, 22:351–357, 2014.

[64] Sura F Yousif. Grayscale image confusion and diffusion based on multiple chaotic maps. In *2018 1st International scientific conference of engineering sciences-3rd scientific conference of engineering science (ISCES)*, pages 114–119. IEEE, 2018.

[65] Wei Zhang, Kwok-wo Wong, Hai Yu, and Zhi-liang Zhu. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Communications in Nonlinear Science and Numerical Simulation*, 18(8):2066–2080, 2013.

[66] Xuncai Zhang, Lingfei Wang, Zheng Zhou, and Ying Niu. A chaos-based image encryption technique utilizing hilbert curves and h-fractals. *IEEE Access*, 7:74734–74746, 2019.

[67] Yicong Zhou, Zhongyun Hua, Chi-Man Pun, and CL Philip Chen. Cascade chaotic system with applications. *IEEE transactions on cybernetics*, 45(9):2001–2012, 2014.

[68] Shuqin Zhu and Congxu Zhu. Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map. *IEEE Access*, 7:147106–147118, 2019.