

Received January 8, 2020, accepted February 6, 2020, date of publication February 17, 2020, date of current version March 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2974226

Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications

OSAMA S. FARAGALLAH^{1,2}, ASHRAF AFIFI^{1,7}, WALID EL-SHAFI³, HALA S. EL-SAYED⁴, ENSHERAH A. NAEEM⁵, MOHAMMED A. ALZAIN¹, JEHAD F. AL-AMRI¹, BEN SOH⁶, (Senior Member, IEEE), AND FATHI E. ABD EL-SAMIE³

¹Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Saudi Arabia

²Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

³Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

⁴Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom 32511, Egypt

⁵Department of Electrical, Faculty of Industrial Education, Suez University, Suez 43518, Egypt

⁶Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia

⁷Department of Electrical Engineering and Computers, Higher Technological Institute, Tenth of Ramadan 228, Egypt

Corresponding author: Osama S. Faragallah (o.salah@tu.edu.sa; osam_sal@yahoo.com)

This work was supported by the Deanship of Scientific Research, Taif University, Saudi Arabia, through a research project under Grant 1-439-6083.

ABSTRACT The need for cybersecurity increases to protect the exchange of information for improving the data privacy. This paper presents an investigation of the encryption efficiency of the chaotic-based image block ciphering in the spatial and Fractional Fourier Transform (FrFT) domains. The main aim of this investigation is to examine the efficiency of different chaotic maps, while considering the parameters of the FrFT as additional keys for encryption and achieving reliable cybersecurity for robust image communication. In this paper, Cat, Baker, and Logistic map confusion approaches are applied in the spatial and FrFT domains to study and analyze the cybersecurity and ciphering efficiency of chaos-based image cryptosystems. The confusion features of the chaotic maps in spatial and FrFT domains are investigated using information entropy, differential analysis, histograms, visual observation, attack analysis, impact of noise, and encryption quality tests. Simulation results prove that the chaotic-based image encryption in the FrFT domain increases the efficiency of the confusion process and achieves a high nonlinear relation between the plainimage and the cipherimage in a symmetric ciphering approach. Moreover, the results demonstrate that the Cat-FrFT scheme is more susceptible to channel noise attacks than the Baker-FrFT and the Logistic-FrFT schemes. Hence, they can be implemented efficiently in the scenarios of noisy channels due to their high robustness to channel noise.

INDEX TERMS Arnold Cat map, chaotic Baker map, confusion, FrFT, Logistic map, image encryption.

I. INTRODUCTION

Cybersecurity comprises data security, the applications, and infrastructure utilized for storing, processing, and transmitting information. It is known as the method that is employed for responding to, monitoring, and preventing cybersecurity events to protect the transmitted data and information. There is a strong focus on information exchange from the cyberse-

The associate editor coordinating the review of this manuscript and approving it for publication was Ramakrishnan Srinivasan¹.

curity perspective. However, current encryption methods are known to be unreliable for effective image encryption [1].

The sensitivity property to initial condition and control parameters that is inherent in chaotic methods can be used to achieve security requirements. The chaos-based framework proposed in [2] has two steps of confusion and diffusion processes. It is most frequently used as a base in current methods of chaotic image encryption [3], [4]. Image data is in general manipulated or processed either in spatial or transform domains. The security of an image ciphering algorithm is estimated based on Shannon's

diffusion and confusion characteristics. Several image cryptosystems have been devised in both spatial and transform domains.

In the literature, several image encryption schemes have been introduced with diffusion and confusion mechanisms [4]–[27]. In [5], a ciphering scheme based on fractional cosine transform was proposed. In this scheme, the chaos is utilized to randomize the phases of the transmitted image in transformation and spatial domains. The results demonstrated the efficiency, validity, and robustness of this ciphering scheme against different attacks.

In [6], the authors introduced an image ciphering framework that employs spatial-temporal chaos maps. This framework has better ciphering features than those of the traditional Logistic map system. The bit-level pixel-based permutation is employed in this framework. In [7], an image ciphering scheme based on the deoxyribonucleic acid (DNA) and sine chaotic map was presented to encrypt the streamed images. The outcomes demonstrate that this encryption scheme performs sufficiently in the presence of different types of attacks due to the utilization of a large key space.

In [8], an image ciphering/deciphering scheme for color image transmission was presented. The original as well as the key main images are divided into RGB components. After that, the encrypted images are produced using the RGB components processed with XOR operation and scrambling. The statistical experimental tests on the ciphered and original images show an appreciated difference, but the approach was not robust to channel noise and different types of attacks. In addition, it was not appropriate for encrypting images of different dimensions.

In [9], a smooth affine transformation was implemented in the Gyrator Transform (GT) for encryption. The GT is utilized twice to enhance the encryption performance. The cipher keys are the affine and GT parameters. This study did not present a statistical security analysis. In [10], a cryptography scheme using one-time keys with chaotic maps was designed to achieve better security. The results introduced robust ciphered images in the presence of transmission noise and common multimedia attacks. The limitation of the works in [9] and [10] is the absence of a statistical security analysis.

In [11], an image ciphering scheme was presented based on chaotic Tent map. The statistical analysis revealed that the problems of the traditional Tent map technique are solved. In [12], a pixel shuffling operator was implemented to hide and mix the primary color components. This scheme is safe, key-sensitive, viable, and resistant to multimedia attacks.

In [13], the authors suggested an image ciphering framework based on the perceptron model within a neural network and Lorenz chaotic scheme. The experimental results show that this ciphering scheme has strong resistance and high security in the presence of multimedia attacks. In [14], a diffusion and confusion scheme for image ciphering based on DNA coding and chaotic maps was introduced. This scheme incurs confusion of the pixels through randomly transforming

the nucleotide into its base pair. Moreover, it generates new keys based on the common keys and the plain image. The obtained results show that it achieves appreciated ciphering results, and it also has a large key space.

In [15], a ciphering technique based on the spatial/temporal lattice map was presented. It has some advantages and cryptography features compared to the traditional lattice map and the Logistic map. The experimental results demonstrated that this technique has a high efficiency and a good security performance compared to the traditional techniques. In [16], the authors suggested an image ciphering scheme that depends on a chaotic map and DNA coding. It utilizes the chaotic map to randomize the pixel positions. It also exploits the DNA coding to generate different ciphering rules. This technique enhances the ciphertext security, and the encoding performance. Moreover, it has a high key sensitivity and a large key space.

In [17], a double autonomous encryption method was suggested for the ciphering of color images based on a hybrid structure of a chaotic map and compressive sensing. The outcomes of this method assured reliable security. In [18], a color image cryptography approach depending on the chaos systems was presented. The chaotic maps are employed to cipher the color image components. The security is enhanced due to the reduction of the correlation values of the plain color image components. The results revealed high efficiency in the presence of multimedia attacks.

In [4], a ciphering system was implemented based on fractional chaotic methods for color images. The output results revealed uniform histograms, zero correlation, and high entropy results. In [19], a color image ciphering technique in the Fresnel zone was presented. The original color image is divided into three different masks using the Gerchberg phase Saxton iterative scheme. In [20], a color masking and shuffling encryption/decryption scheme was proposed. In order to improve the encryption performance, the fractional dual random masking and the chaotic Baker map were used. The experiments assured the success of this image communication scheme.

In [21], an image cryptography scheme depending on a chaotic map and DNA operations was introduced. This scheme comprises an XOR operation on the plainimage pixels based on the spatial/temporal chaotic map. After that, the DNA operation is applied to further confuse the plainimage. The tests showed that this scheme can resist the transmission multimedia attacks, efficiently. In [22], a hybrid structure comprising Double Random Phase Encoding (DRPE) and Baker map encryption was implemented. The Discrete Wavelet Transform (DWT) is performed to divide the original input image into approximate and detail components. Then, the chaotic Baker map is employed to encrypt the detail components. After that, to minimize the auto-correlation between the encrypted pixels, the DRPE is performed. The output results demonstrated appreciated key sensitivity and robustness to channel noise.

In [23], a color image ciphering algorithm based on a high-dimension chaotic map framework and a bit-level spatial permutation technique was investigated. In this algorithm, the scrambling is performed with a Piece-Wise Linear Chaotic Map (PWLCM) due to its ciphering efficiency. The security analysis results prove robustness, and large key space to resist different types of common attacks.

In [24], a dynamic random growth-based hybrid chaotic maps block image ciphering scheme was proposed. In this scheme, the Cat map is utilized as another security key to improve the suggested scheme security performance and efficiency. The simulation outcomes prove that this ciphering scheme is more robust and secure against different types of attacks.

In [25], a cybersecurity technique was presented for the purpose of intrusion detection. It proved efficiency for stopping and mitigating the serious malicious activities. This technique introduced an accuracy of 94.50%.

In [26], the authors introduced a chaos-based selective image cryptosystem to achieve minimization of the communication overhead, low computational cost, and an efficient security performance in the presence of different types of multimedia attacks. This cryptosystem is based on employing the skew Tent chaotic map. The simulation results demonstrated efficient selective image ciphering, higher security, good correlation, diffusion, good histograms, and large entropy.

In [27], a fast and parallel-processing image cryptosystem was presented. It exploits the image permutation process to achieve and guarantee an efficient permutation performance, low space, and less complexity. A parallel image diffusion process is implemented to ensure the utmost parallelism of the diffusion in order to guarantee robust subjective and objective results.

It is known that the most serious issue of image communication through wireless networks is the problem of security. Hence, in this paper, the encryption efficiency of the different confusion chaotic maps in the spatial and FrFT domains is studied. The objective is the selection of the most appropriate, suitable, convenient, and proper chaotic maps for encrypting images in the spatial and FrFT domains for communication scenarios. The influence of the FrFT parameters as additional encryption keys is also investigated. The Cat, Baker, and Logistic maps are considered in the spatial and FrFT domains.

The main advantage of employing the proposed image cryptosystem in the FrFT domain is to achieve more permutation, high cipher key sensitivity, and more immunity to transmission noise. The security performance of the suggested image cryptography scheme is carefully investigated through information entropy, differential analysis, visual inspection, attacks analysis, histograms, ciphering quality analysis, and effect of channel noise. The whole experimental outcomes ensure that the proposed image cryptography scheme in this paper is robust and secure compared to the ordinary techniques. Therefore, it can be utilized for robust and secure multimedia transmission applications and systems.

The main contribution of this work is investigating and combining the main advantages of the FrFT and chaotic map encryption schemes for efficient transmission of digital images, securely. The paper sections are arranged as follows. Section II explores and discusses the FrFT basics and different types of chaotic maps. Section III gives in detail the explanation of the suggested image ciphering technique. The simulation and performance tests are introduced in section IV. In section V, the communication noise impact on the decryption mechanism is investigated. The effect and influence of the FrFT angles upon the encryption process is tested in section VI. In section VII, a comparative study amongst the suggested technique and peer-reviewed and recent previous techniques is given. Finally, the conclusions are summarized in section VIII.

II. RELATED PRELIMINARY BASICS

A. FRACTIONAL FOURIER TRANSFORM (FrFT)

The FrFT can be considered as a linear transformation, which rotates, in the counterclockwise direction, the input signal with spatial coordinates (t, w) to new coordinates (u, v) by an angle $\alpha = a\pi/2, 0 \leq a \leq 1$, in the continuous time-frequency plane. The FrFT is named rotational FT or angular FT. It is formulated with the aid of a transform kernel as follows [28]:

$$K_{\alpha}(t, u) = \begin{cases} \sqrt{\frac{1-j\cot\alpha}{2\pi}} \cdot \exp(j\frac{t^2+u^2}{2}\cot\alpha - j\frac{tu}{\sin\alpha}) & \text{if } \alpha \neq n\pi \\ \delta(u-t) & \text{if } \alpha = n\pi \\ \delta(u+t) & \text{if } \alpha = (2n+1)\pi \end{cases} \quad (1)$$

If there is a given $x(t)$, its FrFT is given by $X_{\alpha}(u)$ as in Eq. 2. The free variable u is treated as a joint frequency/time variable.

$$X_{\alpha}(u) = \int_{-\infty}^{\infty} x(t) K_{\alpha}(t, u) dt \quad (2)$$

Similarly, a function $f(x)$ has the following form of transformation:

$$\begin{aligned} f_a(u) &= F^a[f(x)] \\ &= C_{\alpha} \int f(x) \exp[j\pi \frac{u^2+x^2}{\tan\alpha} - 2j\pi \frac{ux}{\sin\alpha}] dx \\ \alpha &= \frac{a\pi}{2}, \text{ and } C_{\alpha} = \frac{\exp[-j(\frac{\pi \cdot \text{sign}(\sin(\alpha))}{4} - \frac{\alpha}{2})]}{|\sin\alpha|^{1/2}} \end{aligned} \quad (3)$$

where a defines the transform fractional order and F^a represents the FrFT. The FrFT has a period of 4, and the transformation magnitude lies in $[-2, 2]$.

The FrFT has one degree of freedom more than the conventional FT as it has an angle in both x and y directions.

The mathematical model of the general discrete FrFT is discussed as follows. Assume $f(x)$ is a function with a

period Δ_0 , the FrFT with p^{th} order of $f(x)$ is computed using Eq. (4) [28]:

$$f_p = \sum_{k=0}^{N-1} f\left(k \frac{\Delta_0}{N}\right) \sum_{n=-\infty}^{\infty} k_p\left(x, \left(n + \frac{k}{N}\right) \Delta_0\right) \quad (4)$$

So, the forward and inverse 2D discrete FrFT of the signal are obtained as [28]:

$$F_{\alpha,\beta}(m, n) = \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} f(p, q) K_{\alpha,\beta}(p, q; m, n) \quad (5)$$

$$f_{\alpha,\beta}(p, q) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{\alpha,\beta}(m, n) K_{-\alpha,-\beta}(p, q; m, n) \quad (6)$$

where (α, β) denotes the 2D discrete FrFT order, $K_{\alpha,\beta}(p, q; m, n) = K_\alpha \otimes K_\beta$ represents the transformation kernel, and K_α, K_β denote the 1D discrete FrFT kernels.

The 2D FrFT has many applications in signal processing. One of the most important and common applications of the 2D FrFT is the encryption process. For the encryption of an image, we may multiply the image with a random phase, followed by applying the 2D FrFT and the resulting intensity is then stored. The extra degree of freedom possessed by the FrFT makes the hacking on the encrypted image more difficult. Thus, in this paper, we consider the parameters of the 2D FrFT as additional keys for an efficient encryption process.

B. CHAOTIC MAP ENCRYPTION

A diversity of chaotic maps can be used for image encryption. They are highly sensitive to their initial conditions. The sensitivity to initial conditions of chaotic systems is usually referred to as the butterfly effect. When utilizing different initial values, the chaotic system is operated in various orbits that are difficult to be analyzed and computed. Therefore, the data obtained from chaotic systems are well-conditioned to obey diffusion and confusion criteria. Arnold’s Cat map, Baker map, and Logistic map are three examples of confusion chaotic maps [16].

C. ARNOLD CAT MAP

Arnold Cat map can directly be iterated to confuse and rearrange the pixel positions of the image without changing their values. The results of the randomization and scrambling process are different for different iterations. Thence, this map can be employed for achieving image ciphering. The generalized 2D-Arnold Cat map is represented as follows [18]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \pmod n \quad (7)$$

$$A = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix}$$

The inverse 2D Arnold Cat map is expressed as follows [18]:

$$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \pmod n \quad (8)$$

$$A^{-1} = \begin{bmatrix} pq + 1 & -p \\ -q & 1 \end{bmatrix}$$

where p and q are two positive constant control variables, n is the number of iterations. The indices x and y refer to the pixel position in the original $N \times N$ image. Both x , and $y \in \{0, 1, 2, \dots, N-1\}$, and x' and y' refer to the pixel position after confusion.

The main important features of the Arnold Cat map are the periodicity and repeatability. The original image can be reconstructed after iterating the Cat map up to a certain number of rounds R . The number of iterations is known as the periodicity value, and this value depends on the image size. By altering the control variables p, q , and the image size, the image is reconstructed after a certain number of iterations. Thence, the parameters p, q , and the image size can be exploited as three different types of cipher keys to perform image encryption with the Arnold Cat map. Moreover, the angle of the suggested FrFT in this paper can be considered as an additional secret key.

D. 2-D CHAOTIC BAKER MAP

The chaotic Baker map is utilized to scramble a square unit using a 2-D mapping mechanism. The chaotic Baker map operation comprises two processes of breaking the input square unit into identical parts, and then the two divided halves are accumulated along one another. The description of the Baker map (B) is formulated as follows:

$$B(x, y) = (2x, y/2), \quad 0 = < x < 0.5$$

$$B(x, y) = (2x - 1, y/2 + 1/2), \quad 0.5 = < x <= 1 \quad (9)$$

The process of dividing the input square unit to two separate identical and similar rectangles is not recommended in the process of random scrambling and distribution because of its simplicity. Therefore, there are two other types of chaotic Baker map utilizing a U operator as a secret key for the splitting process. The U operator consists of k different elements, where the square unit is split into k different vertical rectangles. The discretized chaotic Baker map mechanism is summarized as:

1. Divide the input square unit with size $N \times N$ into a number of k different vertical rectangles of width n_i and height N , where $N = n_1 + n_2 + \dots + n_k$.
2. Stretch the vertically divided rectangles into horizontal rectangles.
3. Rearrange the reformatted rectangles to put the right rectangle at the top and the left rectangle at the bottom.

Therefore, the Baker map moves each pixel within the input square unit to a new location within the square in a bijective manner. The 2D discretized chaotic Baker map is symbolized

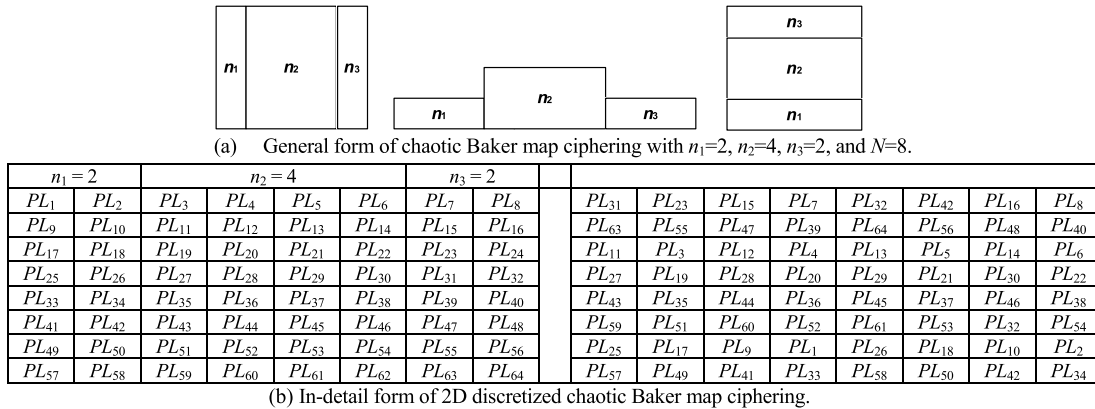


FIGURE 1. The chaotic Baker map ciphering process of an 8 x 8 image.

as $B(n_1, n_2, \dots, n_k)$. The k integers sequence (n_1, n_2, \dots, n_k) is selected so that every integer n_i divides N , and $N_i = n_1 + \dots + n_i$. Each pixel at location (r, s) with $0 \leq s < N$ and $N_i \leq r < N_i + n_i$ is mapped to:

$$B_{(n_1, \dots, n_k)}(r, s) = \left[\frac{N}{n_i} (r - N_i) + s \bmod \left(\frac{N}{n_i} \right), \frac{n_i}{N} \times \left(s - s \bmod \left(\frac{N}{n_i} \right) \right) + N_i \right] \quad (10)$$

Therefore, the general operation of the chaotic Baker map is that each input $N \times N$ square array is divided into k vertical different rectangles of width n_i and height N . After that, each vertical rectangle with dimensions $N \times n_i$ is further divided into n_i small boxes, where each box has N points. Each small box is mapped into a row of pixels in a column-by-column form, where the right box is mapped at the top and the left box is mapped at the bottom. For example, the permutation process of an 8×8 input square image is shown in Fig. 1. The B operator works with a key $(2, 4, 2)$, where $n_1 = 2, n_2 = 4, n_3 = 2$, and $N = 8$. Fig. 1(a) demonstrates the general form of the Baker map ciphering process and Fig. 1(b) demonstrates the discretized ciphering process of the Baker map.

E. CHAOTIC LOGISTIC MAP

The 2D Logistic map may be considered as an expansion of the 1D Logistic map. It is utilized to overcome the problems of the 1D Logistic map. The 2D Logistic map $F(x, y)$ is defined as:

$$x_{i+1} = \alpha_1 x_i (1 - x_i) + \beta_1 N_i^2 \quad (11)$$

$$y_{i+1} = \alpha_2 y_i (1 - y_i) + \beta_2 (x_i^2 + x_i y_i) \quad (12)$$

where $\alpha_1, \beta_1, \alpha_2, \beta_2, N_i$ are control parameters, and i varies as $0, 1, 2, \dots$, and so on. The x_0 and y_0 are initial conditions. In this paper, we focus on the parameters that make the system chaotic. The ranges of the control parameters are $2.75 \leq \alpha_1 \leq 3.4, 0.15 \leq \beta_1 \leq 0.21, 2.7 \leq \alpha_2 \leq 3.45, 0.13 \leq \beta_2 \leq 0.15$. The large key space makes it hard to predict the secret information.

III. THE PROPOSED ENCRYPTION SCHEME

In the suggested ciphering scheme, we employ three different types of chaotic maps, which have different characteristics to investigate the confusion efficiency in the spatial and transform domains. The suggested ciphering scheme comprises two different sections. Firstly, the FrFT is employed on the input image. Secondly, the suggested confusion technique using Arnold Cat map, 2D chaotic Baker map, or 2D Logistic map is performed, separately.

Therefore, the confusion process is performed in the FrFT domain, in which the angle works as an additional cipher key, and this presents a high degree of scrambling and randomization. The framework of the suggested ciphering/deciphering scheme is given as follows.

The steps of the ciphering technique are summarized as follows:




1. Read the input image.
2. Apply the FrFT on the input image.
3. Apply chaotic map ciphering (Cat, Baker, or Logistic).
4. Apply the inverse FrFT on the output of step 3.
5. Transmit the encrypted image to the receiver side through a communication channel.

The steps of the deciphering technique are summarized as follows:

1. Receive the encrypted image.
2. Apply the FrFT on the encrypted image.
3. Apply chaotic map deciphering (Cat, Baker, or Logistic).
4. Apply the inverse FrFT on the decrypted image.

Therefore, the proposed image encryption scheme applies FrFT on the input plainimage. Then, the resulting image coefficients are scrambled by applying different types of chaotic maps. The efficiency and security of the suggested scheme are studied considering the effect of noise, information entropy, visual inspection, histograms, attacks, differential and encryption quality metrics. All numerical results confirm that the suggested image encryption scheme preserves a good confusion property.

TABLE 1. Different samples of source images.

Name	Cameraman	Peppers	Boat
Image			

IV. SIMULATION RESULTS

To evaluate the proposed encryption scheme, it is tested on the standard Cameraman, Peppers, and Boat images of 256 × 256 pixels as shown in Table 1. The obtained results are evaluated depending on entropy, visual results, histograms, ciphering quality, and differential analysis [29]–[31].

A. VISUAL RESULTS

The visual results are the most remarkable factor in evaluating the ciphered image, where a greatly hidden ciphered image means that the suggested ciphering technique is better and recommended. The resulting ciphered images in the spatial and FrFT domains utilizing various chaotic maps are shown in Table 2 for the Cameraman, Peppers, and Boat images. From the introduced results, ciphering using the suggested technique succeeded in hiding the main distinctive features of the input plain images.

B. ENTROPY ANALYSIS

The structural features of the main image must not be seen in an enciphered image. Entropy is a measure of the degree of unpredictability of structural characteristics. The formula used to calculate the entropy value $E(x)$ for a cipherimage x is [32]:

$$E(x) = - \sum_{i=1}^{2^N-1} P(x_i) \log_2 P(x_i) \tag{13}$$

where $P(x_i)$ is the probability of occurrence of symbol x_i in the cipher image x , N is the number of bits for the symbol x_i and \log_2 is used to compute the entropy as a function of bits. The resulting pixel values are in the interval $[0, 255]$. It is a fact that the most desirable entropy value for an enciphered image is 8. The closer it gets to 8, the more secure is the cryptosystem.

The entropy values of the enciphered images in the spatial and FrFT domains using different confusion chaotic maps are introduced in Table 3. It is clear from the presented results that the entropies of the enciphered images tend to 8, which is the optimal entropy value. Consequently, the information leakage during the ciphering can be neglected. Thus, the proposed confusion-based image encryption scheme is robust to entropy attack.

C. HISTOGRAM ANALYSIS

The image histogram is used to count and graph the pixels at each gray intensity level. The results of histogram test for the source images and also for the enciphered images using the

proposed chaotic maps in the spatial and FrFT domains are presented in Table 4. In the histogram results, the horizontal axis shows the possible intensity values, and the vertical axis shows the number of pixels for each of these intensity values.

As the proposed ciphering technique involves permutation only, there is no change in the pixel values. Hence, we can see from the histogram results presented in Table 4 that the histograms of enciphered images in the spatial and FrFT domains using different chaotic maps are identical to the histograms of the corresponding source images. Thus, the statistical metrics of an enciphered image are identical to those of the corresponding source image.

D. ENCRYPTION QUALITY ANALYSIS

In this section, we evaluate the suggested image encryption scheme by investigating the most commonly used ciphering quality parameters like the correlation coefficient (r_{xy}) between the source and the enciphered images, histogram deviation (D_H) between the source and the enciphered images, and the irregular deviation (D_I) of the enciphered image. They are utilized to present a comparison between the proposed chaotic maps in the spatial and FrFT domains.

The correlation coefficient (r_{xy}) between the source and the enciphered images can be computed if they are transformed to 1D sequences using Eq. (14) [33]:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

where x is the main image and y is the enciphered image,

$$\begin{aligned} \text{cov}(x, y) &= \frac{1}{L} \sum_{i=1}^L (x(i) - E(x))(y(i) - E(y)), \\ D(x) &= \frac{1}{L} \sum_{i=1}^L (x(i) - E(x))^2, \\ D(y) &= \frac{1}{L} \sum_{i=1}^L (y(i) - E(y))^2, \end{aligned}$$

and L defines the pixel count in the image. The main target is to achieve low values of correlation amongst the enciphered and source images. The correlation values between the source and enciphered images are tabulated in Table 5.

The histogram deviation (D_H) estimates the suggested ciphering scheme quality by measuring how it increases the deviation between the source and enciphered images [34]. So, it is calculated as the difference between the areas under the histogram curves, and thus it can be estimated using the formula:

$$D_H = \frac{\left(\sum_{i=0}^{255} d(i) \right)}{W \times H}, \tag{15}$$

where $d(i)$ defines the histogram difference between the source and enciphered images with pixel level i . The original or the enciphered image dimensions are denoted by

TABLE 2. Encryption results of the test images using the different proposed chaotic maps in spatial and FrFT domains.

Images	Enciphering with different chaotic maps in spatial and FrFT domains					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman						
Peppers						
Boat						

TABLE 3. Entropy of the enciphered images using the proposed chaotic maps in spatial and FrFT domains.

Image	Enciphering scheme					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman	7.0097	7.0097	7.0229	7.0097	7.0097	7.0097
Peppers	7.5937	7.5937	7.5807	7.5937	7.6056	7.6068
Boat	7.1238	7.1238	7.0944	7.1238	7.1238	7.1237

$W \times H$. The main target is to achieve higher values of D_H . The histogram deviation values between the source and enciphered images are tabulated in Table 6.

The proposed ciphering scheme quality can be ascertained using the estimated irregular deviation (D_I) [30]. It is used to measure the amount of irregular deviations resulting from ciphering of the main source image. The D_I value can be estimated by Eq. (16) as:

$$D_I = \frac{\left| \sum_{i=0}^{255} h_d(i) \right|}{W \times H}, \quad (16)$$

$$h_d(i) = |h(i) - M|, \quad (17)$$

where the enciphered image histogram at intensity value i is $h(i)$, and M is the average of a pre-supposed histogram with a uniform distribution for an ideally enciphered image. The main target is to achieve lower values of D_I . The irregular deviation results for the enciphered images are introduced in Table 7. It is noticed from the introduced results that the efficiency of the suggested chaotic maps for ciphering of images in the FrFT domain is more appreciated and recommended than that of ciphering of images in the spatial domain.

E. DIFFERENTIAL ANALYSIS

The working principle behind the differential attack is changing a pixel or a bit in the main image and then enciphering to discover the difference between the two enciphered images. Therefore, the resistance of proposed confusion-based image ciphering scheme to differential attacks is studied using values of the Number of Pixel Change Rate (NPCR) and the Unified Averaged Changed Intensity (UACI). These results are estimated to check the sensitivity efficiency of the proposed

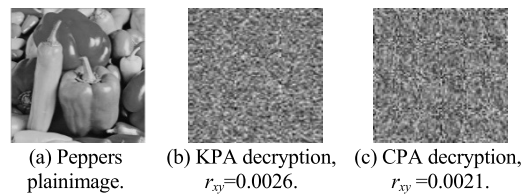


FIGURE 2. The resistance of the proposed FrFT-Logistic image cryptosystem to KPA and CPA.

ciphering scheme. Let us consider two enciphered images C_1 and C_2 for two source images SI_1 and SI_2 , which have a size of $H \times W$. If the pixel values for any component of the enciphered images C_1 and C_2 at position (i, j) are different, then $D(i, j) = 1$. The NPCR and NPCR values are calculated for the enciphered images C_1 and C_2 utilizing Eq. (18) and (19) [35]–[37]:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\%, \quad (18)$$

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{C_1(i, j) - C_2(i, j)}{255} \right] \times 100\%, \quad (19)$$

It is observed from the introduced results in Tables 8 and 9 that the Logistic-FrFT scheme offers the highest NPCR score, and the UACI score is zero for all tested images. This proves that the suggested encryption scheme is a highly sensitive to little variations in the source images, and thus it is robust to differential attacks.

F. KPA AND CPA ANALYSIS

The resistance of the proposed image cryptosystem is examined to both Known Plaintext Attack (KPA) and Chosen Plaintext Attack (CPA). Fig. 2(a) depicts the Peppers plainimage. The deciphering outcomes of both KPA and CPA are shown in Fig. 2(b) and Fig. 2(c). The correlation values of KPA and CPA results are 0.0026 and 0.0021, respectively. These correlation coefficient values ensure the immunity of the proposed Logistic-FrFT scheme to both KPA and CPA.

V. EFFECT OF NOISE

The PSNR, SSIM, and FSIM are computed for the purpose of evaluation of the visual quality of the decrypted images

TABLE 4. Histogram results of the source images and enciphered images using the different proposed chaotic maps in the spatial and FrFT domains.

Image	Source image	Enciphering scheme					
		Spatial Domain			FrFT Domain		
		Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman							
Peppers							
Boat							

TABLE 5. The correlation values between the source and enciphered images using the different proposed chaotic maps in the spatial and FrFT domains.

Image	Enciphered image					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman	0.0031	0.0359	0.0011453	-0.0029	-0.0025	0.002036
Peppers	-0.0031	0.0080	-0.000167	-0.0039	0.0115	0.00362
Boat	5.22×10^{-4}	-0.0213	0.000776	0.0085	0.0234	-0.000811

TABLE 6. Histogram deviation between source and enciphered images using the different proposed chaotic maps in the spatial and FrFT domains.

Image	Enciphered image					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman	0	0	0	0	0.0681	0.0680
Peppers	0	0	0	0	0.4517	0.4516
Boat	0	0	0	0	0.4591	0.4590

TABLE 7. Irregular deviation between source and enciphered images using the different proposed chaotic maps in the spatial and FrFT domains.

Image	Enciphered image					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman	0.7166	0.7139	0.00180	0.7125	0.7299	0.7176
Peppers	0.8232	0.8296	0.000208	0.7623	0.7623	0.7579
Boat	0.8010	0.8017	0.000203	0.7711	0.7711	0.7645

TABLE 8. NPCR values between the two encrypted images using the different proposed chaotic maps in the spatial and FrFT domains.

Image	Enciphering scheme					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman	99.0601	98.8461	99.3518	99.9105	98.9429	98.9665
Peppers	99.4175	99.4221	99.4720	99.4286	99.5262	99.5032
Boat	99.0589	99.0467	99.1470	99.0383	99.1734	99.1761

TABLE 9. UACI values between the two encrypted images using the different proposed chaotic maps in the spatial and FrFT domains.

Image	Enciphering scheme					
	Spatial Domain			FrFT Domain		
	Cat	Baker	Logistic	Cat-FrFT	Baker-FrFT	Logistic-FrFT
Cameraman	27.8645	25.8819	24.6636	28.0218	25.9371	25.1708
Peppers	24.2452	24.0829	22.0482	24.4607	24.2046	22.2943
Boat	21.8402	22.0848	20.2863	21.7849	22.3703	20.3304

TABLE 10. PSNR results of the deciphered images in the existence of channel noise for various chaotic maps in the FrFT domain.

Image	Cipher	PSNR (dB)				
		0.01	0.05	0.1	0.15	0.20
Cameraman	Cat-FrFT	9.8348	8.9174	8.2511	7.8289	7.5321
	Baker-FrFT	20.3842	13.8885	11.5520	10.3371	9.5591
	Logistic-FrFT	20.3791	13.9026	11.5322	10.2972	9.5437
Peppers	Cat-FrFT	9.9372	8.9437	8.2709	7.8607	7.5646
	Baker-FrFT	18.8286	13.6450	11.4502	10.3256	9.6391
	Logistic-FrFT	18.8387	13.6338	11.4813	10.3611	9.6252
Boat	Cat-FrFT	9.3670	8.5187	7.9358	7.5784	7.3166
	Baker-FrFT	19.5130	13.7715	11.5617	10.4126	9.6832
	Logistic-FrFT	19.5278	13.7582	11.5371	10.4276	9.6639

and to measure the performance efficiency of the proposed confusion-based ciphering scheme in the existence of channel noise (with zero mean (μ) and different noise variances (σ^2)) during the deciphering mechanism.

A. PEAK SIGNAL-TO-NOISE RATIO

The deciphering mechanism efficiency is tested by the PSNR between the original and decrypted images based on pixel differences. It is formulated as [38]:

$$PSNR = 10 \log \frac{(255)^2}{\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [f_1(i, j) - f_2(i, j)]^2} \quad (20)$$

where $f_1(i, j)$ and $f_2(i, j)$ are, respectively, the gray level values of the pixels at the i^{th} row and j^{th} column of the $W \times H$ original and decrypted images. For the decrypted images, a higher value of the PSNR is needed for utmost noise invulnerability. The PSNR values for several decrypted images with respect to their corresponding images have been calculated. The PSNR computed results of the three test images are introduced in Tables 10 and 11, where the parameters μ and σ^2 in the presented tables are the mean and variance of the existing noise, respectively. The PSNR results for the deciphered images are decreased, when the noise variance values are increased for all chaotic maps. The PSNR values for the Baker-FrFT and the Logistic-FrFT schemes are greater than the those for the Cat-FrFT scheme. The test results demonstrate that the Cat-FrFT scheme is more susceptible to channel noise. Therefore, it may be suitable for the channel-noise-free case. The Baker-FrFT and the Logistic-FrFT schemes can work efficiently in the noisy channel state due to their high robustness to channel noise.

B. THE STRUCTURAL SIMILARITY INDEX

The structural similarity (SSIM) index is widely used to measure the similarity between two images and for evaluating the performance efficiency of the deciphered process. The resultant SSIM index is a decimal value in $[-1, 1]$, where 1 means identical images. It is computed as follows [38]:

$$SSIM_{R/G/B}(x, y | w) = \frac{(2\bar{w}_x\bar{w}_y + C_1)(2\sigma_{w_x w_y} + C_2)}{(\bar{w}_x^2 + \bar{w}_y^2 + C_1)(\sigma_{w_x}^2 + \sigma_{w_y}^2 + C_2)} \quad (21)$$

where \bar{w}_x represents the mean value of w_x region, while \bar{w}_y is the mean value of w_y region. C_1 and C_2 are constants. $\sigma_{w_x w_y}$ denotes the covariance between the two regions, $\sigma_{w_x}^2$ denotes the variance of $\sigma_{w_y}^2$.

For the decrypted images, a higher SSIM value is preferred, which is a mandatory requirement for better noise immunity. The computed results of SSIM for the test images are introduced in Table 12. In all test cases, it was found that the SSIM results for the deciphered images are decreased when the variance values are increased for all chaotic maps, but the results are still accepted at different noise variances. Therefore, the introduced results confirm the performance efficiency of the suggested confusion-based image ciphering scheme in the existence of channel noise. The SSIM values for the Baker-FrFT and the Logistic-FrFT schemes are greater than the those for the Cat-FrFT scheme. Thus, the Baker-FrFT and the Logistic-FrFT schemes are highly efficient in the existence of channel noise. Thence, they may be used efficiently over a noisy channel.

C. FEATURE SIMILARITY INDEX

To calculate the local similarity between the main and deciphered images, the FSIM can be utilized. It is calculated as follows [38]:

$$FSIM_{R/G/B} = \frac{\sum_{x \in \Omega} S_L(x) \cdot PC_m(x)}{\sum_{x \in \Omega} PC_m(x)} \quad (22)$$

where $S_L(x)$ defines the estimated similarity between the two images. Ω denotes the spatial domain for the image, while $PC_m(x)$ is an estimate for the phase congruency.

For the decrypted images, a larger FSIM value is preferred, which is a mandatory requirement for better noise immunity. The computed results of FSIM for the test images are introduced in Table 13. In all test cases, it is found that the FSIM results for all deciphered images are accepted at different noise variances. It is also found that the FSIM values for the deciphered images are decreased, when the variance values are increased for all chaotic maps, but the results are still accepted at different noise variances. The FSIM values for the Baker-FrFT and the Logistic-FrFT schemes are greater than the FSIM values for the Cat-FrFT scheme. It is observed that the results ensure again that the suggested Baker-FrFT and Logistic-FrFT ciphering schemes are not affected greatly

TABLE 11. Deciphered images in the existence of channel noise for different chaotic maps in the FrFT domain.

Image	Cipher	Deciphered image				
		0.01	0.05	0.1	0.15	0.20
Cameraman	Cat-FrFT					
	Baker-FrFT					
	Logistic-FrFT					
Peppers	Cat-FrFT					
	Baker-FrFT					
	Logistic-FrFT					
Boat	Cat-FrFT					
	Baker-FrFT					
	Logistic-FrFT					

TABLE 12. SSIM results of the deciphered images in the existence of channel noise for various chaotic maps in the FrFT domain.

Image	Scheme	SSIM				
		0.01	0.05	0.1	0.15	0.20
Cameraman	Cat-FrFT	0.1325	0.0533	0.0361	0.0286	0.0229
	Baker-FrFT	0.5660	0.3151	0.2381	0.2003	0.1733
	Logistic-FrFT	0.5641	0.3164	0.2384	0.1973	0.1717
Peppers	Cat-FrFT	0.1084	0.0454	0.0316	0.0257	0.0228
	Baker-FrFT	0.5987	0.3376	0.2490	0.2047	0.1782
	Logistic-FrFT	0.5999	0.3381	0.2494	0.2065	0.1781
Boat	Cat-FrFT	0.0829	0.0384	0.0309	0.0235	0.0206
	Baker-FrFT	0.6281	0.3802	0.2849	0.2355	0.2078
	Logistic-FrFT	0.6296	0.3804	0.2848	0.2395	0.2061

by channel noise. Therefore, they may be implemented sufficiently in severe channel noise states.

VI. EFFECT OF FRFT ANGLES

The FrFT angles are considered as additional keys for encryption. So, we tested the encryption process with different FrFT angles. Table 14 shows the simulation results of the encryption quality metrics for the Logistic-FrFT scheme on the Cameraman image. It is noticed that the correlation, histogram deviation, and irregular deviation results are appreciated at different FrFT angles. So, the parameters of the FrFT can be used as additional keys for encryption and achieving reliable cybersecurity for robust image communication. Table 15 presents the subjective encryption and decryption results of the test images at different FrFT angles. It is

TABLE 13. FSIM results of the deciphered images in the existence of channel noise for the different chaotic maps in the FrFT domain.

Image	Scheme	FSIM				
		0.01	0.05	0.1	0.15	0.20
Cameraman	Cat-FrFT	0.5123	0.4689	0.4475	0.4347	0.4304
	Baker-FrFT	0.8355	0.6730	0.5996	0.5601	0.5322
	Logistic-FrFT	0.83596	0.6726	0.6031	0.5596	0.5325
Peppers	Cat-FrFT	0.5778	0.5073	0.4714	0.4518	0.4398
	Baker-FrFT	0.8333	0.6651	0.5914	0.5455	0.5177
	Logistic-FrFT	0.8331	0.6654	0.5881	0.5444	0.5177
Boat	Cat-FrFT	0.5152	0.4918	0.4802	0.4697	0.4664
	Baker-FrFT	0.8510	0.7062	0.6350	0.5962	0.5691
	Logistic-FrFT	0.8533	0.7063	0.6374	0.5959	0.5667

also shown that the encryption and decryption results of the Logistic-FrFT scheme for the test images are appreciated and recommended. It is also noticed that the FrFT-based encryption process has good key sensitivity results, where the decryption process is not valid when introducing a little difference in the FrFT angle.

VII. COMPARATIVE ANALYSIS AND DISCUSSIONS

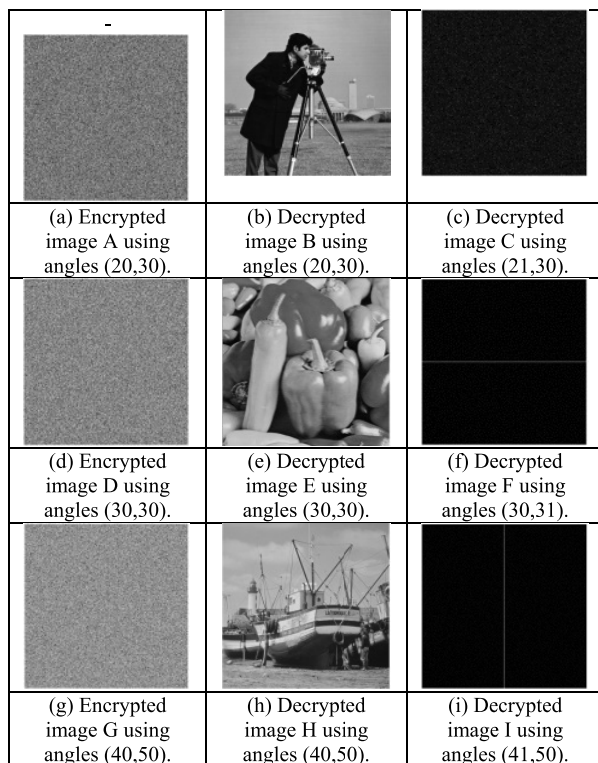
To verify and ensure the proposed encryption schemes effectiveness for reliable image transmission over insecure channels, various experiments have been carried out to compare the statistical security based on NPCR, correlation coefficient, PSNR, UACI, and entropy [4, 6-8, 11-18, 21-23].

The comparative study between the proposed encryption schemes and the traditional schemes is performed on the color

TABLE 14. Encryption quality results for the Logistic-FrFT scheme on the Cameraman image.

Angles of FrFT	r_{xy}	H_D	D_I
M1(30,20)	-897.5581×10^{-6}	68.0771×10^{-3}	715.3391×10^{-3}
M2(30,30)	-854.6761×10^{-6}	68.0770×10^{-3}	713.2111×10^{-3}
M3(40,50)	-392.0038×10^{-3}	68.0771×10^{-3}	715.2905×10^{-3}
M4(40,40)	-152.9726×10^{-6}	68.0771×10^{-3}	714.5004×10^{-3}
M5(43,64)	6.9893×10^{-3}	1.3381	870.7886×10^{-3}
M6(20,31)	-1.3768×10^{-3}	1.3384	861.3739×10^{-3}
M7(22,37)	-8.2376×10^{-3}	1.3347	874.5637×10^{-3}
M8(78,83)	-1.9829×10^{-3}	1.3348	872.3221×10^{-3}
M9(45,45)	-2.5965×10^{-3}	1.6738	978.1494×10^{-3}
M10(0,10)	-4.1398×10^{-3}	68.0771×10^{-3}	717.1124×10^{-3}
M11(0,22)	-1.2992×10^{-3}	68.0771×10^{-3}	716.8655×10^{-3}
M12(0,35)	-5.3082×10^{-3}	1.3343	871.2768×10^{-3}
M13(0,40)	2.9440×10^{-3}	68.07708×10^{-3}	716.1636×10^{-3}
M14(0,73)	-619.4967×10^{-6}	1.3359	866.1727×10^{-3}
M15(0,95)	-8.5473×10^{-3}	1.3337	871.0174×10^{-3}
M16(20,0)	1.3339×10^{-3}	68.0771×10^{-3}	717.4581×10^{-3}
M17(34,0)	1.4024×10^{-3}	68.0770×10^{-3}	716.6617×10^{-3}
M18(46,0)	-1.1239×10^{-3}	68.0770×10^{-3}	716.2322×10^{-3}
M19(60,0)	-3.1264×10^{-3}	68.0771×10^{-3}	714.8971×10^{-3}
M20(82,0)	-1.7061×10^{-3}	68.0771×10^{-3}	716.7511×10^{-3}

TABLE 15. Encryption and decryption with different FrFT angles.



Lena image. The values of entropy, correlation coefficient, NPCR, UACI, and the PSNR results are listed in Table 16

TABLE 16. The estimated entropy, correlation coefficient, NPCR and UACI results of the enciphered Lena image and the PSNR (dB) results of the deciphered Lena image for the proposed schemes and the literature-related schemes in [4], [6]–[8], [11]–[18], [20]–[22].

Scheme	Entropy	r_{xy}	NPCR	UACI	PSNR
Cat-FrFT	7.5937	-0.0002	99.82	29.73	42.79
Baker-FrFT	7.7190	0.0017	99.76	26.48	43.28
Logistic-FrFT	7.7771	-0.0219	99.74	27.52	43.17
Ref. [4]	7.5890	-----	-----	-----	-----
Ref. [6]	-----	0.0013	99.58	31.02	-----
Ref. [7]	-----	-----	-----	-----	-----
Ref. [8]	-----	0.1955	-----	-----	-----
Ref. [11]	7.6251	0.0435	99.71	33.45	-----
Ref. [12]	-----	0.0985	-----	-----	-----
Ref. [13]	-----	0.0056	-----	-----	-----
Ref. [14]	-----	0.0021	99.60	28.13	-----
Ref. [15]	-----	0.0024	99.57	27.53	-----
Ref. [16]	7.7594	0.0046	-----	-----	-----
Ref. [17]	-----	0.0219	-----	-----	-----
Ref. [18]	-----	-0.0064	-----	-----	-----
Ref. [21]	-----	0.0001	99.56	31.17	41.51
Ref. [22]	-----	0.0020	99.65	33.48	-----
Ref. [23]	-----	-0.0006	-----	-----	42.88

for the proposed and traditional schemes in [4], [6]–[8], [11]–[18], [20]–[22].

We notice that the entropies of the cipherimages for the proposed schemes are closer to 8 compared to those of the other schemes. So, the information leakage during the encryption process can be neglected, ensuring the robustness of the proposed schemes to the entropy attack compared to the other-related schemes. Also, it is obvious that the proposed schemes correlation coefficient values are closer to zero than the other related schemes. In other words, the cipherimage and the plainimage are not correlated. Moreover, the numerical values of NPCR and UACI demonstrate that the proposed ciphering schemes are better in the presence of differential attacks. Furthermore, based on the PSNR values (dB) of the decrypted Lena image using the proposed ciphering schemes, it is noticed that the proposed ciphering schemes are more efficient than the traditional schemes.

VIII. CONCLUSION

This paper provided an investigation of image encryption using different chaotic maps in spatial and FrFT domains. The parameters of the FrFT are considered as additional keys for encryption. Experimental results and theoretical security analysis proved that the suggested encryption schemes are more secure and effective. Based on the numerical results presented, the proposed encryption schemes demonstrate three advantages. They have a high level of efficiency represented in the confusion property. The enciphered images have good statistical properties. The proposed encryption schemes are immune to noise. Furthermore, it is noticed that the Cat-FrFT scheme is more susceptible to channel noise than the Baker-FrFT and the Logistic-FrFT schemes. Therefore, the Cat-FrFT scheme may be suitable for the channel-noise-free case. However, the Baker-FrFT and the Logistic-FrFT schemes can work efficiently in the cases of channel noise due to their high

robustness to the channel noise. For robust and reliable transmission and storage of digital multimedia data, we intend, as a future work, to develop and implement algorithms that include deep-learning-based cybersecurity mechanisms.

REFERENCES

- [1] S. Zhu, G. Wang, and C. Zhu, "A secure and fast image encryption scheme based on double chaotic S-Boxes," *Entropy*, vol. 21, no. 8, p. 790, Aug. 2019.
- [2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 08, no. 06, pp. 1259–1284, Nov. 2011.
- [3] J. Li, X. Di, X. Liu, and X. Chen, "Image encryption based on quantum-CNN hyperchaos system and anamorphic fractional Fourier transform," in *Proc. 10th Int. Congr. Image Signal Process., BioMed. Eng. Inform. (CISP-BMEI)*, Oct. 2017, pp. 1–6.
- [4] T. Dasgupta, P. Paral, and S. Bhattacharya, "Colour image encryption based on multiple fractional order chaotic systems," in *Proc. The Int. Conf. Control, Instrum., Energy Commun. (CIEC)*, Jan. 2014, pp. 583–587.
- [5] X. Z. Luo, N. R. Zhou, Q. M. Zhao, and J. H. Wu, "Color image encryption based on the multiple-order discrete fractional cosine transform and chaos in YCbCr space," *Appl. Mech. Mater.*, vols. 182–183, pp. 1839–1843, Jun. 2012.
- [6] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
- [7] B. Awdun and G. Li, "The color image encryption technology based on DNA encoding & sine chaos," in *Proc. Int. Conf. Smart City Syst. Eng. (ICSCSE)*, Nov. 2016, pp. 539–544.
- [8] S. Somaraj and M. A. Hussain, "A novel image encryption technique using RGB pixel displacement for color images," in *Proc. IEEE 6th Int. Conf. Adv. Comput. (IACC)*, Feb. 2016, pp. 275–279.
- [9] H. Chen, X. Du, Z. Liu, and C. Yang, "Color image encryption based on the affine transform and gyration transform," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 768–775, Jun. 2013.
- [10] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.
- [11] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel colour image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
- [12] X. Kang and R. Tao, "Color image encryption using pixel scrambling operator and reality-preserving MPPRHT," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 7, pp. 1919–1932, Jul. 2019.
- [13] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Jun. 2010.
- [14] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012.
- [15] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft Comput.*, vol. 26, pp. 10–20, Jan. 2015.
- [16] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps," *AEU-Int. J. Electron. Commun.*, vol. 68, no. 3, pp. 186–192, 2014.
- [17] F. Han, X. Liao, B. Yang, and Y. Zhang, "A hybrid scheme for self-adaptive double color-image encryption," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 14285–14304, Jul. 2017.
- [18] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
- [19] Z. Liu, C. Guo, J. Tan, W. Liu, J. Wu, Q. Wu, L. Pan, and S. Liu, "Securing color image by using phase-only encoding in fresnel domains," *Opt. Lasers Eng.*, vol. 68, pp. 87–92, May 2015.
- [20] R. Jain and J. B. Sharma, "Symmetric color image encryption algorithm using fractional DRPM and chaotic baker map," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 1835–1840.
- [21] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
- [22] R. Jain and J. B. Sharma, "Multi-domain image encryption using chaotic map with DRPE," in *Proc. Int. Conf. Adv. Inf. Commun. Technol. Comput. (AICTC)*, 2016, pp. 10–16.
- [23] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.
- [24] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.
- [25] A.-U.-H. Qureshi, H. Larijani, J. Ahmad, and N. Mtetwa, "A novel random neural network based approach for intrusion detection systems," in *Proc. 10th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2018, pp. 50–55.
- [26] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, May 2018.
- [27] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
- [28] S. Liangsheng, Z. Xiao, H. Chongtian, T. Ailing, and A. Krishna Asundi, "Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms," *Opt. Lasers Eng.*, vol. 113, pp. 29–37, Feb. 2019.
- [29] S. Ergun, "Security analysis of a chaos-based random number generator for applications in cryptography," in *Proc. 15th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Oct. 2015, pp. 319–322.
- [30] A. Roy, A. P. Misra, and S. Banerjee, "Chaos-based image encryption using vertical-cavity surface-emitting lasers," *Optik*, vol. 176, pp. 119–131, Jan. 2019.
- [31] Y. Zhai, S. Lin, and Q. Zhang, "Improving image encryption using multi-chaotic map," in *Proc. Workshop Power Electron. Intell. Transp. Syst.*, Aug. 2008, pp. 14–38.
- [32] P. Puteaux and W. Puech, "Reversible data hiding in encrypted images based on adaptive local entropy analysis," in *Proc. 7th Int. Conf. Image Process. Theory, Tools Appl. (IPTA)*, Nov. 2017, pp. 1–6.
- [33] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Apr. 2017.
- [34] G. Jiao, X. Peng, and K. Duan, "Image encryption with the cross diffusion of two chaotic maps," *Trans. Internet Inf. Syst.*, vol. 13, no. 2, pp. 1064–1079, 2019.
- [35] B. Nini, A. Zitouni, and A. Ounzar, "Analysis of the use of some statistical measures in deciding about the efficiency of an image encryption algorithm," in *Proc. Int. Image Process., Appl. Syst. (IPAS)*, Nov. 2016, pp. 1–6.
- [36] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.
- [37] A. D. Dwivedi, P. Morawiecki, and G. Srivastava, "Differential cryptanalysis of round-reduced SPECK suitable for Internet of things devices," *IEEE Access*, vol. 7, pp. 16476–16486, 2019.
- [38] E. A. Naeem, M. M. Abd Elnaby, N. F. Soliman, A. M. Abbas, O. S. Faragallah, N. Semary, M. M. Hadhoud, S. A. Alshebeili, and F. E. Abd El-Samie, "Efficient implementation of chaotic image encryption in transform domains," *J. Syst. Softw.*, vol. 97, pp. 118–127, Nov. 2014.



OSAMA S. FARAGALLAH received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently a Professor with the Department of Information Technology, College of Computers and Information Technology, Taif University, and the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator, from 1997 to 2002, and an Assistant Lecturer, from 2002 to 2007. He has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, since 2007. He is the coauthor of about 200 articles in international journals and conference proceedings, and two textbooks. His current research interests include network security, cryptography, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.



communication security, image processing, and image encryption.



ASHRAF AFIFI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electronics and communications engineering from Zagazig University, Egypt, in 1987, 1995, and 2002, respectively. He is currently an Associate Professor with the Department of Information Technology, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. He is the coauthor of about 30 articles in international journals and conference proceedings. His research interests include

WALID EL-SHAFAI was born in Alexandria, Egypt. He received the B.Sc. degree in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, the M.Sc. degree from the Egypt-Japan University of Science and Technology (E-JUST), in 2012, and the Ph.D. degree from the Faculty of Electronic Engineering, Menoufia University, in 2019. He is currently a Lecturer and an Assistant Professor with the ECE Department, FEE, Menoufia University. His research interests are in the areas of wireless mobile and multimedia communications systems, image and video signal processing, efficient 2D video/3D multiview video coding, multiview video plus depth coding, 3D multiview video coding and transmission, quality of service and experience, digital communication techniques, cognitive radio networks, adaptive filters design, 3D video watermarking, steganography, and encryption, error resilience and concealment algorithms for H.264/AVC, H.264/MVC and H.265/HEVC video codecs standards, cognitive cryptography, medical image processing, speech processing, security algorithms, software-defined networks, the Internet of Things, medical diagnoses applications, FPGA implementations for signal processing algorithms and communication systems, cancellable biometrics and pattern recognition, image and video magnification, artificial intelligence for signal processing algorithms and communication systems, modulation identification and classification, image and video super-resolution and denoising, and deep learning in signal processing and communication systems applications.



HALA S. EL-SAYED received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electrical engineering from Menoufia University, Shebin El-Kom, Egypt, in 2000, 2004, and 2010, respectively. She is currently an Assistant Professor with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University, where she was a Demonstrator, from 2002 to 2004, and an Assistant Lecturer, from 2004 to 2010. Since 2010, she has been a Teaching Staff Member with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University. She is the coauthor of about 50 articles in international journals and conference proceedings, and one textbook. Her research interests include database security, network security, data hiding, image encryption, wireless sensor networks, secure building automation systems, medical image processing, and biometrics.



ENSHERAH A. NAEEM received the B.Sc., M.Sc., and Ph.D. degrees in electronics and electrical communications engineering from the Faculty of Engineering, Tanta University, Tanta, Egypt, in 2006, 2012, and 2017, respectively. Her Current research areas of interest include cyber security, wireless communications and networking, image and video compression, image encryption, cancellable biometrics, deep learning, artificial intelligence, signal processing, and watermarking.



MOHAMMED A. ALZAIN received the bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2004, the master's degree in information technology from La Trobe University, in 2010, and the Ph.D. degree from the Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia, in September 2014. His Ph.D. research is in cloud computing security. His thesis title was Data Security, Data Management, Performance Evaluation for a Multi-Cloud Computing Model. He is currently the Vice-Dean and an Assistant Professor with the College of Computers and Information Technology, Taif University, Saudi Arabia. His areas of interest include cloud computing security and multimedia security.



JEHAD F. AL-AMRI is graduated from the Centre for Computing and Social Responsibility, De Montfort University. He is currently an Assistant Professor in computer informatics with the Department of Information Technology, Faculty of Computers and Information Technology, Taif University, Saudi Arabia.



BEN SOH (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering with La Trobe University. He is currently an Associate Professor with the Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia. Since then, he has had numerous successful Ph.D. graduates, and he has published more than 150 peer-reviewed research articles. He has made significant contributions in various research areas, including fault-tolerant and secure computing, and web services.



FATHI E. ABD EL-SAMIE received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. He received the Most-Cited Paper Award from the *Digital Signal Processing* journal, in 2008.

...