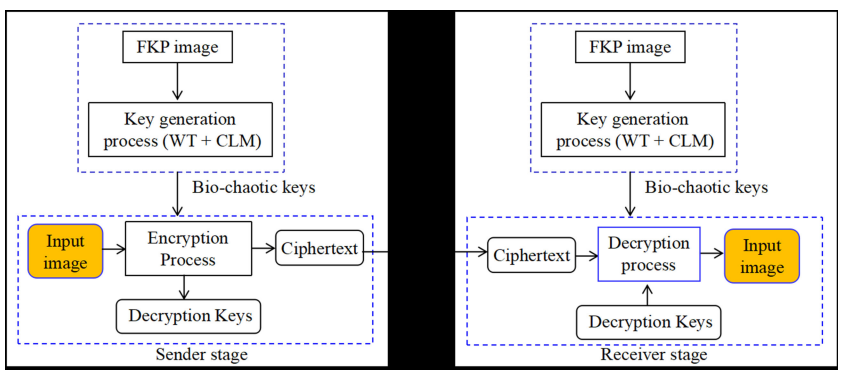
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Securing Multiple Information Using Bio-Chaotic Keys

Volume 13, Number 1, February 2021

Gaurav Verma
Wenqi He
Dajiang Lu
Meihua Liao
Xiang Peng
John Healy
John Sheridan



DOI: 10.1109/JPHOT.2020.3047806

Securing Multiple Information Using Bio-Chaotic Keys

Gaurav Verma,[1] **Wenqi He**,[1] **Dajiang Lu**,[1] **Meihua Liao**,[1] **Xiang Peng**,[1] **John Healy**,[2] **and John Sheridan**[2]

[1]Key Laboratory of Optoelectronic Devices and Systems of Ministry of Education and Guangdong Province, College of Physics and Optoelectronic Engineering, Shenzhen University, Shenzhen 518060, China
[2]School of Electrical, Electronic and Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland

DOI:10.1109/JPHOT.2020.3047806

Manuscript received September 26, 2020; accepted December 24, 2020. Date of publication December 29, 2020; date of current version January 14, 2021. This work was supported in part by the National Natural Science Foundation of China under Grants 61875129, 61805152, and 61705141, in part by the Sino-German Center for Sino-German Cooperation Group (GZ1391), in part by the Guangdong Natural Science Foundation and Province Project 2018A030310561, 2017B020210006, Shenzhen Science, and in part by the Technology R&D and Innovation Foundation under Grants JCYJ20180305124754860 and JCYJ20170817095047279. Corresponding authors: Wenqi He; Xiang Peng (e-mail: he.wenqi@qq.com; xpeng@szu.edu.cn).

Abstract: To advancement in security applications, for the first time, a bio-chaotic key generated from the emerging biometric trait "finger knuckle print (FKP)" has been proposed for data security and authentication. In the system, the feasibility to generate multiple keys from the single FKP image has been exploited to secure multiple information, which results in significant enhancement of the security strength. The encryption and decryption processes keep the user-specificity and perform better in reducing space for key storage and transmission. The research contribution is to facilitate a simplified optical implementation. Simulation results show the validity and effectiveness of the proposed scheme.

Index Terms: Imaging systems, security and encryption, image analysis.

1. Introduction

The rapid proliferation of optical information processing systems provides several degrees of freedom for securing data, information, or images that can be processed because of advantages such as two dimensional (2D) imaging capabilities, high speed, and the parallelisms [1], [2]. To secure image, double random phase encoding (DRPE) scheme based on the 4-*f* system was first proposed in the concept of optical encryption by Refregier and Javidi [3]. Subsequently, various extended encryption techniques based on optical transform have been proposed [2]–[6]. Unnikrishnan *et al*. [4] introduced an approach to implement optical encryption based on fractional Fourier domain. Situ *et al*. [5] proposed an image encoding method by using the Fresnel transform. In these schemes, some parameters (such as fractional order in FrFT, distance, angle, etc.) can be considered as additional security keys.

In the reported systems, the random phase mask (RPM) keys used for encryption and decryption are located at the input and the Fourier plane [3], [7]–[9]. Moreover, optical cryptosystems can be classified into the symmetric and asymmetric types based on the key's involvement [3], [10]. In the optical domain, the phase-truncated Fourier transform scheme has been introduced to solve the

issue of key distribution [10]. However, the reported optical techniques have also been detected susceptible to attacks such as known-plaintext attack and ciphertext-only attack, when the RPMs are employed as an encryption key [7]–[9], [11], [12]. Recently, it has been illustrated [13]–[16] that optical authentication can be further used into optical encryption systems to increase security.

With advances in computer technology and data acquisition devices, various encryption techniques for multiple image, three-dimensional(3D) object and multimedia content are becoming more attractive due to its potential features for recording, storage, and transmission over communication channels [17]–[30]. Especially, optical multiple-image encryption has received a considerable amount of attention by researchers due to its high efficiency of data transmission, in which several images can be encoded into one image. In this aspect, many digital or optical multiplexing approaches have been proposed for multiple-image encryption [17]–[30], which also helps to enhance system capacity. Situ *et al*. proposed the concept of multiple image encryption by using wavelength multiplexing [24] and position multiplexing [27]. Deng *et al.* reported multiple image security schemes based on phase retrieval and intermodulation in the Fourier domain [26]. In this scheme, images are encoded and then multiplexed into a single-phase data without involving cross-talk and loss of information [23], [25]–[29]. Kong *et al*. proposed a multi-image encryption scheme based on the interference of a computer-generated hologram. In this scheme, multi-user authentication is implemented by assigning different keys to different users [30]. It has been pointed out that large numbers of keys or parameters are required in securing multiple images, multispectral, and 3D images, which increases key storage space and complexity of the system. Also, the research concern is to involve a user signature in order to access the information. On the other hand, optical encryption systems combined with biometric technology or other technologies have become a research focus of many researchers [31]–[42]. In the modern world, biometrics techniques have been widely deployed in public and private sectors because biometrics characteristics are unique and permanent throughout the life of a human being [32], [36], [38]–[42]. From a security and authentication perspective, the use of a new biometric identity is a challenging task with keeping factors such as biometric availability, user acceptability, performance, and circumvention. In the system, the biometric data are utilized for encoding information with the application of transforms or mathematical functions [43]–[55]. In comparison to other biometrics such as fingerprint, voice, iris, and face, finger knuckle print (FKP) has been found as an innovative trait when the finger is bent on a small degree that forms a unique skin pattern full of textural features [43]–[47]. Moreover, the knuckle patterns are formed behind the finger dorsal surface so it does not leave any print or impression on the device due to contact-less. Over the last few years, interest in algorithms and concepts to investigate the utility of FKP characteristics is growing rapidly. From a more recent research perspective, Kumar *et al*. proposed a smartphone-based on the Android operating system that supports unlocking using the FKP signature [47]. Therefore, the aim of the paper is to generate multiple keys from the single FKP image and used it to secure multiple information.

In this work, we present a novel bio-chaotic key generation scheme for securing information. The contribution of this idea is to extract initial seed parameters for chaotic function by using the FKP image based on wavelet analysis that constructs an encryption key named bio-chaotic key. In the process of key generation, the FKP data adds an additional layer of personal authentication, while the combination of wavelet and chaotic analyses inherently provides more complex features and randomness. Moreover, the feasibility of multiple keys generation from the single FKP image is exploited to secure multiple information. This work is the first attempt to develop an optical encryption system in which encryption keys obtained from the FKP image are involved. The significant advantages of the system ensure the user's specificity, who is authorized for sending and receiving the data. The research implemented by simulation presented its effectiveness in achieving higher security performance, and also has its simplified implementation over existing methods. The rest of this paper is organized as follows. Section 2 discusses the working principles of the proposed scheme, which include the details of the bio-chaotic key generation process, and the encryption and decryption processes. Section 3 presents the simulation results of the proposed scheme. In section 4, concluding remarks are discussed.

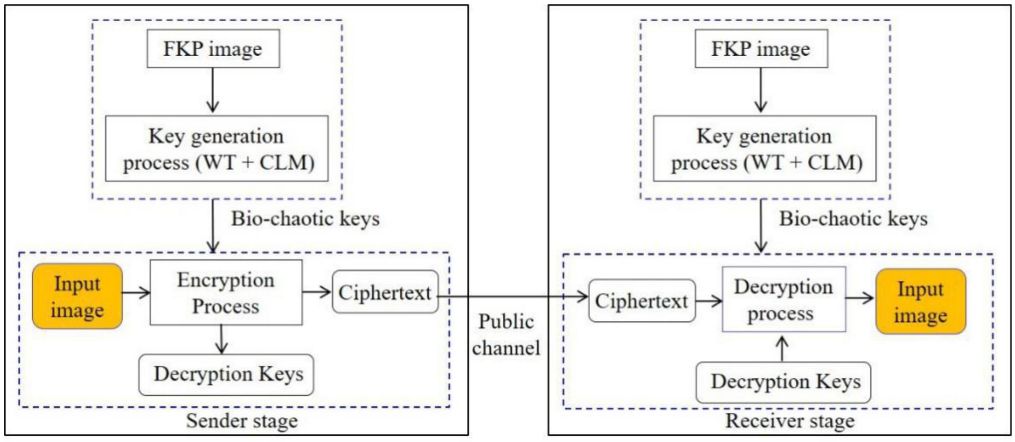


Fig. 1. Proposed system description; WT: wavelet transform, CLM: chaotic logistic map.

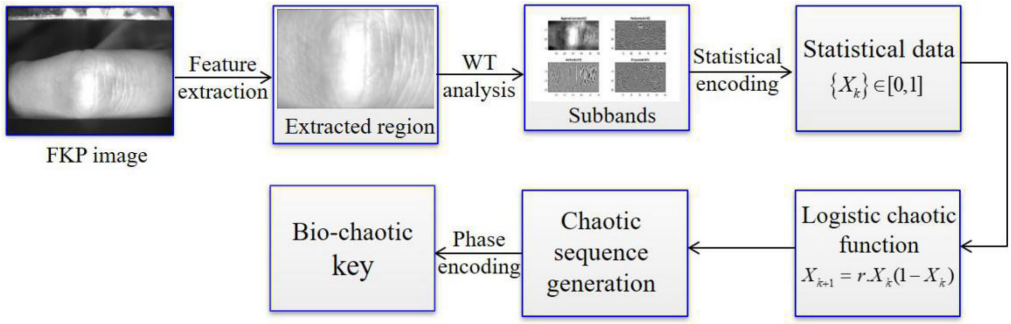


Fig. 2. Schematic description of the bio-chaotic key generation process.

2. Proposed System

To provide a higher level of security, biometrics is one of the most advanced techniques used. Since biometric traits are unique merit and are always associated with the person, which can be used as a key. The use of the FKP trait for the security system offers several useful features such as flexibility and versatile in terms of non-contact, high reliability, and accuracy in processing steps [39]–[43]. Figure 1 shows a diagram of the proposed system for securing multiple images by using the bio-chaotic keys. In this system, the wavelet analysis is performed to decompose the FKP data into several frequency sub-bands, which are utilized to create the system parameters of the chaotic function. These system parameters help in generating a bio-chaotic phase mask for encryption and decryption purposes. These parameters can be explored as private keys. The key generation procedure enables the significant ability to generate multiple bio-chaotic keys from the FKP image. Moreover, the attractiveness of the wavelet analysis offers low computational cost while the chaotic analyses inherently provide more complex features. It is important to note that the type of wavelet, as well as chaotic function, must be known to the system designer at the sender and receiver stages. This scheme can be realized using the following processes: (1) Bio-chaotic key generation (2) Encryption and (3) Decryption.

2.1 Bio-Chaotic Key Generation

Figure 2 shows the process of the bio-chaotic key generation, which relies on the wavelet transform and chaotic approach. Initially, the feature extraction processing steps are performed to extract a specific region of the FKP, as reported in the published work [44], [45].

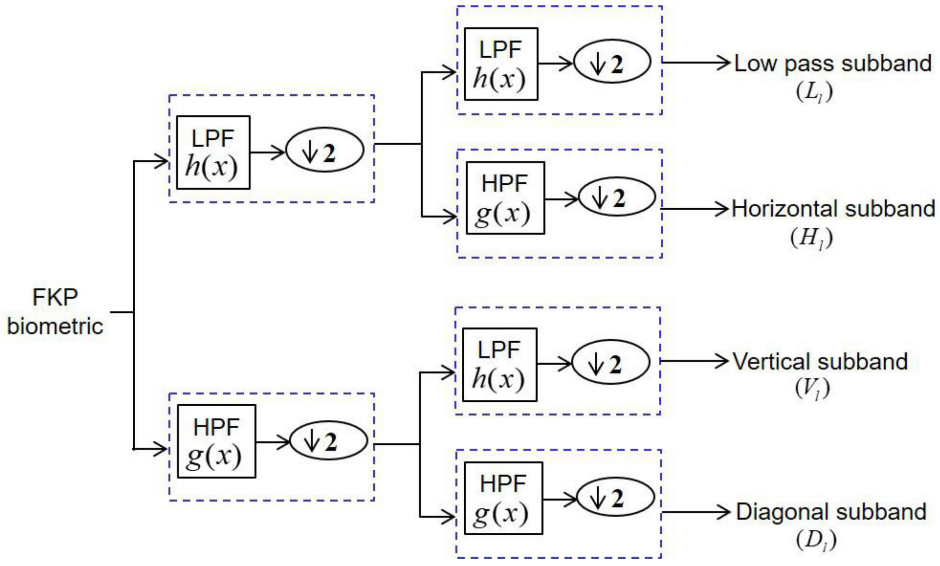


Fig. 3. Subbands; LPF: low pass filters, HPF: high pass filters, l: decomposition level.

2.1.1. Wavelet Analysis: In this part, WT is one of the most used techniques to decompose image into several frequency subbands at different levels of resolution [48]–[51]. This structure is realized by using filter banks, [low pass filters $h(x)$, and high pass filters $g(x)$] and sub-sampling operation by a factor of ($\downarrow 2$) as

$$A_{low}(u) = \sum_{n} h(x - 2\alpha) FKP(x). \tag{1}$$

$$D_{high}(u) = \sum_{n} g(x - 2\alpha) FKP(x). \tag{2}$$

where $A_{low}(u)$, and $D_{high}(u)$show the coefficient of the low-frequency subbands and high-frequency subbands, respectively. The selection of the wavelet and the number of decomposition levels are crucial factors. The implementation of the one level decomposition of the FKP image through filter banks is shown in Fig. 3.

From the wavelet-based analysis, high pass frequency subbands are obtained by a combining operation of low pass and high pass filtering in three directions such as horizontal (H_l), vertical (V_l), and diagonal (D_l) details as given

$$\begin{aligned} WT(FKP) &= [L_l,\ H_l,\ V_l,\ D_l] \\ &= [subbands_l]. \end{aligned} \tag{3}$$

The high pass subbands provide valuable information in spatial/and frequency, are normalized, which significantly helps subband coding [48]–[51]. The way to estimate the importance of the feature contained in each subband is appropriate to calculate the statistical data. Several statistics parameters such as mean, standard deviation, variance, entropy, and energy have been successfully applied by many researchers to texture classification purposes [51]. In our work, the standard deviation coefficient for each high-frequency subband is found most efficient that can be calculated as

$$Standarddeviation(SD) = \sqrt{\frac{1}{N}\left(\sum_{i=1}^{N} [Subbands_l - mean]^2\right)}. \tag{4}$$

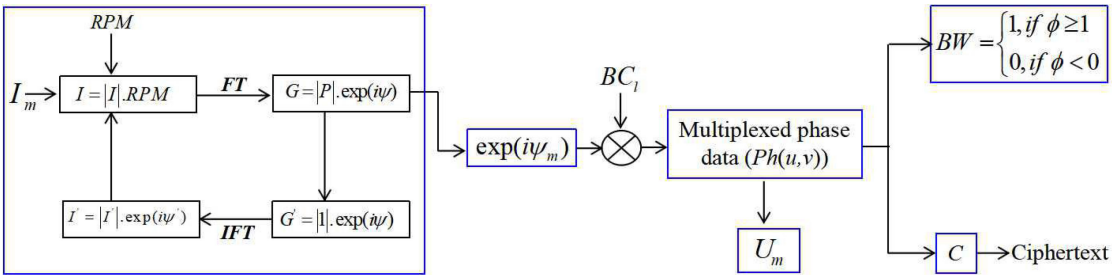


Fig. 4. Flow diagram of multiple image encryption process.

Where N is the size of the subband. Since each subband carries useful and distinct features, it is possible to create different statistical data from (4). As results, the steps state to yield the statistical significance as

$$(Subbands_l)^{SD} = (H_l^{SD}, V_l^{SD}, D_l^{SD}). \tag{5}$$

It is interesting to note from (5) that the statistical data belong in the range $\in$ [0, 1], which could be utilized as initial conditions independently to the chaotic approach for random sequence generation. Hence, analysis of the chaotic process is of great importance.

2.1.2. Chaotic Approach: The chaotic system possesses unique properties such as keen sensitivity to the initial values, ergodicity, randomness, and non-periodicity that are become more attractive to the field of chaotic cryptography [52]–[55]. Recently, many cryptographic ways to generate the initial conditions for the chaotic systems are focused. Han *et al.* proposed a new method for the initial values of the chaotic function generation using the fingerprint image encryption method via the multi-scroll chaotic attractors [54]. To perform analysis, the chaotic logistic map (CLM) function is described by using the following equation.

$$X_{k+1} = r.X_k(1 - X_k). \tag{6}$$

Where r is the control parameter and $X_k$is an initial condition or value. It has been confirmed from the chaos theory that if parameters $r\in$[3.564996, 4], and $X_k \in$ [0, 1] are in this region, then the system generates the dynamical outputs in entirely random and chaotic states. In this study, the CLM function as given in Eq.(6) is utilized the initial values (X_k) obtained from the FKP image while the control parameter (r) is kept the same.

$$CS_l = CLM(Subbands_l^{SD}). \tag{7}$$

Equation (7) represents the obtained chaotic sequence (CS), which possesses the features in terms of random distribution and sensitivity to the initial value that depicts a complete pseudorandom sequence [52], [53]. Finally, the CS values are encoded in the phase domain that can be expressed as

$$BC_l = \exp(2.\pi.i.CS_l). \tag{8}$$

The phase mask constructed by a chaotic sequence of the deterministic nonlinear system is coined as the bio-chaotic (BC_l) phase keys and its results are presented in Section 3.1. To explore the utility of the bio-chaotic keys, a new framework of multiple image encryption scheme is presented.

2.2 Encryption

Figure 4 shows the flowchart of the proposed multiple image encryption scheme using bio-chaotic keys based on the phase retrieval algorithm. In this study, [$I_m(x, y)$ $(m = 1, 2 \ldots, M)$]present the 'm' input images to be encrypted, where M shows the total number. In the process, each image is

initially encoded into its respective phase function by performing the k^{th} iteration number, which is combined with the bio-chaotic keys and then showed phase multiplexing.

The details of the process can be expressed as follows:

Step 1: Fourier transformed (*FT*) of the image can be written as

$$\begin{aligned} G_k(u, v) &= FT[I(x, y).RPM(x, y)] \\ &= \left|P(u, v)\right| . \exp[i\psi_k(u, v)]. \end{aligned} \tag{9}$$

Here, (*x, y*) and (*u, v*) denote features in the spatial and Fourier domain, respectively.

Step 2: In this step, the amplitude in the Fourier domain is changed to unity while kept its phase unchanged.

$$G'_k(u, v) = 1. \exp[i\psi_k(u, v)]. \tag{10}$$

Step 3: Now, the inverse Fourier transform (*IFT*) is performed as

$$I'_k(x, y) = IFT[G'_k(u, v)] = I''(x, y) \cdot \exp[i\psi'_k(x, y)]. \tag{11}$$

Step 4: Now, the recovered amplitude $I''(x, y)$of the input image is replaced with amplitude $I(x, y)$.

$$I'_k(x, y) = I(x, y) \cdot \exp[i\psi'_k(x, y)]. \tag{12}$$

The iteration process is stopped when convergence between the recovered image and the original image is completed [35]–[37], [41]. The above steps are used to encode each image into its phase-only function, respectively. It is important to note that the inverse FTs of the phase functions retrieve the corresponding input images. In our approach, to enhance the non-linearity of the encryption process, the obtained phase functions are combined with the bio-chaotic keys $[BC_l(l = 1, \ldots., m)]$.

$$\exp(i\theta_m) = \exp(i\psi_m) \times BC_l. \tag{13}$$

As mentioned in (13), the involvement of the bio-chaotic keys is not only used to increases more complexity and nonlinearity into the process but also adds a security layer. In these processing steps, different bio chaotic keys $[BC_l(l = 1, \ldots., m)]$ are multiplied to *m* phase function, respectively. Also, the multiplexing process to produce combined phase data as described in the paper [20]–[24] is further used. This can be written as

$$Ph(u, v) = \exp(i\phi(u, v)) = \exp\left[i\sum_{k=1}^{M}\theta_k(u, v)\right]. \tag{14}$$

Using the single-phase data as reported in the papers [24]–[30]], the individual keys are produced as

$$U_m(u, v) = \sum_{k\neq m}^{M} Ph_k(u, v), \qquad (m, k) \in [1, M] \tag{15}$$

From (14), the resultant phase ($\phi(u, v)$) can be further distributed into two parts. Among them, one part contains only absolute information (*abs*), i.e., amplitude, and the other part has its sign distribution. Most importantly, the sign distributions of the resultant phase are indispensable towards the retrieval of the data $Ph(u, v)$ which are encoded by using the identity as given

$$BW = \begin{cases} 1, \ if\, \phi(u, v) \geq 1 \\ 0, if\, \phi(u, v) < 0 \end{cases}. \tag{16}$$

Using (16), the obtained matrix is served as a binary (*BW*) key. If the *BW* key is missing, it will make the process hard to decrypt the process. As discussed above, the intensity or amplitude distributions of the phase are utilized to produce the ciphertext as

$$C = abs(\phi(u, v)). \tag{17}$$

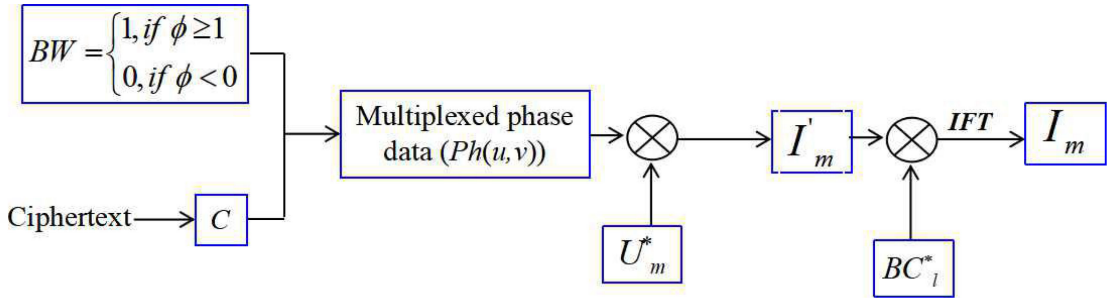


Fig. 5. Flow diagram of the decryption process.

The real distribution obtained using (17) is called the ciphertext, which is more convenient for recording and transmission. The proposed scheme generates the individual keys and *BW* keys as given in (15) and (16) for decrypting the information.

2.3 Decryption

Figure 5 shows the flow diagram of multiple image decryption. In the decryption process, the person who goes for decrypting the information should provide the FKP data for the bio-chaotic keys generation that further allow the process to retrieve the original images. Therefore, this approach can be utilized to verify the user specificity for decrypting the information.

In the first step of decryption, ciphertext (C) is utilized to combine with the binary key (BW) to retrieve the multiplexed phase data ($Ph(u, v)$) and is expressed as

$$\phi(u, v) = C \times BW. \tag{18}$$

$$Ph(u, v) = \exp(i\phi(u, v)). \tag{19}$$

Thereafter, the individual keys (U_m) as mentioned in (15) are multiplied with the $Ph(u, v)$ to demultiplexed phase data for all images as

$$I_m{}' = Ph(u, v) \times U^*{}_m(u, v). \tag{20}$$

In the final step, the involvement of the corresponding bio-chaotic keys to decrypt images are necessarily required, and then the IFT operation is carried out.

$$I_m = IFT(I'_m \times BC^*{}_l). \tag{21}$$

The '$*$' indicates a complex conjugate operation. The modulus of the 'I_m' yields the decrypted image. In the proposed scheme, encryption and decryption processes can be experimentally realized by using one set of optoelectronic devices such as lens, SLM (Spatial light modulator), CCD (Charge-coupled device), and a personal computer (PC).

Fig. 6 shows the proposed experimental setup for decrypting the information. First, the ciphertext combined with the binary key to retrieve single-phase data digitally that is displayed by the SLM, and then multiplied with individual decryption keys, and the BC keys, respectively. The obtained data are illuminated through laser light to perform an optical Fourier transform. In the last, the resultant input information in the form of the intensity is recorded by the CCD.

3. Result and Analysis

In this section, several simulation experiments to test the feasibility of the proposed system have been carried out on a Matlab platform. All numerical experiments are conducted on an Intel Core i3-7100 CPU with 3.90 GHz and 8 GB of RAM. In our tests, we first present the results of the encryption algorithm.

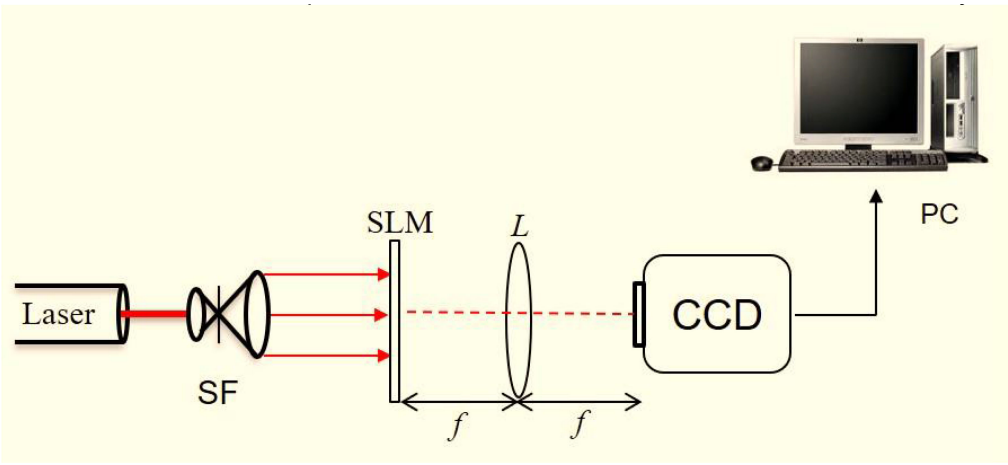
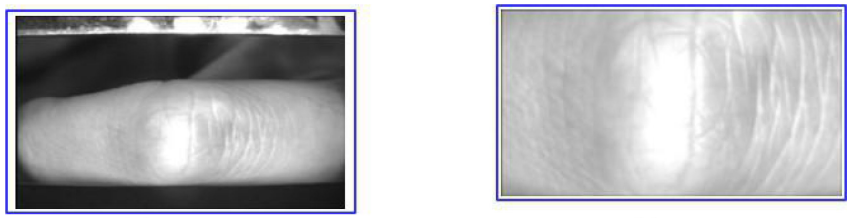


Fig. 6. Simplified experimental setup for decryption: SF: spatial filtering, SLM: Spatial light modulator, *f*: focal length of the lens (*L*), CCD: Charge-coupled device, PC: personal computer.



(a) (b)

Fig. 7. (a) FKP image (384 × 288 pixels) (b) Extracted FKP (110 × 220 pixels).

3.1 Bio-Chaotic Key Generation Results

For the demonstration point of view, Figs. 7(a)–7(b) show the original FKP image (384 × 288 pixels) and the extracted FKP region (110 × 220 pixels) by using the feature extraction steps as discussed in references [44], [45], which is further involved into the wavelet analysis.

To select the wavelet family, tests are carried out with different types of wavelet that gives maximum usability to the process. Based on results, the wavelet "Symlet 4" is utilized to decompose till the third decomposition level, as shown in Fig. 8. The high pass subbands are encoded to yield statistics significance, as described in Section 2, which are given below:

$$\left\{\begin{array}{l}(H_1)_{std} = 0.1405,\ (V_1)_{std} = 0.1640,\ (D_1)_{std} = 0.0716,\\ (H_2)_{std} = 0.1858,\ (V_2)_{std} = 0.2547,\ (D_2)_{std} = 0.1963\\ (H_3)_{std} = 0.4035,\ (V_3)_{std} = 0.2311,\ (D_3)_{std} = 0.2034\end{array}\right\} \in [0, 1]. \quad (22)$$

It is evident from (22) that the obtained parameters lie in the range $\in [0, 1]$. For the bio-chaotic keys, the setting of the LCM parameters are independently given as $BC_1 \in 0.1405$, $BC_2 \in 0.1640$, $BC_3 \in 0.0716$, $BC_4 \in 0.1858$, $BC_5 \in 0.2547$, $BC_6 \in 0.1963$, $BC_7 \in 0.4035$, $BC_8 \in 0.2311$, and $BC_9 \in 0.2034$ while the control parameter ($r = 3.78$) are kept the same. The generated bio-chaotic keys with size (256 × 256 pixels) are shown in Fig. 9.

3.2 Encrypted Data

Based on the bio-chaotic keys generated in Fig. 9, grayscale images with varying patterns of size (256 × 256 pixels) are used as shown in Figs. 10(a)–10(i), respectively. First, each image is

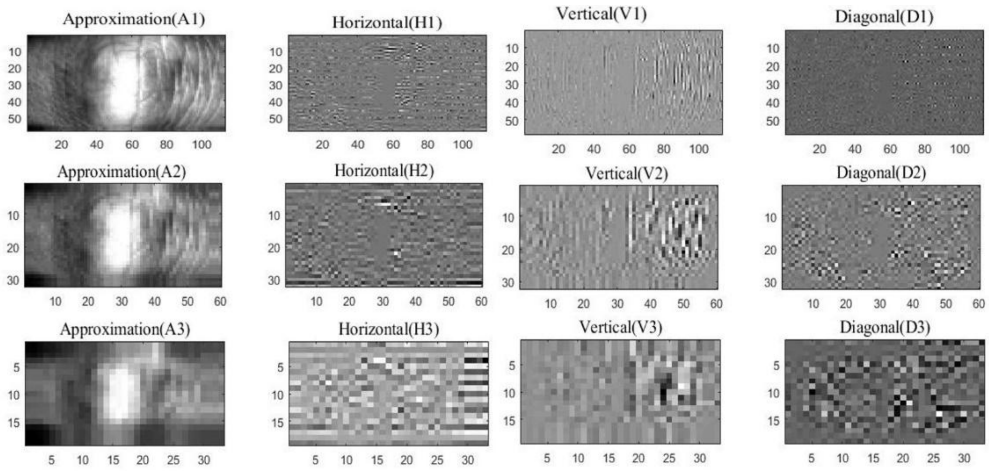


Fig. 8. FKP decomposition structure.

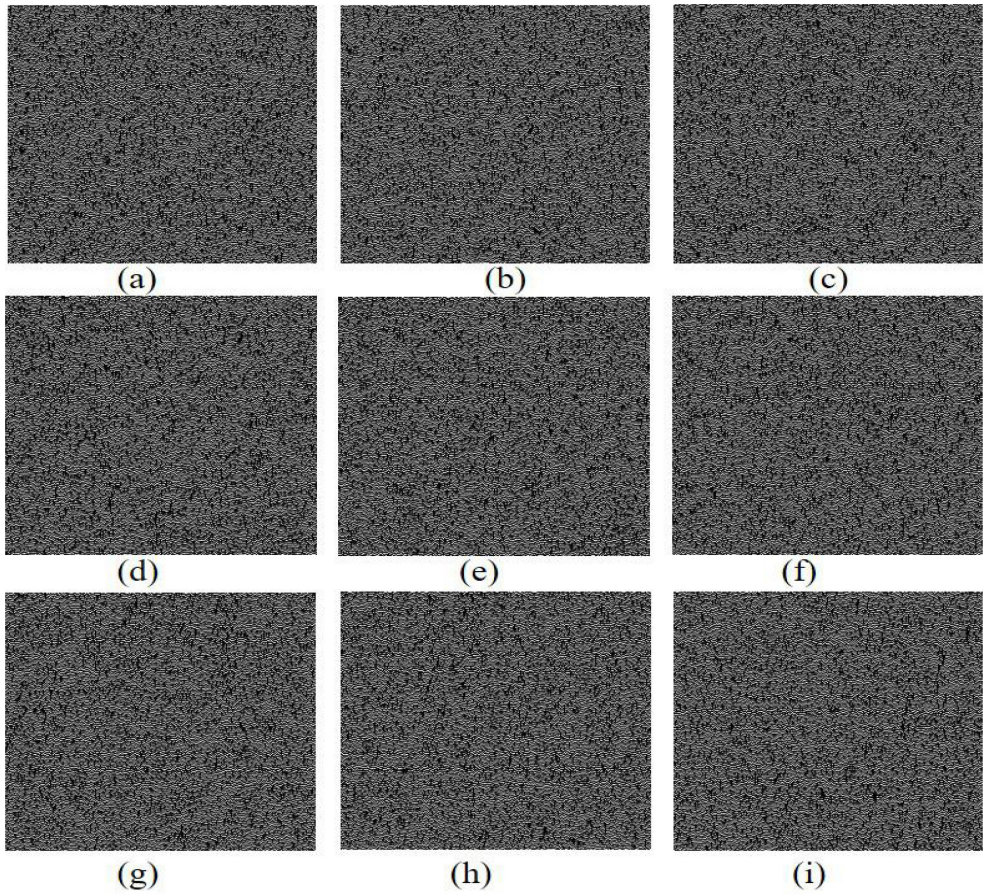


Fig. 9. Generated bio-chaotic keys at parameters; $r = 3.76$ (a) $BC_1 \in 0.1405$ (b) $BC_2 \in 0.1640$ (c) $BC_3 \in 0.0716$ (d) $BC_4 \in 0.1858$ (e) $BC_5 \in 0.2547$ (f) $BC_6 \in 0.1963$ (g) $BC_7 \in 0.4035$ (h) $BC_8 \in 0.2311$ (i) $BC_9 \in 0.2034$.

Fig. 10. Multiple images.

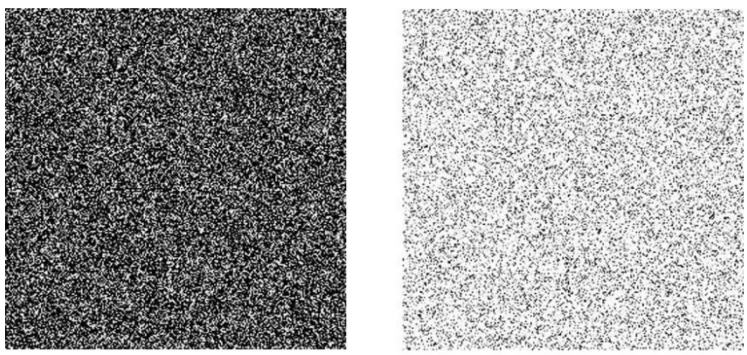


Fig. 11 (a) Multiplexed phase data ($Ph(u, v)$) (b) Ciphertext (E).

encoded into the phase-only domain using the iterative algorithm at 200 number iterations, which are combined with different bio-chaotic keys. Using the multiplexing process by (14), the multiplexed phase data ($Ph(u, v)$) obtained is shown in Fig. 11(a). The decryption keys are received during the encryption process by (15) and (16). The final ciphertext (E) produced using the proposed scheme is shown in Fig. 11(b).

Fig. 12. Decryption results using all correct keys.

3.3 Decryption Results

In the decryption process, the correct decryption results, as shown in Figs. 12(a)–12(i), are obtained by using the BW key, individual keys, and the BC keys in the right order. To check the quality of the decrypted images, the mean-square error (MSE) values between Figs. 12(a)–12(i) and the corresponding input images (see Figs. 10(a)–10(i)) are found to be 7.3035×10^{-4}, 3.8676×10^{-4}, 2.1502×10^{-4}, 6.0784×10^{-4}, 4.7283×10^{-4}, 1.3237×10^{-4}, 1.6510×10^{-4}, 1.2929×10^{-4}, and 3.9226×10^{-4}, respectively, while the correlation coefficient (CC) values are all greater than 0.99, which show exactly the same retrieval of the input images.

Furthermore, to check the robustness, the decryption processes are performed to retrieve the information against unauthorized attempts using incorrect bio-chaotic keys combinations, while the BW and individual keys are correctly used. Fig. 13(a) shows the decrypted image without using the bio-chaotic key. Fig. 13(b) shows the decoded result when the bio-chaotic keys are put in the wrong position. Fig. 13(c) shows the decrypted information after using any arbitrary RPM in place of the bio-chaotic key. The results in Fig. 13 shows corresponding to Fig. 10(a), while similar results are obtained to remaining all images (Figs. 10(b)–10(i)), respectively.

In the following decryption experiment, the sensitivity of the bio-chaotic key is checked when the initial parameters are slightly varied ($\Delta BC = 10^{-15}$). It can be observed from Fig. 14 that the recovered image is unrecognizable and bears no resemblance to the original image. Figs. 14(a)–14(c) show the results corresponding to Figs. 10(a)–10(c), respectively, while similar behavior is observed to remaining images (Figs. 10(d)–10(i)), respectively.

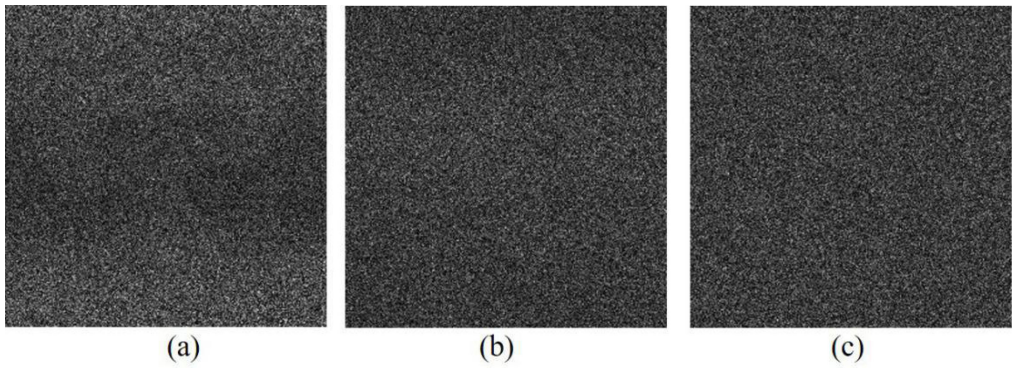


Fig. 13. Decryption results using: (a) No bio-chaotic key (b) bio-chaotic key in wrong positions (c) Different RPM key in place of the original bio-chaotic key.

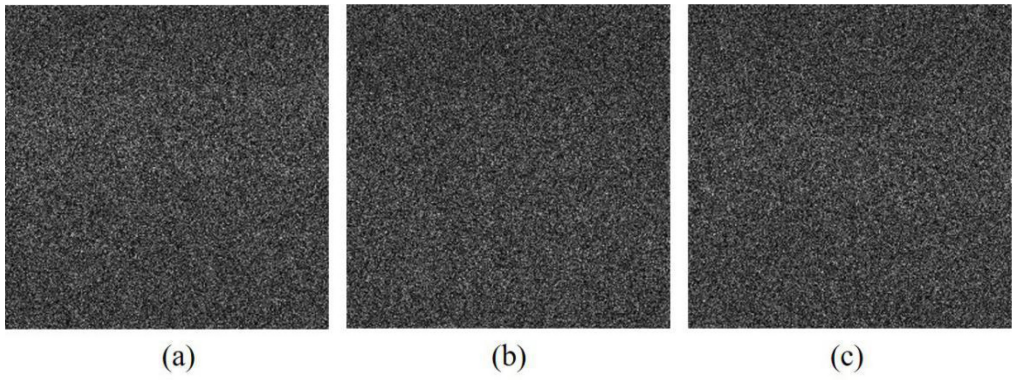


Fig. 14. (a–c) Decrypted results when the parameters slight changes ($r = 3.76$, $\Delta BC = 10^{-15}$).

Moreover, the sensitivity of the proposed scheme is also evaluated with the MSE and CC curves with respect to the variation of the key parameter. From this point, the relationship between correct bio-chaotic keys (used during encryption) and incorrect bio-chaotic keys (used during decryption) is given by

$$BC_l' = BC_l + \Delta BC. \tag{23}$$

where,BC_l' and BC_l as modified bio-chaotic keys and correct bio-chaotic keys, respectively. The deviation (ΔBC) value is of the order of 10^{-15} for initial conditions while the control parameter is kept the same. The obtained MSE and CC values are plotted to the variation of deviation (ΔBC) in keys (BC_1–BC_3) for decrypted images as shown in Figs. 15(a)–15(c), respectively. Fig. 15 shows that deviation (10^{-15}) in any of the bio-chaotic keys results in high MSE (low CC) value between the original image and the decrypted image. Thus, the graph presents the high sensitivity of the proposed scheme.

In addition, to check the robustness against noise and occlusion contaminations during the storage or transmission process, the proposed scheme is further analyzed. Figs. 16(a)–16(b) show the retrieved image when the ciphertext is affected by the different intensity of noise. Figs. 17(a)–17(b) show the recovered images when we occlude 12.5% and 43.75% of the encrypted image pixels, respectively. It can be observed that the decrypted image remains recognizable against contaminations of the noise and occlusion. Fig. (16) and Fig. (17) show the results corresponding to Fig. 10(a), while similar results are obtained to remaining all images (Figs. 10(b)–10(i)), respectively.

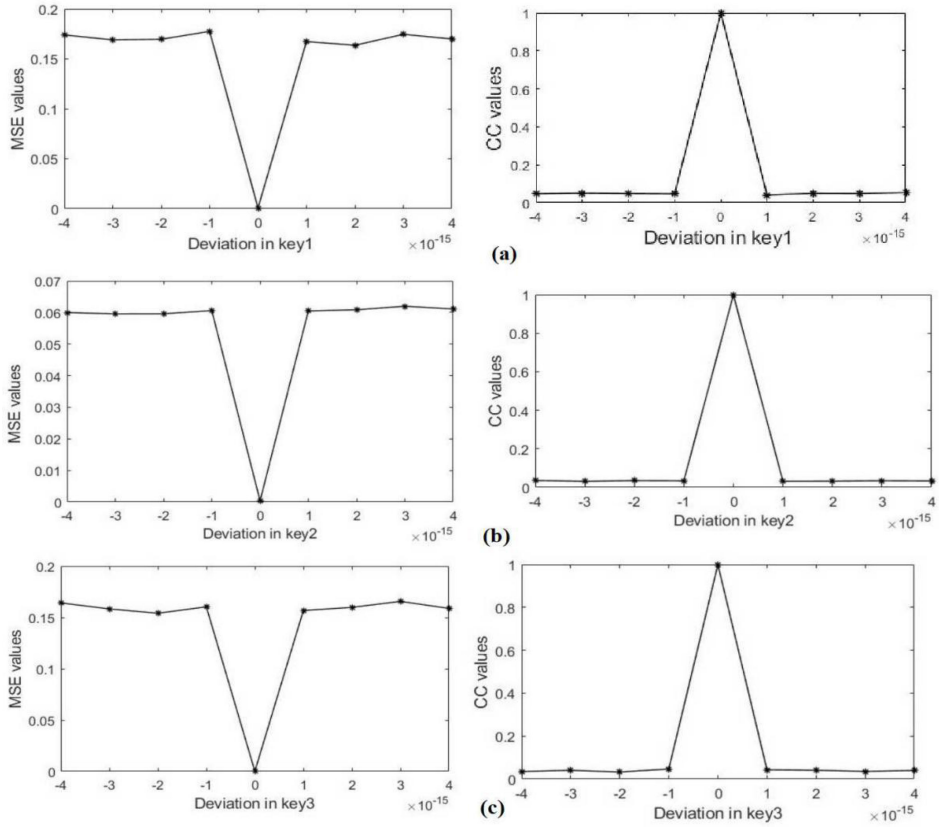


Fig. 15. (a–c) MSE and CC plots to illustrate key sensitivity for deviation in correct key (BC_1–BC_3), respectively.

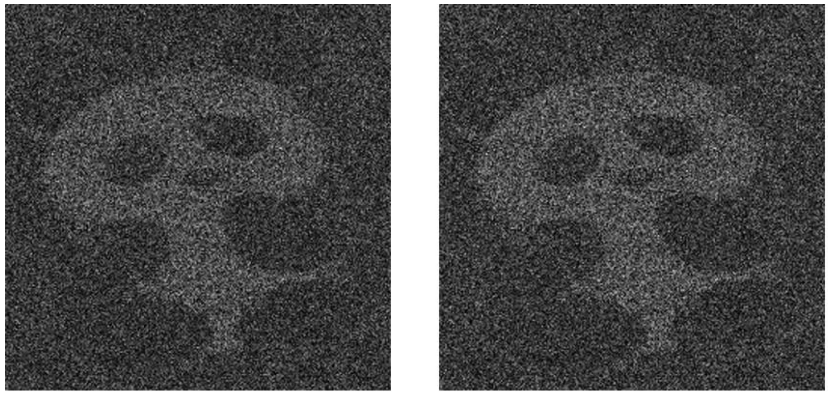


Fig. 16. Results of noise attacks. (a) Salt &Paper (0.5var) (b) Gaussian (0.5 var).

3.4 Security Analysis

In the proposed scheme, the input images are converted into its phase-only function by discarding its amplitude part by using the phase retrieval scheme. Furthermore, the obtained phase data is combined with the different bio-chaotic phase keys. These keys are generated using the acquired initial conditions of the chaotic function from the FKP image-based on wavelet analysis. According

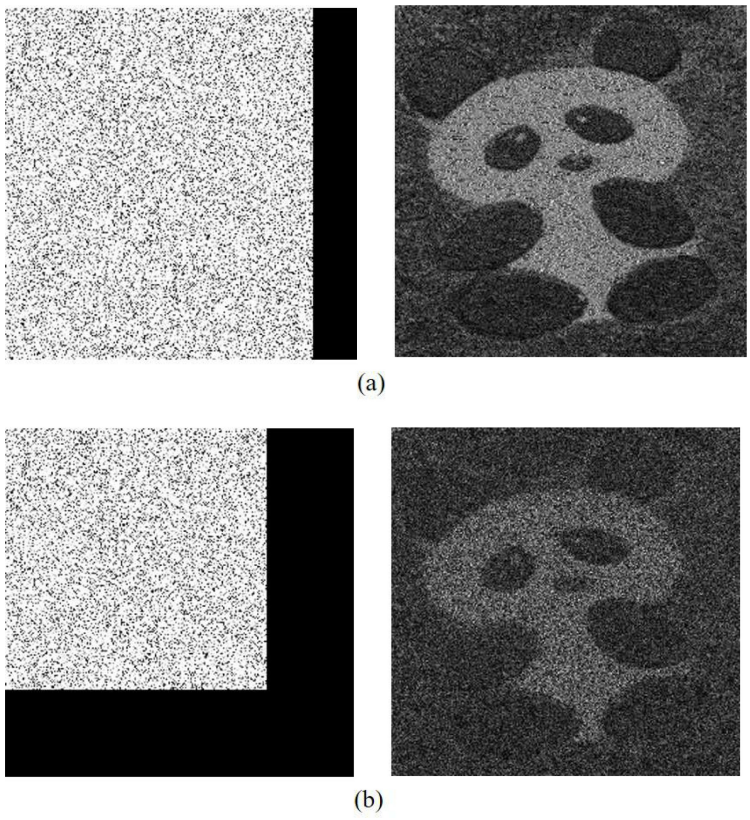


Fig. 17. Results of occlusion attacks. (a) When 12.5% pixels of Fig. 11(b) are occluded and the recovered image (b)When 43.75% pixels of Fig. 11(b) are occluded and the recovered image.

to the results depicts in Fig. (14) and Fig. (15), if we involve a slight change in the key's parameter, then it causes to generate ultimately differently BC features, which have a significant impact on the encryption approach. The process enhances non-linearity, complexity, and mixing of the encryption process that comes from the nonlinear operations carried in the Fourier domain. Moreover, the decomposing of the multiplexed phase data in terms of the binary key and the ciphertext make it more difficult for an attacker to hack the correct keys. Hence, the proposed scheme can resist existing attacks.

To check the robustness of the proposed scheme, the known-plaintext attack (KPA) has been tested. In this attack, an attacker is supposed to know resources such as input images, binary key, and the ciphertext which are utilized to retrieve the phase keys in between the input and Fourier planes with the help of the phase retrieval algorithm. During the decryption process, the retrieved phase keys, as well as the correct bio-chaotic key, are applied to the known ciphertext to recover the input information. The recovered information as shown in Fig. 18 depicts the results corresponding to Fig. 10(a), while similar results are obtained to remaining all images (Figs. 10(b)–10(i)), respectively. Hence, the proposed scheme proves high robustness against the iterative attacks.

3.5 Comparative Analysis

In comparison to the related work [3], [10], [18]–[30], the usage of several RPMs to secure information increases the complexity of the encryption process since the knowledge of each RPM is required at the decryption stage. Our scheme has the key advantage over RPMs based scheme that the number of keys by using single FKP data can be obtained. This approach is not only

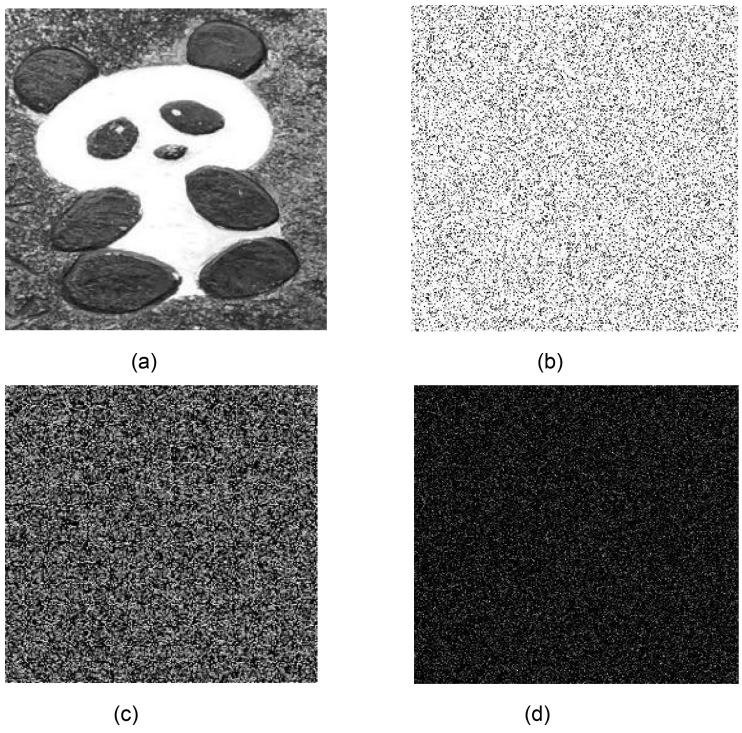


Fig. 18. (a) Input image (b) Encrypted (c) Retrieved phase key (d) KPA result.

offering in reducing the space for key storage and transmission but also provides an additional layer of security to the system. The computer simulation results demonstrate effectiveness in achieving higher accuracy, robustness, and security against KPA attack as well as the ability to resist noise attack and occlusion attack. In addition, its simple optical/digital implementation process offers low computational complexities and need less feature storage, which makes it more attractive, convenient, and versatile.

4. Conclusion

In this paper, a novel scheme is proposed to secure multiple information by using the bio-chaotic keys. In this work, our main contribution is related to the bio-chaotic key, in which the system parameters (i.e., initial conditions) of the chaotic function are created from the FKP image-based wavelet analysis. The process has the ability to generate multiple bio-chaotic keys from the single FKP image, which makes it more effective in reducing space for key storage space and transmission. Also, the bio-chaotic keys are further involved in securing multiple images, which ensures the user's specificity in the encryption and decryption process, who is authorized for sending and receiving the data. Numerical results of the proposed system are presented to achieve higher security, complexity, and robustness against existing attacks. Consequently, the proposed method offers a highly simplified and more convenient optical implementation in comparison with the previously reported techniques. The simulation result demonstrates the effectiveness and efficiency of the proposal, as well as encouraging further research development of more advanced and secure multimedia related application scenarios.

References

[1] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, no. 2, pp. 120–155, 2014.

[2] S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," *Opt. Laser. Technol.*, vol. 57, pp. 327–342, 2014.

[3] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, 1995.

[4] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.*, vol. 25, no. 12, pp. 887–889, 2000.

[5] G. Situ and J. Zhang, "Double random-phase encoding in the fresnel domain," *Opt. Lett.*, vol. 29, no. 14, pp. 1584–1586, 2004.

[6] L. F. Chen and D. M. Zhao, "Optical image encryption with hartley transforms," *Opt. Lett.*, vol. 31, no. 23, pp. 3438–3440, 2006.

[7] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Opt. Lett.*, vol. 31, no. 8, pp. 1044–1046, 2006.

[8] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lens less double-random phase encoding in the fresnel domain," *Opt. Lett.*, vol. 31, no. 22, pp. 3261–3263, 2006.

[9] U. Gopinathan, D. S. Monaghan, T. J. Naughton, and J. T. Sheridan, "A known-plaintext heuristic attack on the Fourier plane encryption algorithm," *Opt. Exp.*, vol. 14, no. 8, pp. 3181–3186, 2006.

[10] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase truncated Fourier transforms," *Opt. Lett.*, vol. 35, no. 2, pp. 118–120, 2010.

[11] X. Wang and D. Zhao, "A special attack on the asymmetric cryptosystem based on phase-truncated fractional Fourier transforms," *Opt. Commun.*, vol. 285, no. 6, pp. 1078–1081, 2012.

[12] S. K. Rajput and N. K. Nishchal, "Known-plaintext attack-based optical cryptosystem using phase-truncated fresnel transform," *Appl. Opt.*, vol. 52, no. 4, pp. 871–878, 2013.

[13] W. Chen, X. Chen, A. Stern, and B. Javidi, "Phase-modulated optical system with sparse representation for information encoding and authentication," *IEEE Photon. J.*, vol. 5, no. 2, Apr. 2013, Art. no. 6900113.

[14] A. Markman, B. Javidi, and M. Tehranipoor, "Photon-counting security tagging and verification using optically encoded QR codes," *IEEE Photon. J.*, vol. 6, no. 1, Feb. 2014, Art. no. 6800609.

[15] X. Wang, W. Chen, and X. Chen, "Optical encryption and authentication based on phase retrieval and sparsity constraints," *IEEE Photon. J.*, vol. 7, no. 2, Apr. 2015, Art. no. 7800310.

[16] M. Liao, D. Lu, W. He, and X. Peng, "Optical cryptanalysis method using wavefront shaping," *IEEE Photon. J.*, vol. 9, no. 1, Feb. 2017, Art. no. 2200513.

[17] D. Fan *et al.*, "Multiple-image authentication with a cascaded multilevel architecture based on amplitude field random sampling and phase information multiplexing," *Appl. Opt.*, vol. 54, no. 11, pp. 3204–3215, 2015.

[18] Z. Liu and S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Opt. Commun.*, vol. 75, no. 2, pp. 324–329, 2007.

[19] A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," *Appl. Opt.*, vol. 48, no. 31, pp. 5933–5947, 2009.

[20] F. Mosso, J. F. Barrera, M. Tebaldi, N. Bolognini, and R. Torroba, "All-optical encrypted movie," *Opt. Exp.*, vol. 19, no. 6, pp. 5706–5712, 2011.

[21] H. Hai, S. Pan, M. Liao, D. Lu, W. He, and X. Peng, "Cryptanalysis of random-phase-encoding-based optical cryptosystem via deep learning," *Opt. Exp.*, vol. 27, no. 15, pp. 21204–21213, 2019.

[22] X. Zhang *et al.*, "Two-level image authentication by two-step phase-shifting interferometry and compressive sensing," *Opt. Lasers Eng.*, vol. 100, pp. 118–123, 2018.

[23] H. E. Hwang, H. T. Chang, and W. N. Lie, "Multiple-image encryption and multiplexing using a modified gerchberg-saxton algorithm and phase modulation in Fresnel-transform domain," *Opt. Lett.*, vol. 34, no. 24, pp. 3917–3919, 2009.

[24] G. Situ and J. Zhang, "Multiple image encryption by wavelength multiplexing," *Opt. Lett.*, vol. 30, no. 11, pp. 1306–1308, 2005.

[25] X. Wang and D. Zhao, "Multiple-image encryption based on nonlinear amplitude-truncation and phase-truncation in Fourier domain," *Opt. Commun.*, vol. 284, no. 1, pp. 148–152, 2011.

[26] X. Deng and D. Zhao, "Multiple-image encryption using phase retrieve algorithm and intermodulation in Fourier domain," *Opt. Laser Technol.*, vol. 44, no. 2, pp. 374–377, 2012.

[27] G. Situ and J. Zhang, "Position multiplexing for multiple image encryption," *J. Opt. A*, vol. 8, no. 5, pp. 391–397, 2006.

[28] W. Liu, Z. Xie, Z. Liu, Y. Zhang, and S. Liu, "Multiple-image encryption based on optical asymmetric key cryptosystem," *Opt. Comm.*, vol. 335, pp. 205–211, 2015.

[29] S. K. Rajput, D. Kumar, and N. K. Nishchal, "Photon counting imaging and phase mask multiplexing for multiple images authentication and digital hologram security," *Appl. Opt.*, vol. 54, no. 7, pp. 1657–1666, 2015.

[30] D. Kong, L. Cao, G. Jin, and B. Javidi, "Three-dimensional scene encryption and display based on computer-generated holograms," *Appl. Opt.*, vol. 55, no. 29, pp. 8296–8300, 2016.

[31] J. Zhu *et al.*, "Computational ghost imaging encryption based on fingerprint phase mask," *Opt. Comm.*, vol. 420, pp. 34–39, 2018.

[32] H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, and N. Ohyama, "Known plaintext attack on double random phase encoding using fingerprint as key and a method for avoiding the attack," *Opt. Exp.*, vol. 18, no. 13, pp. 13772–13781, 2010.

[33] A. Yan, T. C. Poon, Z. Hu, and J. Zhang, "Optical image encryption using optical scanning and fingerprint keys, *J. Mod. Opt.*, vol. 63, no. S3, pp. S38–S43, 2016.

[34] A. Yan, Y. Wei, Z. Hu, J. Zhang, P. W. M. Tsang, and T. C. Poon, "Optical cryptography with biometrics for multi-depth objects," *Scientific Reports*, vol. 7, 2017, Art. no. 12933.
[35] G. Verma and A. Sinha, "Securing information using optically generated biometric keys," *J. Opt.*, vol. 18, no. 11, 2016, Art. no. 115701.
[36] G. Verma, M. Liao, D. Lu, W. He, X. Peng, and A. Sinha, "An optical asymmetric encryption scheme with biometric keys," *Opt. Lasers Eng.*, vol. 116, pp. 32–40, 2019.
[37] T. Zhao, Q. Ran, L. Yuan, Y. Chi, and J. Ma, "Image encryption using fingerprint as key based on phase retrieval algorithm and public key cryptography," *Opt. Lasers Eng.*, vol. 72, pp. 12–17, 2015.
[38] S. K. Rajput and O. Matoba, "Optical voice encryption based on digital holography," *Opt. Lett.*, vol. 42, no. 22, pp. 4619–4622, 2017.
[39] M. Takeda, K. Nakano, H. Suzuki, and M. Yamaguchi, "Encrypted sensing based on digital holography for fingerprint images," *Opt. Photon. J.*, vol. 5, no. 1, pp. 6–14, 2015.
[40] S. K. Rajput and O. Matoba, "Security enhanced optical voice encryption in various domains and comparative analysis," *Appl. Opt.*, vol. 58, pp. 3013–3022, 2019.
[41] G. Verma, M. Liao, D. Lu, W. He, and X. Peng, "A novel optical two-factor face authentication scheme," *Opt. Lasers Eng.*, vol. 123, pp. 28–36, 2019.
[42] M. Jridi, T. Napoléon, and A. Alfalou, "One lens optical correlation: Application to face recognition," *Appl. Opt.*, vol. 57, no. 9, pp. 2087–2095, 2018.
[43] A. Kumar and C. Ravikanth, "Personal authentication using finger knuckle surface," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 1, pp. 98–109, Mar. 2009.
[44] L. Zhang, L. Zhang, D. Zhang, and H. Zhu, "Online finger knuckle print verification for personal authentication," *Pattern Recognit*, vol. 43, no. 7, pp. 2560–2571, 2010.
[45] G. Verma and A. Sinha, "Finger knuckle print based verification using minimum average correlation energy filter," *Int. J. Electron. Commer. Stud.*, vol. 5, no. 2, pp. 233–246, 2014.
[46] G. Verma and A. Sinha, "Finger knuckle print recognition based on wavelet and gabor filtering," *Proc. Int. Conf. Comput. Vis. Image Process.*, vol. 459, pp. 35–45, 2017.
[47] A. Kumar, "Toward pose invariant and completely contactless finger knuckle recognition," *IEEE Trans. Biometrics, Behav., Identity Sci.*, vol. 1, no. 3, pp. 201–209, Jul. 2019.
[48] I. Mehra and N. K. Nishchal, "Wavelet-based image fusion for securing multiple images through asymmetric keys," *Opt. Commun.*, vol. 335, pp. 153–160, 2015.
[49] S. Pittner and S. V. Kamarthi, "Feature extraction from wavelet coefficients for pattern recognition tasks," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 21, no. 1, pp. 83–88, Jan. 1999.
[50] M. Unser, "Texture classification and segmentation using wavelet frames," *IEEE Trans. Image Process.*, vol. 4, no. 11, pp. 1549–1560, Nov. 1995.
[51] G. V. D. Wouwer, P. Scheunders, and D. V. Dyck, "Statistical texture characterization from discrete wavelet representation," *IEEE Trans. Image Process.*, vol. 8, no. 4, pp. 592–598, Apr. 1999.
[52] G. Bhatnagar and Q. M. J. Wu, "Chaos-Based security solution for fingerprint data during communication and transmission," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 4, pp. 876–887, Apr. 2012.
[53] G. Bhatnagar and Q. M. J. Wu, "A novel chaos-based secure transmission of biometric data," *Neurocomput.*, vol. 147, pp. 444–455, 2015.
[54] F. Han, J. Hu, X. Yu, and Y. Wang, "Fingerprint images encryption via multi-scroll chaotic attractors," *Appl. Math. Comput.*, vol. 185, no. 2, pp. 931–939, 2007.
[55] E. Soujeri, G. Kaddoum, and M. Herceg, "Design of an initial condition-index chaos shift keying modulation," *Electron. Lett.*, vol. 54, no. 7, pp. 447–449, 2018.