International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 6, December 2020, pp. 5736~5748
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i6.pp5736-5748

Color image encryption based on chaotic shit keying with lossless compression

Ashwaq T. Hashim, Bahaa D. Jalil
Control and Systems Engineering Department, University of Technology-Iraq, Iraq

Article Info

Article history:

Received Jan 2, 2020
Revised May 7, 2020
Accepted May 20, 2020

Keywords:

Chaotic map
Cryptography
CSK
Image compression
Image encryption

ABSTRACT

In order to protect valuable data from undesirable readers or against illegal reproduction and modifications, there have been various data encryption techniques. Many methods are developed to perform image encryption. The use of chaotic map for image encryption is very effective, since it increases the security, due to its random behavior. The most attractive feature of deterministic chaotic systems is the extremely unexpected and random-look nature of chaotic signals that may lead to novel applications. A novel algorithm for image encryption based on compression and hyper chaotic map techniques is suggested. First, the RGB image is broken down into R, G and B subbands after that each band is compressed using lossless technique. The generated chaotic sequences from the 3D chaotic system are employed to code the compressed results by employing the idea of chaotic shift encoding (CSK) modulation to encode the three bands to generate the encrypted image. The experiments show that the proposed method give good results in term of security, feasibility, and robustness.

Corresponding Author:

Bahaa Dhiaa Jalil,
Department of Control and Systems Engineering,
University of Technology-Iraq,
Baghdad, Iraq.
Email: 60042@uotechnology.edu.iq

1. INTRODUCTION

Recently, computer technology has developed rapidly, so digital image processing has its share from this development and it entered into many life aspects like investigation, industrial detection, communication, remote sensing, intelligent robots, medicine, meteorology, etc. Therefore, image information entices widespread awareness. In many fields; especially in military and medical fields, security of image data is very significant. So a way to protect transmission of digital images is needed which leads to found the image encryption. Classical encryption algorithms like Advanced Encryption Standard(AES) and Data Encryption Standard (DES) don't offer image encryption needs because of the image data characteristics such as the data amount, the highly redundanc and the strong interrelationship which present low protection and low efficiency encryption [1].

As a result of high redundancy, data compression is the main thrust in multimedia applications because with no compression, communication resources and storage will be used inefficiently. Due to power and bandwidth restrictions, low-bit-rate compression is required for power-limited devices and low-bandwidth communication channels. Furthermore and especially for open-access network, encryption is needed for integrity and privacy of information. Algorithms of encryption are improved to a particular kind of data based on many characteristics like power of processing, sensitivity to bit changes and ciphered speed [2].

Compression contains two approaches which are lossless and lossy. In the case of lossless compression, the compressed data maintains its original format devoid of losing information, whereas

compressed data that loses data will lose some of the original information, but the loss is small to noticeable through a person's sense of eye and ear. Lossless compression is used for critical mission application such financial document and lossy is for application can be tolerated in slightly loss of information such as pictures. Compression required algorithm and several prominent compression algorithm techniques such as the Huffman, Run Length Encoding, arithmetic, and entropy. The main objective of proposed lossless compression is to reduce the size of image file, maintain quality of the reconstruction image from compression, and can be managed in available transmission bandwidth and secured during transmission [3].

Encryption algorithms like Blowfish, RC6, and AES which intended for text data encryptions are not appropriate for image data encryption. Particular encryption techniques are wanted for encryption of image because of the strong correlation and the redundancy among neighboring pixels. Chaotic map cryptosystems, compared with the classical techniques of encryption, are more appropriate to encryption of image. With its high sensibility for both elementary conditions and system parameters like false arbitrariness, non-repetition, retrograde, and accurately generated and regenerated of chaotic sequences, chaos is particularly appropriate for ciphered image. Therefore, the chaotic system is used as a base for many image encryption algorithms. In 1998, American scientist Friedrich introduced alternative architecture for publishing images to encrypt images [4].

Later, this structure was widely received, and today, most image encryption patterns depend on this chaotic structure [5-16], but the only using of the low dimensional chaotic system in image encryption doesn't present enough security. Compression is on the same importance of encryption, and if these two processes are separated, the high degree of uncertainty in cipher image length cannot be achieved. By using both encryption and compression techniques [2, 17-19], secure and efficient image transmission over non-private network can be guaranteed and that leads to increase the difficulty level that the attackers would be experienced due to the size of the encrypted image which would be uncertain.

Emad et al., [20], presented a secured image compression system for image satellite communication based on the fractal compression theory combined with the enhanced hill multimedia cryptosystem (EHMC) algorithm for encryption. Somaya et al., [21], proposed image-encryption technique by combining two techniques: encryption and compression. A wavelet transform was used to decompose the image and decorrelate its pixels into approximation and detail components. The more important component (the approximation component) is encrypted using a chaos-based encryption algorithm. The remaining components (the detail components) are compressed using a wavelet transform. Tabash et al., [22], introduced an image encryption technique based on three chaotic logistic maps and multi-pseudo random block permutation. The encryption process has been divided mainly into three steps; the first step is to encrypt the whole image using logistic map, the second step is to divide the image into a random number of blocks, the third step is to generate a random permutation for these blocks.

Borislav et al., [23], suggested an algorithm for image encryption which stands on two pseudorandom bit generators, one is based on Chebyshev map and the other on rotation equation. The Chebyshev map part is for variation while the rotation equation is for replacement. Zhang et al., [24], proposed a scheme that can simultaneously encrypt and compress a medical image using compressive sensing (CS) and pixel swapping based permutation approach. Poorani et al., [25], proposed a scheme of compressing encrypted images with auxiliary information. Some auxiliary information with uncompressed encrypted image is used for data compression and image reconstruction. Jiaojiao et al., [26], proposed a sparse decomposition and the Chinese remainder theorem to compress the image, and then chaos map was used in encryption process. That is done to achieve the joint compression and encryption effect.

Sireesha et al., [27], presented an encryption algorithm of pixel level image based on chaotic mapping and Chinese remainder theorem. Nasrullah et al., [2], proposed a combined algorithm of image compression with encryption which is stands on integer wavelet transform (IWT) beside a set of subdivide in hierarchical trees (SPIHT), Kd-tree and multiple chaotic maps. Shuqin et al., [1], proposed an algorithm for image encryption that stands on chaos and SHA-256 firstly by surrounding the plaintext image by a hash value sequence, then scrambling the image, finally adopting the feedback mechanism of the dynamic index. Saravanan et al., [28], proposed an image encryption algorithm in which discrete wavelet transform (DWT) is applied and randomly generated 256 bit key is used to create the measurement matrix used in compressive sensing. Osama et al., [29], proposed an image encryption algorithm, which involves a chaotic block image scrambling followed by a two–dimensional (2D) discrete linear chirp transform.

This research present a combined image compression and encryption structure which stands on CSK modulation is offered. The using of 3D chaotic system which is used for the diffusion and permutations of image pixels is the contribution of the work. In the proposed joint compression and encryption was performed. Firstly, only lossless compression is used, then 3D chaotic maps are used to perform the encryption. By comparing the suggested method with the remaining joint image compression and

encryption methods, it offers high security and much more compression and its effectiveness is clearly demonstrated by the experimental results which are obtained.

The remains of this paper is organized as follows: In Section 2, related works are discussed, while section 3 illustrate the proposed structure of the image compression and encryption. Section 4 shows the experimental results and security analysis of the suggested structure and finally, the conclusions are discussed in section 5.

2. RELATED WORKS

In this section the related works of the proposed system are reviewed in next two sub sections:

2.1. Hyper-chaotic system and chebyshev map

The system suggested by [1] is employed to generate the three random sequences constructed by hyper chaotic system and two Chebyshev maps. This approach utilized a hyper-chaotic system of four dimensional in addition to four initial conditions and five system parameters which is showed by (1):

$$dx/_{dt} = a(y - x) + w$$

$$dy/_{dt} = dx - xz + cy$$

$$dz/_{dt} = xy - bz$$

$$dw/_{dt} = yz - ew \quad (1)$$

The system parameters are a, b, c, d and e. and the system is hyper-chaotic if a=35, b=3, c=12, d=7 and e∈(0.085, 0.798), and it has two positive Lyapunov exponents, LE1=0.596, LE2=0.154. So the system is in a hyper-chaotic state. The two Chebyshev maps are designed by (2):

$$u_1(i+1) = cos\left(4 \times arcos\left(u_1(i)\right)\right)$$

$$u_2(i+1) = cos\left(4 \times arcos\left(u_2(i)\right)\right) \quad (2)$$

The initial values are $u_1(1)$ and $u_2(1)$.

After iterated the hyper-chaotic system, four sequences are generated which are signified as X=[x(i)], Y= [y(i)], Z=[z(i)] and W=[w(i)], respectively, where, i=1, 2, ... On the other hand two Chebyshev maps with $u_1(1)$ and $u_2(1)$ as initial values are repeated for constructing U_1 and U_2 sequences respectively. Three sequences of real values D_1, D_2 and D_3 are transformed to six chaotic sequences X, Y, Z, W, U_1 and U_2 to extra enhance sequences complication. The interval of the three sequences is in [0, 1]. By the following Formulas (3)-(5) the D_1, D_2 and D_3 are calculated.

$$D_1 = cos^2\left((X + Y + Z)/3\right) \quad (3)$$

$$D_2 = cos^2\left((W + U_1 + U_2)/3\right) \quad (4)$$

$$D_3 = cos^2\left((X + Z + U_2)/3\right) \quad (5)$$

2.2. Chaotic shift keying

In binary CSK modulation, the binary information is conveyed by chaotic signals which are taken energies of different bit. By means of transferring one chaotic signal $x_1(t)$ or $x_0(t)$ at a time, the encoding of information signal is done. So chaos signal $x_1(t)$ will be transferred if the information signal binary bit is "1", otherwise, $x_0(t)$ will be transferred. The modulation and demodulation of CSK are shown in Figure 1. By using either the same chaos system with different parameters or by two different systems, the two chaotic signals be obtained. The transmitted signal can be given [30] as describe by the following formula:

$$S(t) = \begin{cases} x_1(t) & ,1\ is\ transmitted \\ x_0(t) & ,0\ is\ transmitted \end{cases} \quad (6)$$

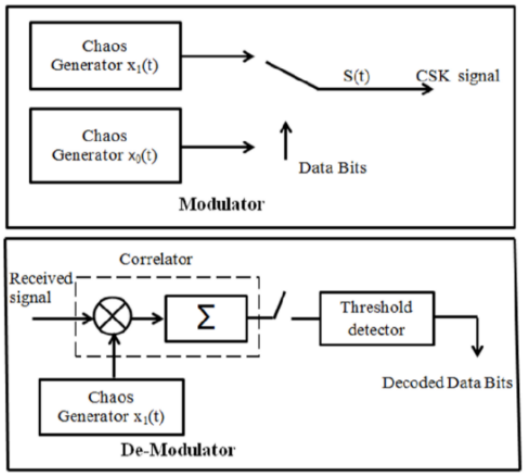


Figure 1. Block diagram of the CSK for modulator and demodulator [31]

3. PROPOSED SYSTEM

To improve the degree of security, dual image compression and encryption which stands on hyper chaotic system is used. The proposed system is divided into two stage at first the image is compressed using proposed lossless compression method and then encrypted by employing the CSK which is used a hyper chaotic system. Figure 2 displays the proposed system block diagram.

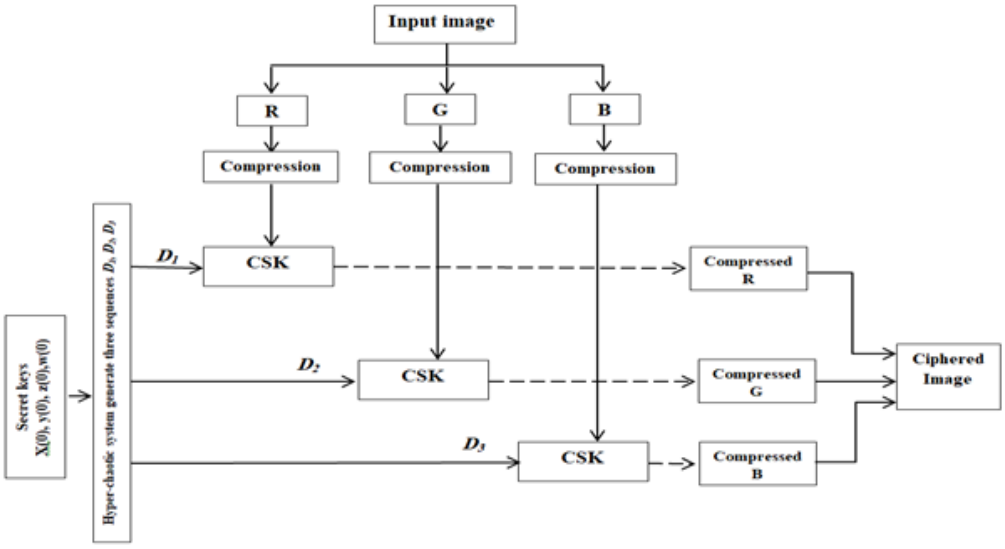


Figure 2. The proposed system block diagram

3.1. Proposed encryption

Many algorithms of encryption, precisely for digital images, are introduced to maintain the needs of strong applications for encryption of image. Chaos-based ciphered algorithms among them, which are became common due to numerous optimal features like unexpected and high sensitivity to initial conditions and various parameters. The chaotic maps security is influenced by the number of parameters of these chaotic cryptosystems. To increase the key space of proposed algorithm, a system proposed by [1] and explained in section (2.1) is used. Algorithm 1 shows the steps of proposed encryption algorithm.

Algorithm 1. Image encryption

Input : I // RGB color image
W, H // width and height of I
Output : E // Encrypted image
Step 1 : Let the size of the color image I is W × H
Step 2 : Separate the three bands R, G, B of the color image I
Step 3 : The band matrices R, G, and B are converted to a one dimensional vector

$R=\{R(1), R(2),..., R(l)\}$, $G=\{G(1), G(2),..., G(l)\}$, $B=\{B(1), B(2),..., B(l)\}$,

where l=W × H
Step 4 : Compressed the three vectors R, G and B separately using algorithm (2) to generate three binary compressed streams *RComp*, *GComp and BComp*
Step 5 : Create the chaotic sequences D_1, D_2, D_3 of length l_1, l_2, l_3 as defined in section 2.1 for encryption.
Step 6 : Convert the range of generated real sequences D_1, D_2, D_3 from [0 1] to [-1 1].
Step 7 : Encoded the compressed streams *RComp*, *GComp and BComp* by embedding them in generated random sequences D_1, D_2, D_3 using formula (6) to generate three real encoded sequences E_1, E_2, E_3.

```
For i= 1 to W×H
       If RComp (i) =1
            E1(i)=D1(i)
    Else
            E1(i)=- D1(i)
    EndIF
EndFor
```

Step 8 : Repeat step7 for *GComp* and *BComp* to generate E_2 and E_3 respectively.
Step 9 : Convert the three real sequences E_1, E_2 and E_3 to binary using following formula

$$\begin{aligned} BinE_1 &= \text{Round}\ (E_1 + 0.5) \\ BinE_2 &= \text{Round}\ (E_2 + 0.5) \\ BinE_3 &= \text{Round}\ (E_3 + 0.5) \end{aligned} \quad (7)$$

where the real numbers less than zero became 0 and the numbers greater than zero become 1.
Step 10 : Combine $BinE_1$, $BinE_2$ and $BinE_3$ into encrypted image E.

3.2. Proposed lossless image compresion

Lossless compressing is proposed to decrease the redundancy and irrelevance of image data to store or transfer data in an efficient form. Hence the image compression raises the transmission speed and decreases the storage requirement. In Lossless technique of image compression, no data get lost while doing the compression. The steps of Algorithm 2 describe the proposed lossless compression method.

Algorithm 2. Lossless image compression

Input : R,G,B // subands of input image
W, H // width and height of suband
Output : RComp, GComp, BComp, // compressed subands
Step 1 : For each subbands do the following:
Step 1.1 : The subband R is amended by defining the differences between adjacent pixels using the following formula:

$$R_i = R_i - R_{i-1} \qquad for\ i=1,..,\ n-1 \quad (8)$$

where n is the length of subband R (i.e., W×H).
Step 1.2 : Mapping the R_i to positive by this point the coding complexity resulting from positive/negative values is removed. The modulated values are converted to be always positive, by performing the following mapping equation:

$$C_i = \begin{cases} 2R_i & if\ R_i \geq 0 \\ -2R_i - 1 & if\ R_i < 0 \end{cases} \quad (9)$$

where C_i is the i^{th} element. According mapping equation all positive values are converted to even numbers while the negative values are became positive odd numbers.
Step 1.3 : Huffman Entropy encoding is used to encode the modulated band C to generate compressed stream *RComp*
Step 4 : Repeat step1 to generate *GComp and BComp*

3.3. Image deciphering

The operation of deciphering for ciphered image is decomposed of two operations. At first the decompressing is performed for each compressed subbands. Secondly, three sequences are generated using the same keys of encryption process. These sequences are used as chaotic signals to transmit or decode decompressed subbands to generate the decrypted image. The steps of decryption algorithm are described in Algorithm 3.

Algorithm 3. Image decryption

```
Input  : E            // Encrypted image
         l1, l2, l3   // length of BinE1, BinE2 and BinE3
Output : I            // decrypted image
Step 1 : Separate the three encrypted subbands BinE1, BinE2 and BinE3 of the encrypted image E
Step 2 : Produce the required chaotic sequences D1, D2, D3 of length l1, l2, l3 used the same
         chaotic parameters used in encryption process.
Step 3 : Convert the range of generated real sequences D1, D2, D3 from [0 1] to [-1 1].
Step 4 : For each encrypted subbands decoded them such as follows:
         For I←1..  to l1
             H (I)=   D1 (I) × Round( (BinE11 (I)+ (- 0.5) ) )
               IF H> T)      //  T is the threshold value
                  RComp1=1
               Else
                  RComp1=0
               EndIf
         EndFor
Step 5 : Repeat step4 to generate GComp1 and GComp1
Step 6 : decompressed the three vectors RComp1, GComp1 and GComp1 separately using Algorithm
         4 to generate three binary streams R, G and B
Step 7 : Combine the three subbands into decrepted image I
```

Algorithm 4. Lossless image decompression

```
Input  : RComp, GComp, BComp   // Compressed streams
Output : R, G, B      // R,G,B subbands
Step 1 : For each compressed subbands RComp, GComp, BComp   ;
         Step 1.1  : Huffman Entropy deccoding is applied on the compressed stream RCom to
                     generate C.
         Step 1.2  : Mapping to Negative is used for the decoded data resulted from step1
                     performing the following equation:
```

$$R_i = \begin{cases} C_i \, div \, 2 & if \; C_i \; is \; even \\ -(C_i + 1) div 2 & if \; C_i \; is \; odd \end{cases} \quad (10)$$

where R_i is the i^{th} element. The previous equation turns the odd values to negative and the even values to positive.

Example of encryption four pixel of subband R without compression to clarify proposed encryption algorithm:

- Encryption
- Let four R subband pixels are 107 149 51 88
- In binary

  107 = 0 1 1 0 1 0 1 1
  149 = 1 0 0 1 0 1 0 1
  51 = 0 0 1 1 0 0 1 1
  88 = 0 1 0 1 1 0 0 0
- 1D of four binary pixels=0 1 1 0 1 0 1 1 1 0 0 1 0 1 0 1 0 0 1 1 0 0 1 1 0 1 0 1 1 0 0 0
- Let D_1 generated from chaotic map after convert its range to [-1 1]

D_1 = -0.5025 0.0000 -1.0000 -0.9899 -0.9699 -0.9301 -0.8509 -0.6933
-0.3797 0.2444 -0.5136 -0.0222 0.9559 0.9022 0.7954 0.5829
0.1601 -0.6815 -0.3561 0.2913 -0.4204 0.1635 -0.6747 -0.3426
0.3182 -0.3668 0.2701 -0.4624 0.0798 -0.8412 -0.6740 -0.3412

- The coded E = 0.5025 0.0000 -1.0000 0.9899 -0.9699 0.9301 -0.8509 -0.6933
-0.3797 -0.2444 0.5136 -0.0222 -0.9559 0.9022 -0.7954 0.5829
-0.1601 0.6815 -0.3561 0.2913 0.4204 -0.1635 -0.6747 -0.3426
-0.3182 -0.3668 -0.2701 -0.4624 0.0798 0.8412 0.6740 0.3412

- Converted to binary using

$BinE$=Round (E + 0.5)=1 1 0 1 0 1 0 0 0 0 1 0 0 1 0 1
0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 1

- Encrypted output in decimal: 212 37 88 15
- Decryption: 212 37 88 15
- Convert to binary

$BinE_{1,=}$ 1 1 0 1 0 1 0 0
0 0 1 0 0 1 0 1
0 1 0 1 1 0 0 0
0 0 0 0 1 1 1 1

- Let D_1 generated from chaotic map after convert its range to [-1 1] using the same parameters of encryption process

D_1 = -0.5025 0.0000 -1.0000 -0.9899 -0.9699 -0.9301 -0.8509 -0.6933
-0.3797 0.2444 -0.5136 -0.0222 0.9559 0.9022 0.7954 0.5829
0.1601 -0.6815 -0.3561 0.2913 -0.4204 0.1635 -0.6747 -0.3426
0.3182 -0.3668 0.2701 -0.4624 0.0798 -0.8412 -0.6740 -0.3412

- The output after this formula: G=Round(($BinE_{11}$ (I)+ (- 0.5))

G=1 1 -1 1 -1 1 -1 -1 -1 -1 1 -1 -1 1 -1 1 -1 1 -1 1 1 -1 -1
- 1 -1 -1 -1 -1 1 1 1 1

H (I)= D_1 (I) × G

H= -0.5025 0.0000 1.0000 -0.9899 0.9699 -0.9301 0.8509 0.6933
0.3797 -0.2444 -0.5136 0.0222 -0.9559 0.9022 -0.7954 0.5829
-0.1601 -0.6815 0.3561 0.2913 -0.4204 -0.1635 0.6747 0.3426
-0.3182 0.3668 -0.2701 0.4624 0.0798 -0.8412 -0.6740 -0.34120

- IF H (i) > T) // T is the threshold value (i.e., T= 0)
$RComp$ (i)=1
Else
$RComp$ (i)=0

$RComp$= 0 1 1 0 1 0 1 1
1 0 0 1 0 1 0 1
0 0 1 1 0 0 1 1
0 1 0 1 1 0 0 0
0 1 0 1 1 0 0 0

- Converted to decimal: 107 149 51 88

4. EXPERIMENTAL RESULTS

In this paper four bmp color images of size 256×256 are tested as depicted in Figure 3. Encryption and decryption operations are implemented using Matlab 2018a and (x_0, y_0, z_0, w_0) are set to (0.398, 0.456, 0.784, 0.982) successively. Figure 4 depicts the encrypted test images by proposed system.

Figure 3. Test images

Figure 4. Encrypted images by proposed system

Table 1 shows the compression ratio (CR) of tested images. The aimed of the compression in this research to reduce the time that is required for coding the image by CSK. At the same time the type of compression is lossless there is no effect on the input image quality. Table 2 displays the time consuming of proposed system for the tested images.

Table 1. The comparison of tested images

Image name	Original size	Compressed Size	CR
A	196608	56008	3.5
Nike	196608	28850	6.8
Peppers	196608	33234	1.48
Lena	196608	120005	1.64

Table 2. The time consuming of tested images

Image name	Compression Time in Sec.	Coding Time in Sec.	Total time in Sec.
A	1.875	1.563	3.438
Nike	1.867	0.851	2.718
Peppers	1.432	3.137	4.569
Lena	1.368	3.922	5.29

4.1. Security analysis

The suggested encryption scheme security is inspect in this section with the RGB color images as an example.

4.1.1. Histogram analysis

A perfect histogram of an efficiently ciphered image must be uniform and much different from the original image. For a 24-bit color image, the histogram for red, green, blue channels are drawn respectively. Thus histograms for red, green, blue channels of Lena and the cipher-image are plotted in Figure 5. It is notice that the histograms of the cipher image are uniform and fully unlike from the original image, necessitating that the redundancy of the original image be successfully hidden after the encryption, and therefore does not provide any valuable information for statistical attacks.

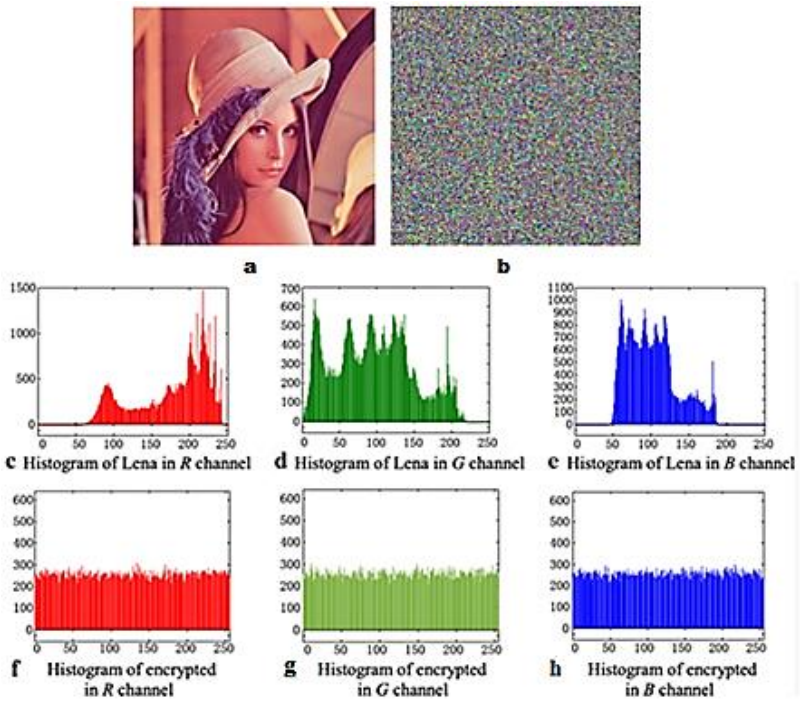


Figure 5. The histogram analysis result, (c)-(e) red, green, blue channel components of plain-image, (f)-(h) red, green, blue channel components of encrypted image

4.1.2. Key space

In cryptography, as much as the key space is large, as much as the capability for resisting force attacks is strong. The keys of the proposed algorithm are represented by the initial values x(0), y(0), z(0), w(0) of the chaotic system in (1), the parameter e of chaotic system and the Chebyshev maps initial values $u_1(1)$, $u_2(1)$ in (2). The x_0, y_0, z_0, w_0, $u_1(1)$ and $u_2(1)$ is precise to 10^{-15}, while the parameter e for $e \in (0.085, 0.798)$ is precise to 10^{-12}, so the size of the key space is $(10^{15})^6 \times 10^{12} = 10^{102} \approx 2^{339}$.

In reference [32], Li mentioned that to avoid brute force attacks, the ciphered system keyspace shouldexceed 2^{100}. Consequently, the algorithm key is large adequate to immune the brute force attacks. Table 3 compare the key space size between the used algorithm and other similar encryption algorithms, and it is clear that utilized algorithm's key space size is larger than that of most analogous algorithms.

Table 3. The key space comparisons

Encryption Algorithm	Key Space
Wang et al. [33]	2^{149}
Guesmi et al. [34]	2^{256}
Li et al. [35]	2^{299}
Li et al. [36]	2^{375}
Curiac et al. [37]	2^{128}
Curiac et al. [38]	2^{357}
Used System [1]	2^{339}

4.1.3. Correlation analysis

In plain-image, the adjacent pixels have high correlation which attacker use in their attacks, so the correlation coefficient is always high. Therefore, the correlation coefficient must be significantly reduced after encryption. By (11), the correlation coefficients of four directions are calculated.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{11}$$

where

$$cos(x,y) = \frac{1}{N}\sum_{0}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big), D(x) = \frac{1}{N}\sum_{0}^{N} x_i - E(x)^2, E(x) = \frac{1}{N}x_i.$$

The values of two adjacent pixels of four directions are represented by x, y, and N is image pixels number. Table 4 lists the correlation coefficients of original images and its encrypted images as well as the vertical (V), horizontal (H), diagonal (D) directions. Table 4 clearly shows that suggested algorithm can resist hacker attacks according to the value of the correlation coefficient which is close to 0 of the cipher-images while it is close to 1 of the plain-images. Figures 6 and 7 show the vertical, horizontal, and diagonal directions for image 'A' and 'lena'.

Table 4. Horizontal, vertical and diagonal correlation coefficients between original and encrypted images

Image name		Correlation of plain image			Correlation of ciphered image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
A	R	0.8993	0.9385	0.9014	0.0126	–0.0114	–0.0077
	G	0.9936	0.9928	0.9897	−0.0009	0.0003	−0.0002
	B	0.9265	0.9192	0.8809	−0.0024	−0.0008	−0.0043
Nike	R	0.9808	0.9907	0.9747	0.0017	–0.0042	0.0015
	G	0.9855	0.9848	0.9783	−0.0019	−0.0004	0.0003
	B	0.9527	0.9527	0.9178	−0.0035	0.0005	−0.0062
Peppers	R	0.9704	0.97739	0.9583	–0.0001	–0.0003	–0.0023
	G	0.8668	0.7759	0.7432	0.0033	0.0018	0.0003
	B	0.9067	0.8844	0.8544	0.0006	0.0004	0.0008
Lena	R	0.9753	0.9853	0.9734	−0.0028	0.0046	0.0013
	G	0.9666	0.9802	0.9630	0.0004	−0.0009	0.0007
	B	0.9334	0.9558	0.9264	−0.0029	−0.0007	−0.0050

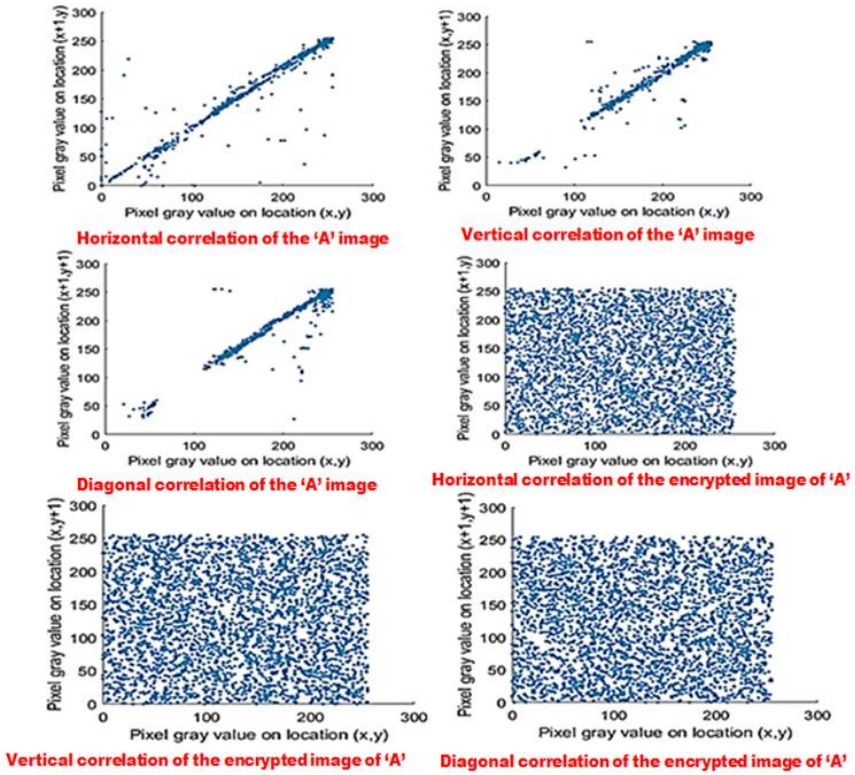


Figure 6. The correlation of the image 'A' with the correspondent encrypted image of 'A'

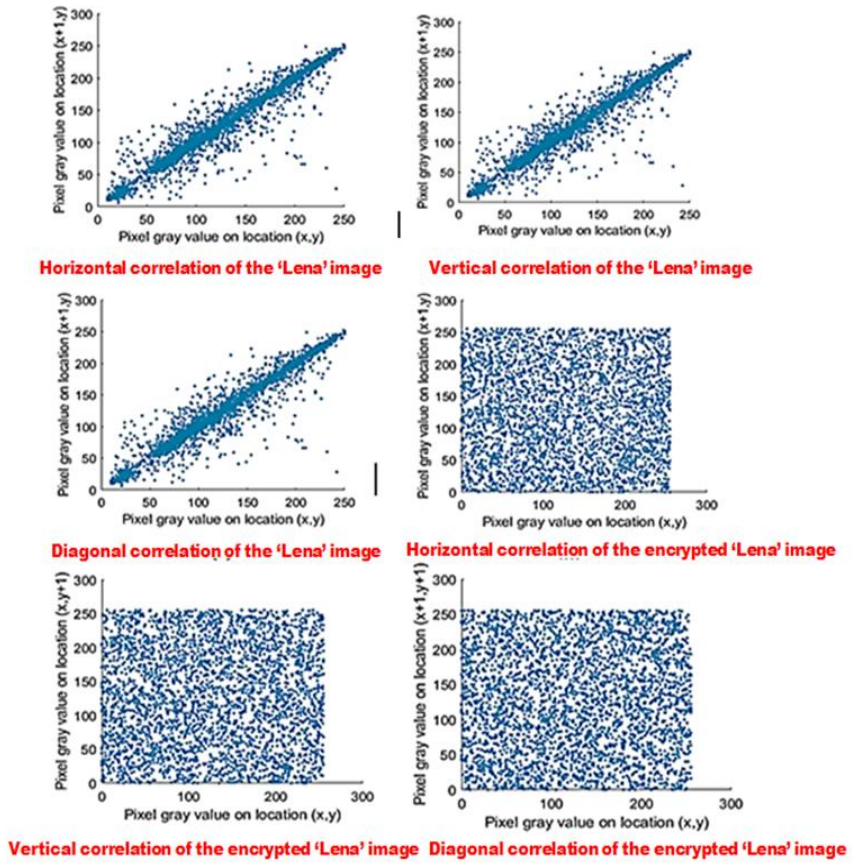


Figure 7. The correlation of the 'Lena' image and the correspondent encrypted image of 'Lena'

4.1.4. Entropy analysis

The ideal value of the information entropy E to an encrypted image which has 256 gray intensities is 8. The information entropy of natural images and their matching ciphered images-which are encrypted using proposed system and compared with other algorithms in the literature-are calculated based on (12) and these data are listed in Table 5. It is noticed that the encrypted images information entropies were totally near to the perfect value. Furthermore, the encrypted images possessed a perfect feature of randomness and the unexpectable.

$$E = -\sum_{i=0}^{n} Pi \log_2(Pi) \quad (12)$$

where p_i is gray value probability

Table 5. The result entropy of information for encrypted images

Images	Plain image			Cipher image		
	R	G	B	R	G	B
A	4.733	4.651	4.021	7.999	7.999	7.999
Nike	3.499	3.444	3.270	7.999	7.999	7.999
Peppers	7.434	7.235	7.057	7.999	7.999	7.999
Lena	5.046	5.457	4.800	7.999	7.999	7.999
Lena in [23]	-	-	-	7.999	7.999	7.999
Lena in [39]	-	-	-	7.991	7.991	7.991
Lena in [40]	-	-	-	7.997	7.997	7.996
Lena in [41]	-	-	-	7.997	7.997	7.997
Lena in [42]	-	-	-	7.997	7.997	7.997
Lena in [43]	-	-	-	7.994	7.994	7.994

4.1.5. Key sensitivity

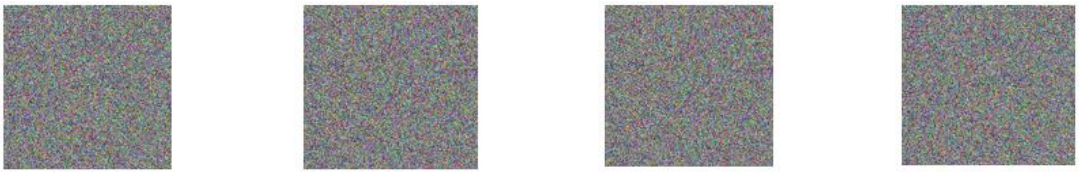
There are to features are employed to assess the key sensitivity the first one is that the ciphered image is wholy differed if the same natural image is ciphered with two keys of slightly different. The change rate of is used to measure the differences of the encrypted images. Second, there is no information available of the plaintext image in the decrypted image using wrong key, although there is a very slight difference between the wrong key and the correct key.

The test results of sensitivity are shown in Table 6 and it has been confirmed that the the proposed algorithm sensitivity to the keys x_0, y_0, z_0, w_0 is very high, and can reach more than 10^{-14}. To assess the key sensitivity in the second features, the following error keys K_1, K_2, K_3 and K_4 are chose to decrypt the original encrypted Lena image, and the result of decryption is depicted in Figure 8.

$K_1=\{x_0, y_0, z_0, w_0\}=(0.367 + 10^{-14}, 0.436, 0.766, 0.991)$,
$K_2=\{x_0, y_0, z_0, w_0\}=(0.367, 0.436 + 10^{-14}, 0.766, 0.991)$,
$K_3=\{x_0, y_0, z_0, w_0\}=(0.367, 0.436, 0.766 + 10^{-14}, 0.991)$,
$K_4=\{x_0, y_0, z_0, w_0\}=(0.367, 0.436, 0.766, 0.991 + 10^{-14})$.

Table 6. Initial key sensitivity tests

Keys	Change Rate
X_0	0.9953
Y_0	0.9972
Z_0	0.9981
W_0	0.9967



(a) (b) (c) (d)

Figure 8. The image deciphered with the erroneous keys, (a) image decryption with K_1, (b) image decryption with K_2, (c) image decryption with K_3, (d) image decryption result of K_4

4.1.6. NPCR and UACI analysis

The satistical tests NPCR and UACI are utilized in the analysis of image by measuring the degree of sensitivity to image encryption algorithms of plaintext. The NPCR and UACI are calculated using following formulas [44]:

$$NCPR = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{S_{ij}}{M\times N}\times 100\%$$

$$S_{ij} = \begin{cases} 1 & X(i,j) \neq X'(i,j) \\ 0 & X(i,j) = X'(i,j) \end{cases}$$

$$UACI = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|X(i,j)-X\prime(i,j)|}{M\times N\times 255}\times 100\%$$

where $M\times N$ is the size of the image and $(i,)$ and $X'(i,j)$ denote the pixel values for the positions matching of plaintext and ciphertext. When the NPCR and UACI of the ciphertext are larger than 99.6% and 33.46% as shown in Table 7, respectively this shows that the algorithm possesses perfect security. So this algorithm is more sensible for plaintext and thus, this algorithm is resisted to differential attacks.

Table 7. The NPCR and UACI of encrypted images

Image	NPCR	UACI
A	99.60	33.51
Nike	99.60	33.47
Peppers	99.62	33.53
Lena	99.63	33.54

5. CONCLUSION

A hyper method of compression and encryption schemes based on CSK is proposed. In the CSK the multiple chaotic systems is employed. The input color image is compressed using proposed lossless image compression method. This stage is required for two goals the first one is to speed up encryption stage and other for enhancing security. The next step is image encryption based on CSK is used. The use of chaotic map for image encryption is very effective, since it increase the security, due to its random behavior. The utmost attractive characteristics of deterministic chaotic systems are the greatly unpredictable and random nature for the chaotic signals which are may guide to unprecedented (engineering) applications. The sequences of chaotic produced from the hyper chaotic map are utilized for coding the compressed results by employing the idea of chaotic shift encoding modulation to encode the three bands to generate the encrypted image. Simulation results manifest that the suggested encryption algorithm possess good performance.

REFERENCES

[1] S. Zhu, et al., "A new image encryption algorithm based on chaos and secure hash SHA-256," *Entropy*, vol. 20, no. 9, pp. 716-733, 2018.
[2] Nasrullah, et al., "Joint image compression and encryption using IWT with SPIHT, Kd-tree and chaotic maps," *Applied Science*, vol. 8, no. 10, p. 1963-1983, 2018.
[3] S. M. S. Hilles and M. S. Shafii, "Image Compression and Encryption Technique," *International Journal of Data Science Research*, vol. 1, no. 2, pp. 1-6, 2018.
[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 06, pp. 1259-1284, 1998.
[5] S. Lian, "Efficient image or video encryption based on spatiotemporal chaos system," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2509-2519, 2009.
[6] V. Patidar, et al., "Modified substitution--diffusion image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 10, pp. 2755-2765, 2010.
[7] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Optics Communications*, vol. 285, no. 1, pp. 29-37, 2012.
[8] Y. Zhang, et al., "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Processing: Image Communication*, vol. 28, no. 3, pp. 292-300, 2013.
[9] W. Zhang, et al., "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 3, pp. 584-600, 2013.
[10] Y. Zhang and D. Xiao, "An image encryption scheme based on rotation matrix bit-level permutation and block diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 74-82, 2014.
[11] X. Tong, et al., "An image encryption scheme based on hyperchaotic Rabinovich and exponential chaos maps," *Entropy*, vol. 17, no. 1, pp. 181-196, 2015.

[12] H. I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Processing*, vol. 117, pp. 281-309, 2015.
[13] X. Chai, "An image encryption algorithm based on bit level Brownian motion and new chaotic systems," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 1159-1175, 2017.
[14] R. K. Singh, et al., "Level by level image compression-encryption algorithm based on quantum chaos map," *Journal of King Saud University - Computer and Information Sciences*, 2018.
[15] Q. Wang, et al., "Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system," *Multimedia Tools and Application*, vol. 77, no. 2, pp. 1715-1734, 2018.
[16] L. Gong, et al., "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," *Optics and Laser Technology*, vol. 103, pp. 48-58, 2018.
[17] M. Zhang and X. Tong, "Joint image encryption and compression scheme based on IWT and SPIHT," *Optics and Lasers in Engineering*, vol. 90, pp. 254-274, 2017.
[18] M. Hamdi, et al., "A selective compression-encryption of images based on SPIHT coding and Chirikov Standard Map," *Signal Processing*, vol. 131, pp. 514-526, 2017.
[19] T. Xiang, et al., "Joint SPIHT compression and selective encryption," *Appl. Soft Comp.*, vol. 21, pp. 159-170, 2014.
[20] E. S. Othman and M. M. Sakre, "Compression and Encryption Algorithms for Image Satellite Communication," *International Journal of Scientific and Engineering Research*, vol. 3, no. 9, pp. 1-4, 2012.
[21] S. Al-Maadeed, et al., "A new chaos-based image-encryption and compression algorithm," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1-11, 2012.
[22] F. K. Tabash, et al., "Image encryption algorithm based on chaotic map," *International Journal of Computer Applications*, vol. 64, no. 13, pp. 1-10, 2013.
[23] B. Stoyanov and K. Kordov, "Image encryption using Chebyshev map and rotation equation," *Entropy*, vol. 17, no. 4, pp. 2117-2139, 2015.
[24] L. Zhang, et al., "Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach," *Mathematical Problems in Engineering*, vol. 2015, pp. 1-9, 2015.
[25] A. Poorani, B. Manju, "Secure image transformation using encryption and compression techniques," *International Journal of Advanced Research in Science, Engineering and Technology*, vol. 3, no. 5, pp. 2079-2084, 2016.
[26] J. Xie, et al., "Joint image compression and encryption method," in *Proceedings of the 2nd Information Technology and Mechatronics Engineering Conference (ITOEC 2016)*, pp. 67-70, 2016.
[27] V. V. M. Sireesha and Y. V. D. P. Latha, "Implementation of Image Encryption and Compression using Chinese Reminder Theorem and Chaotic Logistic Maps," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 6, no. 6, pp. 579-585, 2017.
[28] K. Saravanan, et al., "Compressive sensing based image encryption scheme," *ARPN Journal of Engineering and Applied Science*, vol. 13, no. 4, pp. 1381-1385, 2018.
[29] O. A. S. Alkishriwo, "An image encryption algorithm based on chaotic maps and discrete linear chirp transform," *Almadar Journal for Communications, Information Technology, and Applications*, vol. 5, no. 1, 2018.
[30] Y. S. Lau, "Techniques in Secure Chaos Communication," *PhD Thesis*, RMIT University, Australia, 2006.
[31] Y. S. Lau and Z. M. Hussain, "A new approach in chaos shift keying for secure communication," in *Third International Conference on Information Technology and Applications (ICITA'05)*, vol. 2, pp. 630-633, 2005.
[32] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129-2151, 2006.
[33] X. Wang, et al., "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Optics and Lasers in Engineering*, vol. 107, pp. 370-379, 2018.
[34] R. Guesmi, et al., "A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123-1136, 2016.
[35] S. Li, et al., "On the dynamical degradation of digital piecewise linear chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119-3151, 2005.
[36] S. Li, et al., "Baptista-type chaotic cryptosystems: problems and countermeasures," *Physics Letters A*, vol. 332, no. 5-6, pp. 368-375, 2004.
[37] D. I. Curiac and C. Volosencu, "Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest," *Mathematical Problems in Engineering*, vol. 2012, pp. 1-18, 2012.
[38] D. I. Curiac, et al., "Chaos-based cryptography: end of the road?" in *International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)*, pp. 71-76, 2007.
[39] M. Farajallah, et al., "Fast and secure chaos-based cryptosystem for images," *International Journal of Bifurcation and Chaos*, vol. 26, no. 02, pp. 1650021-1650041, 2016.
[40] M. A. Murillo-Escobar, et al., "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119-131, 2015.
[41] M. Mollaeefar, et al., "A novel encryption scheme for colored image based on high level chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 607-629, 2017.
[42] W. Liu, et al., "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26-36, 2016.
[43] L. Teng, et al., "A chaotic color image encryption using integrated bit-level permutation," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6883-6896, 2018.
[44] Y. Wu, et al., "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary J. in Sci. and Tech., Journal of Selected Areas in Telecommunications*, vol. 1, no. 2, pp. 31-38, 2011.