A Novel Image Encryption Algorithm Based on Advanced Hill Cipher and 6D Hyperchaotic System

Mohammed Naim and Adda Ali Pacha

(Corresponding author: Mohammed Naim)

Laboratory of Coding and Security of Information & University of Sciences and Technology of Oran Mohamed Boudiaf
PoBox 1505 Oran M'Naouer 31000 Algeria

Email: mohammed.naim@univ-usto.dz, adda.alipacha@univ-usto.dz

(Received Dec. 8, 2022; Revised and Accepted Aug. 1, 2023; First Online Aug. 25, 2023)

Abstract

Digital images play an important role in the Internet and network communications era. And hence how to enhance the security of images has become a very attractive and interesting topic in information security. Therefore, image encryption is an efficient technology to protect private images. To cope with this issue, this paper introduces a novel image encryption algorithm based on a combination of advanced Hill cipher and a 6D hyperchaotic system. The proposed method used the prime number 257 as a modulo, where all the zero pixels are replaced by pixels with a value of 256. Firstly, the original image is divided into four equal parts to process each part individually. Then, each part is divided into several blocks, each consisting of four pixels. Secondly, four variables of the hyperchaotic system are used to apply the permutation operation on the blocks, where each variable is used to permute one single part. Thirdly, the remaining two variables of the hyperchaotic system are used to generate the Hill matrices. Finally, each block of each part is encrypted by the Hill cipher using one Hill matrix to obtain the final cipher image. The experimental simulation and performance analysis data demonstrated that this encryption algorithm has an extremely sensitive secret key, can resist various security attacks, and performs better than several advanced image encryption algorithms.

Keywords: Hill Cipher; Hyperchaotic System; Image Encryption; Permutation

1 Introduction

With the coming of the information age, the rapid development of the Internet, and the advancement of computer technology, there are a large number of images are transmitted on the internet every day. Therefore; the image security field received a lot of attention from researchers, governments, and companies to more enhancement and development in this field [4, 5, 16, 30].

For this reason, image encryption technology has been widely used in various fields and is considered one of the most effective and used means of image information security. In the last few years, many encryption approaches have been developed to increase the level of security of image transmissions [7, 28, 29]. Classic encryption methods, such as the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), the Advanced Encryption Standard (AES), and the Rivest Shamir Adleman (RSA) are unable to meet the current image encryption requirements due to their large data volume, high redundancy, Strong correlation between pixels of the image [2, 6, 17, 27, 37].

For this purpose, many recent efficient image encryption algorithms are based on different theories and techniques, where the most popular and used method is chaos theory which has interstice characteristics such as pseudo-randomness, high sensitivity to the initial value, and unpredictability. Those characteristics make it very suitable for image encryption systems [23]. The recent works on chaotic cryptosystems are based on the classical confusion and diffusion architecture proposed by Shannon. The intrinsic characteristics of chaotic systems offer many advantages such as high speed in encryption, high-security level, low computational overheads, increased flexibility, increased modularity, and relative simplicity [12].

There are too many recent works that used the chaotic system in their proposed techniques to produce efficient encryption algorithms such as [25]. which used DNA computing and chaos to secure digital medical images. And that paper [12] used the chaotic system for the permutation operation in the compressive sensing (CS) technique. Other recent works that used chaotic systems are listed in the paper.

In many recent works, there is a combination between the chaotic systems and other known symmetric cipher systems to produce an effective image encryption algo-

rithm; one of the most known symmetric and efficient cipher systems is the Hill cipher.

Hill cipher is one of the known symmetric encryption algorithms based on linear matrix transformation which is invented by Lester Hill in 1929 [14]. The Hill cipher has many advantages such as hiding letter frequencies of the plain text, using simple matrix multiplication and inversion for enciphering or deciphering, high speed, and high throughput. Although that, some problems have been noticed in the encryption scheme. The inverse of a matrix may not exist due to which encryption will not be possible. Due to its linear nature, it succumbs to known-plaintext attacks. In the application of the image encryption algorithm, there is a setback, where it reveals certain trends and does not hide all the characteristics of the image (images with a strong correlation of adjacent pixels) [8].

For increasing the Hill cipher efficiency, several image encryption algorithms have been proposed [9, 10, 15, 18, 19, 24].

Essaid *et al.* [10] proposed an image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps. The algorithm consists of two basic processes: confusion and diffusion processes. Firstly, the confusion process is ensured by the product of a vector consisting of the key-pixel couple and a 2 ×2 Hill matrix, and the addition of another pseudo-random translation vector. While the diffusion process is ensured by a strong avalanche effect that links each encrypted pixel to its adjacent. The used chaotic sequences come from 1D chaotic maps with excellent statistical proprieties. Hraoui *et al.* [15] suggested a new cryptosystem of color images using a dynamic-chaos Hill Cipher algorithm based on the improvement of the Hill cipher by using an affine transformation applied by a three-order invertible matrix and a dynamic translation vector. Where the used vector is dynamically transformed at each iteration by an affine transformation composed of a chaotic matrix, not necessarily invertible, and a pseudo-random translation vector. Dawahdeh *et al.* [9] proposed a new image encryption technique combining an elliptic curve cryptosystem with Hill Cipher to convert Hill Cipher from a symmetric technique to an asymmetric, where the self-invertible key matrix is used to generate encryption and decryption secret key. Both sender and receiver can produce the secret key with no need to share it through the internet or unsecured communication channel. Khalaf *et al.* [18] proposed an enhancement to overcome the drawbacks of Hill Cipher by using a large and random key with a large data block, besides overcoming the Invertible-key Matrix problem. Kumar *et al.* [24] proposed a chaos and Hill Cipher-based image encryption for mammography images. The algorithm consists of a permutation and diffusion process where the input grayscale image pixel positions are permuted by using an Arnold cat map. Then, the permuted image undergoes a hill cipher (matrix multiplication) with an involuntary matrix generated from the chaotic map. Mahmoud & Chefranov [19] proposed Hill Cipher modification based on pseudo-random eigenvalues for generating a new key matrix for each plaintext block by using pseudo-random eigenvalues instead of static eigenvalues exponentiated to pseudo-random powers in the algorithm. If the sender, A, and the receiver, B, want to communicate using the algorithm, they share a secret value, SEED, that is used to generate pseudo-randomly.

Despite all previously proposed approaches, there are limitations to improving the Hill cipher. The motivation for our work is to reuse the Hill cipher in a modern fashion using new techniques while preserving the mathematical concept of the Hill cipher (using Matrix) to improve the encryption of digital images. Using the matrix in the Hill cipher to find the matrix inverse for all used matrices is our idea to reuse the Hill cipher in modern techniques. The proposed solution to avoid these limitations is the proposed new image encryption algorithm based on the advancement of Hill cipher and hyperchaotic system. As demonstrated in [1] the prime number 257 can guarantee the perfect reconstruction on the decryption side by replacing the pixel values of zero with 256.

This paper presents a novel image encryption algorithm based on a combination between an advanced Hill cipher and a 6D hyperchaotic system. To enhance the efficiency of the Hill cipher, we use the prime number 257 as a modulo and change the pixels of zero value by 256 to avoid the loss of data. The proposed encryption algorithm consists of two main processes: the confusion process and the diffusion process. The diffusion process is based on the permutation operation by using four variables of the 6D hyperchaotic system, where each variable is used to shuffle one single part. While the remaining two variables of the hyperchaotic system are used in the confusion process by applying the Hill cipher to obtain the final cipher image. In addition to digital images, the proposed algorithm is good enough for the secure encryption of satellite images too.

The remainder of the paper is organized as follows. Section 2 summarizes the preliminaries. Section 3 describes the proposed encryption algorithm in detail. The simulation results and security analyses are presented in Section 4. Finally, the conclusions are given in Section 5.

2 Preliminaries

This section introduces background knowledge on the hyperchaotic system and Hill cipher.

2.1 Hyperchaotic System

This subsection presents a 6-D hyperchaotic system that will be used in the confusion and diffusion operations in the proposed encryption algorithm. In 2020, a new 6-D hyperchaotic system is introduced by, and given by Yang

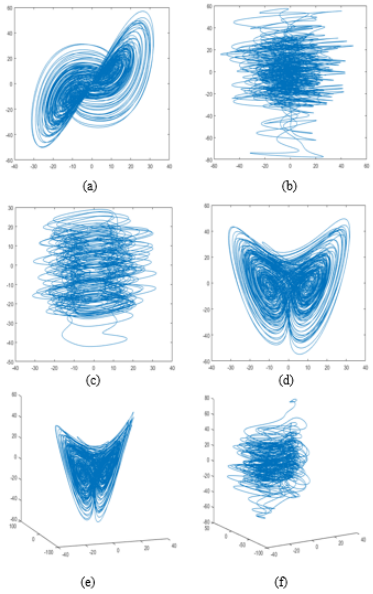

Figure 1: Phase diagram of the system: (a) x-y, (b) z-v, (c) x-w, (d) x-z, (e) x-y-z, (f) x-z-u

et al. [36], and given by

$$\begin{aligned} x' &= h(y-x)+v \\ y' &= -fy-xz+u \\ z' &= -l+xy \\ v' &= -y-w \\ w' &= ky+v \\ u' &= gx+my \end{aligned} \tag{1}$$

where $h > 0, l > 0, f, k, g$, and $m \neq 0$ are constant parameters. When $h = 10, l = 100, f = 2.7, k = 2, g = -3$, and $m = 1$; the proposed 6-D hyperchaotic system is in a hyperchaotic state, and the Lyapunov exponents for initial value (1, 1, 1, 1, 1, 1) are: $LE_1 = 1.3613, LE_2 = 0.0733, LE_3 = 0.0478, LE_4 = 0.0189, LE_5 = 0.0000, LE_6 = -14.2010$.

The phases of the 6-D hyperchaotic system are shown in Figure 1. Where Figure 1(a) represents the hyperchaotic behavior (2D) between (x and y), Figure 1(b) represents the hyperchaotic behavior (2D) between (z and v), Figure 1(c) represents the hyperchaotic behavior (2D) between (x and w), while Figure 1(d) represent the hyperchaotic behavior (2D) between (x and z), Figure 1(e) represent the hyperchaotic behavior (3D) among (x, y, and z) and Figure 1(f) represent the hyperchaotic behavior (3D) among (x, z, and u).

Compared to other chaotic systems, the proposed 6-D hyperchaotic system has the following advantages: First, four Lyapunov exponents of the 6-D hyperchaotic system are greater than zero. Second, the dynamic behavior of the 6-D hyperchaotic system (as shown above in Figure 1) is more complicated and the phase trajectories are separated in more directions. Based on these, the 6-D hyperchaotic system can improve the security of chaotic information encryption and secure communication.

2.2 Hill Cipher

Hill Cipher algorithm is one of the most famous algorithms of cryptography which is based on linear algebra. The core of the Hill cipher is matrix manipulations where the idea is a simple matrix transformation [21].

The main concept of this technique for images is based on assigning each pixel a numerical value beginning with 1 to 256 (the proposed advanced Hill cipher is based on replacing each zero-pixel value with 256). Then, the plain image is divided into blocks consisting of the same size m depending on the key matrix size mxm. After that, module 257 is taken for each block matrix element obtained by multiplication. The taken key matrix should be invertible; otherwise, decryption will not be possible.

During the inverse operation, the block matrix of the ciphered image is encrypted by the inverse of the key matrix multiplied, and finally, its module 257 is taken to obtain the original block matrix of the plain image. For example, if the block size is four ($I_{4\times1}$) then the key matrix ($K_{4\times4}$) should be of size (4×4), and the encryption process will produce a cipher text block of the image with four numerical values ($CI_{4\times1}$) as follows: For encryption,

$$\begin{aligned} \begin{bmatrix} CI_1 \\ CI_2 \\ CI_3 \\ CI_4 \end{bmatrix} &= \begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \end{bmatrix} \bmod 257 \\ &= \begin{bmatrix} (K_{11}\times I_1 + K_{12}\times I_2 + K_{13}\times I_3 + K_{14}\times I_4) \\ (K_{21}\times I_1 + K_{22}\times I_2 + K_{23}\times I_3 + K_{24}\times I_4) \\ (K_{31}\times I_1 + K_{32}\times I_2 + K_{33}\times I_3 + K_{34}\times I_4) \\ (K_{41}\times I_1 + K_{42}\times I_2 + K_{43}\times I_3 + K_{44}\times I_4) \end{bmatrix} \\ &\bmod 257 \end{aligned}$$

And for decryption, $I = K^{-1} \times CI$; where K^{-1} is the Modular Arithmetic inverse of the key matrix. $K \times K^{-1} = I$, and I is the identity matrix. The Modular Arithmetic inverse of the encryption matrix must be found. Therefore, the proposed algorithm presents the solution to find the inverse matrix always.

3 The Proposed Encryption Algorithm

In this work, we propose a new image encryption algorithm to increase encryption and transmission security. This proposed encryption algorithm is based on a combination of an advanced Hill cipher and a 6D hyperchaotic system.

3.1 The Encryption Process

Figure 2 illustrates the proposed encryption algorithm. The encryption process consists of several steps as follows:

Step 1: The original image is divided into four parts of the same size $m \times m$.

Step 2: The diffusion process (permutation operation) is applied on each part (1, 2, 3, and 4) by using four variables of the hyperchaotic system v, w, u, and z respectively, which means the permutation operation will be applied individually on each part by using one variable for each part. But the permutation operation will not permute the position of the four parts, it will permute the blocks inside each part. Because each part consists of several blocks, and each block consists of four adjacent pixels. The permutation operation is applied to change the position of each block.

Step 3: The hyperchaotic system generates six different sequences by using the initial values $x_0, y_0, z_0, u_0, v_0, and w_0$. Then, four sequences v, w, u, and z are taken to be used in the permutation operation by taking N values (where N is the number of blocks of each part) to generate four sequences V, W, U, and Z. The values of the sequences are sorted in ascending order, and the index sequences are considered as new sequences IV, IW, IU, and IZ respectively which are used for shuffling the N blocks. The new sequences are given by:

$$\begin{aligned} V &= [v_p, v_{p+1}, ...v_{p+N-1}] \\ (!, IV) &= sort(V) \\ W &= [w_p, w_{p+1}, ...w_{p+N-1}] \\ (!, IW) &= sort(W) \\ U &= [u_p, u_{p+1}, ...u_{p+N-1}] \\ (!, IU) &= sort(U) \\ Z &= [z_p, z_{p+1}, ...z_{p+N-1}] \\ (!, IZ) &= sort(Z) \end{aligned} \tag{2}$$

where p represents the starting number. The permutation operation is based on changing the positions of the blocks according to the generated index sequences to obtain the four shuffled parts.

Step 4: After the permutation operation, the vector transformation is applied on each shuffled part to obtain four different vectors $V1, V2, V3$, and $V4$.

Step 5: Each variable of the remaining two variables of the hyperchaotic system is used to generate N matrix to be used as Hill matrices ($D1$, $D2$). Each element of the used matrices is calculated by:

$$\begin{aligned} x_i &= mod(floor(x \times 10^7), 256) + 1 \\ y_i &= mod(floor(y \times 10^7), 256) + 1 \end{aligned} \tag{3}$$

$$D_1 = \begin{bmatrix} x_i & x_{i+4} & x_{i+8} & x_{i+12} \\ x_{i+1} & x_{i+5} & x_{i+9} & x_{i+13} \\ x_{i+2} & x_{i+6} & x_{i+10} & x_{i+14} \\ x_{i+3} & x_{i+7} & x_{i+11} & x_{i+15} \end{bmatrix} \tag{4}$$

$$D_2 = \begin{bmatrix} y_i & y_{i+4} & y_{i+8} & y_{i+12} \\ y_{i+1} & y_{i+5} & y_{i+9} & y_{i+13} \\ y_{i+2} & y_{i+6} & y_{i+10} & y_{i+14} \\ y_{i+3} & y_{i+7} & y_{i+11} & y_{i+15} \end{bmatrix} \tag{5}$$

Step 6: Hill cipher takes the matrix which has the highest determiner to minimize the possibility of choosing a matrix with a determiner equal to zero (in this case, the matrix is not invertible). On the other hand, if the two matrices have a determiner equal to zero, the proposed algorithm ignores these two matrices and generates another two until finding at least one matrix without a determiner equal to zero.

Step 7: The confusion process applying the Hill cipher encryption by matrix manipulations between Hill matrices and each block of the four vectors to obtain HC_1, HC_2, HC_3, and HC_4, where each block of the four vectors is encrypted with the same matrix. The obtained vectors are given as follows

$$\begin{aligned} HC_1 &= mod(HC_1, 256) + 1 \\ HC_2 &= mod(HC_2, 256) + 1 \\ HC_3 &= mod(HC_3, 256) + 1 \\ HC_4 &= mod(HC_4, 256) + 1 \end{aligned} \tag{6}$$

The main aim of using the modulo operator is to reconstruct vectors for the decryption operation.

Step 8: Finally, the obtained vectors of the previous step are combined in four parts (Ciphered parts), then the four ciphered parts are combined to obtain the final cipher image.

3.2 The Decryption Process

The decryption process is the inverse of the encryption one, where the decryption process received the secret key that is used to encrypt the original image, and it is described in the following steps:

Step 1: The cipher image is divided into four cipher parts of the same size m x m.

Step 2: Each cipher part consists of N blocks, where these blocks consist of four adjacent pixels. Then, the inverse vector transformation is applied to each cipher part to obtain four encrypted vectors.

Step 3: The inverse of Hill cipher encryption is applied to each vector by using the same inverse matrices in the encryption process.

Step 4: The matrix transformation is applied to the transformed vectors of the previous step to obtain four square parts.

Step 5: The inverse of permutation operation is applied on each part obtained in Step 4.

Step 6: The four obtained parts are combined to obtain the plain image.

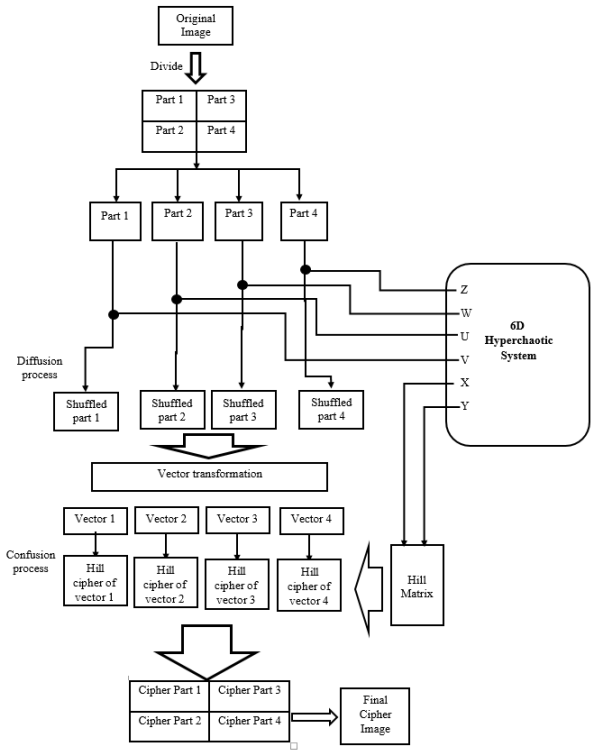

Figure 2: The proposed encryption algorithm

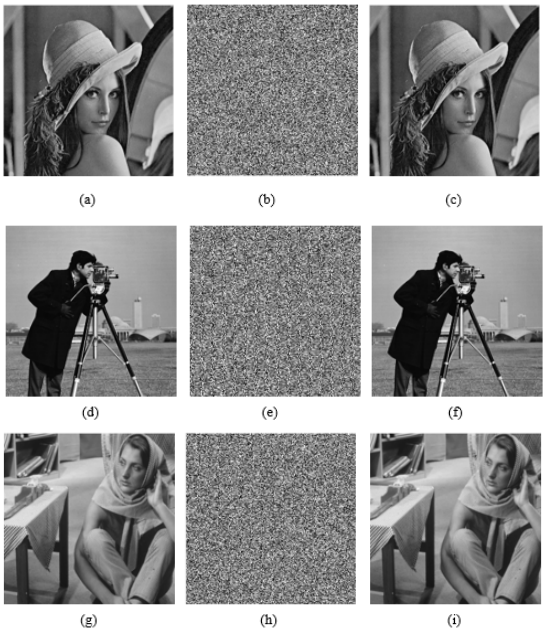

Figure 3: (a) Original image of Lena, (b) encrypted image of Lena, (c) decrypted image of Lena, (d) original image of Cameraman, (e) encrypted image of Cameraman, (f) decrypted image of Cameraman, (g) original image of Barbara, (h) encrypted image of Barbara, (i) decrypted image of Barbara.

3.3 Discussion

The proposed image encryption algorithm has the following advantages. Firstly, the proposed encryption algorithm adopts the well-known chaotic behavior by using the 6-D hyperchaotic system, which produces the desired behavior to apply in the image encryption process. Secondly, the permutation operation by the four variables of the hyperchaotic system can efficiently permute the positions of the blocks. Thirdly, the advanced Hill cipher has a high ability to encrypt and decrypt each block efficiently. Finally, the proposed algorithm has high-performance analyses and it can achieve a strong ability to resist security risks, such as differential attacks. It will be experimentally verified in Section 4.

4 The Simulation Results and Security Analyses

In this section, well-known security measures are applied to test the effectiveness of the proposed image encryption algorithm against cryptanalysis. Simulation and performance evaluation of the proposed encryption algorithm were performed on a Pentium I-3, 2.2 GHz PC with Windows 7 and 2 GB RAM. The implementation was done using Matlab 2017a software on three different images Lena, cameraman, and as shown in Figure 3. The initial parameters used in the proposed encryption algorithm to obtain the well-known hyperchaotic behavior are $x(0) = 0.25, y(0) = 0.3, z(0) = 0.5, v(0) = 0.44, w(0) = 0.06, u(0) = 0.73$.

4.1 Histogram Analysis

The histogram analysis of an image shows the distribution information of pixel values in the image by using plotting the number of observations of each brightness value. The histogram of an original image is usually unevenly distributed while it is more uniformly distributed for images encrypted by a good encryption scheme. A uniform distribution of the histogram indicates a random image and the least probability of recovering its original image and prevents the adversary from extracting any meaningful information from the fluctuating histogram of the ciphered image [31]. Figure 4 shows the histogram of the original, encrypted, and decrypted images of Lena, the cameraman, and Barbara respectively, to examine the statistical distribution by calculating and analyzing the histograms of these images.

The histogram of the ciphered images is fairly uniform and completely different from that of the plain image and decrypted one. Therefore, the proposed image encryption algorithm does not provide any clue for statistical attacks.

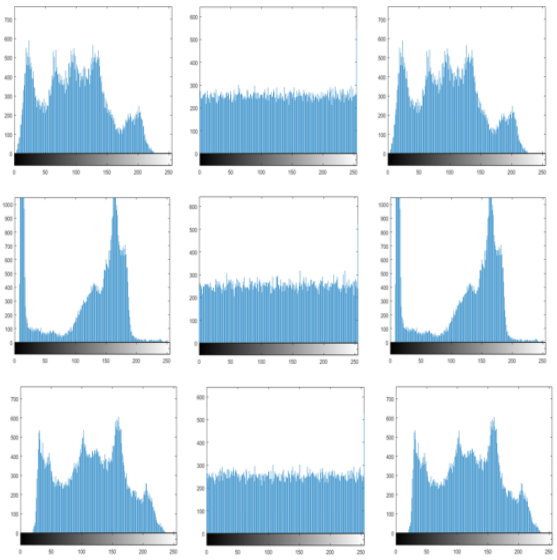

Figure 4: The histograms of Lena, Cameraman, and Barbara respectively (a) the histogram of original images, (b) the histogram of encrypted images, (c) the histogram of decrypted images

4.2 Key Space

The key space should be large enough ($>2^{100}$) to resist brute-force attacks [26]. In the proposed algorithm, the secret key includes the initial conditions of the chaotic system (x_0, y_0, z_0, v_0, w_0 and u_0). If the computing precision of the computer is 10^{-15}, the keyspace is Key $=(x(0) = 10^{15})(y(0) = 10^{15})(z(0) = 10^{15})(v(0) = 10^{15})(w(0) = 10^{15}(u(0) = 10^{15})) = 10^{90} > 2^{300} > 2^{100}$. As a result, the key space of the proposed algorithm is large enough to resist all kinds of brute-force attacks and can offer a high-security level.

4.3 Key Sensitivity Analysis

The Key sensitivity is a very essential feature for an optimal encryption system. This means that the secret key must show high sensitivity to any slight change in its values and when that happens, the encryption algorithm must produce a completely different encrypted image. The very high sensitivity to the key guarantees the security of the encryption system against attacks [20]. To test the sensitivity of the key, Lena's image is taken as the plain image and encrypted twice, one with the right secret key and the other with a tiny change (10^{-15}) in the secret key. The key sensitivity analysis results are shown in Figure 5 and Figure 6.

From Figure 5, it can be seen that the encrypted images are different when the key slightly changes. Figure 6 shows the results of the decryption process. From Figure 6, any small change in the key will result in poor decryption. Therefore, our proposed algorithm is very sensitive to the key in both encryption and decryption

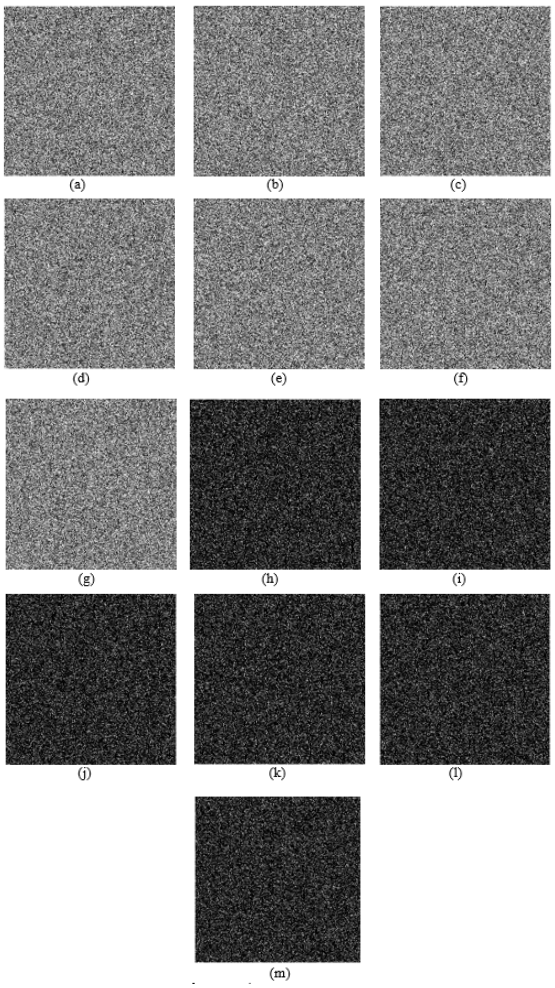

Figure 5: Secret key sensitivity in the encryption process; (a) Encrypted image with the right secret key, (b) Encrypted image with $(x(0) + 10^{-15})$, (c) Encrypted image with $(y(0) + 10^{-15})$, (d) Encrypted image with $(z(0) + 10^{-15})$, (e) Encrypted image with $(v(0) + 10^{-15})$, (f) Encrypted image with $(w(0) + 10^{-15})$, (g) Encrypted image with $(u(0) + 10^{-15})$, (h) Subtraction between (a) and (b), (i) Subtraction between (a) and (c), (j) Subtraction between (a) and (d), (k) Subtraction between (a) and (e), (l) Subtraction between (a) and (f), (m) Subtraction between (a) and (g)

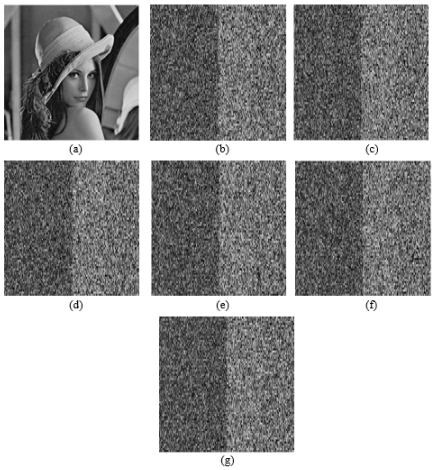

Figure 6: Secret key sensitivity in the decryption process; (a) Decrypted image with the right key. (b) Decrypted image with $(x(0) + 10^{-15})$, (c) Decrypted image with $(y(0)+10^{-15})$,; (d) Decrypted image with $(z(0)+10^{-15})$,; (e) Decrypted image with $(v(0) + 10^{-15})$,; (f) Decrypted image with $(w(0) + 10^{-15})$,; (g) Decrypted image with $(u(0) + 10^{-15})$

processes.

4.4 Correlation Coefficients Analysis

In the plain image, there is a strong correlation between the adjacent pixel values. Therefore, the image encryption algorithms should break up this high correlation between the adjacent pixels to resist the attackers' analyses [32]. To analyze the correlations of adjacent pixels of the plain image and cipher image, Lena's image is used as the test image, and we randomly pick out 5000 pairs of adjacent pixels from images in three different directions: horizontal, vertical, and diagonal. The correlation coefficient values of neighboring pixels are shown in Table 1 for Lena, Cameraman, and Barbara images of encrypted images in (Figure 3) by our proposed encryption algorithm. The correlation of adjacent pixels for the plain and cipher images (Lena image) is shown in Figure 7 in three directions: horizontal, vertical, and diagonal.

As can be seen from Figure 7 that the difference between the three directions of an encrypted image cannot be observed by the naked eye, thus for the accurate comparison, we computed the correlation coefficient measure of the plain image and the three directions of the encrypted image. For this purpose, we used the following correlation coefficient formula [3]:

$$r_xy = \frac{Con(x,y)}{\sqrt{D(X)}\sqrt{D(y)}} \tag{7}$$

$$Con(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{8}$$

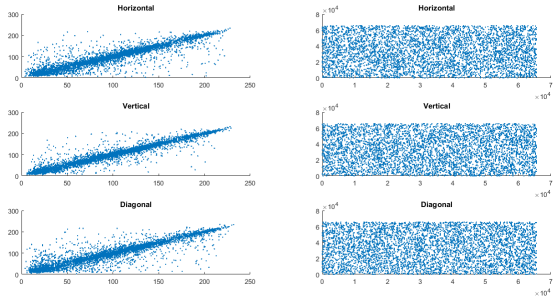

Figure 7: Adjacent pixels correlation at horizontal, vertical, and diagonal directions: (a) Plaintext image, (b) encrypted image

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \tag{9}$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i) \tag{10}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{11}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2 \tag{12}$$

where r_xy is the correlation coefficient of two adjacent pixels, and $E(x)$ and $D(x)$ are the expectation and variance of variable x, respectively. $E(y)$ and $D(y)$ are the expectation and variance of variable y, respectively.

Table 1: Correlation coefficients of the proposed algorithm

Images	Horizontal	Vertical	Diagonal
Lena	0.0017	-0.0027	0.0002
Cameraman	0.0028	-0.0019	0.0004
Barbara	0.0024	-0.0038	0.0065

As shown in Table 1 the correlation coefficients of the proposed algorithm are very low or practically zero. Thus, the proposed algorithm resisted statistical attacks. Table 2 shows a correlation coefficient comparison with recent works by using Lena image 512 ×512.

As shown in Table 2, the proposed encryption algorithm has better correlation coefficient values in horizontal and diagonal directions compared with other works, while for vertical direction Ref [33] has better vertical correlation coefficient values compared with others.

4.5 Differential Attack Analysis

According to the theory of cryptography, an image encryption scheme should effectively resist the differential

Table 2: Correlation coefficients of the proposed algorithm

Algorithms	Horizontal	Vertical	Diagonal
The Proposed	0.0003	-0.0029	0.00015
[10]	0.0005	0.0006	0.0029
[33]	0.0017	0.0004	0.0028
[35]	0.0056	0.0037	0.0032

attack, where the differential attack is an attack method in which the attacker chooses plaintext; then, change a part of the pixel values of the plaintext image to compare the differences between the two encrypted images to find the possibility of deciphering. Thus a good image encryption algorithm needs to be very sensitive to the original images; that is, any trivial change in the secret key should lead to a completely different encrypted image. The resistance of encryption algorithms against differential attacks can be tested by the number of pixels changing rate (NPCR), unified averaged changed intensity (UACI), and Hamming distance (HD) which are acquired as follows [11]:

$$D(i,j) = \begin{cases} 0 & \text{if } C^1(i,j) = C^2(i,j) \\ 1 & \text{if } C^1(i,j) \neq C^2(i,j) \end{cases} \quad (13)$$

$$NPCR : N(C^1, C^2) = \sum_{i=1}^{N} \frac{D(I,j)}{T} \times 100 \quad (14)$$

$$UACI : U(C^1, C^2) = \sum_{i=1}^{N} \frac{|C^1(i,j) - C^2(i,j)|}{F \times T} \times 100 \quad (15)$$

$$HD : H(C^1, C^2) = \sum_{i=1}^{N} \frac{|C^1(K) XOR C^2(K)|}{n_b \times T} \times 100 \quad (16)$$

where $C^1(i,j)$ and $C^2(i,j)$ are two-pixel values of the same position (i,j) in the two different encrypted images. F and T represent the image dimensions. The NPCR, UACI, and HD results by using three different images are listed in Table 3.

Table 3: The NPCR, UACI, and HD values of three different images

Images	NPCR	UACI	HD
Lena	99.6207	33.4907	50.1699
Cameraman	99.5819	33.6051	50.0755
Barbara	99.5667	33.6404	50.1038

The results in Table 3 indicate that the differential attack analysis tests demonstrated the sensitivity of the encrypted image with NPCR, UACI, and HD of the proposed encryption scheme are close enough to the ideal values. Table 4 shows the performance comparison in terms of differential attack analysis (NPCR and UACI) between the proposed algorithm and the recent works by using Lena image 256 ×256.

Table 4: Performance comparison in terms of Differential attack analysis (NPCR and UACI)

Algorithms	NPCR	UQCI
Proposed Algorithm	99.62	33.49
[15]	99.74	33.52
[10]	99.64	33.47
[34]	99.62	33.41

As it is illustrated in Table 4, the proposed algorithm has an NPCR value close enough to the ideal value of (99.61), while for the UACI, the proposed encryption algorithm is close enough to Ref [10] which has the closest value to the ideal value of UACI (33.46).

4.6 Information Entropy Analysis

Information entropy is a significant parameter to reflect the randomness of information. In image encryption applications, the higher the level of image confusion is, the greater the value of information entropy is [13]. The calculation formula is as follows [22]:

$$H(m) = \sum_{i=0}^{255} P(m_i) log_2 \frac{1}{P(m_i)} \quad (17)$$

where m is a set of information symbols and $P(m_i)$ represents the probability of occurrence of m_i. For grayscale images, the closer the information entropy is to 8, the stronger the randomness of the pixel value arrangement of encrypted images is. Table 5, shows the information entropy of encrypted images by applying the proposed algorithm.

Table 5: The information entropy values of three different images

Images	Entropy
Lena	7.9914
Cameraman	7.9907
Barbara	7.9896

The results of all encrypted images obtained by our proposed algorithm are close enough to the ideal value 8. Therefore, the proposed encryption algorithm demonstrates better performance, so it is enough to resist attacks. Table 6 shows the performance in terms of Entropy between the proposed algorithm and recent works.

As it is illustrated in Table 6, the proposed algorithm and Ref [15] have an Entropy value close enough to the ideal value (8).

Table 6: Performance comparison in terms of Entropy

Images	Entropy
Proposed Algorithm	7.9997
[15]	7.9998
[10]	7.9996
[34]	7.9972

4.7 Robustness Analyses

4.7.1 Noise Attack Analysis

The attackers use noise attacks such as Gaussian noise (GN), Salt and Pepper noise (SPN), and Speckle noise (SN) for disrupting the integrity of the cipher text information. Then, the receiver of the cipher text cannot decrypt the image correctly. In this paper, the proposed algorithm is used to test if it can resist noise attacks. Lena image and its cipher image without noise are shown in Figure 3, and different kinds of noise are added to it, the decrypted images of noisy images are shown in Figure 8. Moreover, to measure the quality of the decrypted image, the Peak signal-to-noise ratio (PSNR) test is used which measures the quality of the decrypted image after image processing, and its equation is given by [22]:

$$PSNR = 10log\frac{255 \times 255}{\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(X(i,j) - Y(i,j))^2} \quad (18)$$

where M and N represent the size of the image; $X(i,j)$ and $Y(i,j)$ are the pixel values of the original image and decrypted image respectively. The higher the PSNR means that the decrypted image has less difference from the original image. The PSNR values between the decrypted with noise images and the original image are listed in Table 7. From Figure 8 and Table 7, it can be seen that the proposed algorithm has the highest resistance to noise for GS, and the decrypted image has a good visual appearance when the intensity is between $7*10^{-8}$and $4*10^{-7}$and PSNR values are more than 26.5 dB. In SN, the decrypted image has a good visual appearance when the intensity is between $5 * 10^{-6}$ and $1.5 * 10^{-5}$ and PSNR values are more than 26 dB. For SPN, our algorithm has the highest resistance, when noise intensity changes from $3 * 10^{-5}$ to $8 * 10^{-3}$ the decrypted image has the most information of an image, and PSNR is more than 22 dB. Therefore, the proposed algorithm is robust to noise to a certain degree.

4.7.2 Data Loss Attack Analysis

The encryption algorithm needs to be able to resist the data loss attack which means if there is a small loss of data in the cipher image, the decrypted image must have most information of the original image. In this paper, the encrypted Lena image loses each time $32x32, 64x64, 128x128$ blocks in the positions of the upper left corner, the middle part, and the bottom right corner. The decrypted images

Figure 8: : Decrypted images under different noise: (a) $7 * 10^{-8}$ GS,(b) $4 * 10^{-7}$ GS, (c) $8 * 10^{-7}$ GS,(d) $5 * 10^{-6}$ SN, (e) $.5 * 10^{-5}$ SN, (f) $2 * 10^{-5}$ SN, (g) $3 * 10^{-5}$ SPN, (h) $8 * 10^{-3}$ SPN, (i) $2 * 10^{-2}$ SPN.

Table 7: PSNR (dB) values between decrypted images of noisy cipher images and plain image

Noise type	Noise intensity	PSNR (dB)
GS	0.00000007	28.4610
GS	0.0000004	26.7559
GS	0.0000008	18.7691
SN	0.0000005	28.4522
SN	0.0000015	26.0495
SN	0.000002	19.8535
SPN	0.00003	28.3356
SPN	0.008	22.4118
SPN	0.02	19.2866

are shown in Figure 9 and their PSNR is listed in Table 8. From Figure 9 and Table 8, it can be seen that the recovered images have important information about the plain image. Therefore, the proposed image encryption algorithm may resist some data loss attacks.

Table 8: PSNR of data loss with different sizes and positions

Size position	Left upper	Middle	bottom right
32 x 32	26.8296	25.4114	24.4397
64 x 64	20.5066	19.1890	18.2623
128 x 128	14.6092	13.0023	12.0264

5 Conclusion

This paper introduced a new image encryption algorithm based on advanced Hill cipher and 6D hyperchaotic system. The use of the hyperchaotic system is to obtain a better diffusion process while the advanced Hill cipher is used to improve the security level of the cryptosystem in the confusion process without losing the advantages of the hyperchaotic systems. The main advantages of the proposed algorithm are a high probability of resisting a brute-force attack, high key sensitivity, the ability to defend against a differential attack, adjacent pixel correlation, and resisting robustness attack. Therefore, the proposed encryption algorithm can achieve higher security performance than several classical image encryption algorithms.

Acknowledgments

This study was supported by the National Science Council of Taiwan under grant NSC 95-2416-H-159-003. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] H. Ali Pacha, N. Hadj Said, A. Ali Pacha, and Ö.Özer, "Significant role of the specific prime number p = 257 in the improvement of cryptosystems," *Notes on Number Theory and Discrete Mathematics*, vol. 26, no. 4, pp. 213–222, 2020.

[2] F. Bao, C. C. Lee, M. S. Hwang, "Cryptanalysis and improvement on batch verifying multiple RSA digital signatures", *Applied Mathematics and Computation*, vol. 172, no. 2, pp. 1195-1200, Jan. 2006.

[3] X. Chai, J. Bi, Z. Gan, X. Liu, Y. Zhang, and Y. Chen, "Color image compression and encryption scheme based on compressive sensing and dou-

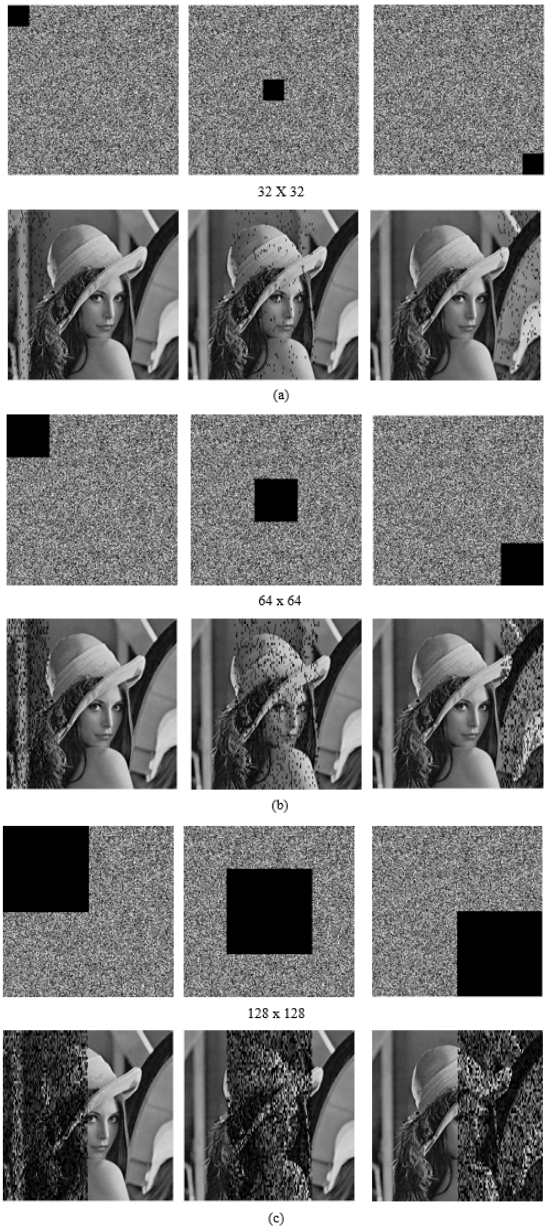

Figure 9: : Encrypted images and decrypted images with data loss of size: (a) 32 x 32 block, (b) 64 x 64 block, (c) 128 x 128 block

ble random encryption strategy," *Signal Processing*, vol. 176, p. 107684, 2020.

[4] C. C. Chang, K. F. Hwang, M. S. Hwang, "Robust authentication scheme for protecting copyrights of images and graphics", *IEE Proceedings-Vision, Image and Signal Processing*, vol. 149, no. 1, pp. 43-50, 2002.

[5] C. C. Chang, K. F. Hwang, M. S. Hwang, "A block based digital watermarks for copy protection of images," in *Asia-Pacific Conference on Communications*, vol. 2, pp. 977-980, 1999.

[6] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[7] C. C. Chang, M. S. Hwang, T. S. Chen, "A new encryption algorithm for image cryptosystems", *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, 2001.

[8] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[9] Z. E. Dawahdeh, S. N. Yaakob, and R. Razif bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University - Computer and Information Sciences*, vol. 30, no. 3, p. 349–355, 2018.

[10] M. Essaid, I. Akharraz, A. Saaidi, and A. Mouhib, "Image encryption scheme based on a new secure variant of hill cipher and 1d chaotic maps," *Journal of Information Security and Applications*, vol. 47, p. 173–187, 2019.

[11] Z. Gan, X. Chai, J. Zhang, Y. Zhang, and Y. Chen, "An effective image compression–encryption scheme based on compressive sensing (cs) and game of life (gol)," *Neural Computing and Applications*, vol. 32, no. 17, p. 14113–14141, 2020.

[12] A. Hadj Brahim, A. Ali Pacha, and N. Hadj Said, "Image encryption based on compressive sensing and chaos systems," *Optics and Laser Technology*, vol. 132, p. 106489, 2020.

[13] T. Haq and T. Shah, "Algebra-chaos amalgam and dna transform based multiple digital image encryption," *Journal of Information Security and Applications*, vol. 54, p. 102592, 2020.

[14] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 3, p. 306–312, 1929.

[15] S. Hraoui, F. Gmira, M. F. Abbou, A. J. Oulidi, and A. Jarjar, "A new cryptosystem of color image using a dynamic-chaos hill cipher algorithm," *Procedia Computer Science*, vol. 148, pp. 399–408, 2019.

[16] L. C. Huang, L. Y. Tseng, M. S. Hwang, "The study on data hiding in medical images", *International Journal of Network Security*, vol. 14, no. 6, pp. 301–309, 2012.

[17] M. S. Hwang, C. C. Lee, Y. C. Lai, "Traceability on RSA-based partially signature with low computation", *Applied Mathematics and Computation*, vol. 145, no. 2-3, pp. 465-468,

[18] E. T. Khalaf, M. N. Mohammed, and N. Sulaiman, "Iris template protection based on enhanced hill cipher," in *ICCIS '16: 2016 International Conference on Communication and Information Systems*, pp. 53–57, Bangkok, Thailand, DEC 2016.

[19] A. Mahmoud and A. Chefranov, "Hill cipher modification based on pseudo-random eigenvalues," *Applied Mathematics and Information Sciences*, vol. 8, no. 2, pp. 505–516, 2014.

[20] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Information Sciences*, vol. 520, p. 46–62, 2020.

[21] S. K. Muttoo, D. Aggarwal, and B. Ahuja, "A secure image encryption algorithm based on hill cipher system," *Bulletin EEI*, vol. 1, no. 1, pp. 51–60, 2011.

[22] M. Naim and A. Ali Pacha, "A new chaotic satellite image encryption algorithm based on a 2d filter and fisher–yates shuffling," *The Journal of Supercomputing*, 2023.

[23] M. Naim, A. Ali Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and josephus problem," *Advances in Space Research*, vol. 67, no. 7, pp. 2077–2103, 2021.

[24] S K Naveenkumar, H T Panduranga, and Kiran, "Chaos and hill cipher based image encryption for mammography images," in *2015 International Conference on Innovations in Information,Embedded and Communication Systems (ICIIECS)*, pp. 1–5, Coimbatore, India, MARS 2015.

[25] D. Ravichandran, A. Banu, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid dna computing and chaos in transform domain," *Medical and Biological Engineering and Computing*, vol. 59, no. 3, pp. 589–605, 2021.

[26] 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.

[27] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Processing*, vol. 141, p. 217–227, 2017.

[28] M. H. Tsai, S. F. Chiou, and M. S. Hwang, "A progressive image transmission method for 2D-GE image based on context feature with different thresholds", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 2, pp. 379–386, Feb. 2009.

[29] M. H. Tsai, S. F. Chiou and M. S. Hwang, "A simple method for detecting protein spots in 2D-GE images using image contrast", *International Journal of Innovative Computing, Information and Control*, vol. 5, no. 12, pp. 4617–4626, Dec. 2009.

[30] C. C. Wu, M. S. Hwang, S. J. Kao, "A new approach to the secret image sharing with steganography and authentication", *The Imaging Science Journal*, vol. 57, no. 3, pp. 140–151, 2009.

[31] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, p. 1154–1169, 2021.
[32] Q. Xu, K. Sun, S. He, and C. Zhu, "An effective image encryption algorithm based on compressive sensing and 2d-slim," *Optics and Lasers in Engineering*, vol. 134, p. 106178, 2020.
[33] X. Wang and N. Guan, "A novel chaotic image encryption algorithm based on extended zigzag confusion and rna operation," *Optics and Laser Technology*, vol. 131, p. 106366, 2020.
[34] X. Wang and Y. Li, "Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and dna sequence," *Optics and Lasers in Engineering*, vol. 137, p. 106393, 2021.
[35] J. Wu, X. Liao, and B. Yang, "Image encryption using 2d hénon-sine map and dna approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.
[36] L. Yang, Q. Yang, and G. Chen, "Hidden attractors, singularly degenerate heteroclinic orbits, multistability and physical realization of a new 6d hyperchaotic system," *Communications in Nonlinear Science and Numerical Simulation*, vol. 90, p. 105362, 2020.
[37] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dynamics*, vol. 75, no. 3, pp. 417–427, 2014.

Biography

M. Naim biography. Mohammed Naim is an assistant professor in both the Department of Engineering and Artificial Intelligence at the University of Palestine and the Department of Networks and Engineering at Al-Aqsa University in Gaza - Palestine. From 2018 to 2022 he was a lecturer at the Department of Electronic Engineering at USTO University and a researcher at the LACOSI laboratory in the field of information security in Oran-Algeria. He published his works in valuable research journals such as Advances in Space Research (Elsevier), The Journal of Supercomputing (Springer), and Information Security Journal: A Global Perspective (Taylor and Francis).

A. Ali Pacha biography. Adda Ali Pacha is a Professor in the Faculty of Electrical Engineering, Department of Electronics at USTO University, and responsible for the LACOSI laboratory in the field of information security in Oran-Algeria. He published his works in valuable research journals such as Advances in Space Research (Elsevier), The Journal of Supercomputing (Springer), and Information Security Journal: A Global Perspective (Taylor and Francis).