IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 25, 2019, accepted June 28, 2019, date of publication July 16, 2019, date of current version August 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2929244

A Selective Image Encryption Scheme Based on 2D DWT, Henon Map and 4D Qi Hyper-Chaos

LISUNGU OTEKO TRESOR AND MBUYU SUMBWANYAMBE
Department of Electrical and Mining Engineering, University of South Africa, Johannesburg 1710, South Africa
Corresponding author: Lisungu Oteko Tresor (lisungu.tresor@gmail.com)

This work was supported by the University of South Africa (UNISA).

ABSTRACT In recent years hyperchaos has found applications in several fields such as medicine and engineering. It has been applied in image-based applications which require reliable, fast, and robust security systems to store or/and transfer images. Given the increased use of images, there is a fundamental requirement among security in ensuring protection, confidentiality, privacy, integrity, and authenticity of such images. This, in essence, has become a major concern. Many preventive and protective algorithms, including chaos-based schemes, have been developed over the past years in trying to prevent directed attacks. However, many existing chaos-based encryption schemes have been successfully decrypted. One of the main reasons for these chaos-based image encryption schemes being successfully attacked is that the degree of randomness of the chaotic system used is not high enough to guarantee robust encryption. The key space lengths of many of the existing cryptosystems are not long enough to guarantee the desired security properties of chaos-based ciphers. Thus, the security level is lowered. In this paper, a selective image encryption algorithm based on 2D Discrete Wavelet Transform, Henon's Map and 4D Qi Hyper Chaos is proposed. This paper is developed such that 2D DWT is used to decompose the image into details and approximations, Henon chaotic map is used to shuffle the decomposed image pixels' positions. The shuffled image is further encrypted with the bit streams generated by Qi hyperchaos using XOR operation. The experimental results demonstrate that the proposed algorithm provides a large key space, high security, and resistance to different types of attacks. When compared to some existing algorithms, the performance of the proposed method displays a better performance with respect to security and encryption making it suited for real-time applications.

INDEX TERMS Discrete wavelet transform (DWT), cryptography, Henon map, shuffling, chaotic system, encryption, decryption, qi hyper chaos.

I. INTRODUCTION

In chaos-based engineering, hyperchaos behavior is a chaotic behaviour with more than one positive Lyapunov exponent. Basically, such chaotic behavior has been applied in different domains such as in telecommunications, medical, engineering and other fields to achieve chaos-based image cryptosystems.

The inability of some of these chaotic systems to prevent attacks, has led to the development of more robust chaotic systems with large topological entropy. The 4D Qi hyperchaotic system, as applied in this paper, is usually characterized by large Lyapunov exponents and are not often impacted by computational parameters and numerical errors unlike most of the standard encryption techniques such as Advanced Encryption Standard (AES), the International Data Encryption Standard (IDEA), Data Encryption standard (DES) and the Rivest Shamir Adleman (RSA). With almost all the networks being interconnected and connected to the internet, different types of multimedia information including but not limited to text, image, audio, videos, etc. are being exchanged over the internet and require robust security to guarantee privacy and confidentiality. Unlike text information, images have different features such intrinsic features which may comprise of bulk volume of data, high redundancy, high correlation among adjacent pixels and low entropy compared to the text. The traditional encryption methods such as the AES, the IDEA, DES and the RSA are computationally intensive hence require more time and are not fit or suitable enough for image encryption. For these reasons, image encryption using various chaotic maps system is introduced in [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Tomasz Trzcinski.

The chaotic systems provide desirable properties of non-linear dynamical systems such as ergodicity, sensitive dependence on initial parameters and great pseudo-random properties. The randomness, correlation and complexity of the pseudorandom sequences generated by chaotic or hyper-chaotic maps provide unique cryptography properties or characteristics. Accordingly, chaotic dynamics are widely employed in the field of image encryption to provide an easy way to design cryptosystems. Generally, a good encryption algorithm should be sensitive to the cipher keys, and the key space should be large enough to resist the brute-force attacks from the attackers as posited in [2].

In recent years many chaos-based image cryptosystems have been proposed [3]–[8]. Image encryption schemes developed and implemented lately can be generally grouped into full image encryption schemes [9]–[12] and into selective (or partial) image encryption (SIE) schemes [14]–[22]. Full image encryption algorithms deal with image data, which consumes much time and resources and may not be appropriate for real-time applications. Selective image encryption techniques offer significant savings in terms of computational time and cost. This is done by encrypting the significant part of the original image [23].

The general concept of selective image encryption consists of separating the image content into two parts. The first part is the public part; it is left unencrypted and made accessible to all users. The second part is the protected part; it is the part that is encrypted. Only authorized users will be granted access to the protected part. One important suggested feature in selective encryption is to make the protected part very small in size as much as possible [24], [25].

The main motivation of selective encryption is to reduce the amount of data to encrypt, hence helping to reduce the computational time for real-time applications while achieving a required level of security. One of most important features of selective encryption is to preserve some functionalities of the original image such as scalability.

In frequency domain, low frequency coefficients contain most of the data of the image and high frequency coefficients contain the fine points [26]. Thus, when only few low frequency coefficients are encrypted instead of the whole frequency domain, it offers some advantages of reduced redundancy. This will lead to easy recognition of the critical part to be encrypted and the less important part not compressible [27].

To provide satisfactory balance between security and speed [28], many algorithms have been used that were encrypting only selective pixels or coefficients of the image [29], [30]. Most of them used methods such as wavelet transform. Wavelet transform has the advantages of decomposing the image into different levels [31]. The levels contain sub-bands which consist of coefficients that describe the horizontal and vertical spatial frequency characteristics of the original image. In this paper, a selective image encryption algorithm is proposed. It is based on two-level DWT to obtain the LL2 component followed by pixel shuffling using Henon chaotic map to achieve the image pixel positions permutation. Then the bit streams generated by the Qi Hyper-chaos are used to encrypt the shuffled image so as to complete the encryption process.

The remainder of this paper is structured as follows. In section II, related work is briefly presented. Discrete Wavelet Transform, Henon chaotic map and Qi Hyper-chaos system are introduced in section III. Proposed image encryption algorithm is presented in section IV. In section V, the experimental results are presented. Security analysis is presented in section VI. Finally, the conclusion is presented in section VII.

II. RELATED WORK

This section provides an overview of previous studies on chaos-based image encryptions systems. There are various ways to achieve a desired security level when using chaos for image encryption. Some authors have developed image encryption algorithms where the desired security level was achieved by either making use of higher dimensional hyper-chaotic map [in this instance see 40] or by cascading multiple chaotic systems [32] or by coupling mutliple chaotic systems [32], [34], [2]. For better results, chaotic Maps usually require a lager parameter space so as to enhance the security of the encrypted image. But even when using chaotic maps that have small parameter space, security can also be improved by either modifying its equation by the means of some iterations or by completing solid and proper confusion and diffusion process. Thus, several algorithms have been developed in the past years which make use of multiple keys to generate either the same chaotic map or multiple chaotic maps. This is normally done so as to achieve multi-level encryption and in so doing enhancing the security of the schemes proposed [36], [13], [38], [39].

For example, in [5], Wu *et al.* make use of the chaotic tent maps (CTM) combined with the rectangular transform (RT) for the design of the image encryption algorithm. The algorithm is made of an n number of image pixel permutation rounds and followed by a layer of pixel-diffusion. An enhanced two-dimensional rectangular transform is used to achieve the image pixel permutations, while the chaotic temt maps control the pixel diffusion layer. Others such as Li *et al.* [4] used a 5D hyperchaotic system for the generation of the pseudorandom numbers used for the encryption. To enhance the security of the cryptosystem, pixel-level permutation, bit-level permutation and diffusion stages were implemented.

More than the 5D which was used by Li et al., Sun *et al.* (as proposed in [37]) made use of a 7D hyperchaotic system to design the cryptosystem which provided a large key space rending the security level very high. However, the author focused more on the encryption only and gave less importance to the computational load if heavy images were to be used. In [59], Matondo and Qi proposed a selective encryption technique using the 4-D Qi hyper-chaotic system. The authors proposed a two-level encryption algorithm

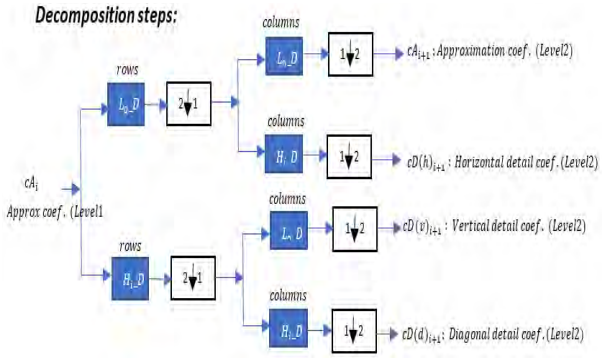


FIGURE 1. DWT image decomposition process.

where the first level was achieved using Discrete Cosine Transform (DCT) coefficients on the frequency domain and the second level was achieved by image pixel shuffling using Qi Hyperchaos. In essence, selective encryption seems to be like the ultimate solution in reducing the amount of data that needs to be encrypted, thus improving, not only the computational time, but also improving the bandwidth utilization for images set for transmission.

III. THEORETICAL FRAMEWORK

The proposed image encryption is based on Discrete Wavelet Transform (DWT) to extract the Low-Low frequecy component (LL2) of the image in the frequency domain, Henon Chaotic Map is used to shuffle the image pixels positions in the spatial domain so as to achieve the first level of encryption. Then, the keys generated by 4D Qi Hyper-chaos is XORed with the shuffled image to complete the encryption. We briefly introduce the background of some of the terms used in this paper.

A. DISCRETE WAVELET TRANSFORM

In DWT, wavelets are discretized using wavelet scales and translations. Both frequency and time domains are captured as suggested in [40]. By performing the discrete wavelet transform (DWT) on the image I, at each level, four sub-images are obtained, which include low pass samples and high pass samples. The low pass samples (sub-band LL) represent the low-resolution approximation of the original image and the other three sub-bands are made of the coefficients of the wavelet decomposition and contain the insignificant details in the approximation. A two-dimensional DWT leads to a decomposition of approximated coefficients at level i into four components: the approximation at level $i+1$, and the details in three orientations (horizontal, vertical, and diagonal) [31]. Fig.1 illustrates the basic discrete wavelet decomposition steps of an image.

DWT has the advantage of reducing the correlation between the adjacent pixels and provides multi scale sparse representation of the image. The sub-bands obtained for two-level wavelet decomposition by applying power complementary low pass and high pass filters, are low-low (Sub-band LL), high-low (Sub-band HL), low-high (Sub-band LH), and high-high (Sub-band HH). Most of the image energy is concentrated in LL component [41].

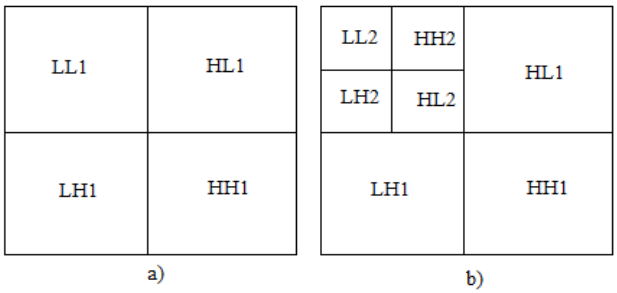


FIGURE 2. Wavelet decomposition (a) one level decomposition; (b) two levels decomposition.

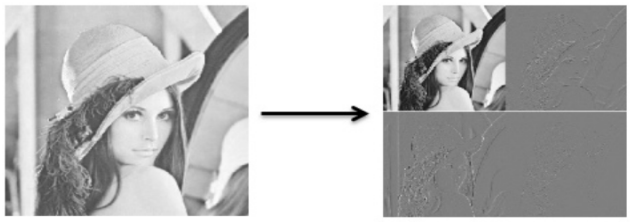


FIGURE 3. One level decomposition.

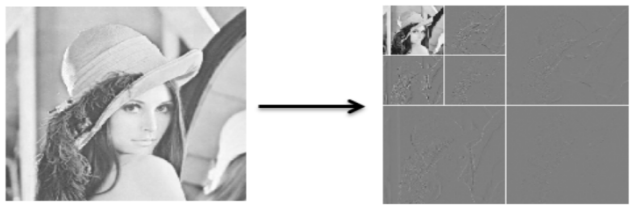


FIGURE 4. Two-level decomposition.

Fig.2 shows the sub-bands obtained after the discrete wavelet decomposition. The sub-bands LL1, HL1, LH1 and HH1 are obtained after the first level decomposition. In the second level decomposition, the sub-image LL1 is further decomposed into four components LL2, HL2, LH2 and HH2.

In spatial domain, the correlattion of the values of adjacent pixels is really high, therefore redundant. As part of the selective encryption that needs to be achieved, the image size has to be reduced by eliminating redundancies that exist among adjacent pixels using DWT. Fig.3 and Fig.4 show, respectively, one level decomposition and two-level decomposition of the Lena image.

The use of the 2D-DWT to convert the image samples into a more compressible form helps to provide image scalability. Thus, the JPEG 2000 standard suggests the use of wavelet transform instead of Discrete Cosine Transform (DCT) because Discrete Wavelet transform offers a better rate/distortion (R/D) performance than the traditional DCT.

B. HENON CHAOTIC MAP

Henon map appears to be one of the most studied examples of the discrete time dynamical systems that exhibit chaotic

behaviour. Henon chaotic map [42], [2] was first discovered in 1978. It is described and represented by the following two-dimensional map with quadratic non-linearity.

$$x_{i+1} = 1 - ax^2 + y_n$$
$$y_{i+1} = bx_n \quad (1)$$

The map depends on two parameters,a and b. For the classical Henon map, the sytem is chaotic when the values of a and b are respectively 1.4 and 0.3. For other values of a and b different from 1.4 and 0.3 respectively, the map may be chaotic, intermittent, or may converge to a periodic orbit. In our scheme, the two variables, a=1.4 and $b = 0.3$, of the Henon chaotic map are adopted to shuffle the image. The pixel shuffling is achieved to permute the position of pixels of the image so that they cannot be detected by the attackers, by creating a random vision in the mind of the attackers. The new pixel values are now stored in a new array.

C. QI HYPERCHAOS

Special chaos properties like wide band spectrum, ergodicity, non-periodic waveform, random-like behavior and easy implementation make the use of chaos attractive candidate for data security [43], [44]. The Qi hyper-chaos as proposed in [45] has two positive Lyapunov exponents of more than 13 and 3 which in essence indicate that the system is highly random; in addition the system has several parameters indicating large key space in chaos-based cryptography. In this study, the Qi hyper chaos was used to generate pseudo random numbers is given as shown in Eq. (2).

$$\dot{x}_1 = a(x_2 - x_1) + x_2x_3$$
$$\dot{x}_2 = b(x_2 + x_1) + x_1x_3$$
$$\dot{x}_3 = -cx_3 - ex_4 + x_1x_2$$
$$\dot{x}_4 = -dx_4 + fx_3 + x_1x_2 \quad (2)$$

For the proposed scheme, the controlling parameters values have been selected as follows: a, b ł R: (a, b) |49≤a≤55; 20≤b≤24, c = 13, d = 7.8, e = 35 and f = 29. The Qi Hyperchaos system has two large positive Lyapunov exponents. The system is hyperchaotic and has Lyapunov exponents of more than 13 and 3 respectively, which makes the system highly random. The system is still hyperchaotic for the values of b, c, d, e and f different from the ones we selected for our study. The frequency spectrum of Qi Hyper chaos is 20 times wider than the ordinary chaotic system and most existing hyperchaotic systems [45]. The hyperchaos is very sensitive to initial condition and its attractors have very irregular forms, neither butterfly nor scroll ones, which are visually very complex as shown in Fig.5.

The initial conditions of $x_0(0) = [-2.510\ 10.3215\ -8\ -7.8]$ and $x_0'(0) = [-2.515\ 10.3215\ -8\ -7.8]$ are the conditions used to plot respectively the states of x_2 and x_2'. Noticeable, is the fact that there is just a slight difference between plotting the conditions of x_2 , $x_1(0) = -2.510$ and plotting x_2', $x_1(0) = -2.515$ with the initial conditions and control parameters unchanged.

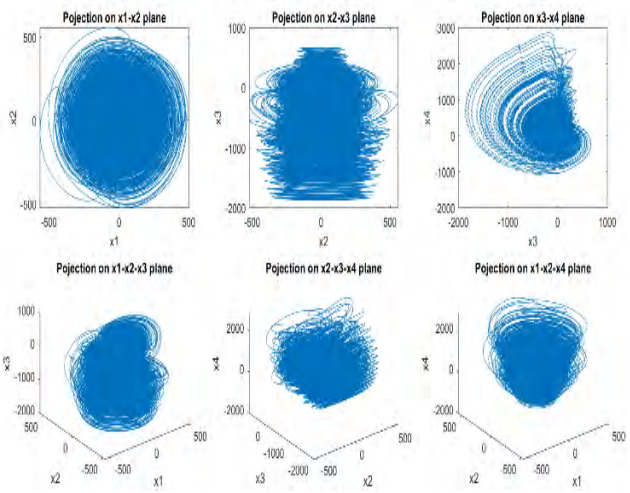


FIGURE 5. Qi's hyper-chaotic attractor.

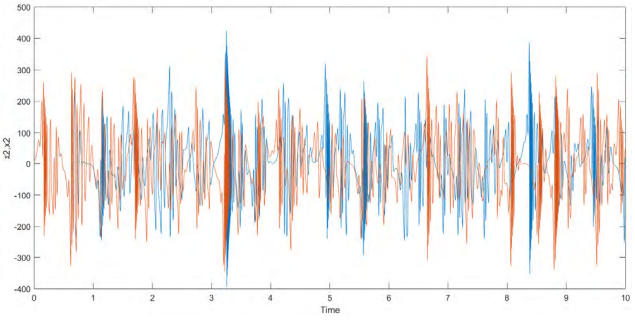


FIGURE 6. Time response of states x_2 and x_2' of Qi Hyper-chaos with slight difference in initial conditions.

Fig.6 demonstrates how sensitive the Qi Hyperchaos system is sensitive to initial conditions and also to the output keys to be used in the encryption process. A slightly different set of initial conditions than the ones used for the encryption process will lead to the image not being decrypted as depicted in Fig.15.

D. KEY VALUES GENERATION

The first phase of the encryption is achieved by carrying out the image pixel shuffling using Henon Map. The key k is used to encrypt the shuffled LL_2 image sub-band; pseudorandom numbers $x_1(i)$ are generated from Qi Hyper- chaos, where $i = 1, 2, 3, \ldots\ldots, n$. n is equal to the coefficient number of the shuffled image. The binary matrices K are obtained by transforming the pseudorandom sequence of $x_1(i)$ as in Eq. (3).

$$K = dec2bin\left(Abs\left(10^4 x_1(i)\right)\right) mod 256 \quad (3)$$

IV. IMAGE ENCRYPTION ALGORITHM

Each enciphering transformation E_K is defined by a specific enciphering algorithm E , which is common to every transformation in the system, and a key K , which distinguishes it from the other enciphering transformations. Similarly, each

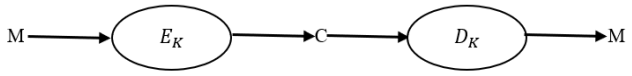


FIGURE 7. Typical Cryptographic system.

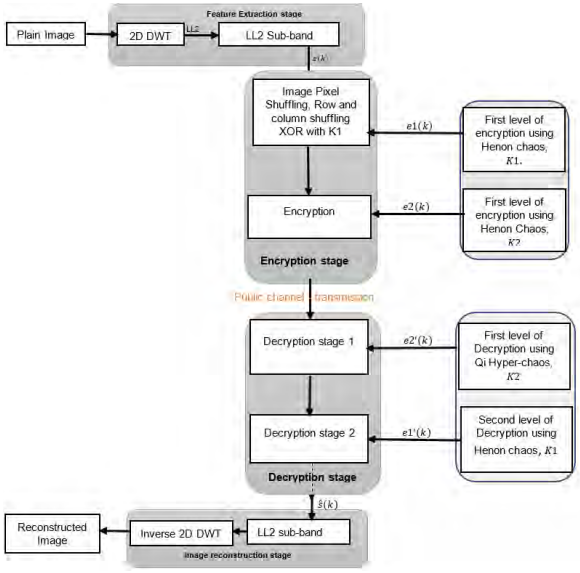


FIGURE 8. Block diagram of the proposed encryption algorithm.

deciphering transformation is defined by a specific deciphering algorithm D and a key K . For a given K, D_K is the inverse of E_K ; that is, $D_K\,(E_K(M)) = M$ for every plaintext message M which can be a text, an image or an audio. In a given cryptographic system, the transformations E_K and D_K are described by parameters derived from K (or directly by K). The set of parameters describing E_K are called the enciphering key, and the set of parameters describing D_K, are the deciphering key.

Fig.7. illustrates the enciphering and deciphering process of data. Cryptosystems must satisfy three general requirements [46]:

1. The enciphering and deciphering transformations must be efficient for all keys.

2. The system must be easy to use.

3. The security of the system should depend only on the secrecy of the keys and not on the secrecy of the algorithms E or D .

A. PROPOSED IMAGE ENCRYPTION ALGORITHM

In this study, secret sequences and keys are generated using 4D Qi hyper-chaos. Henon's chaotic map is used for shuffling the pixels of the LL_2 image before being encrypted with the keys generated by Qi Hyper-chaos system using XOR operation to complete encryption process. The complete image encryption consists of the steps as shown in Fig.8.

The main steps of the developed algorithm are described as follows;

1. Read a plain image of jpg, png or tif format, of $M \times N$ dimension as an input.

Algorithm 1 Image Pixel shuffling Algorithm

Input: $I(m, n)$, of dimension MxN,
0<m≤ M and 0<n≤ N
Define the initial conditions, a=1.4 and b=0.3
Define the number of iteration N_iteration=256
Output: *Ishuffled(I(m,n)), of dimension MxN*
0<m≤ M and 0<n≤ N
for k from 1 to N_iteration
for i from 1 to m
for j from 1 to n
r = mod([round(abs(1-(a∗(i^2))+j)),
round(abs(b∗i))],[m n]);
x(i,j)=I(r(1)+1,r(2)+1);
end
end
Ishuffled = x;
end

2. One component of the input image (grey scale) is used.
3. Two-Level DWT is applied to the grey image to obtain the Low-Low Component (LL_2) of the image.
4. **Algorithm1**: Shuffling of pixels of the LL_2
5. image is done using the Henon's chaotic map to obtain the shuffled image with a number of iterations, n=256. Generation of the pseudo-random or key values numbers from Henon Map and the 4D Qi Hyper-Chaos system. The sequence generated is converted into decimal sequences. $K = K_1, K_2$ the family of keys used for the first level and second level of encryption.
6. The first level of encryption is achieved by combining the shuffled image with K_1 using the XOR operation to obtain *Ishuffled_enc1*.
7. The diffusion process is accomplished Exclusive OR operation and is achieved by bit-by-bit between the key's values generated by Qi Hyper chaos values and the matrix of the first level encrypted image, *Ishuffled_enc1* to obtain E.
8. Cipher image is completed successfully, and encryption process is over.

$$E = XOR(K; I) \tag{4}$$

where I = *Ishuffled,, Ishuffled_enc1*, the image matrix to be encrypted, $K = K_1, K_2$ are the family of keys used for the first level and second level of encryption and E is the encrypted image.

The inverse of the encryption rules is applied to the cipher image to recover the original image. As in a symmetric encryption, the same keys used in the encryption should be used to successfully decrypt the image.

V. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

A. HISTOGRAM ANALYSIS

Image histogram illustrates that the distribution of the pixels of the image by plotting the values of pixels. For a

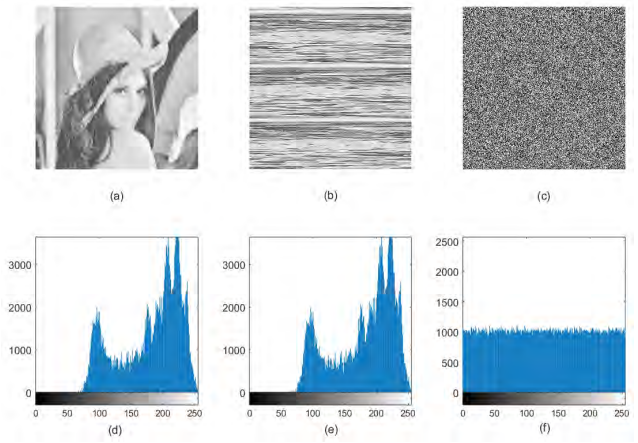


FIGURE 9. (a) Plain Image, (b) Shuffled image and (c) Ciphered Image, (d) Histogram of plain image, (e) Histogram of Shuffled image and (f) Histogram of ciphered image.

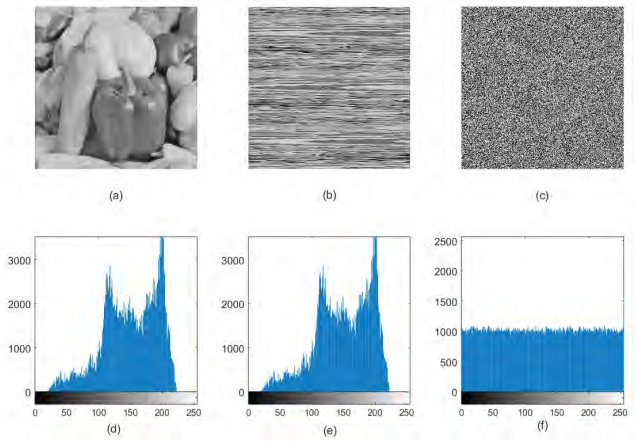


FIGURE 10. Peppers image: (a) Plain Image, (b) Shuffled image and (c) Ciphered Image, (d) Histogram of plain image, (e) Histogram of Shuffled image and (f) Histogram of ciphered image.

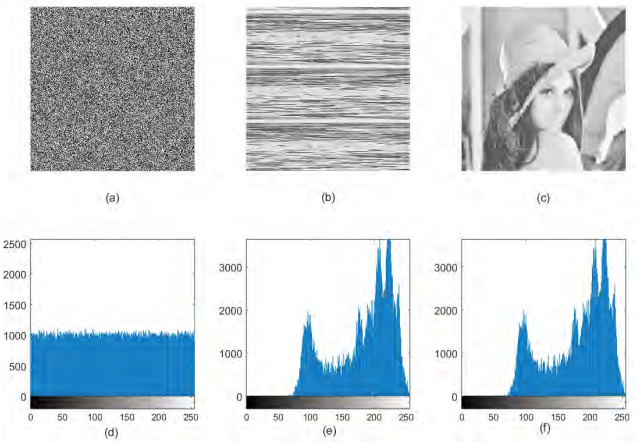


FIGURE 11. Lena image: a) Ciphered Image, (b) Shuffled image after Decryption and (c) Original image (decrypted image), (d) Histogram of the ciphered image, (e) Histogram of decrypted shuffled image and (f) Histogram of the decrypted image.

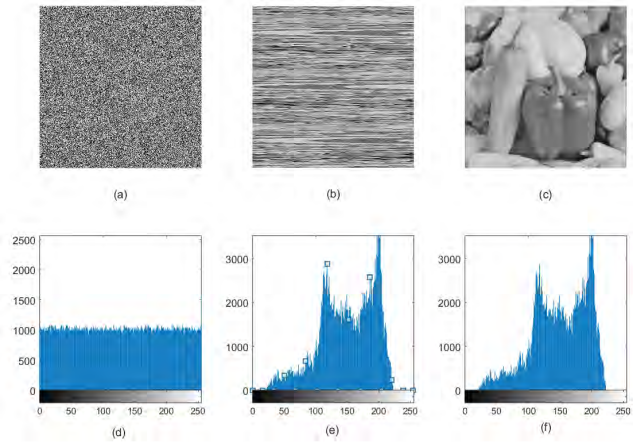


FIGURE 12. Peppers image: (a) Ciphered Image, (b) Shuffled image after Decryption and (c) Original image (decrypted image), (d) Histogram of the ciphered image, (e) Histogram of decrypted shuffled image and (f) Histogram of the decrypted image.

highly secure encryption algorithm, the histogram plot of the ciphered image should display an ideal uniformity of intensity. Fig. 9(c) and Fig. 10(c) show that the ciphered image has uniform histogram, random-like distribution and appears totally different from the histogram of plaintext image. Hence, it does not provide any useful information to the attackers to perform any type of statistical attack on the encrypted image.

The Henon shuffled histogram's distributions for both Lena and Peppers image appear closer to the origin when compared to the original image histogram distribution. This is an indication of selective encryption achieved using the 2D-DWT where the image content to be encrypted is just a part of the total image content.

Fig. 11 and Fig. 12 show the decryption results related to the images and their histogram representations at different levels of the decryption process.

A good enciphering transformation should guarantee both the encryption and the decryption when the same set of keys are used. It should be extremely sensitive to the secret keys used in both the encryption and decryption processes.

B. COEFFICIENT CORRELATION ANALYSIS

The correlation coefficients, Cr , of adjacent pixels (x, y) of the original image and the encrypted images are calculated using the following equation:

$$Cr = \frac{N\sum_{j=1}^{N}(x_j X y_i) - \sum_{j=1}^{N} x_j X \sum_{j=1}^{N} y_j}{\sqrt{N\sum_{j=1}^{N}(x_j^2 - (\sum_{j=1}^{N} x_j)^2) X (\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \tag{5}$$

In Eq. (4) x and y are the value of two adjacent pixels and N is the total number of the selected image pixels used for calculation.

Fig. 13 and Fig. 14 show the correlation coefficients of two adjacent pixels in the original image, in the shuffled

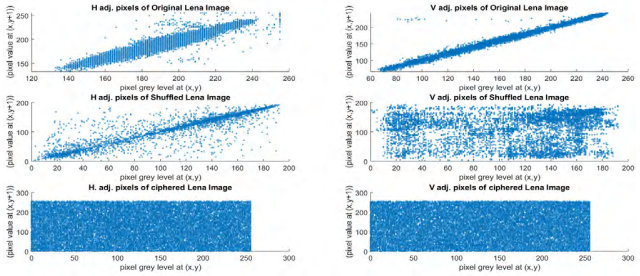


FIGURE 13. Lena image: Horizontal and Vertical Correlation coefficients of Two adjacent pixels distribution for plain Lena image, Shuffled Lena image and cipher Lena image.

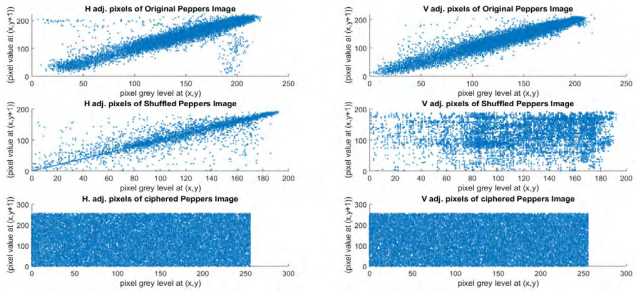


FIGURE 14. Horizontal and Vertical Correlation coefficients of Two adjacent pixels distribution for plain Peppers image, Shuffled Peppers image and cipher Peppers image.

TABLE 1. Correlation coefficients of adjacent pixels.

Image	*Direction of Adjacent pixels*	*Plain-Image*	*Shuffled image*	*Ciphered-Image*
Lena (512x512)	Vertical	0.9707	0.1469	-0.0019
	Horizontal	0.9946	0.9841	0.0105
	Diagonal	0.9721	0.1606	-0.0019
Tiger (225x225)	Vertical	0.9576	0.2592	-0.0041
	Horizontal	0.9803	0.9772	0.0040
	Diagonal	0.9682	0.2201	-0.0046
Peppers (256x256)	Vertical	0.9655	0.1257	0.0010
	Horizontal	0.9364	0.9658	0.0044
	Diagonal	0.9564	0.1221	-0.0006

image and in the ciphered image for Lena and Peppers images respectively.

Table 1. shows the correlation coefficients of adjacent pixels of Lena.jpg, Tiger.jpg and peppers.tif images.

The results from Fig. 13, Fig. 14 and Table 1 show that the correlation coefficients of adjacent pixels of the cipher images of different sizes and formats is significantly reduced after the encryption process based on Qi Hyper- chaos and is very small close to 0. It can be concluded that the proposed algorithm could effectively resists statistical attacks.

C. KEY SPACE ANALYSIS

It is a basic requirement to have the key space of the chaotic or hyperchaotic map used to design a crytosytem large enough in order to resist against the brute force attack. From a security standpoint, the size of the key space should not be smaller than 2^{100} to provide a high level of security [48], [60]. The key space of the Qi based cryptosystem consists of four initial conditions $x_1(0), x_2(0), x_3(0), x_4(0)$ and the controlling parameters a, b, c, d, e, f .

When a and b are in the range: $49 \leq a \leq 55$; $20 \leq b \leq 24$, the system remains a hyper chaotic even when the values of the parameters c, d, e and f can vary in a large space.

If we consider the precision of initial values being 10^{14}, the Qi Hyper system has 6 parameters and 4 initial conditions, which translate the key space to being at least $10^{14\,x(number\ of\ parameterst\ number\ of\ initial\ condtions)} = 10^{140} \sim 2^{465}$. For instance, the system proposed in [49] has a key space of 2^{232} . The result show that Qi Hyper-chaos has more than 2^{100} which is the bear minimum key space for good encryption, and it is larger than most security chaos algorithms. It has large enough security level against brute force attacks. This is one of the reasons why the proposed scheme is good enough to be used for the image encryption.

In Table 2, the study compares the proposed schemes with the existing ones and the results show that Qi Hyper-chaos has a very large key space.

TABLE 2. Key space analysis of different systems.

Method	Proposed	Ref. [60]	Ref. [32]	Ref .[57]	Ref. [35]	Ref. [49]
Key Space	2^{465}	2^{256}	2^{256}	2^{199}	2^{128}	2^{232}

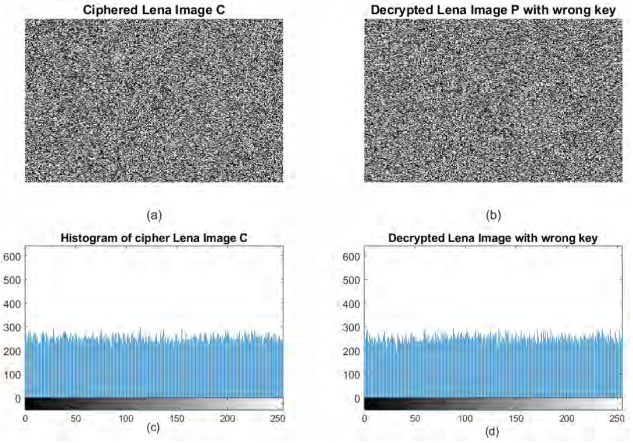
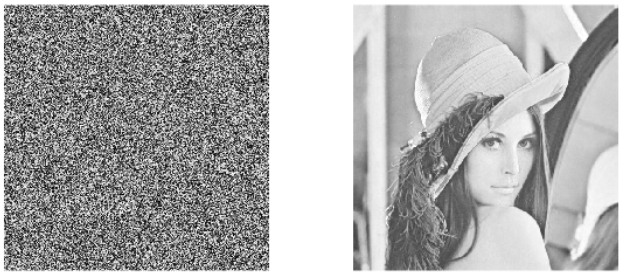


FIGURE 15. Key sensitivity test, a) cipher image, b) decrypted image using keys slightly different from that in encryption, (c) Histogram of the ciphered image and (d) Histogram of the image decrypted with a slightly different key.

D. KEY SENSITITY ANALYSIS

A secure image encryption should be very sensitive to the secret key; decrypting a ciphered image with slightly different secret keys than the one used for the encryption of the original image should not result in the original image. The encrypted image is decrypted with a slight difference in the initial condition $x_1(0)$. Fig.15 (a) depicts the encrypted image with initial condition $x_1(0) = -2.510$ and Fig. 15 (b) shows



(a) (b)

FIGURE 16. Key sensitivity test, a) cipher image, b) decrypted image using the same key as used in encryption.

TABLE 3. Information entropy of cipher images.

Image	*Lena*	*Tiger*	*Cameraman*	*Peppers*
Entropy	7.9987	7.9982	7.9986	7.9979

the decrypted image with a slight difference key in the initial condition where $x_1(0) = -2.515$ instead of $x_1(0) = -2.510$ considered in the encryption process, with the remaining of initial conditions and control parameters remaining unchanged. Obviously, the decrypted image does not recover the original one. However, if the same key used for the encryption is to be used to decrypt the ciphered image, the image will be recovered as shown in Fig. 16.

The chaotic systems are extremely sensitive to the initial conditions and control parameters. Meaning a small change in the main key will result in different outputs. The decrypted image will not be identical to the original image if there is a slight change in the major key ([48], [49]).

E. INFORMATION ENTROPY ANALYSIS

Entropy is one the most important statistical measure of randomness of cryptosystem. The mathematical expression of entropy H(m) is defined as follows:

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \times \log_2\left(\frac{1}{p(m_i)}\right) \quad (6)$$

where is the probability of occurrence of symbol (mi), N is the total number of symbol m and $log2$ denotes that the entropy values are represented in bits. For a true random source that emits 2^8 symbols, its ideal entropy value is $H(m) = 8$. The value of entropy for Lena ciphered image calculated using Eq. 5 is 7.9987. This means that the ciphertext image is very close to a true random source and shows that the proposed scheme has resistance against entropy attack.

Table3. summarizes the entropy information of different images using the proposed encryption algorithm and the results show that the obtained entropy values averaging 7.9983 are close to the ideal value (E=8).

The results of Information Entropy of the proposed scheme, display a better performance when compared with some methods previously developed [4], [5], [8], [37].

TABLE 4. Information entropy comparison with other algorithms.

Scheme	*Proprosed*	*Ref. [37]*	*Ref. [5]*	*Ref. [8]*	*Ref. [4]*
Entropy	7.9983	7.9980	7.997287	7.902512	7.9970

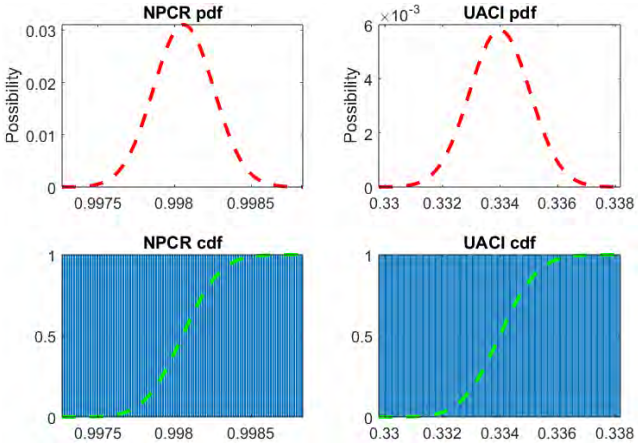


FIGURE 17. NPCR and UACI distribution for 512 x 512 Lena images.

F. DIFFERENTIAL ATTACK ANALYSIS

To test the impact of one-pixel change on the whole image encrypted by the proposed algorithm, two common metrics, NPCR and UACI, are often used. NPCR means the change rate of the number of pixels of ciphered image while one pixel of plain image is changed. UACI stands for the unified average changing intensity and measures the average intensity of the differences between the plain-image and ciphered image. NPCR can be calculated as ([51], [52]):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{WxH} x100\% \quad (7)$$

UACI is used to find the impact of one-pixel alteration, a significant modification in the encryption image because of a little alteration in original image. UACI can be measured as ([53], [55], [56]):

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{E_1(i,j) - E_2(i,j)}{255}\right] x100\% \quad (8)$$

The fig.16 shows the distribution of the NPCR and UACI of Lena 512x512 images.

Table 5. provides the NPCR and UACI values for different keys generated from Qi Hyperchaos applied on Lena, Tiger and Cameraman images.

The greater the value of NPCR and UACI, the better the encryption algorithm. The mean values of the NPCR and UACI tests for the images are shown in Table. 5 which are close to the ideal values [54]. Therefore, it can be said that the proposed encryption algorithm has high key sensitivity.

TABLE 5. NPCR and UACI tests results for lena.jpg, Tiger.jpg and Cameraman.tif images.

Image	Lena.jpg (512x512)		Tiger.jpg (225x225)		Cameraman.tif (225x225)	
Keys	Key1	Key2	Key1	Key2	Key1	Key2
NPCR %	99.81	99.81	99.59	99.58	99.63	99.57
UACI %	33.40	33.39	33.48	33.48	33.48	33.48

Table.5 shows the NPCR and UACI test results of different images of different sizes when Key1 and Key2 are used for the encryption.

The average for different images, that is, the NPCR and UACI values in [4], are 99.61% and 33.46%, and in 99.62% and 33.53% in [37] respectively. The values of NPCR and UACI in our proposed method are 99.70% and 33.44%. The NPCRs and UACIs are shown in Table 5 for different images and for different keys. The results show that the proposed scheme in this paper can resist differential attacks.

VI. CONCLUSION

In this paper, an efficient new image encryption algorithm based on hyper-chaos is presented; the two-level discrete wavelet decomposition of the original image is applied followed by the Henon chaotic map to shuffle the pixels positions of the LL2-image. The bit streams generated by Qi hyper-chaos is used to change the grey values of the shuffled image using XOR operation. The security analysis of the proposed scheme has been conducted through various differential and statistical tests. The choice of Qi Hyper-chaos system for the proposed algorithm was because it is hyperchaotic and has two large positive Lyapunov exponents more than 13 and 3 respectively, which makes the system orbital degree of disorder and randomness very high.

The experimental results demonstrate that the proposed scheme displays a very good image encryption performance. The proposed scheme has a large key space and is very sensitive to initial conditions and controlling parameters used for the secret keys. Also, it can resist different types of attacks such as entropy attack and differential attack. Thus, providing a high security level. When compared with some schemes previously proposed by other authors, in most areas of the image encryption security and performance assessment, the proposed method displays a better performance. In our future work, we will include a compression stage to the proposed scheme in order to handle larges images and especially videos, adding some complexity into our enciphering transformation approach.

REFERENCES

[1] M. R. C. Mansi, "An audio multiple shuffle encryption algorithm," *Int. J. Eng. Comput. Sci.*, vol. 4, no. 9, pp. 14098–14104, Sep. 2015.

[2] L. Guo-Hui, Z. Shi-Ping, X. De-Ming, and L. Jian-Wen, "An intermittent linear feedback method for controlling henon-like attractor," *J. Appl. Sci.*, pp. 288–290, Dec. 2001.

[3] G. Alvarez, P. Montoya, G. Pastor, and M. Romera, "Chaotic cryptosystems," in *Proc. IEEE 33rd Annu. Int. Carnahan Conf. Secur. Technol.*, Oct. 1999, pp. 332–338.

[4] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

[5] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[6] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[7] L. Guo, J. Li, and Q. Xue, "Joint image compression and encryption algorithm based on SPIHT and crossover operator," in *Proc. 14th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP)*, Chengdu, China, Dec. 2017, pp. 185–188.

[8] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.

[9] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons Fractals*, vol. 38, no. 1, pp. 213–220, 2008.

[10] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Opt. Commun.*, vol. 1282, no. 11, pp. 2123–2127, 2009.

[11] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "A novel image cipher based on mixed transformed logistic maps," *Multimedia Tools Appl.*, vol. 56, no. 2, pp. 315–330, 2012.

[12] Y. Liu, S. Tian, W. Hu, and C. Xing, "Design and statistical analysis of a new chaotic block cipher for wireless sensor networks," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 8, pp. 3267–3278, 2012.

[13] K. Prabhavathi, C. P. Sathisha, and K. M. Ravikumar, "Region of interest based selective medical image encryption using multi Chaotic system," in *Proc. Int. Conf. Elect., Electron., Commun., Comput., Optim. Techn. (ICEECCOT)*, Mysuru, India, Dec. 2017, pp. 1–5.

[14] W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "A novel selective image encryption method based on saliency detection," in *Proc. Vis. Commun. Image Process. (VCIP)*, Chengdu, China, Nov. 2016, pp. 1–4.

[15] H. Qiu, N. Enfrin, and G. Memmi, "A case study for practical issues of DCT based bitmap selective encryption methods," in *Proc. 3rd Int. Conf. Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Shanghai, China, Oct. 2018, pp. 1–7.

[16] A. Kaur and G. Singh, "A random selective block encryption technique for secure image cryptography using blowfish algorithm," in *Proc. 2nd Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Coimbatore, India, Apr. 2018, pp. 1290–1293.

[17] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption DWT-based algorithm for medical images," in *Proc. 14th Int. Conf. Comput. Graph., Imag. Vis.*, Marrakesh, Morocco, May 2017, pp. 79–84.

[18] T. Xiang, K.-W. Wong, and X. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos*, vol. 17, no. 2, 2007, Art. no. 023115.

[19] N. Tanejaa, B. Ramanb, and I. Gupta, "Selective image encryption in fractional wavelet domain," *AEU-Int. J. Electron. Commun.*, vol. 65, pp. 338–344, Apr. 2011.

[20] R. Munir, "Security analysis of selective image encryption algorithm based on chaos and CBC-like mode," in *Proc. IEEE 7th Int. Conf. Telecommun. Syst., Services, Appl. (TSSA)*, Oct. 2012, pp. 142–146.

[21] G. Bhatnagar and Q. M. J. Wu, "Selective image encryption based on pixels of interest and singular value decomposition," *Digit. Signal Process.*, vol. 22, no. 4, pp. 648–663, 2012.

[22] A. M. Yousif and M. M. Ali, "A selective image encryption based on chaos algorithm," *J. Kerbala Univ.*, vol. 11, no. 1, pp. 136–149, 2013.

[23] L. Li, Y. Yao, and X. Chang, "Plaintext-dependent selective image encryption scheme based on chaotic maps and DNA coding," in *Proc. Int. Conf. Dependable Syst. Their Appl. (DSA)*, Beijing, China, Oct./Nov. 2017, pp. 57–65.

[24] A. Ramesh and A. Suruliandi, "Performance analysis of encryption algorithms for information security," in *Proc. Int. Conf. Circuits, Power Comput. Technol. (ICCPCT)*, Mar. 2013, pp. 840–844.

[25] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J. J. Quisquater, "Overview on selective encryption of image and video: Challenges and perspectives," *EURASIP J. Inf. Secur.*, vol. 2008, Jan. 2008, Art. no. 179290.

[26] G. A. Spanos and T. B. Maples, "Performance study of a selective encryption scheme for the security of networked, real-time video," in *Proc. 4th Int. Conf. Comput. Commun. Netw.*, Las Vegas, NV, USA, Sep. 1995, pp. 2–10.
[27] W. Zeng and S. Lei, "Efficient frequency domain selective scrambling of digital video," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 118–129, Mar. 2003.
[28] Y. Miao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.
[29] L. Krikor, S. Bab, T. Ari, and Z. Shaaban, "Image encryption using DCT and stream cipher," *Eur. J. Sci. Res.*, vol. 32, no. 1, pp. 47–57, 2009.
[30] X. Liu and A. M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," in *Proc. IASTED Commun., Internet Inf. Technol. (CIIT)*, 2003, pp. 527–533.
[31] S. G. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11, no. 7, pp. 674–693, Jul. 1989.
[32] H. Zhu, Y. Zhao, and Y. Song, "2D Logistic-modulated-sine-coupling-Logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.
[33] S. Lian, G. Chen, A. Cheung, and Z. Wang, "A chaotic-neural-network-based encryption algorithm for JPEG2000 encoded images," in *Proc. ISNN*, vol. 3174, 2004, pp. 627–632.
[34] M. K. Khan and J. S. Zhang, "Investigation on pseudorandom properties of chaotic stream ciphers," in *Proc. IEEE Int. Conf. Eng. Intell. Syst.*, Apr. 2006, pp. 1–5.
[35] R. Li, Q. Liu, and L. Liu, "Novel image encryption algorithm based on improved logistic map," *IET Image Process.*, vol. 13, no. 1, pp. 125–134, 2019.
[36] M. A. Al-Khasawneh, S. M. Shamsuddin, S. Hasan, and A. A. Bakar, "An improved chaotic image encryption algorithm," in *Proc. Int. Conf. Smart Comput. Electron. Enterprise (ICSCEE)*, Shah Alam, Malaysia, Jul. 2018, pp. 1–8.
[37] S. Sun, Y. Guo, and R. Wu, "A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping," *IEEE Access*, vol. 7, pp. 28539–28547, 2019.
[38] M. A. B. Hernández, C.-S. Chen, S.-H. Tsai, and S.-Y. Li, "Authorization-sensitive image encryption based on moving shuffling in bit-level via using novel fuzzy hyperchaotic systems," in *Proc. Int. Autom. Control Conf. (CACS)*, Pingtung, Taiwan, Nov. 2017, pp. 1–6. doi: 10.1109/CACS.2017.8284237.
[39] G. S. Charan, N. K. S. S. V, K. B, V. V, and D. L. K, "A novel LSB based image steganography with multi-level encryption," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Coimbatore, India, Mar. 2015, pp. 1–5.
[40] R. C. Gonzalez and E. W. Richard, *Digital Image Processing*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2002, pp. 508–523.
[41] N. Chaturvedi and S. J. Basha, "Comparison of digital image watermarking methods DWT and DWT- DCT on the basis of PSNR," *J. Innov. Res. Sci., Eng. Technol.*, vol. 1, pp. 147–153, Dec. 2012.
[42] E. Petrisor, "Entry and exit sets in the dynamics of area preserving Hénon map," *Chaos, Solitons Fractals*, vol. 17, pp. 651–658, Aug. 2003.
[43] M. P. Kennedy and G. Kolumbán, "Digital communications using chaos," *Signal Process.*, vol. 80, pp. 1307–1320, Jul. 2000.
[44] X.-Y. Wang and X.-J. Wang, "A new chaotic encryption algorithm based on the ergodicity of chaos," *Int. J. Modern Phys. B*, vol. 25, no. 15, pp. 2047–2053, 2011.
[45] G. Qi, M. A. van Wyk, B. J. van Wyk, and G. Chen, "On a new hyperchaotic system," *Phys. Lett. A*, vol. 372, pp. 124–136, Jan. 2008.
[46] D. E. R. Denning, *Cryptography and Data Security*. Reading, MA, USA: Addison-Wesley, 1982, p. 8.
[47] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken, NJ, USA: Wiley, 1995, ch. 2, p. 15.
[48] A. H. A. E.-A. Hossam and E. H. Ahmed, "Image encryption using development of chaotic logistic map based on feedback stream cipher," in *Recent Advances in Telecommunications, Informatics and Educational Technologies: Tele-Info '14, Edute '14*, Wseas LLC Staff, Ed. Informatics and Educational Technologies, 2014.
[49] C. Guanghui, H. Kai, Z. Yizhi, Z. Jun, and Z. Xing, "Chaotic image encryption based on running-key related to plaintext," *Sci. World J.*, vol. 2014, Feb. 2014, Art. no. 490179.
[50] Y. Şekertekin and Ö. Atan, "An image encryption algorithm using Ikeda and Henon chaotic maps," in *Proc. 24th Telecommun. Forum*, Nov. 2016, pp. 1–4.
[51] J. Ahmad, S. O. Hwang, and A. Ali, "An experimental comparison of chaotic and non-chaotic image encryption schemes," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 901–918, 2015.
[52] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.
[53] K. Gupta and S. Silakari, "New approach for fast color image encryption using chaotic map," *J. Inf. Secur.*, vol. 2, no. 4, p. 139, 2011.
[54] C. Zhu, Y. Hu, and K. Sun, "New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern," *J. Electron. Inf. Technol.*, vol. 34, no. 7, pp. 1735–1743, 2012.
[55] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Phys. Lett. A*, vol. 366, nos. 4–5, pp. 391–396, 2007.
[56] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.
[57] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and S-Box," in *Proc. 6th Int. Conf. Modeling, Simulation, Appl. Optim. (ICMSAO)*, May 2015, pp. 1–6.
[58] W. Wang, H. Tan, Y. Pang, Z. Li, P. Ran, and J. Wu, "A novel encryption algorithm based on DWT and multichaos mapping," *J. Sensors*, vol. 2016, Mar. 2016, Art. no. 2646205.
[59] S. B. Matondo and G. Qi, "Two-level image encryption algorithm based on Qi hyper-chaos," in *Proc. 5th Int. Workshop Chaos-Fractals Theories Appl.*, Dalian, China, Oct. 2012, pp. 181–185.
[60] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

LISUNGU OTEKO TRESOR received the B.Tech. degree *(cum laude)* in electrical engineering from the Tshwane University of Technology and the master's (M.Tech.) degree in electrical engineering from the University of South Africa (UNISA), in 2019. His research interests include mobile networks, information security, image processing, machine learning, cloud computing, the Internet of Things, and pattern recognition. He has a strong industry experience, where he was Telecommunications Consultant in South Africa, Kenya, Nigeria, and Italy.

MBUYU SUMBWANYAMBE received the M.Eng. degree in electrical and electronic engineering and the Ph.D. degree in engineering management from the University of Johannesburg, South Africa. He is currently a Lecturer with the University of South Africa (UNISA). He has a wide range of industry and lecturing experience which he gained in South Africa and Zambia.