Chapter

Multiple-Image Fusion Encryption (MIFE) Using Discrete Cosine Transformation (DCT) and Pseudo Random Number Generators

Lee Mariel Heucheun Yepdia, Alain Tiedeu and Zied Lachiri

Abstract

This chapter proposes a new multiple-image encryption algorithm based on spectral fusion of watermarked images and new chaotic generators. Logistic-May (LM), May-Gaussian (MG), and Gaussian-Gompertz (GG) were used as chaotic generators for their good properties in order to correct the flaws of 1D chaotic maps (Logistic, May, Gaussian, Gompertz) when used individually. Firstly, the discrete cosine transformation (DCT) and the low-pass filter of appropriate sizes are used to combine the target watermarked images in the spectral domain in two different multiplex images. Secondly, each of the two images is concatenated into blocks of small size, which are mixed by changing their position following the order generated by a chaotic sequence from the Logistic-May system (LM). Finally, the fusion of both scrambled images is achieved by a nonlinear mathematical expression based on Cramer's rule to obtain two hybrid encrypted images. Then, after the decryption step, the hidden message can be retrieved from the watermarked image without any loss. The security analysis and experimental simulations confirmed that the proposed algorithm has a good encryption performance; it can encrypt a large number of images combined with text, of different types while maintaining a reduced Mean Square Error (MSE) after decryption.

Keywords: spectral fusion, chaotic generators, image encryption, watermarked images

1. Introduction

Several image encryption algorithms are being developed today to meet privacy needs in multimedia communications [1–33]. With the rapid expansion of the Internet, innovative technologies, and cryptanalysis, it has become necessary to build new and appropriate cryptosystems for secured data transfer, especially for digital images. Nowadays, a large quantity of images is produced in various fields and exchanged sometimes with text through different channels, favoring the development of multiple-image encryption (MIE) instead of single-image encryption (SIE). A secure technique to protect the large amounts of data (image and text)

exchanged in unsecured communication channels is to combine cryptography and watermarking [26, 27]. These two combined approaches help to produce a two-level security of the text and image, especially when the message is hidden in the image to be encrypted. Various watermarking techniques are proposed in the literature [28–32], and the most used are discrete wavelet transformation (DWT) and discrete cosine transformation (DCT). For instance, if an information, such as a signature, a logo, or a text is embedded in low- or medium-frequency DCT coefficients, then it may be recovered without any loss; however, only high-frequency DCT coefficients are lost in low-pass filtering.

In literature, many encryption algorithms, such as International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), and Data Encryption Standard (DES) have been proposed [1]. However, these standard algorithms do not seem to be appropriate for image encryption, because of the intrinsic features of images, such as huge data capacity, high redundancy, strong correlation among adjacent pixels, and low entropy [2]. Some basic properties of chaotic systems such as the sensitivity to the initial condition and control parameters, sensitivity to plain text, ergodicity and randomness behavior, meet the requirements for a good cryptosystem. Consequently, several cryptosystems were developed by researchers, based on chaotic systems because the latter provided a good combination of speed, high security, complexity, reasonable computational overheads, and computational power [3]. With these features, chaotic-based cryptosystems have excellent properties of confusion and diffusion, which are desirable in cryptography. Therefore, many techniques involving different chaotic systems have been published [2–12, 23], and we can distinguish one-dimensional (1D) chaotic maps and high-dimensional (HD) chaotic maps.

Among the chaotic encryption algorithms developed, the ones using a one-dimensional (1D) chaotic system like Logistic, May, Tent, and Sine map have proven to have some strengths, such as: high-level efficiency, simplicity, and high-speed encryption. 1D chaotic structures have been widely used [4] due to their simple structures, as opposed to the complex ones of higher dimensional chaotic system (which causes a relative slowness in computation). However, some schemes using the 1D map have been broken due to their weaknesses like nonuniform data output, small key space, periodic data output, and poor ergodicity properties for some ranges of control parameters [5, 6]. To overcome this drawback, some researchers stated that the 1D chaotic map should not be used alone [7, 8]. Others proposed new 1D chaotic systems with better properties like Spatiotemporal chaos in [9], coupled with the 1D chaotic map [6], the Nonlinear Chaotic map Algorithm (NCA) [10], and, more recently, nonlinear combinations of two different 1D chaotic maps [3, 11, 12]. For example, Abanda and Tiedeu [3] combined outputs of Duffing and Colpitts chaotic systems to encrypt gray and color images. Kamdeu and Tiedeu [11] proposed a fast and secured encryption scheme using new 1D chaotic systems obtained from Logistic, May, Gaussian, and Gompertz maps. In [12], Chenaghlu et al. proposed a polynomial combination of 1D chaotic maps for image encryption using dynamic functions generation.

Recently, in order to increase the efficiency of cryptosystems for multiple images, some authors proposed algorithms integrating the concept of fusion or mixing images as a step in the encryption process. Image fusion has been proven to have potential for encryption in both spatial and frequency domains. In the last 8 years, much effort has been devoted to compressing and encrypting images at the same time [13], which is considered as a new tool used to reduce the amount of data to be transmitted and protecting the use of these data against unauthorized access. In particular, the discrete cosine transformation (DCT) is employed as a useful tool for spectral fusion in most of these methods. The widely used application DCT for image compression is mainly based on its energy

compaction property, which means that the low-frequency coefficients are located around the top-left corner of its spectral plane [24]. In 2018, Jridi and Alfalou [14] proposed a cryptosystem to improve a Simultaneous Fusion, Compression and Encryption (SFCE) scheme [15] in terms of time consumption, bandwidth occupation, and encryption robustness. In [16], Dongfeng et al. proposed a new scheme for simultaneous fusion, imaging and encryption of multiple target images using a single-pixel detector. This algorithm achieves good performance in terms of robustness as the number of images to multiplex increases, but suffered from reduced key space and poor quality of images recovered. Mehra and Nishchal [17] proposed an image fusion encryption based on wavelets for securing multiple images through asymmetric keys. It offers a large key space, which enhances the security of the system. In 2016, Qin et al. [18] proposed an optical multiple-image encryption scheme in diffractive imaging using spectral fusion and nonlinear operations.

More recently, Zhang and Wang [19, 20] proposed two schemes of multiple-image encryption (MIE): the first algorithm based on mixed image element and permutation, and the second MIE algorithm based on mixed image element and chaos. The cryptosystem shows good performances, but can be improved in terms of compression to reduce the size of the multiplex big image when the number of target images increases. In [21], Zhu and Zhang proposed an encryption algorithm of mixed image element based on an elliptic curve cryptosystem. Experimental results and theoretical analysis show that the algorithm possesses a large key space and can accomplish a high level of security concerning information interaction on the network platform, but the encryption and decryption computational time is long. In 2013, Abdalla and Tamimi [22] proposed a cryptosystem, which combines two or more images of different types and sizes by using a shuffling-substitution procedure. Here, the process of mixing image combines stream cipher with block cipher, on the byte level.

After analyzing most MIE algorithms operating in the spectral domain, the robustness of the cryptosystem increases with the number of input images. Consequently, the quality of decrypted images is degraded. Therefore, it is important to design cryptosystems that can keep a good compromise between a large number of images added to text to encrypt, a small MSE after decryption, and a good performance in terms of robustness and efficiency.

As a result, this chapter suggests a new MIE algorithm based on the spectral fusion of different types of watermarked images of same size using discrete cosine transformation (DCT) associated with a low-pass filter and chaotic maps. The proposed scheme has several strengths: it is robust, combines watermarking and cryptography, which produce a two-level security, uses chaotic maps with good properties, encrypts a large number of watermarked images into two hybrid ciphered images, and the quality of the reconstructed images and text is good (reduced MSE). The encryption process comprises three main steps: in the first step, target images are fused into two images through DCT and low-pass filter; in the second step, the small blocks with the size of (4×4) images are permuted in a certain order; and in the last step, which is the diffusion phase, the two scrambled images are fused by a nonlinear mathematical expression based on Cramer's rule to obtain two hybrid encrypted images. The key generation of the cryptosystem is made dependent on the plain images.

The rest of the chapter is organized as follows: Section 2 presents an overview of chaotic generators used in the cryptosystem and the description of the watermarking process. In Section 3, spectral fusion of plain images is detailed. The proposed encryption/decryption scheme is given in Section 4. In Section 5, experimental results and algorithm analyses are presented, then compared with others in the literature. We end with a conclusion in Section 6.

2. Brief review on 1D chaotic systems used

2.1 1D logistic, May, Gaussian, and Gompertz maps

The equations of 1D Logistic, May, Gaussian, and Gompertz maps are described from Eqs. (1) to (4), respectively [11].

2.1.1 1D logistic map

$$x_{n+1} = rx_n(1 - x_n) \tag{1}$$

where $x_n \in [0, 1]$ is the discrete state of the output chaotic sequence and r is the control parameter with values in the range $(0, 4]$. The chaotic behavior of the Logistic map is observed in the range [3.5, 4].

2.1.2 May map

$$x_{n+1} = x_n \exp\left(a(1 - x_n)\right) \tag{2}$$

where $x_n \in [0, 10.9]$ and the control parameter a belongs to the range $[0, 5]$.

2.1.3 Gaussian map

$$x_{n+1} = \exp\left(-\alpha x_n^2\right) + c \tag{3}$$

where $\alpha \in [4.7, 17]$, $c \in [-1, 1]$.

2.1.4 Gompertz map

$$x_{n+1} = -bx_n \ln x_n \tag{4}$$

where the control parameter $b \in (0, e]$, e = 2.71829 ... and is the exponential function.

2.2 Combination of new 1D chaotic maps

The chaotic properties of 1D Logistic, May, Gaussian, and Gompertz maps are not suitable to build a secure cryptosystem when they are used alone. To solve this problem, Zhou et al. [23] proposed to combine the different seed maps. **Figure 1** shows the new map obtained from a nonlinear combination of two different 1D chaotic maps.

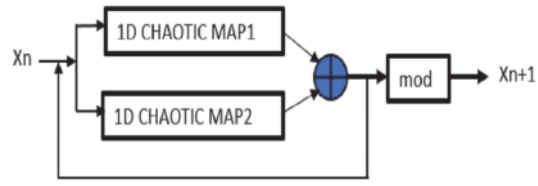

Figure 1.
New chaotic scheme.

2.2.1 Logistic-May map (LM)

Its equation is defined by Eq. (5)

$$x_{n+1} = (x_n \exp((r+9)(1-x_n)) - (r+5)x_n(1-x_n)) \bmod 2 \tag{5}$$

where $x_n \in [0,1]$ and $r \in [0,5]$. From its bifurcation diagram, we can observe that chaotic properties are excellent within [0, 5], with a maximum Lyaponuv exponent equal to 8.3.

2.2.2 May-Gaussian (MG)

Eq. (6) defines the May-Gaussian (MG) map

$$x_{n+1} = \left(x_n \exp((r+10)(1-x_n)) + \frac{(r+5)}{4} + \exp\left(-\alpha x_n^2\right) \right) \bmod 2 \tag{6}$$

where $x_n \in [0,1]$, $r \in [0,5]$, $\alpha \in [4.7, 17]$. From its bifurcation diagram, the Lyaponuv exponents are positive and belong to the range [2.5, 5.6].

2.2.3 Gaussian-Gompertz

It is defined by Eq. (7)

$$x_{n+1} = \left(\frac{(r/5+26)}{4} + \exp\left(-\alpha x_n^2\right) - (r/5+26)x_n \log x_n \right) \bmod 2 \tag{7}$$

where $x_n \in [0,1]$, $r \in [0,5]$, $\alpha \in [4.7, 17]$. It has a mean Lyaponuv exponent around 2.5.

Figure 2 illustrates the bifurcation diagram and the Lyaponuv exponent graphics of these maps. Referring to **Figure 2**, all the previous 1D chaotic systems present a wider chaotic range and a more uniform distribution of their density functions. Furthermore, the maximum Lyaponuv exponent values obtained are respectively 8.1, 5.6, and 2.5. Then, these combined 1D systems are more suitable for secure and high-speed encryption if the encryption algorithm is built around a good algebraic structure. Additively, in order to confirm the good performance of the previous pseudo random number generators, we performed the NIST statistical tests. Analysis of these results (see **Table 1**) showed that all the 15 tests were congruent for the three chaotic maps.

2.3 Description of the watermarked process

Before multiplexing the target images, a binary information in the form of a logo was inserted in one of the target images. To do this, we used a simple watermarked algorithm, which makes the hidden message imperceptible in the watermarked image. Taking advantage of the benefits of DCT, it is possible to embed an information or watermark (text, logo, image) in low- or medium-frequency DCT coefficients. In fact, DCT decomposes an image into three frequency regions: low, medium, and high frequencies. It is recommended to insert the watermark in the low- and medium-frequency regions of the host image in order to ensure imperceptibility [32]. In this work, we adopted the watermarking technique

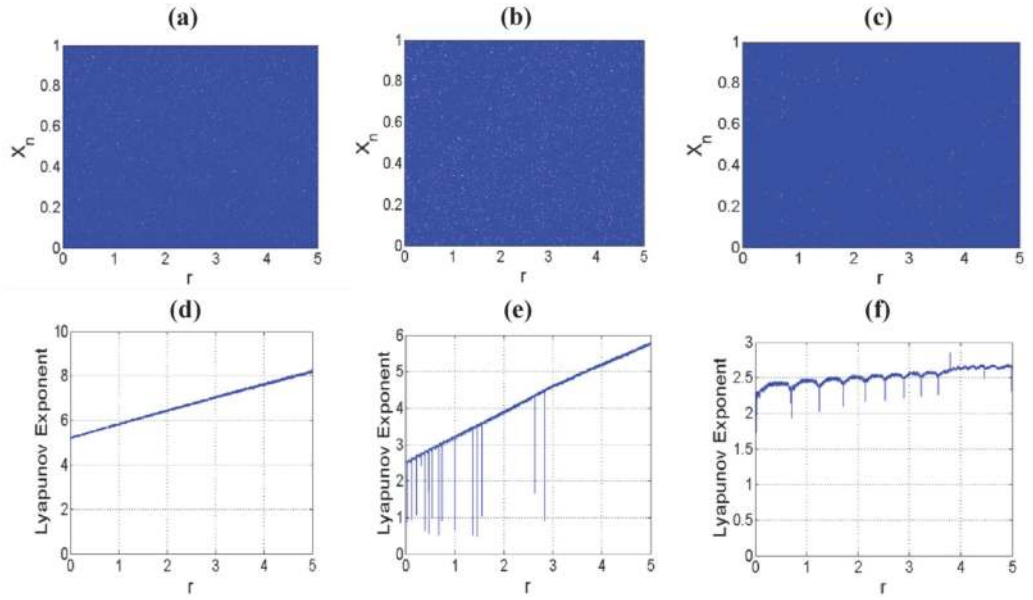

Figure 2.
Bifurcation diagrams and Lyaponuv exponent graphics of combined chaotic maps, (a) and (d) logistic-may, (b) and (e) May-Gaussian, (c) and (f) Gaussian-Gompertz.

Statistical test	Logistic-May map (LM)		May-Gaussian map (MG)		Gaussian-Gompertz map	
	p-Value	Result	p-Value	Result	p-Value	Result
Frequency	0.98147	98/100	0.99680	100/100	0.99438	100/100
Block-frequency	0.6929	97/100	0.69842	98/100	0.678415	97/100
Cumulative-sums	0.78621	96/100	0.87124	97/100	0.9014	100/100
Runs	0.88052	99/100	0.92735	100/100	0.87246	98/100
Longest-runs	0.98654	99/100	0.99815	100/100	0.97729	98/100
Rank	0.54702	97/100	0.57914	98/100	0.5873	99/100
FFT	0.87531	97/100	0.89678	98/100	0.82670	98/100
Nonoverlapping-templates	0.78951	100/100	0.75091	99/100	0.77856	98/100
Overlapping-templates	0.28435	99/100	0.18942	97/100	0.25167	98/100
Universal	0.38277	99/100	0.34834	98/100	0.37051	100/100
Approximate entropy	0.45393	98/100	0.49357	99/100	0.41560	98/100
Random-excursions	0.195257	60/60	0.192410	59/60	0.19478	59/60
Random-excursions Variant	0.14358	58/60	0.13871	57/60	0.15120	59/60
Serial	0.42962	97/100	0.47359	99/100	0.41757	97/100
Linear-complexity	0.08945	98/100	0.32876	100/100	0.15762	98/100
Final result		success		success		success

Table 1.
Statistical NIST tests results of 1,000,000 bits.

described in [33] in which the message to hide is added to the medium-frequency region discrete cosine coefficients in selected pixel blocks of size 8×8. All the blocks satisfying the condition $Ds > Av \times \alpha$ are eligible blocks suitable for watermark embedding, where Av is the average for all pixels in the block considered from

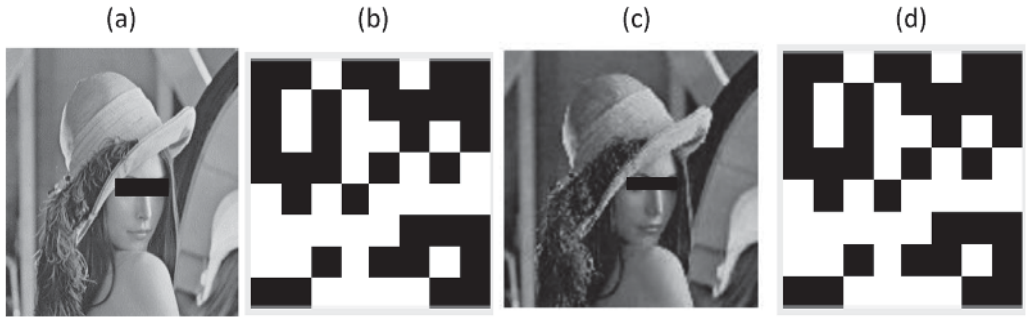

Figure 3.
Results of the watermarked process. (a) Host image (512 ×512), (b) watermark (64 ×64), (c) watermarked image, (d) recovered watermark.

the host image; *Ds* represents the difference sum for all the pixels used in the block; and α is a constant threshold value selected. The value of α must be high to ensure the most hidden message imperceptibility in the watermarked image; $\alpha \in [0, 255]$.

To illustrate an embedded process, as can be seen in **Figure 3**, we used a host image of size 512×512, and a binary watermarked image of size 64×64. We can notice from **Figure 3** that the binary image (watermarked) is recovered without loss of information.

In order to protect the watermarked and host image from unauthorized access and noise attack, the watermarked image was encrypted with other images in a mixed process.

2.4 Spectral fusion of target images

In this section, N target images of size (M, M) are combined into two images, each containing $\{N/2\}$ target images. As described in [24], discrete cosine transformation (DCT) is first applied separately to each of the target images. In the second step, every spectrum is multiplied by a low-pass filter, of size (*M'*, *M'*) pixels, as indicated in **Figure 4**. In this manner, it is possible to reconstruct every target image through the relevant information contained in each block. At this step, the compression rate C_p is:

$$C_p = 1–(\textit{size of multiplexed DCT spectral plane/size of N inputs images})$$

$$c_p = 1 - \left(M^2/N \times M^2\right) = 1 - 1/N \tag{8}$$

Then, after all of these target images are grouped together by a way of simple addition, the inverse discrete cosine transformation (IDCT) of the multiplex image

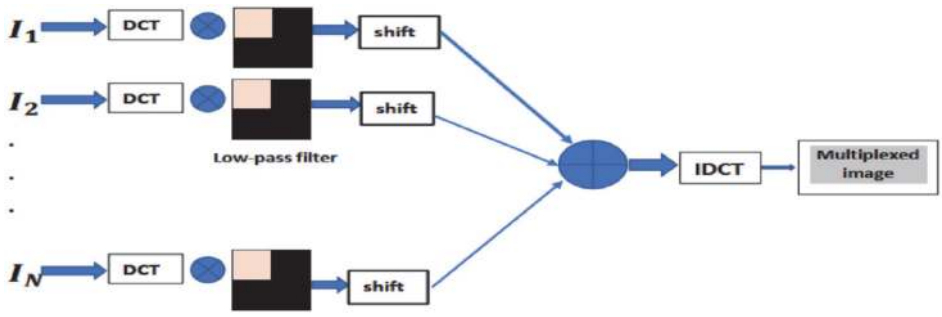

Figure 4.
Spectral fusion of target images.

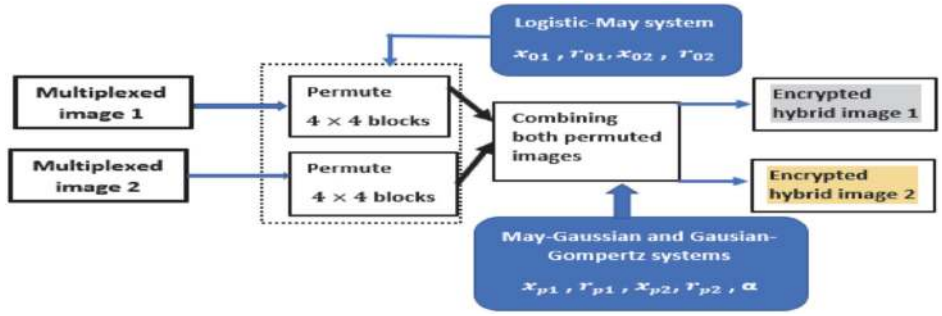

Figure 5.
Encryption scheme.

is performed. A simple rotation is performed on each of these blocks before spectral multiplexing, to prevent from information overlap. **Figure 4** illustrates the description of the process. It is possible to multiplex a large number of target images by selecting a smaller size of the filter. However, in this case, the recovered images will be highly altered. To keep a good quality of reconstructed images while maintaining a large number of target images to encrypt, we chose to group these images in two multiplex images of the same size.

2.5 Proposed encryption/decryption scheme

This section presents the proposed cryptosystem, which comprises blocks-permutation and diffusion steps using chaotic generators. **Figure 5** illustrates the entire process.

2.5.1 Encryption process

A. Blocks-permutation

The plain image is each of the two multiplex images obtained in Section 3. The plain image is decomposed into small blocks of the same size; let us choose blocks size of (4×4) pixels. In fact, increasing the number of blocks by using smaller block size resulted in a lower correlation and higher entropy; then, the intelligible information contained in the image will be reduced.

The permutation of blocks is realized as follows:

1. Divide the plain image I I of size $M \times M$ into k blocks of size (4×4), with $k = \frac{M}{4} \times \frac{M}{4}$

2. Use initial condition and control parameters x_{01}, r_{01} of Logistic-May system to generate a chaotic sequence by iterating k times Eq. (5). The values of the sequence X obtained are ranged in a row vector P of size $(1, k)$.

3. Repeat step 2 to generate a new sequence, using new initial condition and control parameters x_{02} and r_{02}. This second sequence is to permute the small blocks of the second multiplex image.

4. Sort the chaotic sequence P in ascending order, and get a new sequence $P' = \{P'_t\}_k = \{P'_{t1}; P'_{t2}, \ldots P'_{tk}\}$. Therefore, the sequence x_{01}, r_{01}, x_{02}, r_{02} is the permutation of the sequence 1, 2, … , k.

Number all the blocks of the plain image obtained in step 1, and adjust their positions with the previous permutation of step 3. Then, the image obtained is a block image permuted.

The values x_{01}, r_{01}, x_{02}, r_{02} are calculated through Eqs. (9) and (10). In this process, we subdivide each multiplex image I_i, $(i = 1, 2)$ in two parts, P_1 and P_2 of same size.

$$x_{0i} = (x_0 + mean(I_i)/255)\text{mod}1 \tag{9}$$

$$r_{0i} = \left(r_0 + 0.1 \times \max(S_1, S_2)/N \times M \times 2^9\right. \tag{10}$$

where, S_1 is the sum of pixels' intensities of the first part P_1 of the multiplex image $I_{i,}$ and S_2 for P_2. $x_0 \in [0, 0.9]$, $r \in [0, 4.9]$.

B. Diffusion of the scrambled images

At this level, the two scrambled images are combined in order to create the final hybrid encrypted images that would be difficult to crack. The May-Gaussian and Gaussian-Gompertz systems in Eqs. (6) and (7) are used as pseudo random generators to generate two chaotic sequences after 2 M × 2 M iterations. These values are arranged in two arrays W and T of sizes 2 M × 2 M, respectively, where M represents the number of rows and columns of each scrambled image. W and T are converted into real values in unit 8 format; *(W = uint8(W×255); T = uint8(T×255)).* The initial conditions and control parameters of the two pseudo random numbers generators are x_{p1}, r_{p1} and x_{p2}, r_{p2}, α, respectively, for May-Gaussian and Gaussian-Gompertz systems. These parameters are determined with Eqs. (11) and (12).

$$x_{pi} = x_0 + 0.1 \times \min(I_i)/256 \tag{11}$$

$$r_{pi} = r + 0.1 \times \min(I_i + 1)/\max(I_i + 2) \tag{12}$$

where *max* (I_i) and *min* (I_i) are, respectively, maximum and minimum pixel's intensities values of I_i. $x_0 \in [0, 0.9]$, $r \in (0, 4.9]$.

$$\mathrm{W} = \left(\begin{array}{c|c} w_{11} & w_{12} \\ \hline w_{21} & w_{22} \end{array}\right) \;;\; \mathrm{T} = \left(\begin{array}{c|c} t_{11} & t_{12} \\ \hline t_{21} & t_{22} \end{array}\right) \tag{13}$$

The arrays W and T are divided into four sub-blocks of same size M × M. The two scrambled images $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$ are linearly combined with the sub-blocks of W and T using the following equations:

$$C_1(i,j) = [w_{11} \times I_1(i,j) + w_{12} \times I_2(i,j))\text{mod}256 \oplus floor(t_{11} \times t_{21}) \times 10^{15})] \tag{14}$$

$$C_2(i,j) = [w_{21} \times I_1(i,j) + w_{22} \times I_2(i,j))\text{mod}256 \oplus floor(t_{12} \times t_{22}) \times 10^{15})] \tag{15}$$

where $C_1(i,j)$ and $C_2(i,j)$ are the two encrypted hybrid images of the cryptosystem, and $\oplus$ is the bit wise XOR operator. The mixed product $t_{ij} \times t_{ji}$ in the above relations enhances the quality of the merged images.

2.5.2 Decryption process

In the decryption process, the encrypted images are first decomposed using Cramer's rule in order to recover the scrambled images. Knowing the fusion keys

$(x_{p1}, r_{p1}, x_{p2}, r_{p2}, \alpha)$, the receiver can get the images I_1 and I_2 by solving the system of equations below:

$$\begin{cases} (I_1[i,j] \times w_{11} + I_2[i,j] \times w_{12})_{mod256} = C_1\big(floor(t_{11} \times t_{21}) \times 10^{15}\big) \\ (I_1[i,j] \times w_{21} + I_2[i,j] \times w_{22})_{mod256} = C_2\big(floor(t_{12} \times t_{22}) \times 10^{15}\big) \end{cases} \tag{16}$$

Then, the two multiplex images can be obtained easily by decrypting $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$ through reverse permutation operations.

3. Experimental results and algorithm analysis

Numerical simulation experiments have been carried out to verify the proposed encryption method using MATLAB 2016 b platform on a PC with Core (TM) i7-353U processor of 2.5GHz. We first take eight images with 512 × 512 pixels and 256 gray levels as the target images to be encrypted, which are combined in two multiplex images as shown in **Figure 6** (*a–h*), respectively. The compression ratio C_p is 0.75 for each multiplex image. The size of low-pass filter is (*M*', *M*') = (256, 256) pixels. Results are analyzed more in terms of statistical attack, differential

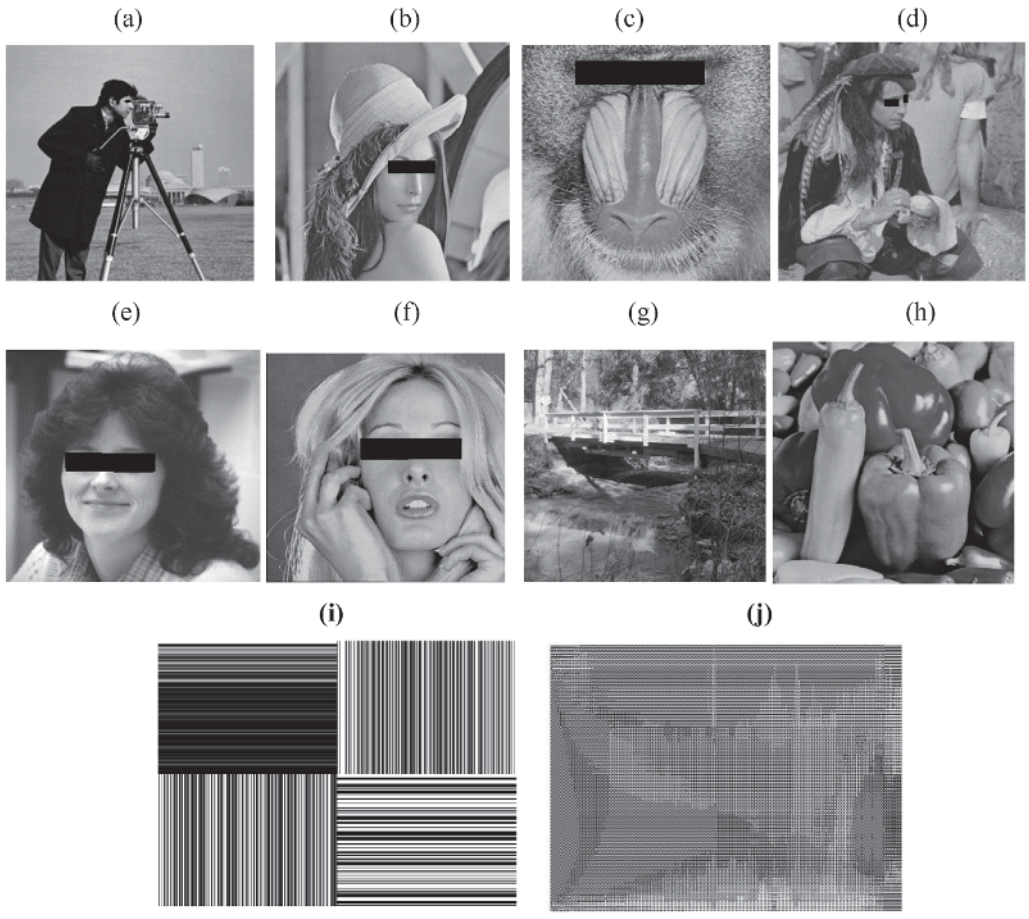

Figure 6.
Plain and combined images. (a–d) Images combined in multiplex image 1, (e–h) images combined in multiplex image 2, (i) multiplex image 1 before IDCT, (j) multiplex image 1 after IDCT.

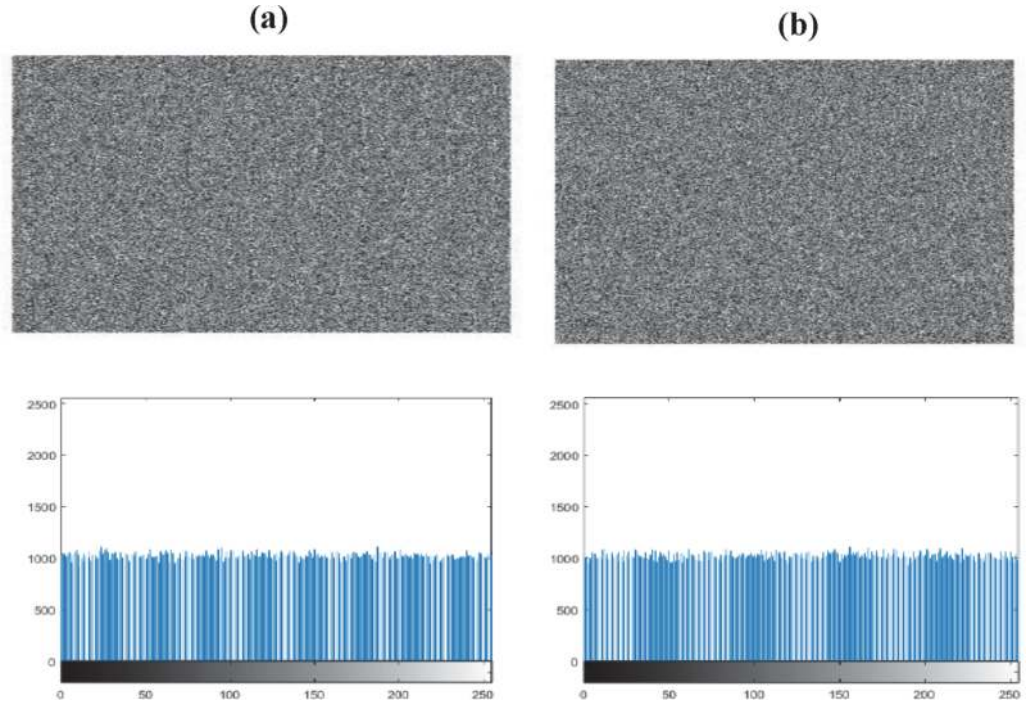

Figure 7.
Encrypted images and their histograms. (a) Multiplexed image 1, (b) multiplexed image 2.

attack, quality of decrypted images, and speed. We chose the different values as keys of the proposed cryptosystem:

x_{01} = 0.351482953177765; x_{02} = 0.972970074275508; r_{01} = 4.988242173292221; r_{02} = 4.909240772131021; x_{p1} = 0.363606938668312; x_{p2} = 0.890363879273465; r_{p1} = 4.841585120587438; r_{p2} = 4.738149127386060; α = 6.187.

The size of the filter (M', M') and the number of target images N constitute additional parameters of the key.

3.1 Statistical analysis

3.1.1 Histogram

For a well-ciphered image, all the frequencies of pixels must be uniformly distributed. As one can see in **Figure 7**, the histogram of the multiplex encrypted images is uniform.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{17}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\left|\frac{C_1(i,j) - C_2(i,j)|}{255}\right]\right] \times 100\% \tag{18}$$

3.1.2 Correlation analysis

A good cryptosystem produces a cipher image with a correlation coefficient close to zero, for two adjacent pixels. Five thousand pairs of adjacent pixels were chosen to calculate the correlation coefficients in horizontal, vertical, and diagonal directions respectively, by using Eq. (17).

$$C_{rxy} = \frac{K \times \sum_{i=1}^{K} X_i Y_i - \sum_{i=1}^{K} X_i^2 \times \sum_{i=1}^{K} {Y_i}^2}{\sqrt{\left(K \times \sum_{i=1}^{K} (X_i)^2 - \left(\sum_{i=1}^{K} X_i\right)^2\right) \times \left(K \times \sum_{i=1}^{K} (Y_i)^2 - \left(\sum_{i=1}^{K} Y_i\right)^2\right)}} \tag{19}$$

where X and Y are the values of two adjacent pixels in the image, C_{rxy} belongs to the range [−1, 1] and K denotes the number of pairs of pixels randomly selected. C_{rxy} tends to be 1 or − 1 for strong correlation and tends to be 0 for every poor correlation. **Table 2** shows the calculated correlation coefficient of 512 × 512 cameraman and peppers images in every direction. A mean value of the proposed encryption algorithm is about 0.0032, which tends to be zero, which is the expected value. The same result can be confirmed in **Figure 8**, where the pixels of encrypted

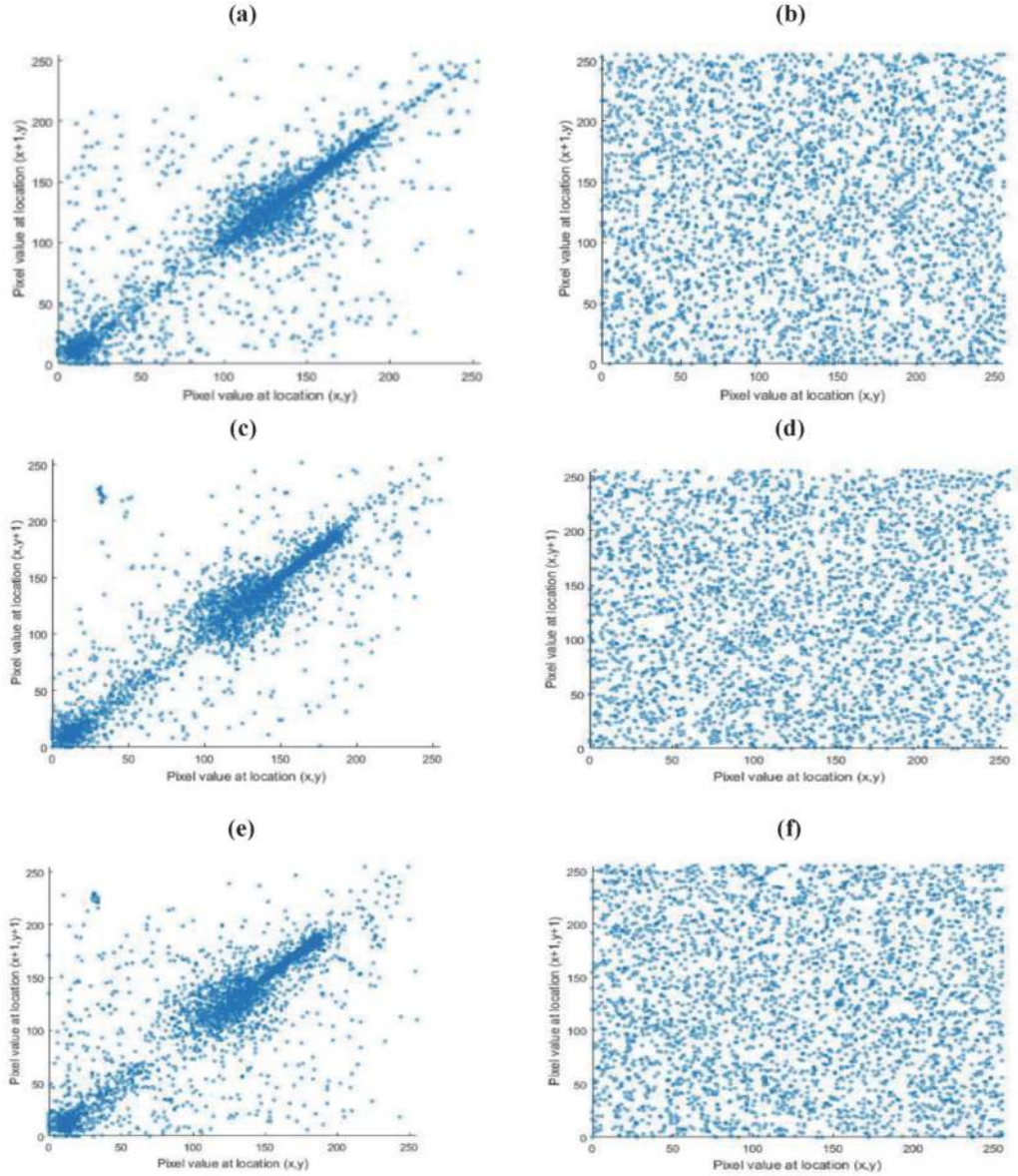

Figure 8.
Plot of correlation coefficients in horizontal, vertical, and diagonal directions of plain and cipher cameraman (512 × 512). (a, c, e) correlation coefficients of plain images in horizontal, vertical, and diagonal directions respectively. (b, d, f) correlation coefficients of ciphered images in horizontal, vertical, and diagonal directions respectively.

Imageq	Test	Plain image	Encrypted multiplex image 1 or 2
Cameraman	HC	0.9314	0.0023
	VC	0.9400	0.051
	DC	0.8931	−0.003
Peppers	HC	0.9934	0.0013
	VC	0.9954	−0.0020
	DC	0.9919	0.0044

Table 2.
Correlation coefficient.

images are not correlated in different directions. Then, these results prove that attacks based on correlation analysis cannot succeed on the proposed cryptosystem.

3.1.3 Information entropy analysis

The information entropy evaluates the level of randomness contained in a sequence m, and it is defined as follows:

$$S(m) = \sum_{i=0}^{2^M-1} p(m_i) \log_2 \left(\frac{1}{p(m_i)} \right) \tag{20}$$

where $p(m_i)$ is the probability of the recurrence of element m_i and M denotes the number of bits of information m. The ideal entropy value of a 256-grayscale image represented on 8 bits with equal probability is 8. **Table 3** shows entropy values of the two multiplex images of the proposed encryption algorithm very close to 8, as expected.

3.2 Key analysis

Key space size is the total number of different keys that can be used in an encryption algorithm. A good encryption algorithm needs to contain sufficiently large key space to make the brute-force attack infeasible. The high sensitivity to initial conditions inherent to any chaotic system, that is, exponential divergence of chaotic trajectories, ensures high security [11].

In literature, a key space of at least 10^{30} is required for the system to be robust [19]. The proposed encryption algorithm actually does have some of the following secret keys: the initial values x_{01}, x_{02}, x_{p1}, x_{p2} and control parameters r_{01}, r_{02}, r_{p1}, r_{p2} and α of the chaotic systems used; the number N of target images and the size $M' \times M'$ of the filter. We suppose that the computer precision is 10^{-15}, so the key space is greater than $10^{15 \times 9} = 10^{135}$. Therefore, this key space is large enough to resist the brute-force attack. Moreover, key sensitivity analysis has been carried out, but the results are not presented here for reasons of space. These results confirm

Gray image	Proposed algorithm	[20] (2017)	[19] (2017)
Multiplex image 1	7.9993	—	—
Multiplex image 2	7.9993	7.9993	7.9992

Table 3.
Information entropy of some ciphered images.

Image	Test	
Multiplex encrypted image 1	NCPR	99.62
	UACI	33.54
Multiplex encrypted image 2	NCPR	99.63
	UACI	33.47

Table 4.
NCPR AND UACI measure after a LSB change.

that by changing only one bit in any parameter of the key, it is not possible to recover the plain images.

3.3 Sensitivity analysis

3.3.1 Differential attack analysis

An excellent encryption algorithm should have the desirable property of spreading the influence of slight change to the plain text over as much of the cipher text as possible. The sensitivity of a cryptosystem is evaluated through Number of Pixel Change Rate (NPCR), see Eq. (19), and Unified Average Change Intensity (UACI), see Eq. (20), criteria, which consist in testing the influence of one-pixel change of a plain image in the resulting cipher image.where C_1 and C_2 are two images with same size $W \times H$. If $C_1(\mathrm{i}, \mathrm{j})$ # $C_2(\mathrm{i}, \mathrm{j})$ $\mathrm{C}_1(\mathrm{i}, \mathrm{j}) \neq \mathrm{C}_2(\mathrm{i}, \mathrm{j})$ then $D(i,j) = 1$ $\mathrm{D}(\mathrm{i}, \mathrm{j}) = 1$, otherwise, $D(i,j) = 0$.

Table 4 gives the measurement of NCPR and UACI between two cipher images of cameraman, Lena and peppers, when a Least Significant Bit (LSB) changed on gray value in the last pixel's position. We can notice that the values obtained are around the mean of 99.61 for NCPR and 33.49 for UACI. This result shows that a slight change to the original images will result in a great change in all the encrypted images. The results also imply that the proposed algorithm has an excellent ability to resist the differential attack.

3.3.2 Quality of reconstructed images

As the number of target images to encrypt increases, the quality of recovered images decreases. In order to reduce the NMSE between plain and decrypted images and enlarge the number of target images, we grouped them into two multiplexed images before encryption. To evaluate quantitatively the quality of decrypted image, we used the normalized mean square error (NMSE) between the original image and the decrypted image. The NMSE is defined as:

$$\mathrm{NMSE} = \frac{\sum_{\mathrm{i}=1}^{\mathrm{N}} \sum_{\mathrm{j}=1}^{\mathrm{M}} [\mathrm{I_D}(\mathrm{i}, \mathrm{j}) - \mathrm{I_E}(\mathrm{i}, \mathrm{j})]^2}{\sum_{\mathrm{i}=1}^{\mathrm{N}} \sum_{\mathrm{j}=1}^{\mathrm{M}} [\mathrm{I_E}(\mathrm{i}, \mathrm{j})]^2} \tag{21}$$

where $\mathrm{M} \times \mathrm{N}$ are the size of the image, $\mathrm{I_D}(\mathrm{i}, \mathrm{j})$ and $\mathrm{I_E}(\mathrm{i}, \mathrm{j})$ are the values of the decrypted image and the original image at the pixel (i, j), respectively. **Table 5** presents the values of NMSE for a set of different target images of size 512×512. From this table, we can observe that for *N = 16* target images combined in one multiplex image, that is, 32 images to encrypt by the proposed cryptosystem,

the NMSE is still low, which attests the good quality of reconstructed images and good performances of the proposed cryptosystem.

3.4 Encryption/decryption time

Table 6 reports a comparison of encryption time by the proposed algorithm with some recent works in literature for different images. The algorithm written under Matlab platform was not optimized. The computer time consumption is 0.27389 s, which is smaller than those of [19, 24].

3.5 Comparison with other encryption algorithms

The performance of the proposed algorithm compared to similar and good standing ones in literature is shown in **Table 7**. From the table, we can observe that the proposed encryption algorithm has a large key space and can encrypt a large number of target images in a good time compared to others. As for UACI and NPCR, they are about the best values expected (respectively >33.3 for UACI and >99.6 for NPCR) as can be seen in the table. Finally, our cryptosystem exhibits the best correlation value and a reduced normalized Mean Square Error (MSE) after decryption step.

Number of target images ($N \times 2$)	**4×2**	**9×2**	**16×2**
NMSE	0.00082	0.0019	0.00376

Table 5.
NMSE for a set of different target images.

Number of images	**Proposed algorithm**	**[19] (2017)**	**[20] (2017)**	**[24] 2016**
08 or 09, size 512×512	0.27389	0.7103	0.191	11.66

Table 6.
Encryption time in seconds.

	Key space	**Average correlation**	**Entropy**	**NPCR**	**UACI**	**Encryption time (s)**	**NMSE**
Proposed algorithm	10^{135}	0.0032	7.9993	99.61	33.49	0.27389	3.7×10^{-3}
Ref. [19] [2017]	10^{60}	0.003	7.9994	99.62	33.50	0.7103	—
Ref. [20] [2017]	10^{56}	—	7.8225	—	—	0.255	—
Ref. [24] [2016]	10^{90}	—	—	—	—	11.66	8.448×10^{-3}
Ref. [14] [2015]	2^{260}	0.0032	—	99.92	—	—	**≈0**
Ref. [25] [2018]	10^{210}	0.0031	7.9986	99.62	33.42	2.386	0.0155

Table 7.
Comparison of the proposed cryptosystem with others.

4. Conclusion

In this chapter, an image encryption algorithm based on spectral fusion of multiple watermarked images and new chaotic generators is proposed. Logistic-May (LM), Gaussian-Gompertz (GG), and May-Gaussian (MG) systems were used as chaotic generators in the processes of confusion and diffusion. The target images were firstly combined in two multiplex images of same size through DCT and a low-pass filter. Secondly, the previous images are scrambled by permuting the blocks size of (4×4) of each multiplex image. Finally, the later scrambled images are fused by a nonlinear mathematical expression based on Cramer's rule to obtain two hybrid encrypted images. At the decryption step, the watermark hidden in one of the target images is recovered without loss of information. The evaluation metrics of the proposed cryptosystem NCPR, UACI, correlation coefficient, entropy, key space, and NMSE, are among the best values in literature. More interestingly, the proposed cryptosystem can encrypt 32 target images simultaneously with a small NMSE$\approx 4.16 \times 10^{-3} \approx 3.7 \times 10^{-3}$, and encrypted images are sensitive to the key. The proposed encryption algorithm can surely guarantee security and speed of all types of digital data (text and images) transfer in a digital network.

Acknowledgements

This work was partly supported by ERMIT, Entrepreneurship, Resources, Management, Innovation and Technologies.

Conflict of interest

The authors declare that they have no conflict of interest.

Author details

Lee Mariel Heucheun Yepdia[1], Alain Tiedeu[1*] and Zied Lachiri[2]

1 Signal, Image and Systems Laboratory, Department of Medical and Biomedical Engineering, Higher Technical Teachers Training College, University of Yaoundé, Ebolowa, Cameroon

2 Department of Electrical Engineering, Signal, Image and Technologies of Information Laboratory, National Engineering School, ENIT, Tunis, Tunisia

*Address all correspondence to: alain.tiedeu@gmail.com

References

[1] Liao X, Lai S, Zhou Q. A novel image encryption algorithm based on self-adaptive wave transmission. Journal of Signal Processing. 2010;**90**:2714-2722

[2] Zhu C. A novel image encryption scheme based on improved hyperchaotic sequences. Journal of Optical Communication. 2012;**285**:29-37

[3] Abanda Y, Tiedeu A. Image encryption by chaos mixing. IET Image Processing. 2016;**10**:742-750

[4] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering. 2015;**66**:10-18

[5] Rhouma R, Belghith S. Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem. Physics Letters A. 2008; **A372**:5790-5794

[6] Wang Y, Liao X, Xiang T, Wong K, Yang D. Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map. Physique Letters. 2007;**A363**:277-281

[7] Patidar V, Pareek N, Sud K. A new substitution-diffusion based image cipher using chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation. 2009;**14**(7):3056-3075

[8] Zhu Z, Zhang W, Wong K, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences. 2011;**181**:1171-1186

[9] Song C, Qia Y, Zhang X. An image encryption scheme based on new spatiotemporal chaos. Optik. 2013;**124**: 3329-3334

[10] Gao H, Zhang Y, Liang S, Li D. A new chaotic algorithm for image encryption. Chaos, Solitons and Fractals. 2005;**29**:393-399

[11] Kamdeu Y, Tiedeu A. An image encryption algorithm based on substitution technique and chaos mixing. Multimedia Tools and Applications. 2018;**77**(19):1-22

[12] Chenaghlu M, Balafar M, Feizi-Derakhshi M. A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. Signal Processing. 2018;**157**:1-22

[13] Alfalou A, Brosseau C, Abdallah N. Simultaneous compression and encryption of color video images. Optics Communication. 2015;**338**:371-379

[14] Jridi M, Alfalou A. Real-time and encryption efficiency improvements of simultaneous fusion, compression and encryption method based on chaotic generators. Optics and Lasers in Engineering. 2018;**102**:59-69

[15] Alfalou A, Brosseau C, Abdallah N, Jridi M. Simultaneous fusion, compression and encryption of multiple images. Optics Express. 2011;**24**: 24023-24029

[16] Dongfeng S, Jian H, Yingjian W, Kee Y. Simultaneous fusion, imaging and encryption of multiple objects using a single-pixel detector. Scientific Reports. 2017;**7**:18-29

[17] Mehra I, Nishchal N. Wavelet-based image fusion for securing multiple images through asymmetric keys. Optics Communications. 2015;**335**:153-160

[18] Qin Y, Gong Q, Wang Z, Wang H. Optical multiple-image encryption in diffractive-imaging-based scheme using spectral fusion and nonlinear operation. Optics Express. 2016;**24**:26877-26886

[19] Zhang X, Wang X. Multiple-image encryption algorithm based on mixed image element and permutation. Optics and Lasers in Engineering. 2017;**92**:6-16

[20] Zhang X, Wang X. Multiple-image encryption algorithm based on mixed image element and chaos. Computers and Electrical Engineering. 2017;**000**: 1-13

[21] Zhu G, Zhang X. Mixed image element encryption based on an elliptic curve cryptosystem. Journal of Electronic Imaging. 2008;**17**(2):023007

[22] Abdalla A, Tamimi A. Algorithm for image mixing and encryption. The International Journal of Multimedia & Its Applications (IJMA). 2013;**5**(2):15-21

[23] Zhou Y, Bao L, Chen C. A new 1D chaotic system for image encryption. Signal Processing. 2014;**97**:172-182

[24] Ren G, Han J, Zhu H, Fu J, Shan M. High security multiple-image encryption using discrete cosine transform and discrete multiple-parameters fractional Fourier transform. The Journal of Communication. 2016;**11**(5):491-497

[25] Karawia A. Encryption algorithm of multiple-image using mixed image elements and two-dimensional chaotic economic map. Entropy. 2018;**20**:801. DOI: 10.3390/e20100801

[26] Al-Haj A, Mohammad A. Crypto-watermarking of transmitted medical images. Journal of Digital Imaging. 2017; **30**(1):26-38

[27] Abdel-Nabi H, Al-Haj A. Efficient joint encryption and data hiding algorithm for medical images security. In: 8th International Conference on Information and Communication Systems (ICICS). Irbid, Jordan: IEEE; 4-6 April 2017. pp. 147-152. DOI : 10.1109/IACS.2017.7921962

[28] Dagadu JC, Jianping L. Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. Multimedia Tools and Applications. 2018;**77**: 24289-24312

[29] Maheshkar S. Region-based hybrid medical image watermarking for secure telemedicine applications. Multimedia Tools and Applications. 2017;**76**(3): 3617-3647

[30] Singh AK, Dave M, Mohan A. Robust and secure multiple watermarking in wavelet domain. Journal of Medical Imaging and Health Informatics. 2015;**5**(2):406-414

[31] Lian S, Liu Z, Yuan D, Wang H. On the joint audio fingerprinting and decryption scheme. In: IEEE International Conference on Multimedia and Expo; Hannover. 2008. pp. 261-264

[32] Abhilasha S, Kumar A, Singh S, Prakash G. Robust and secure multiple watermarking for medical images. Wireless Personal Communications. 2017;**92**:1611-1624

[33] Obin A, Varghese P. Image watermarking using DCT in selected pixel regions. In: International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). Kanyakumari; 2014. pp. 398-402. DOI : 10.1109/ ICCICCT.2014.6992994