Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19771-y

Image encryption framework based on multi-chaotic maps and equal pixel values quantization

Hoshang Kolivand[1,2,3] · Sabah Fadhel Hamood[4] · Shiva Asadianfam[5] · Mohd Shafry Mohd Rahim[4] · William Hurst[6]

Received: 5 September 2023 / Revised: 9 May 2024 / Accepted: 20 June 2024

Abstract

The importance of image encryption has considerably increased, especially after the dramatic evolution of the internet and network communications, due to the simplicity of capturing and transferring digital images. Although there are several encryption approaches, chaos-based image encryption is considered the most appropriate approach for image applications because of its sensitivity to initial conditions and control parameters. Confusion and diffusion methods have been used in conventional image encryption methods, but the ideal encrypted image has not yet been achieved. This research aims to generate an encrypted image free of statistical information to make cryptanalysis infeasible. Additionally, the motivation behind this work lies in addressing the shortcomings of conventional image encryption methods, which have not yet achieved the ideal encrypted image. The proposed framework aims to overcome these challenges by introducing a new method, Equal Pixel Values Quantization (EPVQ), along with enhancing the confusion and diffusion processes using chaotic maps and additive white Gaussian noise. Key security, statistical properties of encrypted images, and withstanding differential attacks are the most important issues in the field of image encryption. Therefore, a new method, Equal Pixel Values Quantization (EPVQ), was introduced in this study in addition to the proposed confusion and diffusion methods to achieve an ideal image encryption framework. Generally, the confusion method uses Sensitive Logistic Map (SLM), Henon Map, and additive white Gaussian noise to generate random numbers for use in the pixel permutation method. However, the diffusion method uses the Extended Bernoulli Map (EBM), Tinkerbell, Burgers, and Ricker maps to generate the random matrix. Internal Interaction between Image Pixels (IIIP) was used to implement the XOR (Exclusive OR) operator between the random matrix and scrambled image. Basically, the EPVQ method was used to idealize the histogram and information entropy of the ciphered image. The correlation between adjacent pixels was minimized to have a very small value ($\times 10^{-3}$). Besides, the key space was extended to be very large (2^{450}) considering the key sensitivity to hinder brute force attacks. Finally, a histogram was idealized to be perfectly equal in all occurrences, and the resulting information entropy was equal to the ideal value (8), which means that the resulting encrypted image is free of statistical properties in terms of the histogram and information entropy. Based on the findings, the high randomness of the generated random sequences of the proposed

Extended author information available on the last page of the article

confusion and diffusion methods is capable of producing a robust image encryption framework against all types of cryptanalysis attacks.

Keywords Image encryption · Sensitive logistic map (SLM) · Henon map · Extended Bernoulli map (EBM) · Equal pixel values quantization (EPVQ)

1 Introduction

Increasing dependence on multimedia data in various applications and fields, such as military, educational, medical, industrial, and social, results in increasing threats to such data. Images are the most common and popular multimedia data type due to the simple and easy way of capturing and transmitting them [1, 2]. On the other hand, the demand to transfer these images in a secure manner has also increased, and encryption is the preferred method to securely transfer image data. Current encryption techniques such as AES(Advanced Encryption Standard), DES(Data Encryption Standard) and RSA(RSA) are unsuitable for image data encrypting because of the huge size and noticeable redundancy of image data [3–5]. In addition, there are several drawbacks and weaknesses, such as the requirement for a powerful computing system and high computational time. Thus, the implementation of these techniques causes a low level of efficiency and cannot guarantee data confidentiality and security. [6, 7].

Chaos theory was first proposed in the 1970's for use in physics, mathematics, biology, and engineering. Cryptographic applications did not appear until the 1980s (Liu et al., 2009). Chaos-based encryption methods are popular due to their randomness, unpredictability, sensitivity and topological transitivity [8, 9]. Also, chaotic systems are similar to noisy systems because they are random, unpredictable, and sensitive to initial conditions (starting point) and control parameters [10, 11]. Therefore, chaotic systems have uses in cryptography [12]. Also, chaotic systems are useful for encryption because they appear to be random data, and their sensitivity to initial conditions allows for this randomness to be unpredicted, therefore allowing a basis for decryption [13]. The main difference between chaos maps and chaos cryptography is that chaos cryptography is defined by finite sets, while chaos maps are defined by real numbers [12].

Despite the use of conventional image encryption methods to achieve a high level of security, there are several issues that should be addressed to improve the quality of encrypted images. The main challenge faced by image encryption designers is the generation of random keys to be used in encryption and decryption processes [14]. A random generator is essential for the confusion process, generating unpredictable numbers that affect the security of the system. Hence, randomness is important in image encryption to make the cipher image as messy as possible [15]. Conventional random functions make the system robust against any statistical attack [16] by quantizing the pixel positions between encryption and decryption processes. Most studies in the last decade have emphasized that good encryption is based on the correlation of pixels inside the image. Obviously, a complex distribution of pixels in the plain image gives better correlation. It's evident that a messy image can be achieved by randomizing pixel positions during encryption and reconstruction of the cipher image [17]. Repositioning pixels inside the image makes it more secure, and the cipher image is more resistant to statistical attacks [14]. Increasing the key space in the encryption system allows it to be more secure and reliable, hence the importance of key space [15]. So, a large initial size in both confusion and diffusion is inevitable,

especially when using 2D random key generation [14]. The image histogram and information entropy of the cipher images should be considered [18]. Statistical attacks are more sensitive to entropy values, thus equalization of pixel values by uniforming the histogram and increasing the entropy is crucial [19]. Also, to avoid a differential attack, in a good image encryption framework, any slight difference in the plain image must cause a significant difference in the encrypted image [18].

Motivated by the challenges mentioned above, this study aims to propose a novel image encryption framework based on multi-chaotic maps and equal pixel value quantization. This framework seeks to address the shortcomings of existing methods and achieve an ideal level of image encryption, making significant contributions to the field of image encryption.

A new image encryption framework based on multi-chaotic maps and equal pixel value quantization was proposed in this study. To achieve the research goal, the following objectives must be accomplished:

- Introduction of a new image encryption framework based on three security processes, aimed at idealizing the obliteration of statistical properties in terms of histogram and information entropy.
- Proposal of a new random number generator based on chaotic maps and additive white Gaussian noise to enhance both confusion and diffusion processes.
- Proposition of a simple and effective diffusion method to increase robustness against differential analysis.

In this study, to achieve ideal results in the image encryption field, a novel encryption framework was introduced, making several contributions to the existing literature. Unlike ordinary chaotic image encryption frameworks that consist of two processes (confusion and diffusion), the proposed framework incorporates a new process named Equal Pixel Values Quantization (EPVQ).

The organization of this paper is as follows: In section 2, a review of previous studies related to image encryption is investigated. In section 3, the methodology of research is presented in detail. In section 4, the experimental results are described. Finally, in Section 5, a general conclusion is drawn.

2 Literature review

One of the most important stages in image encryption is confusion, which concerns the positions of pixels in the plain image. Many efforts have aimed to mitigate the dependence of pixels on their neighbours by exchanging positions under certain conditions to maintain the correlation of the pixels [20]. Prediction of new pixel positions under the condition of a random function still needs more attention [21]. The correlation of these pixels can be mapped under the key generated from the random function, and this function should be strong and reliable for using the generated key in both the encryption and decryption processes [22]. The confusion process is responsible for generating a good cipher image from the encryption process, and any weakness in this stage will affect the security of the system [23]. Previously, more effort has been spent in this regard to improve confusion to avoid any tamper detection, but there is still a need to outsmart the warden and aggressor.

On the contrary to confusion, which concerns pixels' positions, the diffusion stage is responsible for changing pixel values [24]. Altering these values is essential as it directly influences the image histogram. Many algorithms in the past years have paid tremendous attention to achieving a uniform histogram for the generated cipher images. Since pixel values range from 0 to 255, representing them in a histogram graphically and concisely is challenging. To overcome statistical attacks, the diffusion process should erase the histogram of the cipher image to eliminate any statistical properties. Moreover, the information entropy of the encrypted image should be 8. Information entropy reflects the uncertainty distribution of pixel values and is highly related to the image histogram [25]. When changing pixel values, the distribution of pixel values should change accordingly. In successful image encryption methods, the information entropy should be close to the ideal value of 8. When the information entropy equals 8, it indicates a truly random sample [26].

In the field of image encryption, various approaches have been proposed to achieve security, but the chaos approach is the most suitable because it shares the same cryptographic features [27]. Currently, many chaos-based image encryption methods utilize confusion and diffusion processes as proposed by Shannon [28] to obtain secure image encryption systems. Although these proposed methods are effective, they still encounter various problems.

In the algorithm proposed by Qais and Aouda [8], both a Rössler chaotic system and a Lorenz chaotic system are used for encryption. The use of two or more chaotic systems in an algorithm is highly unusual. Long-term chaotic behaviour is periodic and dependent on initial variables [29]. Both the Rössler and Lorenz frameworks are dependent on three variables, thereby increasing the security of the proposed chaotic system because all parameters are now dependent on six variables, making it highly secure. This algorithm shuffles an image's pixels and changes its grayscale values for a set number of iterations before storing the randomized image data in a chaotic matrix the same size as the original image. XOR operations are used for both encryption and decryption. The key space of the proposed algorithm is good in terms of increasing the total number of initial values to six instead of three for each one of the used chaotic systems. Additionally, because the proposed method uses XOR operation between the plain image and the random one without making any permutations to the image's pixels, the expected correlation value between the adjacent pixels of the encrypted image will be moderate.

RuiLiu and Tian [30] proposed a coloured image encryption algorithm based on chaotic maps and spatial bit-level permutations (SBLP). Image pixel positions were shuffled using a sequence generated from two chaotic logistic maps before the shuffled image is transformed into a binary matrix. A permutation of the binary matrix is created by scrambling the map generated from the (SBLP) process. A second sequence was generated from a chaotic logistical map to rearrange the pixel positions of the new images. The proposed framework deals with the bit-level of image pixels and the random sequences generated by the implementation of two logistic maps that are used in both confusion-diffusion processes. The first step in the proposed method is the generation of the two random sequences using two initial conditions and two control parameters. The first of these generated sequences is used to permute the image pixels. The permutation is done by converting the image from a two-dimensional matrix into a one-dimensional array and rearranging this array according to the randomness order of the random sequence. The resulting array will be analyzed into bit-level matrix (each element in this array will be analyzed into its bits component). The second chaotic sequence resulted from using the second initial condition and the second control parameter will be used in the permutation process of bit-level matrix element. The

analysis achieved by this method is weak in image encryption security criteria because the expected resulting histogram will not be close to a uniform one.

To reduce the complexity of image encryption, Abhinav and Verma [31] proposed a simple image encryption method based on Dual-Tree Complex Wavelet Transformations (DT-CWT). The first process in this framework is to transform the plain image using wavelet transformation, then a pixel chaotic scrambling is used for approximation, and an Arnold transformation is used for the details. Although the suggested image encryption method is simple, it expects to obtain low results in terms of histogram analysis.

As mentioned in the above brief survey, the development of encryption methods for secure transmission of images over the internet still faces many remaining challenges. One of the main challenges in encryption algorithms is the generation of random numbers known as encryption keys. These random numbers must satisfy several principles of unpredictability, long series period, and the ability to regenerate these sequences many times. Initial key size is another issue in the image encryption field, and the criteria for this issue are based on the key size, key sensitivity, level of randomness, and regenerating ability. The statistical properties of the cipher image, such as a correlation between adjacent pixels, the correlation coefficient between plain and cipher images, histogram, and information entropy, are considered important issues in the field of image encryption. Additionally, the ability to withstand differential attacks has become a critical issue, especially after the increased interest in such attacks. These challenges and issues can be explained in detail as follows:

In the field of cryptography, random number generators play an essential role, and the properties of the cipher text fully depend on the generated key [32]. The random number generator is basically used to generate the secret key to be used later in the encryption algorithm and to produce the desired random keys. There are generally two types of these generators. The first one is True Random Number Generator (TRGN). To produce randomness in this type, a non-deterministic source (entropy source) should be sampled and processing outside the computer [26]. Actually, it is very simple to get the source of entropy, like the time interval between keystrokes or some variations of mouse movement. However, it is difficult to obtain entropy by tracking user inputs, as keystrokes are often buffered by the operating system after collecting several keystrokes to be sent to a waiting program. A radioactive source is considered a really good entropy generator. Another good entropy source is the noise of the atmosphere, which can be acquired by radio [33]. The output of TRNG is sometimes used directly as the random number, or sometimes used as the input of Pseudo Random Number Generator (PRNG). To use it directly (no extra processing implemented), it should satisfy the randomness criteria. For encryption purposes, some of the entropy sources (e.g., time/date vectors) are sometimes predictable; it can lighten the predictability by the combination of different types of sources [34]. However, there are still weaknesses and drawbacks in using TRNG in cryptography fields, such as the time consumption required to produce TRNG, which makes this generator undesirable when large-size random sequences are required. In addition, TRNG is deficient when it is evaluated using statistical tests.

The second type is Pseudo Random Number Generator (PRNG). In this type of random number generator, one or more values can be used as the input (seed) to produce a pseudorandom series of unpredictable behaviour as the output [35]. Randomness and unpredictability are the properties of the used seed value itself, and typically PRNG output is deterministic and is a function of the seed. The term pseudorandom is an indication of the deterministic nature of the used process, and because of this nature, the pseudorandom sequence is reproducible by using the same seed value [14]. Thus, the used seed should be

saved if a reproducing or validation process is required. It is worth noting that the pseudorandom number series is most often more random than the true random numbers generated from a physical source. Another feature of the PRNG that makes it more usable is that each of the generated pseudorandom number values is fully dependent on random input that is already generated by the previous implementation of the PRNG. The correlation between input and output can be eliminated by using PRNG rather than TRNG. Thus, the random series generated by PRNG is better in terms of statistical properties, in addition to the short time of implementation [33, 36].

In cryptographic applications, both TRNG and PRNG produce random bit series and sometimes combine these random bits into random blocks. The most important properties of the produced random series are randomness and unpredictability [14]. Randomness can be explained as the result of flipping a fair (unbiased) coin, which has two faces labelled "0" and "1," and the flipping process is independent of the previous result i.e., the current flip result is not affected by the previous result and would not affect the next result. Thus, the perfect random generator is resulted from the unbiased (fair) coin flip, since the distribution of zero and one values is random and [0, 1] are distributed uniformly. Each bit in the random series is generated independently of the other elements of the same random series, and the next value in the series cannot be predicted, regardless of how many bits have already been generated. Unpredictability is the second property of the produced random series. For cryptographic applications, both TRNG and PRNG must be unpredictable. In PRNG, if the seed value is unknown, the next generated value will be unpredictable, a feature known as forward unpredictability. The knowledge of any value in the random series should not lead to revealing the seed value (also, it should be unpredictable in the backward direction). There should be no clear correlation between the seed and any value in the generated series, and the appearance probability of each element in the generated random series should be equal to 50% [33, 35].

Key security is the procedure to be taken to ensure the confidentiality of the used key. There are two main issues in the key security field, which are key space and key sensitivity. Key space can be defined as the total number of possible keys that can be used to decrypt the cipher text [37]. Key space size is an important criterion in the field of cryptography, and in a good encryption system, the large key space indicates good resistance against brute force attacks [38]. In addition, strong encryption should have an encryption key no smaller than 2^100 [19], with the exponent indicating the number of bits in a key. The large encryption keys provide greater security against brute force attacks [39]. Therefore, the design of an encryption system must consider the size of key space. In a brute force attack, the cryptanalyst tries different keys and may eventually guess the true key, thus a large key space size makes this type of attack infeasible. Key sensitivity is another issue related to key space size. In key sensitivity criteria, any slight change in the used key, even by one bit, should produce a totally different encrypted image [40]. Therefore, key sensitivity must be considered in the design of any image encryption system.

Otsu's method [59] is widely used for histogram thresholding-based image segmentation but may not perform optimally for images with non-Gaussian intensity distributions. The proposed model enhances Otsu's algorithm by estimating mean values using heterogeneous mean filters, making it compatible with various types of images and improving segmentation output. Experimental results on medical images of MRI brain tumours and dermoscopic skin lesions demonstrate the effectiveness of the proposed model compared to existing methods, with heterogeneous mean filters contributing to improved segmentation accuracy. Nyo et al. [60] focus on MRI image segmentation, particularly brain tumour segmentation, using Otsu's thresholding method. Their analysis shows that only one of the

classes achieves the highest positive rate (68.7955%) and accuracy (95.5593%). Mundada et al. [61] propose a novel methodology for automating the detection and classification of brain tumours and swelling using MRI images, achieving higher accuracy rates compared to existing methodologies. Yasmin et al. [62] address the challenge of over-segmentation in brain tumour detection and segmentation by combining morphology-based partitioning and marker-controlled watershed transformation. The proposed method shows promise in reducing over-segmentation and aligns with our aim of enhancing security and accuracy in image encryption frameworks.

Our proposed method in image encryption frameworks focuses on enhancing security and accuracy rather than segmentation, leveraging existing techniques like Otsu's thresholding for preprocessing steps in medical imaging to ensure optimal results in image-based applications. Unlike the segmentation-focused approaches, our method addresses the encryption process's robustness and security by employing innovative encryption techniques. Additionally, while some methods, such as Nyo et al.'s [60] and Mundada et al.'s [61], demonstrate promising results in brain tumour segmentation and classification, our approach targets broader applications in image encryption, encompassing both medical and non-medical domains. Moreover, Yasmin et al.'s [62] method, which aims to reduce over-segmentation in brain tumour detection, aligns with our interest in improving segmentation techniques but lacks the encryption focus of our proposed method. Overall, while these methods contribute valuable insights to the field of image processing, our approach emphasizes enhancing security and accuracy in image encryption frameworks, ensuring robust protection of sensitive data across various applications.

The statistical properties of the cipher image can be exploited by cryptanalysts to decipher the encryption algorithm [41]. Correlation between adjacent pixels in the cipher image, correlation coefficient between cipher and plain images, histogram, and information entropy is the most important statistical features in the image encryption field. A good encryption system should obliterate all statistical features of the plain image because the cryptanalyst always tries to find any weakness in the encryption system to use it in his analysis. There are several types of statistical-based attacks, such as Histogram analysis, in which the plain image consists of semantic information that can be analyzed according to the frequency of the grey level. Thus, it is essential to deface the histogram of the plain image using a strong encryption method. In correlation analysis, similar to the histogram, the correlation between adjacent pixels can reveal good statistical information about the plain image and can also reflect the relationship between the adjacent pixels. This type of information (correlation) can be minimized by suggesting a powerful encryption method [42]. Differential analysis is a general form of cryptanalysis, primarily developed to be applicable for block ciphers, but recently several differential attack methods have been designed especially for stream cipher analysis [43]. In this analysis type, the cryptanalyst tries to find any relationship between two cipher images produced by making one-pixel value alteration of the plain image before implementing the encryption process. If a significant difference between the two cipher images is obtained, the encryption method is differential attack-proof; otherwise, it is easy to reveal good information about the plain image [44].

The literature review encompasses various approaches to image encryption, highlighting the significance of chaos-based encryption due to its sensitivity and unpredictability. While chaos-based methods offer randomness, their effectiveness in achieving an ideal encrypted image remains a challenge. The proposed encryption framework in our work aims to overcome these challenges by introducing a new method, Equal Pixel Values Quantization (EPVQ), alongside enhancing confusion and diffusion processes

using chaotic maps and additive white Gaussian noise. Unlike conventional methods that focus on achieving secure segmentation, our approach prioritizes security and accuracy in image encryption frameworks. While Nyo et al. [60] and Mundada et al. [61] demonstrate promising results in brain tumour segmentation, our method extends to broader applications, including medical and non-medical domains, ensuring robust protection of sensitive data. Moreover, while Yasmin et al.'s [62] method aims to reduce over-segmentation in brain tumour detection, our approach emphasizes enhancing encryption techniques to ensure the statistical properties of the cipher image are obliterated, safeguarding against cryptanalysis attacks. Overall, our approach contributes to the field by focusing on enhancing security and accuracy in image encryption, addressing key challenges such as the randomness of generated sequences and resistance against statistical attacks.

3 Research methodology

A new image encryption framework was proposed in this study, with the main contribution being the addition of a new process, the EPVQ process. Other contributions were applied to the sub-frameworks of the existing two processes, confusion, and diffusion. Here is a brief explanation of the proposed framework (Fig. 1 illustrates the framework of the proposed research).

In the confusion process, a Henon map, SLM, and white Gaussian noise are used. Initially, a Henon map generates a set of values equal to the number of rows in the plain image. Each value generated by the Henon map is used as the initial value of the SLM, resulting in a set of random number series, with each row having its own series. This forms a random matrix, with each sequence based on its respective initial value generated by the Henon map. Additive white Gaussian noise is then added to this random matrix to enhance framework security. Once the random confusion matrix is formed, its elements are arranged in ascending order, and corresponding elements of the image matrix (pixels with the same indices as the confusion matrix elements) change their location accordingly.

In the diffusion process, a set of chaotic maps (EBM, Tinkerbell, Burgers, and Ricker maps) are utilized. Each of these four maps generates its own sequences of random numbers. The random numbers generated from the Tinkerbell, Burgers, and Ricker maps are used to form the random diffusion matrix, with one element chosen from each of these three generated series. The selection of elements from each map series is randomly controlled based on the EBM.

In the new EPVQ process, XOR operators are used to achieve a histogram for the encrypted image with equal frequency values for all colour scales, along with a perfect result for information entropy (8 out of 8). Since information entropy indicates uncertainty, an ideal histogram produces ideal entropy in an encrypted image [25].

3.1 Preprocessing

This part of the methodology is responsible for selecting and analyzing the chosen image before implementing any action on it. Initially, an image is selected from the chosen dataset. If the chosen image is an 8-bit grayscale image, the proposed framework will deal with it directly. However, in the case of 24-bit RGB images, analysis of its RGB channels should be implemented to deal with each channel separately. After complete separation,

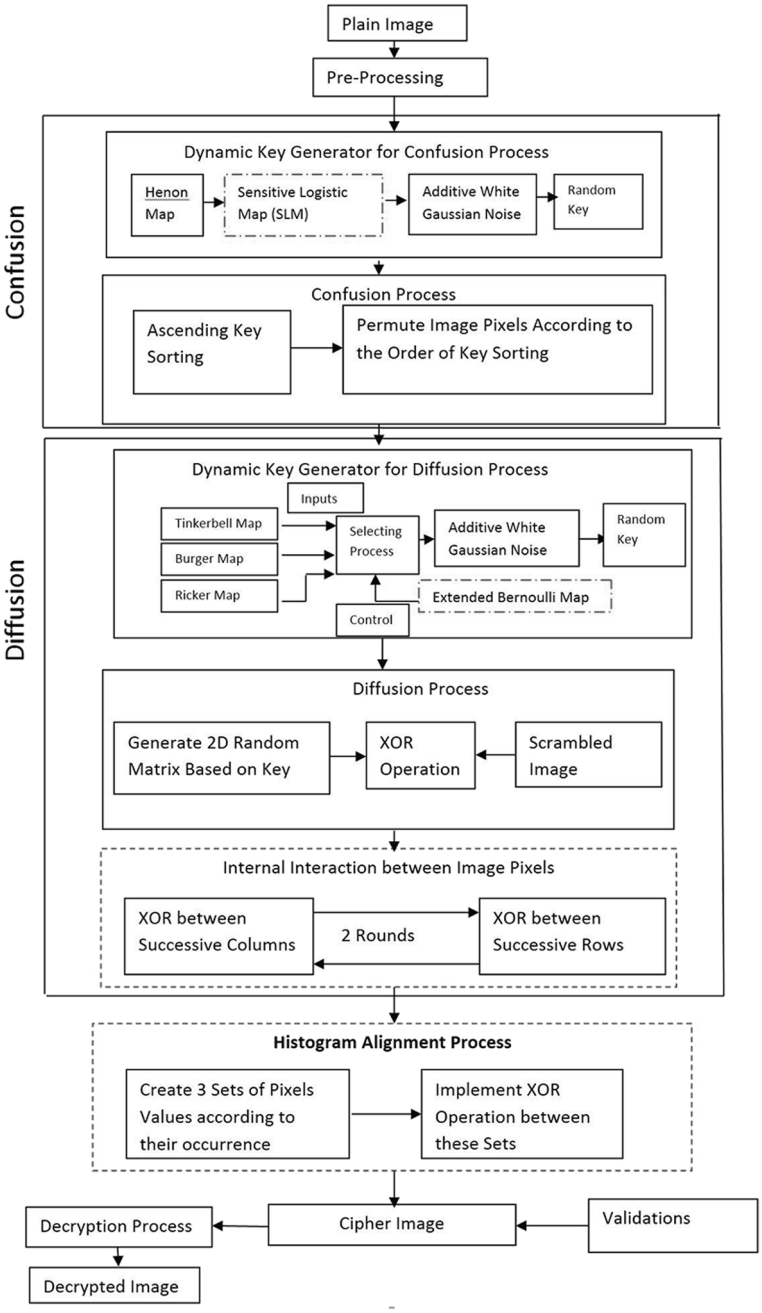


Fig. 1 General Framework for the Proposed Research

each image channel is stored in a single 8-bit matrix with dimensions equal to those of the original image. The implementation of this part produces a three-channel image, with each channel being an 8-bit image. Figure 2 illustrates this procedure.

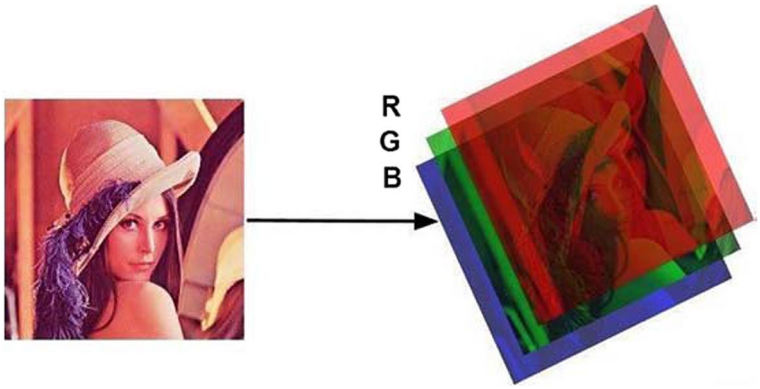


Fig. 2 Illustrate analysis of RGB channels

3.2 Confusion process

The proposed confusion method consists of two main processes. First, the random number generating process consists of the amendment of the logistic map equation to improve the sensitivity of the well-known logistic map and using the Henon map, Sensitive Logistic Map (SLM), and additive white Gaussian noise (AWGN) to perform random number generator. Second, image pixel permutation units are used as random numbers in the process of changing the locations of each plain image pixel to increase the performance of the proposed study.

3.2.1 Chaotic maps (Henon and SLM) used in the proposed confusion process

Two chaotic maps are used in the proposed confusion method. The Sensitive Logistic Maps (SLM) and Henon map in addition to additive white Gaussian noise are used in the proposed confusion method to obtain random sequences with better criteria. The following sections explain the proposed SLM.

The Proposed Sensitive Logistic Map (SLM) To achieve the research objectives, an amendment to the logistic map was proposed in this study. This new form of logistic map aims to increase the randomness of the confusion process by increasing sensitivity to initial conditions. To achieve this goal a multiplication between the output of each iteration of the logistic map with an integer K (which must be >1) to increase the difference between the input and output values for each iteration. Multiplication will make the resulting values exceed the boundaries of the logistic map i.e. the output will be greater than 1. The logistic map is an iterated equation and the output of each iteration will be the input for the next iteration. The input limits for the logistic map are greater than (0) and smaller than (1), which leads to some imperfection. Therefore, to solve this problem a modulus of (1) was used to make the resulting values within an acceptable range ($0 < X < 1$). Eq. 9 1) shows the proposed Sensitive Logistic Map (SLM).

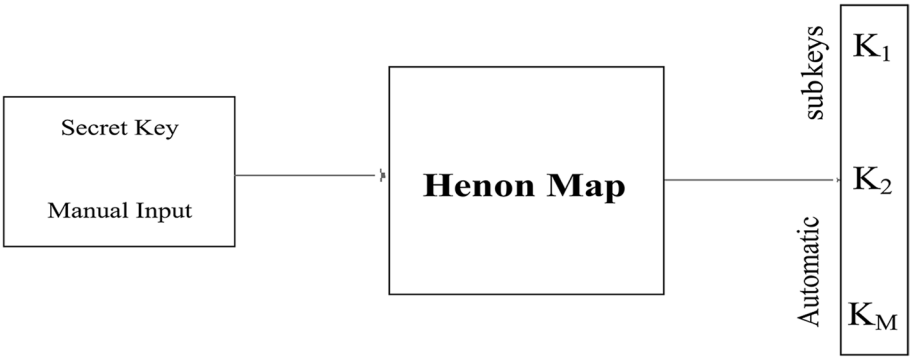


Fig. 3 The process of generating automatic sub-keys

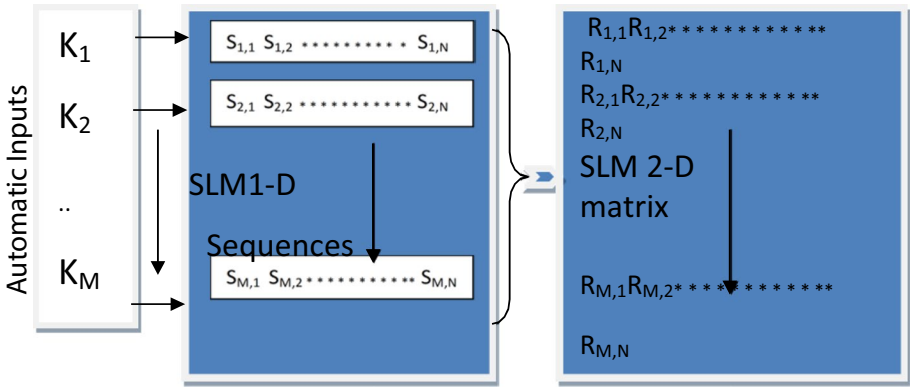


Fig. 4 Using of Automatic Key to be as SLM Inputs

$$X_{n+1} = \left(r\mathrm{X_n}\left(1 - \mathrm{X_n}\right)\right) * \mathrm{K} \bmod 1 \tag{1}$$

Introducing a new parameter (K) to SLM will produce dynamical systems with more randomness by applying multiplication between (rXn(1 − Xn)) and K (which is >1) to amplify the result of each iteration to produce a more sensitive random number generator. The k parameter is used to increase the sensitivity of the new iteration to the old input that resulted from the previous iteration. While (mod 1) is to reduce the accumulation when feedback the result of the equation of the random generator keeps the range of random numbers between 0 and 1 to avoid the over exceed the range.

Henon map At first, the initial conditions and control Parameters are initiated manually to be used as the inputs for the Henon map. The output of the Henon map is a random sequence consisting of random numbers equal to the number of image rows as seen in Fig. 3.

The proposed SLM was used in the second phase of the random key generator. The generated sub-keys (K1 to KM) were used as inputs in the proposed SLM to generate a

random sequence for each row and the size of each of these sequences was equal to the size of the plain image columns, which is N. Figure 4 explains this process.

Where K is the sub-key, S is the random number sequence generated by SLM, and R is a two-dimension random number matrix assembled from random sequences. After obtaining the random matrix from executing the Henon map and the proposed SLM to increase the quality of the random number generator, an additive white Gaussian noise was implemented to the random matrix as shown in Fig. 5.

where V is a two-dimensional matrix of additive white Gaussian noise and F is the final random matrix to be used in the confusion process to control image permutation.

3.2.2 Confusion process

The confusion process is a description of the image permutation method. In this study image pixels were scrambled to reduce the high correlation between adjacent pixels to increase resistance to statistical attacks. To accomplish this goal this study proposed the creation of a random matrix, which it already explained in detail and this matrix is dedicated to controlling pixel scrambling in the image confusion process. The first step of the confusion process is to convert a two dimensions random number matrix into a one-dimension random array as illustrated in Fig. 6.

After the conversion process ascending sorting was implemented to the one-dimension random array to consider the new order of the old indices of the sorted array (when any value in the random array changes its location to the new location in the sorted array the original index of this value before sorting follows the value to the new location). A table of three variables was created as shown in Fig. 7.

Thus, random values and their new indices are in ascending order but the old indices are ordered in a random way, therefore it is necessary to create a lookup table consisting of old indices against new indices.

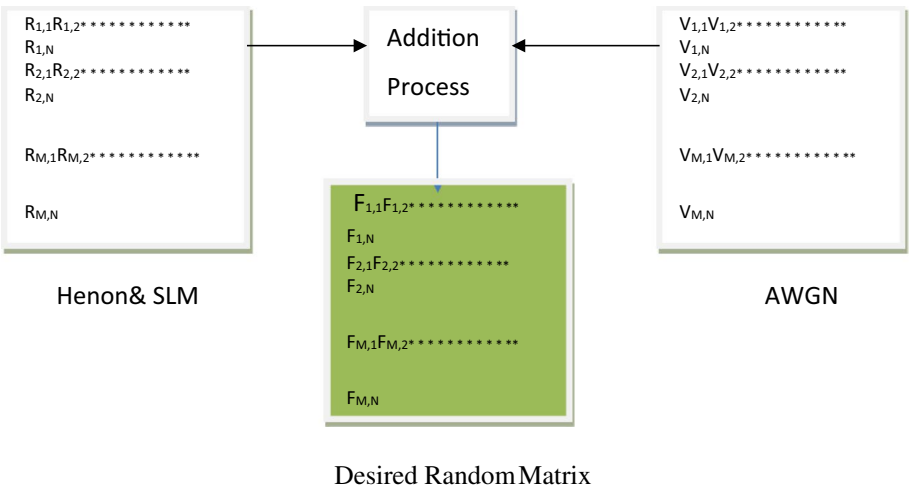


Fig. 5 Final Random Matrix for confusion Process

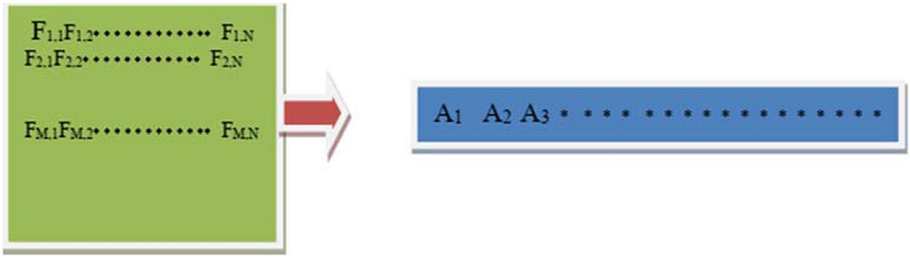
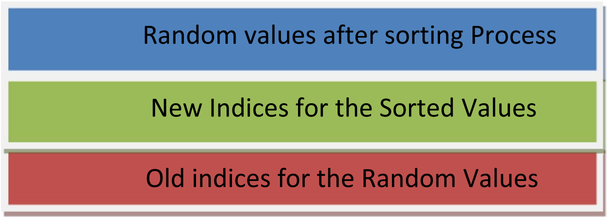


Fig. 6 Two Dimensions to One Dimension Random Matrix Conversion

Fig. 7 Table of the Random Array Fields after the Sorting Process



The new step is the conversion of the plain image from a two dimensions matrix into a one-dimension array with the same size as the sorted random array. Although the conversion process makes reshapes the plain image the correlations between successive elements in the new one-dimension image array are still high. To minimize this high correlation the image pixels are scrambled using the previously mentioned lookup table to change the location of pixels in the one-dimension image array to a new location. To get the scrambled image a conversion from the one-dimension image array after scrambling into a two-dimension scrambled image was made. The scrambled image is considered an intermediate encrypted image with minimum correlation between adjacent pixels, but other characteristics like the histogram and information entropy are still the same.

3.3 Diffusion process

For the obliteration of the statistical information of the encrypted image, the diffusion process is considered the most important process in all chaotic image encryption systems. This study suggests a new diffusion process to achieve image encryption frameworks with high criteria. Several points have been considered in the proposed diffusion process such as increased key space, key sensitivity, removal of histogram and information entropy, and increased resistance to differential attacks.

The proposed framework for the diffusion method consists of three sub-processes which are; the random number generator process, the Internal Interaction between Image Pixels (IIIP) sub-process and the diffusion process. The random number generator is designed by the using channel hopping technique which is performed by implementing the Tinkerbill map, Burger map and Ricker map in addition to the Extended Bernoulli Map (EBM) which is used to control the selection process. IIIP method is proposed to achieve a robust image encryption method against differential attacks this process is proposed by this research while the diffusion process is implemented to efface

the statistical properties of the encrypted image by the the execution of XOR operator between the image generated from IIIP process and the random matrix that derived from the random number generator.

3.3.1 Random numbers generator for diffusion

To generate random numbers for the diffusion process four chaotic maps are used, which are Extended Bernoulli Map (EBM), Tinkerbell, Burgers and Ricker maps, in addition to additive white Gaussian noise. More explanations for the Extended Bernoulli Map are as follows.

Extended Bernoulli Map Brute force attacks are famous in cryptanalysis for attacking encrypted information and the most effective technique used to make such attacks infeasible is increasing secret key space as much as possible. In this study, two techniques are used to increase key space. One of these techniques is by implementing multiple chaotic maps with consideration for key sensitivity, while the other technique is by proposing an amendment to the Bernoulli map to increase the key space of the proposed generator. Bernoulli map uses one initial key as the input and this study suggests increasing the initial values to two as seen in Eq. (2).

$$\boldsymbol{X_n = \left(2 * \left(X_{n-1}\right) + \left(X_{n-2}\right)\right) \mathbf{mod1}} \tag{2}$$

In addition to the increasing of key space size by increasing the total number of initial conditions, the response of the proposed Extended Bernoulli Map (EBM) shows more randomness and more unpredictable behaviour which is achieved because the generating is dynamical for both initial conditions which affect the whole random number generating process. The existence of two initial conditions with variable values (for each iteration) causes the dynamical behaviour of these initials which increases randomness and unpredictability for the generated random key.

Channel hopping The used technique to produce random numbers is channel hopping. After the selection process, additive white Gaussian noise is used on selected random numbers. The process of selecting random numbers is as follows: At first, four sequences (VEx_B,VT, VB, and VR, which belong to the Extended Bernoulli Map (EBM), Tinkerbell, Burgers and Ricker maps, respectively) are generated by the initial conditions and control parameters for these four chaotic maps. The length of each of these sequences is N*M where N and M are the row and column numbers, respectively for the image to be encrypted. Random number values will be chosen from one of the sequences of the three used chaotic maps (Tinkerbell, Burgers and Ricker maps) and the Extended Bernoulli Map is used to control the value selecting process. The last step in the random number generating process is the implementation of additive white Gaussian noise (w) to the selected random sequence (V). The resulting sequence (R) is the desired random number sequence, which will be used in the process of image diffusion. The generation of random number sequences is explained in Fig. 8.

After generating the desired random sequence, a conversion from a one dimension into a two dimensions matrix is implemented and the dimensions of the produced matrix are the same dimensions as the plain image (M×N) to be encrypted.

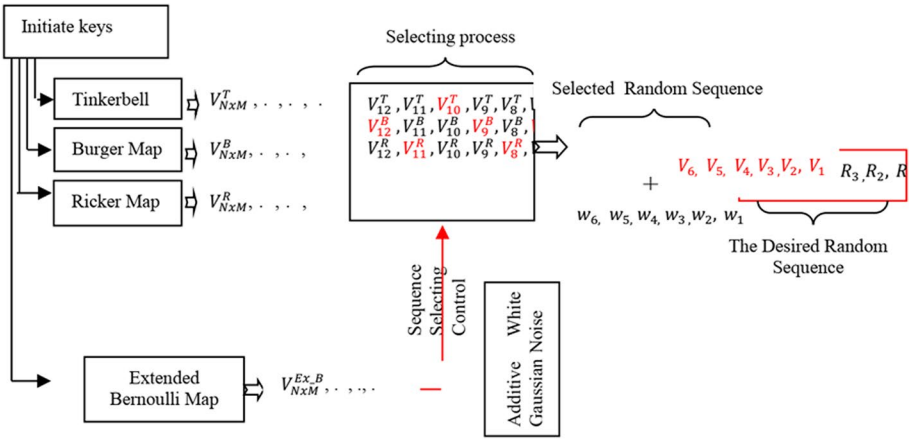


Fig. 8 Channel hopping process

3.3.2 Internal interaction between image pixels (IIIP)

Nowadays the importance of differential attacks has increased due to its high performance in cryptanalysis and researchers have concentrated on developing new techniques based on this type of attack. This study suggests a technique to resist this type of attack. The proposed technique is simple and depends on a produced random number matrix. In a differential attack cryptanalysis encrypts an image multiple times with the same encryption method and the same control parameter and initial conditions but every time it makes a slight change (one pixel) to the plain image, after which a number of encrypted images are created for comparison purposes to find relationships between the plain image and the encrypted image. To resist this type of attack encryption methods should produce significant differences between encrypted images after making minor alterations [45].

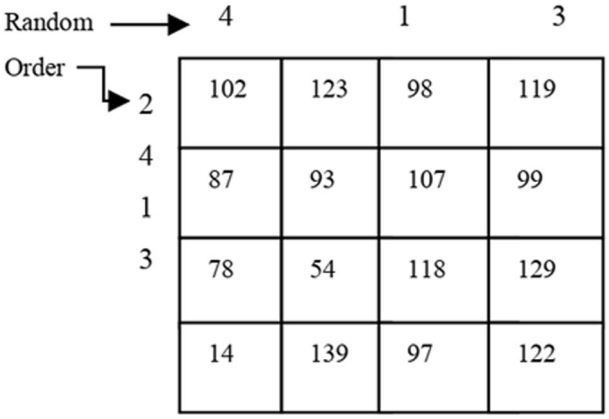
This study suggests implementing XOR operators between image pixels. The first row and first column of the random number matrix are used to control the XOR operation. The implementation of XOR operators is done between each column and its successive (according to the random order obtained from the first row in the random matrix) column. Then the XOR operator is implemented for the first row and it's successive (according to the random numbers obtained from the first column of the random matrix) rows.

To ensure any minor changes in the plain image after even one-pixel alterations produce significant changes in the encrypted image, this study suggests the XOR implementation process is repeated twice. A numerical example to explain the proposed technique is as follows:

Suppose the plain image is a 4×4-pixel image and the random order for the columns is (4,1,3, and 2) and the random order for the rows is (2,4,1, and 3), which were obtained from the first row and first column of the random matrix, respectively. This is illustrated in Fig. 9.

The first process was done by implementing XOR operators between the values of the second column (first column in random order) as seen in Fig. 9 and the values of the fourth column (second column in random order). The resulting values will replace the values of the fourth column while the values of the second column will stay the same. After that a new implementation of the XOR operator is done between the new values of the fourth

Fig. 9 4×4 plain image



column and the values of the third column (the random order for the third column is three) and the resulting values will replace the third column values. Then with the same process, XOR operations will take place between the first and third columns, the values of the first column will be updated by the new values. Finally, XOR operations will be done between the first and second columns (fourth and first random columns order). The resulting values will be saved in the second column instead of the old values. The same procedure will be done between the successive (in random order) rows.

After completing the first round of XOR operations between successive columns and successive rows, another implementation of the same process was done to ensure that any change of even one pixel would affect the entire image as shown in Fig. 10.

To verify the performance of the proposed method against differential attacks, only one pixel in the original image (the pixel located at the address (2, 3)) was changed from 107 to 152 as seen in Fig. 10. After that, the implementation of XOR operations will take place between successive columns and successive rows. This process is repeated for the second round as shown in Fig. 11.

The red value in Fig. 11 is the altered value, while the red values in Fig. 12 represent changes in the resulting image due to the small alterations in the original image after two rounds of XOR operations.

Altering the pixel located at address (2, 3) as seen in Fig. 11 leads to significant changes in the resulting image as shown in Fig. 12 (d). Because in differential attacks cryptanalysis makes small changes to the plain image and encrypts it to find patterns or relationships between the plain image and its encrypted images, significant changes make differential attacks infeasible (Kumar et al., 2016) and it is clear that the resulting images are entirely different from those encrypted without any pixel alterations.

3.3.3 Equal pixel values quantization (EPVQ) method

In this study, an additional process was designed to achieve perfect randomness in the ciphered image itself as indicted by the image histogram and information entropy. The desired histogram is absolutely uniform while information entropy is equal to eight. The aim of the proposed method is to produce a ciphered image with equal probabilities p(x) for all pixel values or image colours to produce an absolutely uniform histogram for the ciphered image and to entirely remove the information of the plain image histogram. This

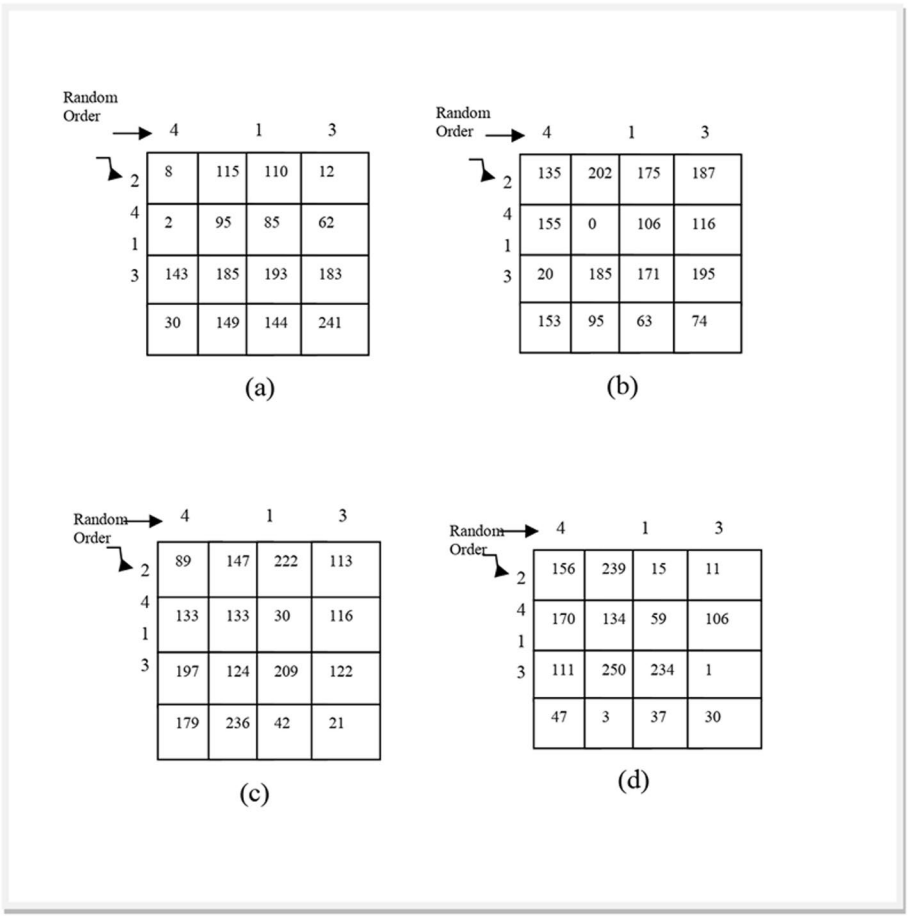


Fig. 10 Implementation of XOR operators between (a) successive columns, successive rows, (c) second round successive columns, (d) and second round successive rows

Fig. 11 The altered image matrix

Random Order

	4	1	3
2	102	123	98	119
4	87	93	152	99
1	78	54	118	129
3	142	139	97	122

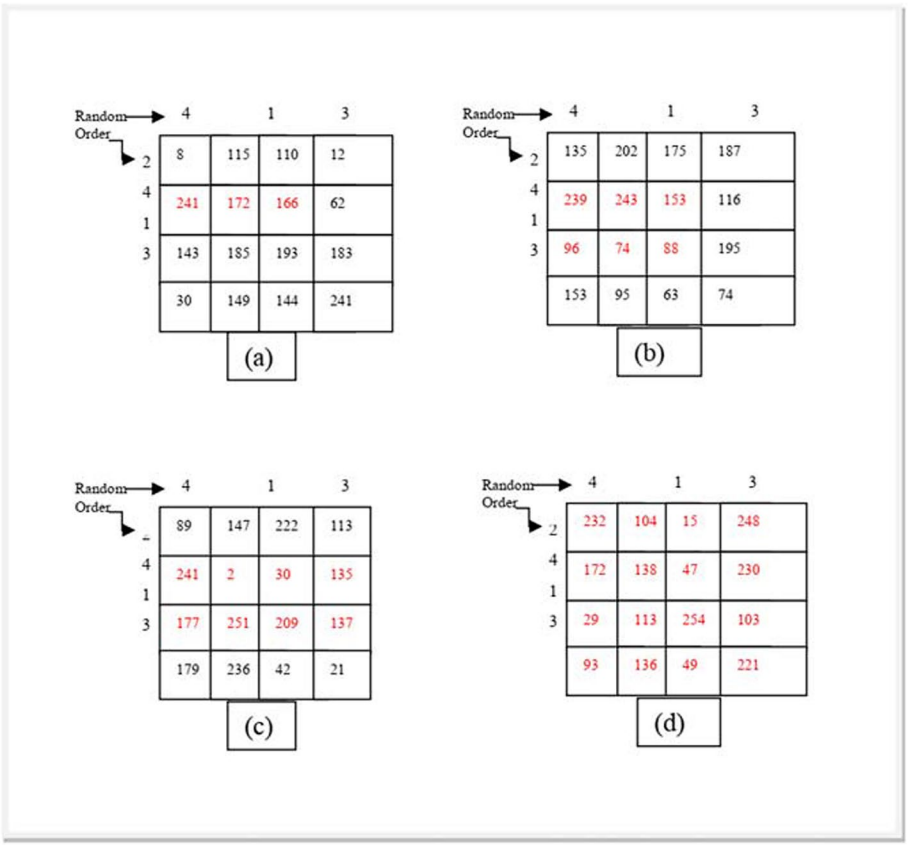


Fig. 12 Changes due to the Small Alterations in the Original Image

is because the information entropy of all images is ideal (equal to 8) when the image pixel values have the same probability [25], so the expected result for information entropy must also be ideal.

The process of the proposed EPVQ Method starts by using the image from the proposed diffusion process as an input for the process. As already explained the histogram of this image is not absolutely uniform and information entropy is not equal to 8. The second process analyzes pixel values according to their occurrence frequencies into three sets, which are over, below and equal to the average occurrence frequency. After that XOR operator are implemented between image pixels to produce an encrypted image with an ideal histogram and perfect entropy. This process produces a text file that contains information about the location of the pixels that underwent XOR operations and the values produced from this operation are used later by the recipient to decrypt the transferred encrypted image. The produced text file is encrypted using powerful existing text encryption methods before being transferred to the recipient.

Method of Equal pixel values quantization Due to the implementation of the EPVQ method, all pixel values for the encrypted image will have the same occurrence i.e. the histogram of the encrypted image will be a straight line. In image encryption, there is a

sender, receiver and attacker, the attacker or cryptanalysis is the person or entity that is trying to obtain the plain image from the encrypted image. Histogram analysis is one of the most powerful methods to deduce a plain image or encryption key and this kind of attack is called a statistical attack [46]. Therefore, defacing the plain image histogram should be considered when designing image encryption systems.

The distribution of image pixel intensity is shown by the histogram and an ideal image encryption method will produce a uniform histogram [7]. This study produced encrypted images without any histogram information because the histogram of the produced image is the same for all input images and cryptanalysis cannot find any valuable information using histogram analysis.

The information entropy of the encrypted image is an uncertainty measurement that indicates system randomness. The greater value for information entropy is more randomness. When there is equality in the probability distribution of image colours in encrypted images, information entropy will be maximized, and the encryption system will be considered effective [47]. The implementation of EPVQ is explained as follows:

After reading the input image (resulting from the diffusion method) histogram. A calculation to find the average frequency of occurrence (ave) is implemented. The image colours are divided into three sets, the first one of these sets (S1) includes image colours greater than the average frequency of occurrence (P(S1) > ave), the second set (S2) includes image colours with the frequency of occurrence equal to average (P(S1) = ave), and the third set (S3) includes image colours with the frequency of occurrence less than average (P(S1) < ave). The difference (diff) between the frequency of occurrence of each element in the two sets (S1 and S2) and the average frequency of occurrence (ave) is calculated.

The next step is done by implementing XOR operators between a number of elements of (S1) and (S3). The number of elements chosen to implement the XOR operators from these two sets equal (diff) times and is chosen randomly. The address of the element (S3) and the result of the XOR process will be saved in a text file for use in the decryption process. The resulting image is the desired encrypted image with an absolute uniform histogram and perfect information entropy. The text file will be encrypted using powerful text encryption methods such as AES, DES, and RSA before being sent to the recipient.

After implementing XOR operations between each element in the (S1) set and the corresponding element in the (S3) set, the values of the (S1) elements will change to be the same as the values of the corresponding (S3) elements. The creation of the text file is important to save essential information on the XOR process implementation. This information is important for the decryption process of the EPVQ Method. The text file must include the addresses of S1 elements that underwent the EPVQ process and the results of the XOR operation.

3.4 Decryption process

The proposed image encryption system consists of confusion, diffusion, and EPVQ. The process of plain image encryption starts with confusion and the output of this method (confused image) is used as the input for the diffusion method. The output of the diffusion method (diffused image) is used as the input for the EPVQ Method. The decryption process starts from the final method (EPVQ Method), then the diffusion method, and the confusion method. Figure 13 illustrates a general flowchart for the decryption process.

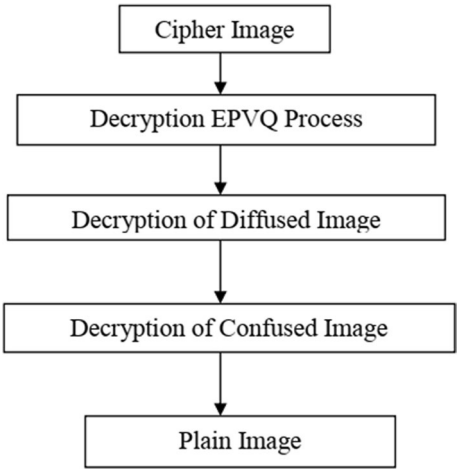


Fig. 13 General Flowchart of Decryption Process

Therefore, the decryption process is done by implementing the three processes discussed in the following sections.

3.4.1 EPVQ decryption process

The first step in the decryption process for the ciphered image is the implementation of XOR operators between the results of the EPVQ process and the pixel value located at the address saved in a text file.

3.4.2 Decryption process for diffused image

After performing the decryption process for the EPVQ method the output image must be the same as the diffused image. The first step in the decryption of a diffused image is the generation of a random key using as inputs the same initial keys and control parameters used in the generation of a random key for the image diffusion process explained in 3.3.1.1. After generating the random key, the process of internal interaction between image pixels will be reversed by implementing XOR operators between successive (in reverse of the random order) rows in the diffused image, starting with implementing XOR operators between the first row and the last row of the random order. The result of the XOR process will be saved in the first row. The second process is done by conducting the same process between the last row and the second to last row. The result is saved in the last row. The XOR process will be continued until the first and first rows. Operations between these two rows and their result will be saved in the second row.

XOR operations will be done to successive rows as mentioned above in the same order (according to the random numbers) as the first round of the XOR process. The second round is implemented the same as the first round on the image resulting from the first round. Finally, an XOR operator is performed between the resulting image and the random key matrix generated to recover the image that was used as the input for the diffusion method (confused image).

3.4.3 Decryption process for confused image

The decryption process for the confused image will recover the plain image. To achieve this there are several processes that must be done. The random number generator used in the confusion method must have the same initial conditions and control parameters used to generate the same random key used in the encryption process.

The generated random key must be sorted in ascending order while keeping the old index, in addition to the new index of the sorted key. The new and old indices are used to permute the confused image by permuting the pixels of the old index to the new index. By following this process for all image pixels, the plain image will be recovered from the confused image.

4 Experimental result

In this section, the detailed results and necessary empirical preparations to verify the efficiency of the proposed methods are reported, and several methods of evaluation are used to make comparisons with recent image encryption methods. A standard image dataset was used to verify the proposed method's performance. Evaluation using image encryption methods is more complex because of parameters that control the whole image encryption framework overlap with each other to produce the desired encrypted image. To overcome this complexity methods of evaluating image encryption methods are concerned with different issues in the encryption system.

4.1 Dataset

In order to achieve the desired goals and objectives of this research, it is very important to define the research scope, which can be explained by the following points:

a) SIPI is the dataset used to test the proposed framework. This dataset contains many images that are suitable to implement the proposed system. In addition to SIPI dataset, the system performance is tested using three images taken via a mobile camera.
b) Different image sizes such as 256*256, 512*512, 1024*1024 pixels are used to test the system Grayscale and 24-bit-coloured images are also used.
c) System tests are done by implementing different performance analysis methods such as random number generating test via the US National Institute of Standards and Technology (NIST), key space and key sensitivity, image histogram analysis, Quantitative histogram analysis by variance metric, information entropy analysis, correlation between adjacent pixels by correlation function, correlation coefficient between original and encrypted images and differential analysis.

4.2 The proposed sensitive logistic map (SLM) response

The response of the proposed SLM shows significant differences between the behaviour of the original logistic map and the behaviour of the proposed SLM in Fig. 14 (a).

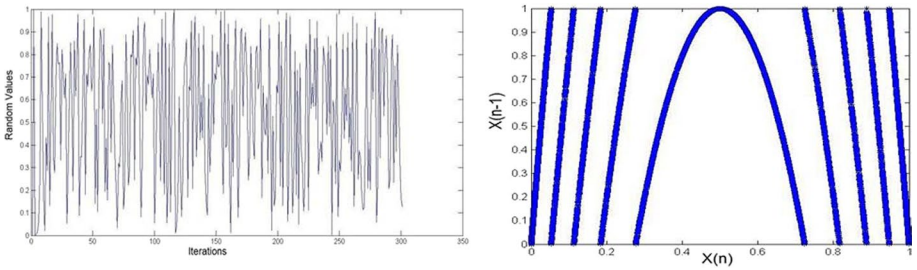


Fig. 14 (**a**) SLM Response, (**b**) SLM Cobweb Diagram

While the cobweb diagram for SLM shows the dynamical behaviour of the proposed map, Fig. 14 (b) indicates chaotic behaviour for the proposed method.

The differences in both the response, cobweb diagram of the logistic map, and SLM increase the randomness of the produced random sequences.

4.3 Extended Bernoulli map behavior

The response of Eq. (1) is shown in Fig. 15 (a) and the behaviour of the successive iteration (control parameter = 0.62) is seen in Fig. 15 (b).

In addition to increasing key space the randomness of the proposed Extended Bernoulli Map (EBM) is also increased as shown in Fig. 15(a) and Fig. 15(b).

4.4 Randomness analysis of the generated number

As illustrated in Table 1 the NIST results for the proposed random number generator for the confusion process are the best due to the using of Henon map, multi-chaotic sequences which resulted from the proposed SLM and additive white Gaussian noise.

As mentioned earlier, the proposed method proposes two random number generators. One of them is designed for the confusion process while the second one is designed for the diffusion process. NIST was implemented to evaluate the randomness of the confusion process as discussed above. The analysis of the random number generator for the diffusion process is discussed in the following paragraphs. As seen in Table 2, the proposed random

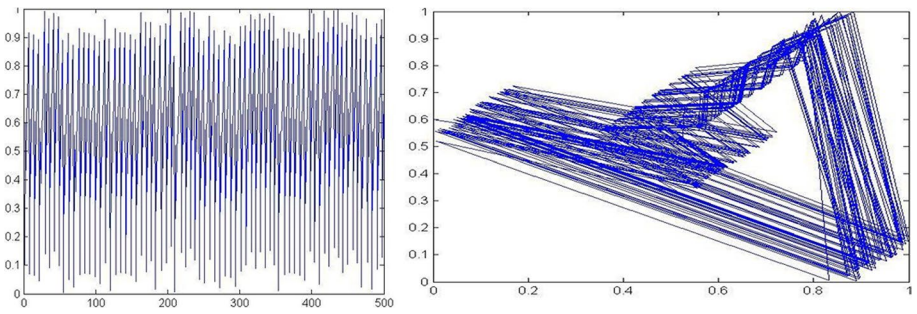


Fig. 15 (**a**) Response of Extended Bernoulli Map, (**b**) Successive Iterations Behavior of Extended Bernoulli Map

Table 1 Comparison between Proposed Random Number Generator for the Confusion Process and Two Recent Methods

Statistical test	[48]		[49]		Proposed Method	
	p value	proportion	p value	proportion	p value	proportion
Frequency	0.33	0.96	0.97	0.99	**0.98**	**0.99**
Block Frequency	0.67	0.99	0.05	0.99	**0.73**	**1.00**
Runs	0.93	0.99	0.53	1.00	**0.96**	**0.99**
Longest-Run	0.45	0.99	0.29	0.99	**0.62**	**0.99**
Binary Matrix Rank	0.16	0.99	0.96	0.97	**0.98**	**0.99**
FFT	0.19	0.99	0.38	0.97	**0.54**	**0.99**
Non- overlapping Template	0.79	0.99	N/A	N/A	**0.93**	**0.99**
Overlapping Template	0.12	0.99	0.63	0.98	**0.87**	**0.99**
Universal	0.35	0.98	0.23	0.98	**0.99**	**0.99**
Linear Complexity	0.31	0.97	0.29	0.99	**0.81**	**1.00**
Serial	0.96	0.97	0.60	1.00	**0.86**	**0.99**
Approximate Entropy	0.07	0.97	0.93	0.99	**0.97**	**0.99**
Cusum	0.73	0.97	N/A	N/A	**0.64**	**0.99**
Random Excursions	0.73	1.00	0.31	0.99	**0.95**	**0.99**
Random Excursions Variant	0.91	1.00	0.29	0.99	**0.96**	**0.99**

Table 2 Comparison between the proposed random number generator for the confusion process and two recent methods

Statistical test	[48]		[49]		Proposed Method	
	p value	proportion	p value	proportion	p value	proportion
Frequency	0.33	0.96	0.97	0.99	**0.99**	**1.00**
Block Frequency	0.67	0.99	0.05	0.99	**0.75**	**0.99**
Runs	0.93	0.99	0.53	1.00	**0.97**	**0.99**
Longest-Run	0.45	0.99	0.29	0.99	**0.67**	**1.00**
Binary Matrix Rank	0.16	0.99	0.96	0.97	**0.98**	**0.99**
FFT	0.19	0.99	0.38	0.97	**0.59**	**0.99**
Non-overlapping Template	0.79	0.99	N/A	N/A	**0.82**	**0.99**
Overlapping Template	0.12	0.99	0.63	0.98	**0.87**	**0.99**
Universal	0.35	0.98	0.23	0.98	**0.66**	**0.97**
Linear Complexity	0.31	0.97	0.29	0.99	**0.47**	**0.99**
Serial	0.96	0.97	0.60	1.00	**0.91**	**1.00**
Approximate Entropy	0.07	0.97	0.93	0.99	**0.97**	**0.99**
Cusum	0.73	0.97	0.83	0.98	**0.92**	**0.99**
Random Excursions	0.73	1.00	0.31	0.99	**0.89**	**0.99**
Random Excursions Variant	0.91	1.00	0.29	0.99	**0.94**	**0.99**

Table 3 Key Spaces for Proposed system

Chaotic Map	Number of Initial Values	Key Space (Decimal)	Key Space (Binary)
Henon	2	10^{30}	2^{100}
Amended Beroulli	2	10^{30}	2^{100}
Tinkerbell	2	10^{30}	2^{100}
Burger	2	10^{30}	2^{100}
Ricker	1	10^{15}	2^{50}
Total	9	10^{135}	2^{450}

Table 4 Comparison between the Proposed Method and Several Recent Method Based on Key Space Size

Method	Key Space Size
[51]	2^{240}
[52]	2^{448}
[53]	2^{212}
[54]	2^{167}
[55]	2^{256}
Proposed Method	$\mathbf{2^{450}}$

number generator for the diffusion process is better than the random number generator proposed by [48, 49]. Due to the proposed generating technique and the proposed EBM which produces a random sequence with high randomness criteria the proposed random number generator for the diffusion process achieves randomness criteria better than recent methods.

4.5 Key space analysis

Ideal key generators for encryption purposes should use large key spaces to ensure that brute force attacks or exhaustive attacks are not possible. Key generators with key spaces smaller than 2128 are not acceptable because they are not sufficiently secure [50]. In the proposed system six chaotic maps are used to increase the security of the key generator and the precision of each initial value is equal to (1015), therefore the key space for the proposed system can be calculated as seen in Table 3.

The length of the key space for the proposed system is 2450, which represents possible key combinations. This key space value is considered to be very large, therefore brute force attacks to break the proposed system are infeasible. The initial condition of SLM is not considered in Table 3 because this initial condition is initiated automatically using the output values from the Henon map it cannot be used as an initial condition. In addition to key space, there are numerous control parameters related to the maps used in this study, which cannot be underestimated. These control parameters will increase possible key combinations.

As it mentioned in Table 3 the key space size equal to 2450 this large key is produced from the using of five chaotic maps and four of these maps (Henon, EBM, Tinkerbell and burger maps) are consist of two initial conditions for each and the last used chaotic map (Ricker map) has one initial condition only, therefore, the algebraic summation of all of

these initial conditions will produce total key space size of 2450 possibilities. A comparison between the proposed method and several recent methods is in Table 4.

As seen from Table 4, it is obvious that the proposed image is better in terms of key space size which is produced from the using of multi-chaotic maps with one or two initial conditions for each of these chaotic maps. To verify the precision of the proposed key, key sensitivity was analyzed.

4.6 Analysis of correlation between adjacent pixels

A ciphered image can be successfully analyzed using a statistical attack. Therefore, an ideal image encryption system must be robust against this type of attack [56]. The correlation of adjacent pixels is a statistical property of a ciphered image, so cryptanalysis always tries to exploit such properties when attacking ciphered images, especially images that show obvious statistical properties. To verify the proposed method a metric was used to analyze the correlation of adjacent pixels. In plain images, the correlation of adjacent pixel values should be close to 1 while the correlation of a successfully ciphered image should be close to zero [57]. The confusion process is concerned with weakening high correlations between adjacent pixels; therefore, a good confusion process produces a ciphered image with smaller correlations between adjacent pixels. The proposed encryption system was implemented on a SIPI standard image dataset and three datasets taken from a mobile phone.

Implementing correlation equations is done by choosing 5000 pixels randomly from the image and analyzing correlations between these pixels and pixels that are located beside these pixels in the horizontal, vertical, and diagonal directions. Table 5 shows the correlation of adjacent pixels for the plain images chosen from the SIPI dataset in addition to the three images taken by a mobile camera.

Table 5 shows that the correlation for the plain image is very high because the difference between the value of pixels and the neighbour pixels is very small in smooth areas while the difference is increasing at sharp edges and it is clear that the smooth area in the used images is greater than the sharp edge, therefore, the correlation is very high (close to

Table 5 Correlation of Adjacent Pixels for Plain-Images

Image Name	Image Type	Size	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Girl	RGB	256×256	0.9893	0.9688	0.9610
Tiffany	RGB	256×256	0.9426	0.9682	0.9945
Elaine	grayscale	512×512	0.9519	0.9801	0.9724
Cameraman	grayscale	256×256	0.9682	0.9583	0.8569
Lena	grayscale	512×512	0.9785	0.9880	0.9855
Baboon	RGB	512×512	0.5119	0.6024	0.6876
Cactus	RGB	512×512	0.9763	0.9902	0.9848
Dolls	RGB	512×512	0.9847	0.9903	0.9624
City	RGB	512×512	0.9738	0.9824	0.9572
Man	grayscale	1024×1024	0.9889	0.9932	0.9789

Table 6 Correlation between the Adjacent Pixels of Encrypted Images

Image Name	Image Type	Size	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
Girl	RGB	256 × 256	0.002713	−0.000792	0.001218
Tiffany	RGB	256 × 256	−0.000982	−0.002321	0.001821
Elaine	grayscale	512 × 512	0.003541	−0.000721	0.001298
Cameraman	grayscale	256 × 256	0.00111	−0.002107	−0.007655
Lena	grayscale	512 × 512	0.000732	0.000391	0.000320
Baboon	RGB	512 × 512	0.000643	0.000433	−0.002219
Cactus	RGB	512 × 512	−0.007272	0.006551	0.002221
Dolls	RGB	512 × 512	−0.002117	0.000457	−0.002994
City	RGB	512 × 512	−0.008188	−0.002218	0.000221
Man	grayscale	1024 × 1024	0.003232	−0.000233	0.002229

one). For baboons, the correlation is relatively low because the ratio of the smooth area and the sharp edge is close to one.

Table 6 shows the correlation between adjacent pixels for the encrypted image resulting from the proposed encryption system on different RGB and grey scale images chosen from the SIPI dataset in addition to the three images taken by mobile phones. As seen in Table 6 the correlation between adjacent pixels for the encrypted image is very low due to the implementation of the proposed confusion method scrambles the image pixels randomly and the relation between the adjacent pixels in horizontal, vertical and diagonal directions is in random order because the difference is highly increases, highly decreases, slowly increases or slowly decreases.

The analysis graphs of correlations between adjacent pixels for both of the plain and encrypted images in the (horizontal, vertical and diagonal) directions are illustrated in Fig. 16 and Fig. 17.

Table 6 and Fig. 17 show that correlations between adjacent pixels of the plain image in the horizontal, vertical, and diagonal directions are very strong, while Table 7 and Fig. 17 show that after the implementation of the proposed method correlations between adjacent pixels of the encrypted image are very low. This is because each pixel in the encrypted image is surrounded by different pixels and the values of these pixels are different from

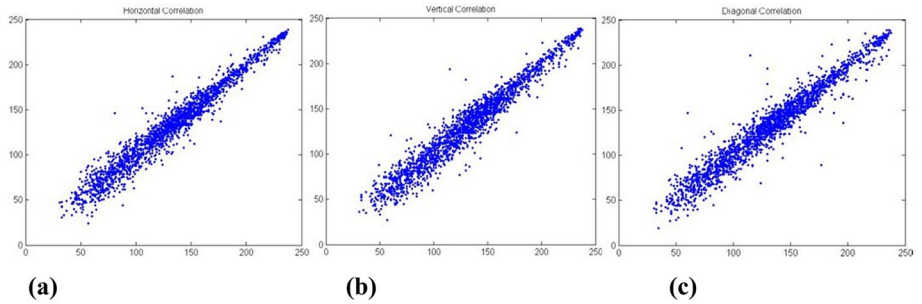


Fig. 16 Analysis Graphs of Correlations between Adjacent Pixels in Plain Image (**a**), Horizontal Direction (**b**), Vertical Direction (**c**), and Diagonal Direction

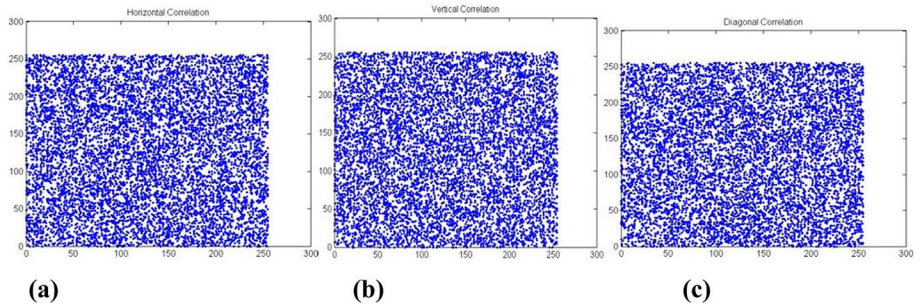


Fig. 17 Analysis Graphs of Correlations between Adjacent Pixels in Encrypted Images in the (**a**) Horizontal Direction, (**b**) Vertical Direction, (**c**) and Diagonal Direction

Table 7 Correlation Comparison between Proposed Method and Recent Methods

Method	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
[51]	0.0008	0.0021	0.0005
[52]	−0.003	−0.004	−0.009
[53]	0.0238	−0.0182	0.0073
[54]	0.0027	0.0005	−0.0045
[55]	−0.0076	−0.0034	−0.0074
Proposed Method	**0.000732**	**0.000391**	**0.00032**

each other, therefore correlation analysis shows very weak correlations between adjacent pixels resulting from the high randomness of the generated random key. To verify the new image encryption system a comparison between the results of the proposed system and the results of several recent methods is shown in Table 7.

Table 7 shows that the proposed method is better than other recent methods in terms of correlation. The image used in this comparison is a Lena 512 * 512 grayscale image. The proposed method achieves better results due to the use of a powerful random number generator in the confusion process because the random number generator plays an essential role in image encryption methods [32].

4.7 Analysis of correlation between encrypted and plain images

To analyze the proposed method and to check for correlations between the plain image and its corresponding encrypted image further analysis was implemented [52]. To perform this analysis 5000 randomly selected pixels were selected from the plain image and the ciphered image. After the selection process, a correlation evaluation was performed. Table 8 shows the correlation between the plain image and the encrypted image.

The low correlation between the plain image and the encrypted image as seen in Table 8 is achieved due to the implementation of the proposed framework. Each process in the proposed framework is responsible for the obliteration of some statistical properties of the plain image therefore the implementation of the whole framework will produce an encrypted image that is totally different from the plain image and Table 8 shows that.

Table 8 Correlation between the plain image and the encrypted image

Image Name	Image Type	Size	Correlation Coefficient
Girl	RGB	256 × 256	−0.000932
Tiffany	RGB	256 × 256	0.000372
Elaine	grayscale	512 × 512	0.00179
Cameraman	grayscale	256 × 256	−0.000826
Lena	grayscale	512 × 512	0.00244
Baboon	RGB	512 × 512	0.000933
Cactus	RGB	512 × 512	−0.000742
Dolls	RGB	512 × 512	0.00109
City	RGB	512 × 512	−0.000854
Man	grayscale	1024 × 1024	−0.000776

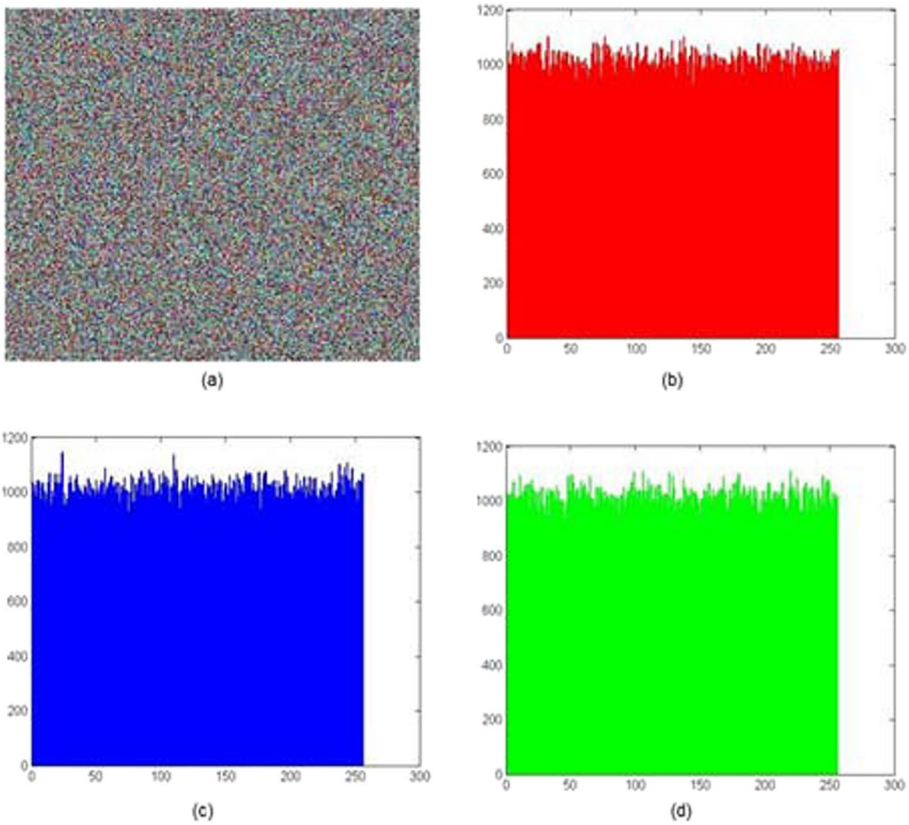


Fig. 18 (**a**) encrypted image after the diffusion process, (**b**) (**c**) (**d**) RGB histogram components for the diffused image

4.8 Histogram analysis

Cryptanalysis can exploit histograms to attack the encrypted image. Therefore, the diffusion process was used to change pixel values to alter the histogram to be resistant to statistical analysis. Image histograms after the diffusion process should be uniform to avoid possible histogram exploitation by cryptanalysis. Fig. 18 shows the histogram of the diffused image. After implementing the proposed diffusion process the produced histogram was almost uniform.

Perfect histograms for encrypted images resulted from the implementation of the proposed third process (EPVQ). This method is designed to create ideal histograms for encrypted images and the resulting histogram was uniform. Therefore, the resulting image will withstand any histogram attack. Cryptanalysis will struggle even to use histogram attacks on the encrypted image. All encrypted images that underwent the EPVQ process produced absolutely uniform histograms, which are perfect in terms of image encryption criteria. Fig. 19 shows the encrypted image and the histogram resulting from the proposed encryption system. In the image encryption literature, many image encryption methods have been proposed, all of these methods tried to produce an encrypted image with a uniform histogram, but they did not achieve this goal, unlike this study.

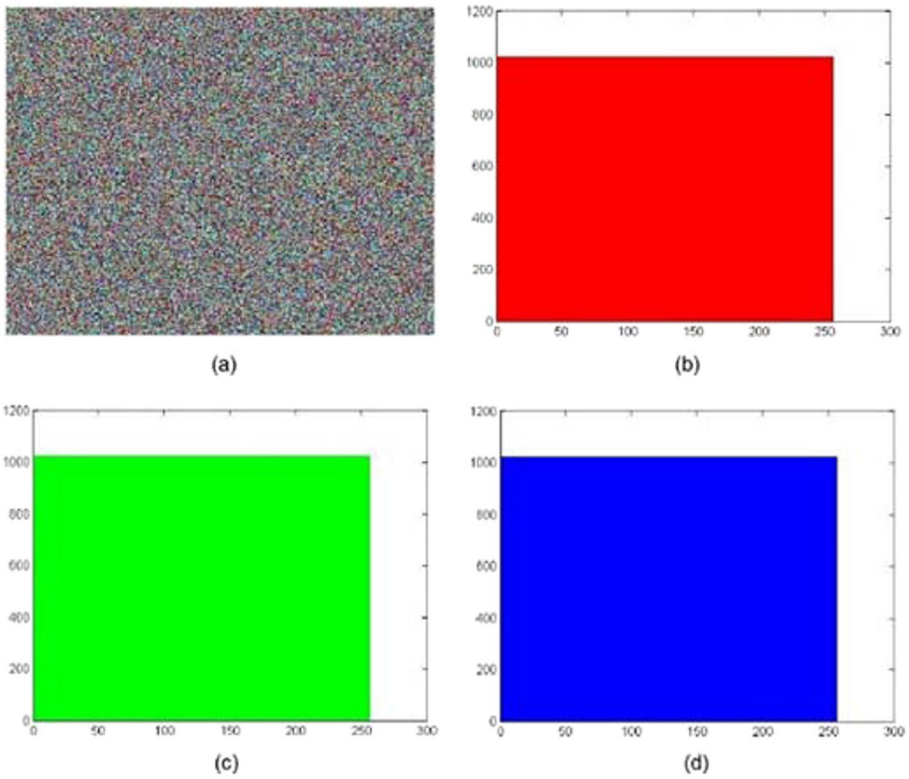


Fig. 19 (**a**) the encrypted image and (**b**) (**c**) (**d**) the RGB histograms of the encrypted image

Table 9 A Comparison between Variance of Proposed Method and Several Recent Methods

Method	[51]	[52]	[53]	[55]	Proposed Method
Variance	5118.094	977.02	5554.82	1209.4	**0**

4.9 Quantitative histogram analysis

To verify that the quantitative histogram analysis for the proposed method is better than other methods a comparison will be held with several recent methods as seen in Table 9.

The proposed method is better than all of the old methods in terms of variance results as seen in the above table because the proposed method achieves an ideal histogram, but all other methods did not achieve such a histogram.

4.10 Information entropy

In recent image encryption systems, entropy is always close to 8 but it is not equal to 8. This can be seen in Table 10.

The results for Table 10 were acquired using a grayscale Lena image with a size of 512*512 pixels using the proposed methods and other methods.

4.11 Mean squared error and peak signal to noise ratio

To measure the performance of the proposed method, Mean Squared Error (MSE) and Peak Signal Noise Ratio (PSNR) were used, which are based on the difference between the plain image and its corresponding encrypted image. To evaluate MSE and PSNR calculations were made using both plain and encrypted images. A big MSE and a small PSNR are desirable for encryption. The evaluation results for MSE and PSNR are shown in Table 11.

Table 10 Results of the Information Entropy Test using Different Methods

Method	[51]	[52]	[53]	[54]	[55]	Proposed method
Average Entropy	7.9994	7.8198	7.9992	7.9972	7.9872	**8.0**

Table 11 MSE and PSNR results for the proposed method

Image Name	Image Type	Size	MSE	PSNR
Girl	RGB	256 × 256	12,748	7.07
Tiffany	RGB	256 × 256	9274	8.45
Elaine	grayscale	512 × 512	8679	8.74
Cameraman	grayscale	256 × 256	13,418	6.85
Lena	grayscale	512 × 512	13,728	8.19
Baboon	RGB	512 × 512	7984	8.95
Cactus	RGB	512 × 512	6816	9.79
Dolls	RGB	512 × 512	8567	8.80
City	RGB	512 × 512	10,332	7.98
Man	grayscale	1024 × 1024	9924	8.16

Table 12 A Comparison of MSE and PSNR for the Proposed Method and Some Recent Methods

Method	MSE	PSNR
[58]	9595	8.31
[55]	9551	8.33
[53]	9465	8.37
Proposed Method	**9864**	**8.19**

To verify the proposed method in terms of the MSE and PSNR results, Table 12 illustrates a comparison of the proposed method with several recent image encryption methods.

In Table 12, both of the proposed methods and other recent methods used a grayscale Lena image with a size of 512*512 pixels. Table 11 and Table 12 show that the MSE and PSNR of the proposed framework achieve good results and it is better than the current methods MSE indicates the difference between the plain image and the encrypted image and the largest value is better. PSNR indicates the similarity between plain image and encrypted image the smallest value is better in results because it means the similarity is at a minimum.

4.12 Differential attack

In successful image encryption methods, the difference between plain images and their corresponding encrypted image should be great as as possible. To verify the proposed method resistance against differential attacks was evaluated. Cryptanalysis tries to make slight changes to the plain image to notice changes in the encrypted image to find a pattern that can be used to attack the encrypted image, therefore if one minor change in the plain image leads to an encrypted image with large differences differential attacks are useless [19]. The Number of Changing Pixel Rate (NPCR) and the Unified Averaged Changed Intensity (UACI) techniques were used to analyze the security of the image encryption methods in terms of differential attacks. A comparison between the proposed method and recent methods is shown in Table 13. This comparison shows that the results for the proposed method are better than the results of t other recent methods in terms of differential attack resistance.

All data shown in Table 13 resulted from the implementation of encryption processes using a grayscale 512*512 Lena image. Table 12 and Table 13 show good results in terms of withstanding differential attack and show that the proposed method is better than other methods for hindering such attacks. NPCR reflect the ratio of the pixels affected by tiny changes in the plain image the ratio is >99 which means more than 99% of image pixels

Table 13 NPCR and UACI Comparison between the Proposed Method and Recent Methods

Method	NPCR	UACI
[51]	99.63	33.59
[52]	99.60	28.62
[53]	72.24	20.06
[54]	99.61	28.60
[55]	99.69	33.50
Proposed Method	**99.83**	**34.10**

are changed when a small change is made to the plain image while UACI reflect the average of the effect of this change to all image pixels.

4.13 Overall discussion

The experimental results presented in Section 4 demonstrate the effectiveness of the proposed image encryption framework in terms of randomness, key space, correlation, histogram analysis, information entropy, mean squared error (MSE), peak signal-to-noise ratio (PSNR), and resistance to differential attacks. Collectively, these findings underscore the robustness and security of the encryption scheme in safeguarding image data.

The randomness analysis confirms the superior performance of the random number generator, ensuring unpredictability and resistance to brute force attacks. The large key space size makes exhaustive key search attacks impractical, bolstering the security of the system. Additionally, the low correlation between adjacent pixels and uniform histograms prevent adversaries from exploiting statistical properties of the images for cryptanalysis.

The high entropy values indicate the randomness and disorderliness of the encrypted data, making it challenging for attackers to extract meaningful information from the ciphertext. Moreover, the competitive performance in terms of MSE and PSNR demonstrates that the encryption scheme effectively preserves image quality while maintaining security.

Furthermore, the high resistance to differential attacks, as evidenced by the NPCR and UACI values, ensures the integrity of the encrypted images. Overall, the proposed method excels in providing robust security measures without compromising image quality.

To sum up, the comprehensive evaluation demonstrates the efficacy of the proposed image encryption framework for secure image transmission and storage. With its strong randomness, large key space, low correlation, uniform histograms, high entropy, and resistance to differential attacks, the proposed method is well-suited for various applications, including medical imaging, military communications, and multimedia content protection. Further research could focus on real-time implementation optimizations, scalability, and investigating potential vulnerabilities to enhance the security of the framework even further.

5 Conclusion and future work

In summary, our study demonstrates that achieving an ideal secrecy system in cryptography can be realized through the integration of the Error Propagation Vector Quantization (EPVQ) method alongside the conventional confusion and diffusion processes. The proposed framework yields promising results in terms of histogram and information entropy for the ciphered image, while also significantly enhancing various statistical properties such as correlation between adjacent pixels, variance, Mean Squared Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). The Secure Logistic Map (SLM) and Enhanced Bit Manipulation (EBM) methods contribute to improving key security by expanding the key space size while maintaining key sensitivity. Additionally, the proposed Iterative Image Improvement Process (IIIP) method addresses vulnerabilities to differential analysis attacks. Our framework deviates from conventional image encryption frameworks by incorporating three processes-confusion, diffusion, and EPVQ-instead of the typical two. The proposed confusion process mitigates high correlations

between adjacent pixels, the diffusion process enhances resistance against differential attacks, and EPVQ idealizes the security properties of the encrypted image.

Today, image encryption is paramount, particularly in critical fields, and many researchers are striving to develop encryption frameworks that produce images with highly secure criteria. While our study achieved perfect results in some criteria and very good results in others, there is still room for improvement. To further optimize correlation criteria, we suggest exploring the additional process proposed in this study, which involves carefully selecting two values for XOR operations to achieve ideal correlation results.

Furthermore, investigating new chaotic maps with large key space requirements is crucial to avoid complexity when using large keys. Current methods often focus on combining multiple chaotic maps to create large key spaces, which can increase computational overhead. Exploring alternative chaotic maps with inherent large key space properties could streamline the encryption process and improve efficiency in handling large keys.

Abbreviations

AES: Advanced Encryption Standard; AWGN: Additive White Gaussian Noise; EBM: Extended Bernoulli map; EPVQ: Equal quantization of image pixel values; SLM: Sensitive logistic map; IIIP: Internal Interaction between Image Pixels; DES: Data Encryption Standard; RSA: Rivest, Shamir, and Adelman Cryptosystem; SBLP: Spatial bit-level permutations; DT-CWT: Dual-tree complex wavelet transformations; TRGN: True Random Number Generator; PRNG: Pseudo Random Number Generator; NPCR: Number of changing pixel rate; UACI: Unified averaged changed intensity; XOR: Exclusive OR

Symbols

E : Encrypted Image; F : Encryption Function; I: Plain Image; (x,y): Spatial Coordinates; Cor : Correlation of Adjacent Pixels; Cov: Image Covariance; M,N: Dimension of Image; CC : Correlation Coefficient between encrypted and plain images P(mi) possibility of occurrence; r : Control Parameter of logistic map; H : Information Entropy; a,b : Control Parameters for Hénon Map; o : Standard Deviations; μ : Average of Noise; N(x,y) : Additive White Gaussian Noise

Funding This paper received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest We certify that there is no actual or potential conflict of interest in relation to this manuscript.

References

1. Munir R (2012) Robustness analysis of selective image encryption algorithm based on Arnold cat map permutation. In: Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics
2. Patel KD, Belani S (2011) Image encryption using different techniques: A review. Int J Emerging Technol Adv Eng 1(1):30–34
3. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108
4. Chen C et al (2013) Improvement of trace-driven I-cache timing attack on the RSA algorithm. J Syst Softw 86(1):100–107
5. Coppersmith D (1994) The data encryption standard (DES) and its strength against attacks. IBM J Res Dev 38(3):243–250
6. Ismail IA, Amin M, Diab H (2010) A digital image encryption algorithm based a composition of two chaotic logistic maps. Int J Netw Secur 11(1):1–10
7. Jolfaei A, Mirghadri A (2010) An image encryption approach using chaos and stream cipher. J Theor Appl Inf Technol 19(2):117–125
8. Alsafasfeh QH, Arfoa AA (2011) Image encryption based on the general approach for multiple chaotic systems. J Sig Inf Process 2(3):238–244
9. Liu L, Miao S (2016) A new image encryption algorithm based on logistic chaotic map with varying parameter. SpringerPlus 5(1):1–12
10. Nesakumari GR, Maruthuperumal S (2012) Normalized image watermarking scheme using chaotic system. Int J Inf Netw Secur 1(4):255
11. Han, S.-S. and L.-Q. Min, A colour image encryption scheme based on generalized synchronization theorem. 2014.
12. Sankpal PR, Vijaya P (2014) Image encryption using chaotic maps: a survey. In: 2014 fifth international conference on signal and image processing. IEEE
13. Al-Maadeed S, Al-Ali A, Abdalla T (2012) A new chaos-based image-encryption and compression algorithm. J Electr Comput Eng 2012
14. Khalique A, Lone AH, Ashraf SS (2015) A Novel Unpredictable Temporal based Pseudo Random Number Generator. Int J Comput Appl 117(13)
15. Behnia S et al (2008) A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons Fractals 35(2):408–419
16. Roohi L, Ibrahim S, Moieni R (2013) Analysis of Statistical Properties of Chaos based Image Encryption by Different Mappings. Int J Comput Appl 62(20)
17. Chandra S et al (2014) A comparative survey of symmetric and asymmetric key cryptography. In: 2014 international conference on electronics, communication and computational engineering (ICECCE). IEEE
18. Min L, Lu H (2010) Design and analysis of a novel chaotic image encryption. In: 2010 second international conference on computer modeling and simulation. IEEE
19. Pareek, N.K. (2012) Design and analysis of a novel digital image encryption scheme. https://arxiv.org/abs/1204.1603.
20. Divya V, Sudha S, Resmy V (2012) Simple and secure image encryption. Int J Comput Sci Issues 9(6):286
21. El-Deen A, El-Badawy E, Gobran S (2014) Digital image encryption based on RSA algorithm. J Electron Commun Eng 9(1):69–73
22. Feruza YS, Kim TH (2007) IT security review: privacy, protection, access control, assurance and system security. Int J Multim Ubiquit Eng 2(2):17–32

23. McCumber J (1991) Information systems security: A comprehensive model. In: Proceedings 14th National Computer Security Conference
24. Wylie JJ et al (2000) Survivable information storage systems. Computer 33(8):61–68
25. Stoyanov B, Kordov K (2015) Image encryption using Chebyshev map and rotation equation. Entropy 17(4):2117–2139
26. Cherkaoui A et al (2013) A very high speed true random number generator with entropy assessment. In: International conference on cryptographic hardware and embedded systems. Springer
27. Lynnyk V, Čelikovský S (2010) On the anti–synchronization detection for the generalized Lorenz system and its applications to secure encryption. Kybernetika 46(1):1–18
28. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28(4):656–715
29. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons Fractals 21(3):749–761
30. Liu, R. and X. Tian, New algorithm for colour image encryption using chaotic map and spatial bit-level permutation. 2012.
31. Jain A (2016) Pixel chaotic shuffling and Arnold map based image security using complex wavelet transform. J Netw Commun Emerg Technol 6(5):8–11
32. Stojanovski T, Kocarev L (2001) Chaos-based random number generators-part I: analysis [cryptography]. IEEE Trans Circuits Syst I Fundam Theory Appl 48(3):281–288
33. Rukhin A et al (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-allen and hamilton inc mclean va
34. Yang K et al (2014) 16.3 a 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS. In: 2014 IEEE international solid-state circuits conference digest of technical papers (ISSCC). IEEE
35. Shankar S, Udupi V (2015) A dynamic security protocol for face recognition systems using seismic waves. Int J Image Graph Signal Process 7(4):28
36. Fan G et al (2015) On the impacts of mathematical realization over practical security of leakage resilient cryptographic schemes. In: International conference on information security practice and experience. Springer
37. Belazi A et al (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50
38. Guesmi R et al (2016) Hash key-based image encryption using crossover operator and chaos. Multimed Tools Appl 75(8):4753–4769
39. Bashardoost M et al (2014) A novel approach to enhance the security of the LSB image steganography. Res J Appl Sci Eng Technol 7(19):3957–3963
40. Norouzi B et al (2014) A novel image encryption based on hash function with only two-round diffusion process. Multimedia Systems 20(1):45–64
41. Wang J (2016) Digital image encryption algorithm design based on genetic hyperchaos. Int J Op 2016
42. Hu F et al (2017) Batch image encryption using generated deep features based on stacked autoencoder network. Math Probl Eng 2017
43. Wu H, Preneel B (2007) Differential cryptanalysis of the stream ciphers Py, Py6 and Pypy. In: Annual international conference on the theory and applications of cryptographic techniques. Springer
44. Kumar M et al (2016) Intertwining logistic map and cellular automata based colour image encryption model. In: 2016 international conference on computational techniques in information and communication technologies (ICCTICT). IEEE
45. Suri S, Vijay R (2016) An implementation and performance evaluation of an improved chaotic image encryption approach. In: 2016 international conference on advances in computing, communications and informatics (ICACCI). IEEE
46. Munir R (2012) Security analysis of selective image encryption algorithm based on chaos and CBC-like mode. In: 2012 7th international conference on telecommunication systems, services, and applications (TSSA). IEEE
47. Li S, Sun W (2016) Image encryption performance evaluation based on poker test. Adv Multimed 2016
48. Hanis S, Amutha R (2018) Double image compression and encryption scheme using logistic mapped convolution and cellular automata. Multimed Tools Appl 77(6):6897–6912
49. Jallouli O et al (2016) An efficient pseudo chaotic number generator based on coupling and multiplexing techniques. In: International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2016)
50. Janke W (2002) Pseudo random numbers: generation and quality checks. Lect Notes John von Neumann Inst Comput 10:447

51. Enayatifar R et al (2017) Image encryption using a synchronous permutation-diffusion technique. Opt Lasers Eng 90:146–154
52. Choi J et al (2016) A fast ARX model-based image encryption scheme. Multimed Tools Appl 75(22):14685–14706
53. Bashir Z, Rashid T, Zafar S (2016) Hyperchaotic dynamical system based image encryption scheme with time-varying delays. Pac Sci Rev A: Nat Sci Eng 18(3):254–260
54. Kulsoom A, Xiao D, Abbas SA (2016) An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. Multimed Tools Appl 75(1):1–23
55. Kar M et al (2016) Bit-plane encrypted image cryptosystem using chaotic, quadratic, and cubic maps. IETE Tech Rev 33(6):651–661
56. Su Y et al (2017) Cascaded Fresnel holographic image encryption scheme based on a constrained optimization algorithm and Henon map. Opt Lasers Eng 88:20–27
57. Jain Y et al (2016) Image encryption schemes: a complete survey. Int J Signal Process Image Process Pattern Recog 9(7):157–192
58. Gu G et al (2016) A chaotic-cipher-based packet body encryption algorithm for JPEG2000 images. Signal Process Image Commun 40:52–64
59. Jumiawi WA, El-Zaart A (2022) Otsu Thresholding model using heterogeneous mean filters for precise images segmentation. In: 2022 international conference of advanced Technology in Electronic and Electrical Engineering (ICATEEE). IEEE, pp 1–6
60. Nyo MT, Mebarek-Oudina F, Hlaing SS, Khan NA (2022) Otsu's thresholding technique for MRI image brain tumor segmentation. Multimed Tools Appl 81(30):43837–43849
61. Mundada K, Kulkarni J (2023) MRI image-based automatic segmentation and classification of brain tumor and swelling using novel methodologies. Int J Image Graph 31:2450051
62. Yesmin T, Lohiya H, Acharjya PP (2023) Detection and segmentation of brain tumor by using modified watershed algorithm and Thresholding to reduce over-segmentation. In: 2023 IEEE international conference on contemporary computing and communications (InC4), vol 1. IEEE, pp 1–6

Authors and Affiliations

Hoshang Kolivand[1,2,3] · Sabah Fadhel Hamood[4] · Shiva Asadianfam[5] · Mohd Shafry Mohd Rahim[4] · William Hurst[6]

✉ Shiva Asadianfam
sh_asadianfam@yahoo.com

Hoshang Kolivand
h.kolivand@ljmu.ac.uk

Mohd Shafry Mohd Rahim
shafry@utm.my

William Hurst
will.hurst@wur.nl

[1] School of Computer Science and Mathematics, Faculty of Engineering and Technology Liverpool John Moores University (LJMU), L3 3AF, Liverpool, UK

[2] School of Computing and Digital Technologies, Staffordshire University, Stoke-on-Trent, UK

[3] Bharath Institute of Higher Education and Research, Chennai, India

[4] MAGICX (Media and Games Innovation Centre of Excellence), Institute of Human Centred Engineering, Universiti Teknologi Malaysia, 81310 Johor, Malaysia

[5] University of Bonab, Bonab, Iran

[6] Wageningen University and Research, Wageningen, The Netherlands