Multiple Image Fusion Encryption (MIFE) using Discrete Cosine Transformation (DCT) and Chaotic Generators

Lee Mariel Heucheun Yepdia, Alain Tiedeu
Dept. of Medical and Biomedical Engineering, Signal, Image and Systems Laboratory
Higher Teachers Technical Training College, ENSET EBOLOWA
Yaounde, Cameroon
Email: yepdiamariel26@gmail.com; alain.tiedeu@gmail.com

Zied Lachiri
Dept. of Electrical Engineering, Signal, Image and Technologies of Information Laboratory
National Engineering School, ENIT
Tunis, Tunisia
Email: ed.lachiri@enit.utm.tn

***Abstract*—This paper proposes a new multiple-image encryption algorithm based on spectral fusion of 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-passed filter of appropriate size are used to combine the target 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 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. The security analysis and experimental simulations confirmed that the proposed algorithm has a good encryption performance; it can encrypt a large number of images of different types while maintaining a reduced Mean Square Error (MSE) after decryption**.

Keywords*—Spectral fusion; chaotic generators; image encryption.

I. INTRODUCTION

Several image encryption algorithms are being developed today to meet privacy needs in multimedia communications. 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. Especially today, a large quantity of images is produced in various fields and exchanged through different channels, favouring the development of Multiple Images Encryption (MIE) instead of Single Image Encryption (SIE).

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 behaviour, 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 can be divided into 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, Tent, and Sine map have proven to have the advantages of 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 weakness like non-uniform 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 state 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

 ISBN: 978-1-61208-746-7

Nonlinear Chaotic map Algorithm (NCA) [10], and more recently, nonlinear combinations of two different 1D chaotic maps [3][11][12]. For example, Y. Abanda and A. Tiedeu [3] combined outputs of Duffing and Colpitts chaotic systems to encrypt grey and colour images. Y. P. Kamdeu and A. Tiedeu [11] proposed a fast and secured encryption scheme using new 1D chaotic systems obtained from Logistic, May, Gaussian and Gompertz maps. In [12], M. A. 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 the spatial or frequency domain. 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 way of decreasing the quantity of data to be transmitted and guarding the use of 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. In 2018, M. Jridi and A. Alfalou [14] proposed an algorithm to enhance an existing optical Simultaneous Fusion, Compression and Encryption (SFCE) scheme [15] in terms of real-time requirements, bandwidth occupation and encryption robustness. In [16], S. Dongfeng et al. proposed a novel technique for simultaneous fusion, imaging and encryption of multiple objects 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 good quality of images recovered. I. Mehra and N. K. 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, Y. Qin et al. [18] proposed an Optical Multiple-Image Encryption scheme in diffractive imaging using spectral fusion and nonlinear operations.

More recently, X. Zhang and X. 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], G. L. Zhu and X. Q. 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, A. M. Abdalla and A. A. Tamimi [22] proposed a new algorithm, which mixes two or more images of different types and sizes by using a shuffling procedure combined with S-box substitution to perform a lossless image encryption. Here, the process of mixing image combines stream cipher with block cipher, on the byte level.

After analysing 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 which can keep a good compromise between a large number of images to encrypt, a small MSE after decryption and a good performance in terms of robustness and efficiency.

As a result, this paper suggests a new MIE algorithm based on the spectral fusion of different types of images of same size using Discrete Cosine Transformation (DCT) associated with a low-passed filter and chaotic maps. The proposed scheme has several strengths: it is robust, uses chaotic maps with good properties, encrypts a large number of images into two hybrid ciphered images, and the quality of the reconstructed images 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-passed filter. In the second step, the small blocks with the size of (4 X 4) images are permuted in a certain order. 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 paper is organized as follows: Section 2 presents an overview of chaotic generators used in the cryptosystem while 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.

II. BRIEF REVIEW ON 1D CHAOTIC SYSTEMS USED

A. 1D Logistic, May, Gaussian and Gompertz maps

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

1) 1D Logistic map

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

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 behaviour of the Logistic map is observed in the range [3.5, 4].

2) May map

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

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

3) Gaussian map

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

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

4) Gompertz map

$$x_{n+1} = -b x_n \ln x_n \quad (4)$$

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

B. 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, Y. 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.

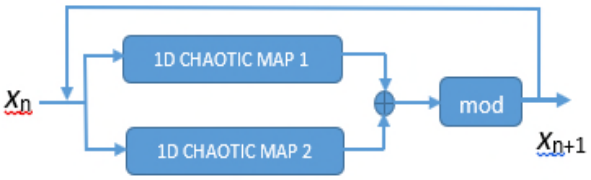

Figure 1. New chaotic scheme.

1) Logistic-May map (LM)

Its equation is defined by (5)

$$x_{n+1} = \begin{pmatrix} x_n \exp\left((r+9)(1-x_n)\right) - \\ (r+5) x_n (1-x_n) \end{pmatrix} \bmod 2 \quad (5)$$

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) May-Gaussian (MG)

Equation (6) defines the May-Gaussian (MG) map

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

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].

3) Gaussian-Gompertz

It is defined by (7)

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

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.

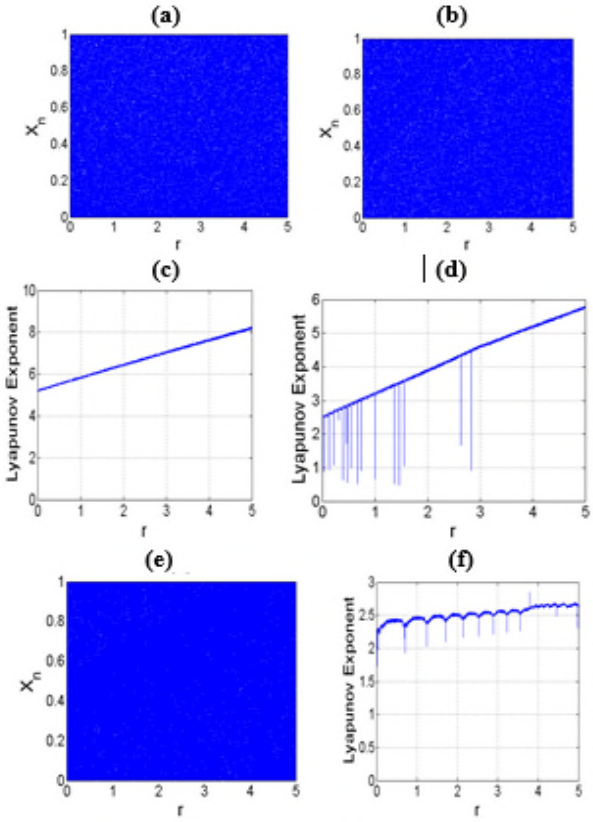

Figure 2. Bifurcation diagrams and Lyaponuv exponent graphics of combined chaotic maps, (a) and (c) Logistic-May, (b) and (d) May-Gaussian, (e) and (f) Gaussian-Gompertz.

 ISBN: 978-1-61208-746-7

III. SPECTRAL FUSION OF TARGET IMAGES

We consider N target images of size (M, M), which are combined with 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. Secondly, every spectrum is multiplied by a low-passed filter, of size (M', M') pixels, positioned in its upper left corner. In this way, a block containing the relevant information for reconstructing every target image is obtained. At this step, the compression rate C_r is:

C_r = 1 – *(size of multiplexed DCT spectral plane) /size of N inputs images*

$$C_r = 1 - (M^2 / N \times M^2) = 1 - (1/N) \quad (8)$$

Then, after all of these target images are grouped together by a way of simple addition, the inverse Discrete Cosine Transform (IDCT) of the multiplex image is performed. To avoid information overlap, these blocks are shifted by a rotation before spectral multiplexing. Figure 3 illustrates the description of the process. It should be noted that the capability of multiplexing can be increased by appropriately selecting the filter size. The smaller the filter size is, the more images can be multiplexed, but the quality of recovered images may be worse. 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.

IV. PROPOSED ENCRYPTION/DECRYPTION SCHEME

This section presents the proposed cryptosystem, which comprises blocks-permutation and diffusion steps using Chaotic generators. Figure 4 illustrates the entire 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 realised as follows:

1. Divide the plain image I of size $M \times M$ into k blocks size of (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 (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 $P' = \{P'_i\}_k = \{P't1; P't2, \cdots, P'tk\}$ .Therefore, the sequence x_{01}, r_{01}, x_{02}, r_{02} is the permutation of the sequence 1, 2,…, k.
5. 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.

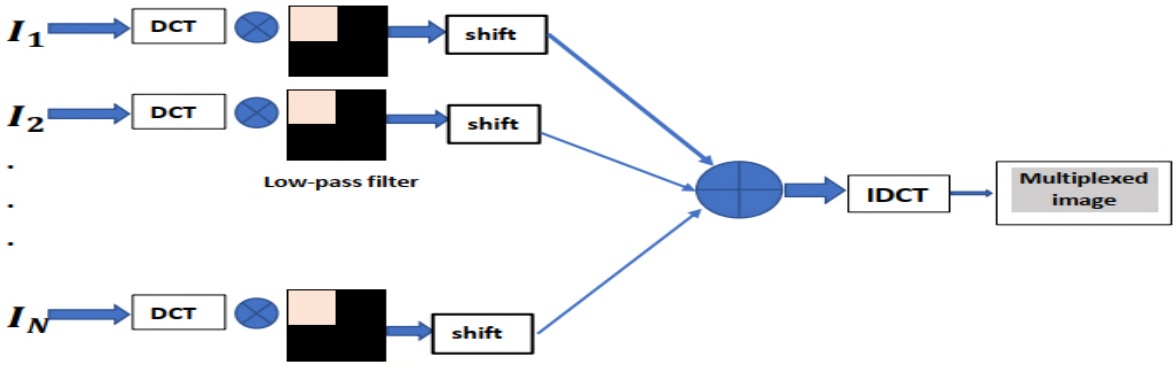

Figure 3. Spectral fusion of target images.

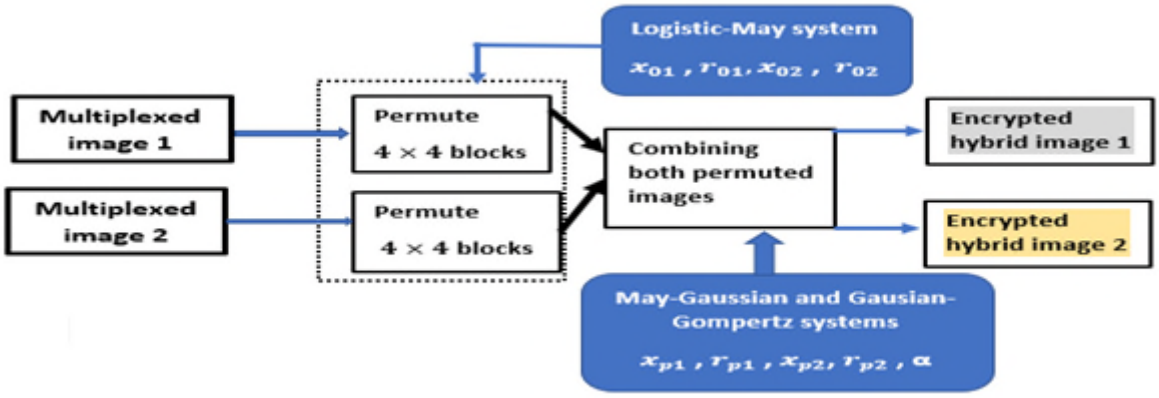

Figure 4. Encryption scheme.

The values x_{01}, r_{01}, x_{02}, r_{02} are calculated through (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.

$$x_{0i} = (x_0 + mean\ (I_i)/255)_{mod1} \quad (9)$$

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

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

1) Description of the fusion process

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 (6) and (7) are used as pseudo random generators to generate two chaotic sequences after 2M*2M iterations. These values are arranged in two arrays W and T of sizes 2M*2M, 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 (11) and (12).

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

$$rpi = r + 0.1 \times [(min(I_i + 1)/max(I_i + 2)] \quad (12)$$

where *mean* (I_i) represents the average of the pixels' intensities values of multiplex image I_i, *(i=1,2); max* (I_i) and *min* (I_i) are, respectively, maximum and minimum pixel's intensities values of I_i. $x_0 \in [0, 0.9]$, $r \in [0, 4.9]$.

The arrays W and T are divided into four sub-blocks of same size M × M.

$$W = \begin{pmatrix} w_{11} & w_{12} \\ w_{21} & w_{22} \end{pmatrix} \ ; \ T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \quad \textbf{(13)}$$

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:

$$C_1[i, j] = [(w_{11} \times I_1[i, j] + w_{12} \times I_2[i, j])_{mod256} \oplus floor(t_{11} \times t_{21}) \times 10^{15})] \quad (14)$$

$$C_2[i, j] = [(w_{21} \times I_1[i, j] + w_{22} \times I_2[i, j])_{mod256} \oplus floor(t_{12} \times t_{22}) \times 10^{15})] \quad (15)$$

where $C_1[i, j]$ and $C_2[i, j]$ are the two encrypted hybrid images of the cryptosystem, and ⊕ 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) Decryption process

At the receiver end, 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}, α), the receiver can get the images $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$ by solving the system of equations below:

$$\begin{cases} \left(I_1[i, j] \times w_{11} + I_2[i, j] \times w_{12}\right)_{mod\,256} \\ = C_1\left(floor\left(t_{11} \times t_{21}\right) \times 10^{15}\right) \\ \left(I_1[i, j] \times w_{21} + I_2[i, j] \times w_{22}\right)_{mod\,256} \\ = C_2\left(floor\left(t_{12} \times t_{22}\right) \times 10^{15}\right) \end{cases} \quad (16)$$

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

 ISBN: 978-1-61208-746-7

V. 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 8 images with 512×512 pixels and 256 grey 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_r is 0.75 for each multiplex image. The size of low-passed filter is (*M'*, *M'*) = (256,256) pixels. Results are analysed more in terms of statistical attack, differential 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; xp_1 = 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.

A. Statistical analysis

1) Histogram

The histogram of a noise-like-image must be uniform. As one can see in Figure 5, the histogram of the multiplex encrypted images is uniform.

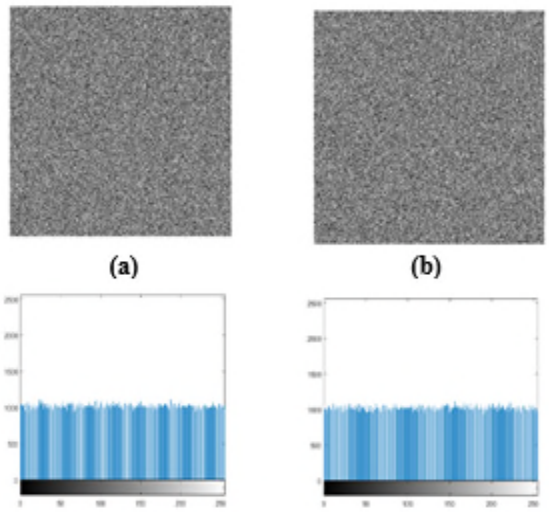

Figure 5. Encrypted images and their histograms. (a) multiplexed image 1, (b) multiplexed image 2.

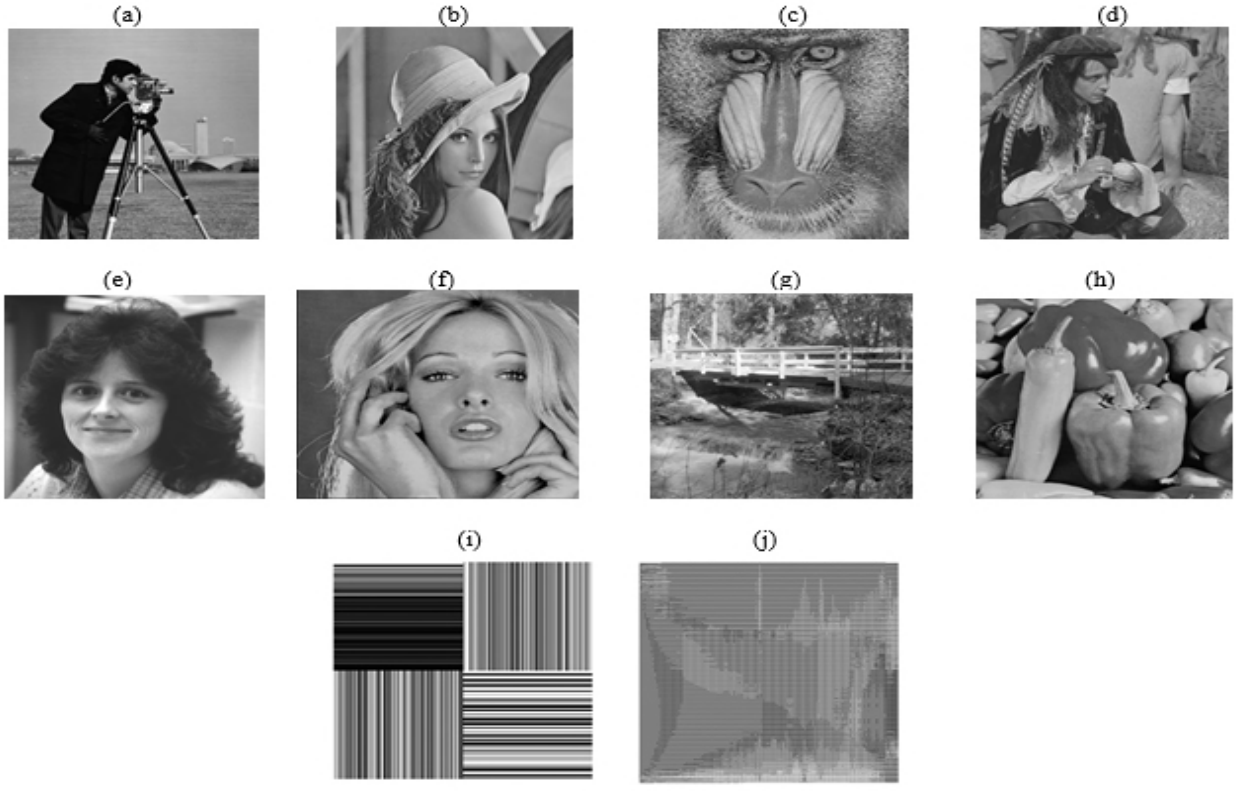

Figure 6. Plain and combined images. (a-d) images combined in multiplex image 1, (e-h) images combined in multiplex image 2 (i) Multiplex image 1 before IDCT. 2 (j) Multiplex image 1 after IDCT.

2) Correlation analysis

In the encrypted image, there must be a very poor correlation between neighbouring pixels in every direction, for this one to resist statistical attack. The common method is to calculate the correlation coefficient *Cr* of randomly chosen 5000 pairs of pixels in horizontal (HC), vertical (VC) and diagonal (DC) direction using (17).

$$Cr = \frac{K \times \sum_{i=1}^{K} X_i Y_i - \sum_{i=1}^{K} X_i^2 \times \sum_{i=1}^{K} Y_i^2}{\sqrt{\left(K \times \sum_{i=1}^{K} (X_i)^2 - \left(\sum_{i=1}^{K} X_i\right)^2\right) \times \left(N \times \sum_{i=1}^{K} (Y_i)^2 - \left(\sum_{i=1}^{K} Y_i\right)^2\right)}} \quad (17)$$

where X and Y are grey scale values of two adjacent pixels in the image, K is the number of pair of pixels. C_r is the value of correlation belonging to the range [-1, 1]. *Cr* tends to be 1 or -1 for strong correlation and tends to be 0 for every poor correlation. Table 1 shows the calculated correlation coefficient of 512×512 cameraman in every direction. A mean value of the proposed encryption algorithm is about 0.0035, which tends to be zero.

Figure 7 shows how grey values of cameraman correlated with the horizontal, vertical and diagonal direction. Statistical attack through correlation analysis between adjacent pixels cannot help to break the proposed encryption algorithm.

TABLE I. CORRELATION COEFFICIENT

Image	*Size*	*Test*	*Plain image*	*Encrypted image*
Cameraman	(512 ×512)	HC	0.9314	0.0023
		VC	0.9400	0.051
		DC	0.8931	-0.003

3) Information entropy analysis

The information entropy gives an account of the quantum of randomness present in a message (m) as follows:

$$H(m) = \sum_{i=0}^{2^k - 1} p(m_i) \log_2 \left(\frac{1}{p(m_i)}\right) \quad (18)$$

where $p(m_i)$ represents the probability of symbol m_i, K is the number of bits of the message and 2^K all possible values. For a 256-grayscale image, the pixel data has 2^8 possible values and the ideal entropy of a true random image must be 8. Table 2 shows entropy values of some images of the proposed encryption algorithm very close to 8, as expected.

TABLE II. INFORMATION ENTROPY OF SOME PLAIN IMAGES AND THEIR CIPHER IMAGE.

Gray image	Proposed algorithm	[20] (2017)	[19] (2017)
Cameraman (512 × 512)	7.9993	-	-
Lena (512 × 512)	7.9993	7.9993	7.9992
Peppers (512 × 512)	7.9994	7.9992	-

B. 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 sensitive to initial conditions inherent to any chaotic system, i.e., exponential divergence of chaotic trajectories, ensure high security.

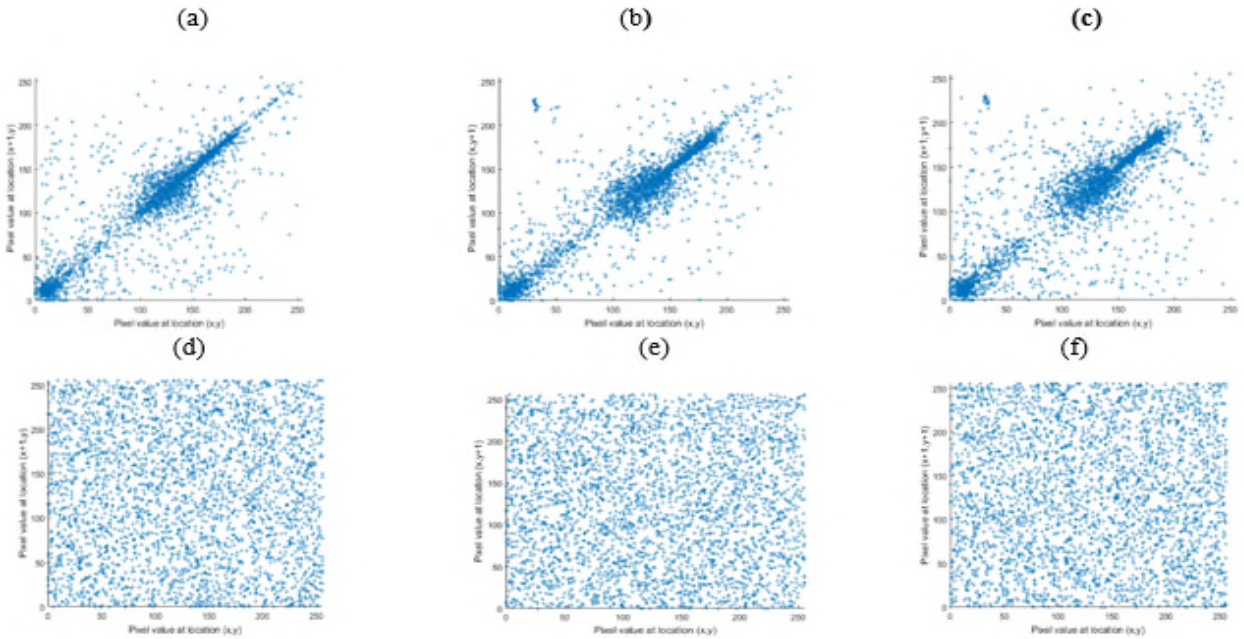

Figure 7. Pixel value distribution of plain and cipher cameraman (512× 512). (a-c) plain images, (d-f) ciphered image

According to [19], a key size of 10^{30} is sufficient. 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 that by changing only one bit in any parameter of the key, it is not possible to recover the plain images.

C. Sensitivity analysis

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) (19) and Unified Average Change Intensity (UACI) (20) criteria, which consist in testing the influence of one-pixel change of a plain image in the resulting cipher image.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (19)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\% \quad (20)$$

where C_1 and C_2 are two images with same size $W \times H$. If $C_1(i, j) \# C_2(i, j)$ then $D(i,j) = 1$, otherwise, $D(i,j) = 0$. Table 3 gives the measurement of NCPR and UACI between two cipher images of cameraman, Lena and peppers, when a Least Significant Bit (LSB) changed on grey 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.

TABLE III. NCPR AND UACI MEASURE AFTER A LSB CHANGE.

Image	Test	
Cameraman	NCPR	99.62
(512×512)	UACI	33.54
Lena	NCPR	99.62
(512×512)	UACI	33.46
Peppers	NCPR	99.63
(512×512)	UACI	33.47

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:

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

where M×N are the size of the image, $I_D(i, j)$ and $I_E(i, j)$ are the values of the decrypted image and the original image at the pixel *(i, j),* respectively. Table 4 presents the values of NMSE of a 512×512 Lena image for different total number of target images. From this table, we can observe that for *N=16* target images combined in one multiplex image, i.e., 32 images to encrypt by the proposed cryptosystem, the NMSE is still reduced, which attests the good quality of reconstructed images and good performances of the proposed cryptosystem.

TABLE IV. NMSE OF 512×512 LENA IMAGE

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

D. Encryption/decryption time

Table 5 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].

TABLE V. ENCRYPTION TIME IN SECONDS.

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

VI. CONCLUSION

In this paper, an image encryption algorithm based on spectral fusion of multiple 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-passed 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. The evaluation metrics of the proposed cryptosystem NCPR, UACI, correlation coefficient, entropy, key space and NMSE are amongst the best values in literature. More interestingly, the proposed cryptosystem can encrypt 32 target images simultaneously with a small NMSE $\approx 3.7 \times 10^{-3}$, and encrypted images are sensitive to the key. The proposed encryption algorithm can surely guarantee security and speed of all types of digital data transfer in a digital network.

ACKNOWLEDGMENTS

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

REFERENCES

[1] X. Liao, S. Lai, and Q. Zhou, ''A novel image encryption algorithm based on self-adaptive wave transmission,'' J. Signal Process., vol 90, pp. 2714–2722, 2010.

[2] C. Zhu, ''A novel image encryption scheme based on improved hyperchaotic sequences,'' J. Opt. Commun., vol 285, pp. 29–37, 2012.

[3] Y. Abanda and A. Tiedeu, ''Image encryption by chaos mixing,'' IET Image Process., vol 10, pp. 742–750, 2016.

[4] X. Wang, L. Liu, and Y. Zhang, ''A Novel Chaotic block image encryption algorithm based on dynamic random growth technique,'' Optics and Lasers in Engineering, vol. 66, pp. 10-18, 2015.

[5] R. Rhouma and S. Belghith, ''Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem,''J. Phys. Lett. vol. A 372, pp. 5790–5794, 2008.

[6] Y. Wang, X. Liao, T. Xiang, K. W. Wong, and D. Yang, ''Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map,'' Physique Letters, vol. A 363, pp. 277-281, 2007.

[7] V. Patidar, N. Pareek, and K. K Sud, ''A new substitution-diffusion based image cipher using chaotic standard and logistic maps,'' Commun. Nonlinear Sci. Numer. simul., vol. 14, No. 7, pp. 3056-3075, 2009.

[8] Z. L. Zhu, W. Zhang, K. W. Wong, and H. Yu, ''A chaos-based symmetric image encryption scheme using a bit-level permutation,'' Info. Sci., vol. 181, pp. 1171-1186, 2011.

[9] C. Y. Song, Y. L. Qia, X. Z. Zhang, ''An image encryption scheme based on new spatiotemporal chaos'', Optik., vol. 124, pp. 3329-3334, 2013.

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

[11] Y. P. Kamdeu and A. Tiedeu, ''An image encryption algorithm based on substitution technique and chaos mixing,'' Multimedia Tools and Applications, vol. 77, No. 19, 2018.

[12] M. A. Chenaghlu, M. A. Balafar, and M. R. Feizi-Derakhshi, ''A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation,'' Signal Processing, 2018.

[13] A. Alfalou, C. Brosseau, and N. Abdallah, "Simultaneous compression and encryption of color video images," Opt. Commun., vol. 338, pp. 371–379, 2015.

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

[15] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, ''Simultaneous fusion, compression and encryption of multiple images'', OSA Opt. Express, 19 November, vol. 24, pp. 24023-9, 2011.

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

[17] I. Mehra and N. K. Nishchal, ''Wavelet-based image fusion for securing multiple images through asymmetric keys,'' Optics Communications, vol. 335, pp. 153-160, 2015.

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

[19] X. Zhang and X. Wang '' Multiple-image encryption algorithm based on mixed image element and permutation,'' Optics and Lasers in Engineering, vol. 92, pp. 6–16, 2017.

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

[21] G. L. Zhu and X. Q. Zhang, '' Mixed image element encryption based on an elliptic curve cryptosystem,'' Journal of Electronic Imaging, vol. 17, No. 2, 023007, Apr-Jun, 2008.

[22] A. M. Abdalla and A. A. Tamimi, ''Algorithm for image mixing and encryption,'' The International Journal of Multimedia & Its Applications (IJMA) Vol. 5, No.2, April, 2013.

[23] Y. Zhou, L. Bao, and C. L. P. Chen, ''A new 1D chaotic system for image encryption,'' Signal Process., vol. 97, pp. 172-182, 2014.

[24] G. Ren, J. Han, H. Zhu, J. Fu, and M. Shan, '' High Security Multiple-image Encryption using Discrete Cosine Transform and Discrete Multiple-Parameters Fractional Fourier Transform,'' Journal of Communications, Vol. 11, No. 5, May 2016.

 ISBN: 978-1-61208-746-7