IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 June 2024, accepted 28 June 2024, date of publication 3 July 2024, date of current version 15 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3422392

RESEARCH ARTICLE

Securing Color Information Based on CEDPM Keys

GAURAV VERMA[1], **WENQI HE**[2], **XIANG PENG**[2], **AND DAJIANG LU**[2,3], **(Member, IEEE)**
[1]Department of Electronics and Communication Engineering, B. K. Birla Institute of Engineering and Technology, Pilani, Rajasthan 333031, India
[2]College of Physics and Optoelectronic Engineering, Shenzhen University, Shenzhen 518060, China
[3]College of Mechatronics and Control Engineering, Shenzhen University, Shenzhen 518060, China

Corresponding author: Dajiang Lu (ludajiang@outlook.com)

This work was supported in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2024A1515010370, and in part by the Sino-German Centre for Research Promotion under Grant M-0044.

ABSTRACT In this paper, a novel approach to generating keys for securing color information by combining discrete wavelet transform (DWT) in conjunction with chaotic functions is presented. This procedure is based on chaotic sequences derived using initial conditions and control parameters of the Logistic map function, which are utilized to decompose in different frequency subbands by applying the DWT. These subbands construct the chaotic encoded directional phase masks (CEDPM) keys. To investigate the potential applications of the CEDPM keys, a nonlinear optical cryptosystem for securing color images has been developed. The color image to be encoded in this study is first separated into three color planes such as red (R), green (G), and blue (B) which are transformed into the phase function using a modified phase retrieval algorithm. Subsequently, for R, G, and B color planes in the encoding procedure, the obtained CEDPM keys are employed, correspondingly. This procedure helps to facilitate the creation of a real-value ciphertext for the color channels R, G, and B. These encrypted images, which correspond to the color channels R, G, and B, are positioned at the horizontal, vertical, and diagonal subbands to combine with low-frequency subbands. After that, inverse wavelet operations are carried out to produce a single covered image. This technique strengthens the system's security by adding an additional layer. The efficacy of the color encryption approaches is confirmed using computer simulations. The results and analysis show that the proposed scheme performs satisfactorily in protecting color image components compared to the other techniques in this area.

INDEX TERMS Chaos, decryption, encryption, Fourier signal processing, image processing.

I. INTRODUCTION

In the digital era, a variety of communication channels are used to access a wide range of information, images, and data due to the internet's and networking technology's rapid expansion [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15]. Among these, images are employed to visualize complex data that helps people comprehend and analyze it [1], [4]. More precisely, digital photographs hold private, sensitive, or secret data that is shared and communicated widely in applications used in industry, defense, education, health, and other fields in the modern period. Data encryption is a crucial approach for information security. It is still difficult to conceal and secure data while it is being transmitted and received via a communication network [5], [6].

Numerous cryptographic methods based on optical and digital techniques have been used extensively in data security, authentication, and compression in recent years [2], [3], [4], [5], [6]. These optical approaches transform the input image into white stationary noise during encryption because of the specific properties of optics, which include intrinsic parallelism, high speed, and multidimensional features [7]. The optically encrypted information exhibits complex distribution which must be captured via a holographic technique, thus, stability of the encryption framework is also required.

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

The primary security key for data encryption in the system is random phase masks (RPMs), which also need to be supplied securely during the decryption stage, posing a key management challenge. Furthermore, several published optical encryption techniques use distinct transforms and parameters that function as additional keys and make information retrieval challenging [3], [8], [9].

Additionally, phase truncated Fourier transform (PTFT) algorithms that generate real-value ciphertext using nonlinear operations have gained popularity in recent years as image encryption techniques [14], [15], [16], [17], [18], [19], [20], [21], [22]. This method is very helpful in producing distinct decryption keys during encryption. To safeguarding multiple images, Mehra et al. suggested optical encryption based on the two-beam interference concept and PTFT technique [22]. Later, it was discovered that a number of nonlinear image encryption techniques utilizing the PTFT operations improved security robustness and performance [15], [16], [17], [18], [19], [20], [21], [22]. Moreover, several optical encryption methods use a monochromatic source to illuminate the image, or object that is digitally recorded, processed, and handled in the grayscale domain using an encryption algorithm [19], [20], [21], [22], [23], [24], [25], [26], [27], [28]. A digital holographic method for encrypting and decrypting images that is based on biometric keys generated by Verma et al. [23], [24], [25] represents effective key management while preserving the individual's authenticity. The color content information of an image is not retrieved during the decryption process in the schemes that have been reported. Additionally, the image loses its color information during the encryption process, which may have added more texture and richness. This can be utilized as important data or information for a variety of contemporary applications, including person recognition, medical imaging, military communication, and navigation.

To take into consideration the color content of the images, numerous researchers have concentrated their efforts in the field of color image encryption [29], [30], [31], [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52]. Initially, Zhang et al. tried optical encryption-based color image encryption [29]. This method creates an indexed image for encoding by first breaking down the color image into its component R, G, and B color channels. During the decryption, the indexed image is transformed into an RGB image to get the color image. Using the PTFT operation in the Fresnel domain, Chen et al. demonstrated effective key distribution and management for color image encryption and decryption [33]. A nonlinear cryptosystem was created by Deng et al. to encrypt the color image. Using this method, three random encryption phase keys are multiplied by the color image that has been divided into the R, G, and B color planes to create white stationary noise [34]. A PTFT-based optical encryption system for color images was proposed by Ding and Chen [36]. In this scheme, position multiplexing was used. Moreover, optical phase retrieval algorithms have been successfully used in information protection to boost the encryption process's robustness [2-1]. We discovered that, in terms of encryption techniques, the goal of color-image encryption research is to multiplex cipher color components on a single channel capacity with reduced computational complexity, reliable transmission over digital media, and implementation.

On the other hand, more research is being done on sophisticated digital techniques like wavelet and chaos for data analysis and image protection [10], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52]. The discrete wavelet transform (DWT) method differs from the conventional Fourier transform in that it breaks the image down into multiple frequency subbands that represents at a different resolution. For security, compression, identification, and authentication, DWT algorithms have been used in a number of research projects [10], [27], [38]. Aburab published a multiple-single-channel color image system using unequal spectrum decomposition and 2D-SLIM (2D sine improved 1ogistic iterative chaotic map) [38]. Furthermore, compared to previous encryption algorithms, cryptographic techniques based on chaotic systems have developed more and more, attaining a superior level of data security [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51], [52]. A color image encryption method based on block scrambling and chaos was described by Hosny et al. [39]. Chaos is more suited for image encryption because of its unique properties, which include its strong sensitivity to initial conditions and control parameters. As a result, it has been demonstrated that the inherent nonlinear characteristics of chaos can strengthen the encryption's security.

Motivated by features of chaos, DWT, and optics, we present a key generation procedure for encrypting color information that is based on DWT and chaotic algorithms. The major goals of the research investigated under this idea are focused on designing chaos-based DWT schemes for security with the characteristics of enhancing embedding efficiency and color image component undetectability while preserving the encryption's resilience. In this concept, we demonstrate our investigations on the chaotic sequence obtained using a logistic chaotic map function that is utilized to decompose it by applying DWT into different frequency subbands such as low, horizontal, vertical, and diagonal features. These subbands do not overlap and are used in the encoding process to generate the CEDPM keys. From a chaotic perspective, these keys possess many appealing properties, including randomness, discriminability, and uniqueness, which put forward the possibility of data encryption. For the first time, we combine the optical phase retrieval algorithm and the PTFT approach to implement a non-linear encryption strategy for color images that demonstrates the utilization of the CEDPM keys. Finally, we also present an efficient process for combining cipher color components into a single cover image to provide a trustworthy data transmission. Computer simulations and performance analysis verify that the proposed scheme is more effective in comparative to other reported methods. The following are the significant contributions of our idea, which are linked to the aforementioned goal:

1. Combining DWT and chaos, a new algorithm for the chaotic encoded directional phase masks (CEDPM) key generation scheme is proposed. Color components in the R, G, and B planes can be encoded by using the CEDPM keys that correspond to the horizontal, vertical, and diagonal subbands, respectively. Algorithm parameters play a crucial role in enhancing the security of cryptosystems by demonstrating a high degree of sensitivity to the keys.

2. A nonlinear encryption approach for color images is designed by using the phase retrieval algorithm, and the PTFT approach that increases encryption efficiency and robustness. It is also pointed out that the decryption phase needs correct key and algorithm parameters to recover the R, G, and B color components. The wrong color component information will be decrypted if there are any variations in the key and algorithm parameters.

3. Therefore, by combining steps 1 and 2, a color image-based encryption system that is efficient, dependable, and secure is constructed using the CEDPM key. This idea increases the features of maintaining embedding efficiency and undetectability of color components. Additionally, it keeps encryption performance safe from any potential attacks both during transmission and storage.

The rest of the paper is organized as follows. Section II covers the basics of chaos, wavelet, and optical encryption. In Section III, the proposed CEDPM key generation process is explained and also focuses on highlighting the role of wavelet, and chaos for information security. This section also describes a nonlinear cryptosystem for securing color images. Additionally, the process of embedding the encrypted color component into a single covered image is presented. In Section IV, the performance analysis of the system is presented together with simulation results that are evaluated using computational tests. Finally, concluding thoughts are reported in Section V.

II. PRELIMINARIES

Chaotic encoded directional phase masks (CEDPM) keys are created using the DWT and chaotic methods and are utilized in color image encryption. Additionally, the PTFT and optical phase retrieval are used in encryption techniques.

A. LOGISTIC CHAOTIC MAPS

A larger interpretation of recently published studies has led to the widespread use of a logistic chaotic map in the design of information security systems. The inherent nature of nonlinear chaotic characteristics such as great sensitivity to the initial parameter and values, non-periodicity, and pseudo-randomness are increasing the use of chaos maps for information encryption [10], [35], [37], [52]. These features have sparked a variety of chaotic types of research aimed at choosing appropriate chaotic functions, with a particular focus on creating random sequences for information encryption. The logistic map function in our investigation can be expressed mathematically as

$$X_{j+1} = rX_j(1 - X_j) \tag{1}$$

As stated in Eq. (1), the initial condition, control parameter, and iteration number are represented by the variables X, r, and j, respectively, The logistic map function parameters, $r = [3.564996,4]$ and $X_j \in (0, 1)$ should be in the interval to demonstrate the chaotic and random behavior. The logistic map function produces dynamically entirely random and chaotic states in this area [34]. Therefore, the involvement of a logistic chaotic map in a key generation to achieve better encryption efficiency.

B. DISCRETE WAVELET TRANSFORM (DWT)

DWT is an important tool used to decompose signals into different subbands at different scales [28]. This framework has been implemented generally by the involvement of using filter banks which contain a set of low pass filters *h(x),* and high pass filters $g(x)$ by performing a sub-sampling operation by a factor of ($\downarrow$ 2) as

$$L_{low}(k) = \sum\nolimits_x h(x-2k) \times CM(x) \tag{2}$$

$$H_{high}(k) = \sum\nolimits_x g(x-2k) \times CM(x) \tag{3}$$

The terms $CM(x)$, $L_{low}(k)$, and $H_{high}(k)$ represent the two-dimensional chaotic matrixes, coefficients of low-frequency, and high-frequency subbands, respectively. In the analysis, the wavelet selections and implementation of the desired decomposition level of the image also serve a crucial role in designing a system for security and authentication.

C. OPTICAL ENCRYPTION ALGORITHM

Due to the inherent parallelism potentialities for high-speed optical information processing and two-dimensional imaging, a variety of optical techniques have recently been devised that are capable of encrypting information. The development and concentration of research on color picture encryption is a result of the advancements in grayscale image encryption technology. Phase retrieval is a versatile technique that can handle 2D complex information and is efficiently used in optical security to strengthen the robustness of the encryption process. This method relies on an iterative transform that can be applied by switching back and forth between the frequency and object planes during the Fourier transforms. Typically, this method converts the input image into a phase function that is pseudo-random. Encryption is strengthened and made more secure by the data securities based on the optical phase retrieve technique [31], [32], [33], [34]. A systematic plan to exploit new areas of color information processing applications that might benefit from this kind of structure is provided by the phase retrieval architecture, which is a versatile characteristic. This framework's ease of use for complicated data processing and its ability to execute encryption and decryption—both optically and digitally—are appealing features.

III. PROPOSED CRYPTOSYSTEM FOR COLOR IMAGE ENCRYPTION

The proposed cryptosystem for color image encryption is formed of three main parts: A. generation of chaotic encoded directional phase masks (CEDPM) keys, B. Encryption scheme, and C. Decryption scheme. The proposed method for producing CEDPM keys is potentially investigated. These keys are subsequently employed to encrypt the color image components of R, G, and B, respectively. Additionally, the steps of combining the encrypted color component into a single covered image are presented which help in achieving reliable data transmission and storage. To further aid in the lossless recovery of the true color image, the decryption procedure operates in reverse of the encryption. The following is a description of the main stages of the proposed work.

A. CHAOTIC ENCODED DIRECTIONAL PHASE MASKS (CEDPM) GENERATION

A flow diagram of the proposed method for producing CEDPM keys is shown in Figure 1. For this purpose, DWT and logistic chaotic map algorithms are employed. In this procedure, the random sequences derived from the logistic chaos function are utilized to decompose into various frequency sub-bands using the DWT operation. These subbands are used to generate the chaotic encoded directional phase mask keys corresponding to the horizontal, vertical, and diagonal directions. These keys are later involved in encrypting components of the color image. To implement the CEDPM key, random sequences using the parameters of the logistic map function given in Eq. (1) are generated that should fall between the interval $r = [3.564996, 4]$ and $X_j \in (0, 1)$, and enlarged in two-dimensional chaotic matrixes (CM) as

$$CM = resize(X_{j+1}) \tag{4}$$

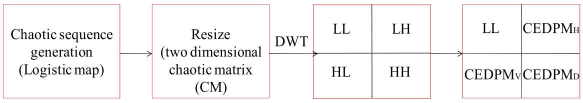
Chaotic sequence generation (Logistic map)
Resize (two dimensional chaotic matrix (CM)
DWT
LL
LH
HL
HH
LL
CEDPMH
CEDPMV
CEDPMD

FIGURE 1. Chaotic encoded directional phase mask (CEDPM) generation process.

Furthermore, as illustrated in Figure 2, chaotic matrices (CM) are decomposed using the Haar wavelet in several frequency sub-bands, such as horizontal (LH), vertical (HL), and diagonal (HH), which is also mathematically given as

$$\begin{aligned} F(u, v)_{Subbands} &= DWT[CM(x, y)] \\ &= [CM_{LL}, CM_{LH}, CM_{HL}, CM_{HH}] \end{aligned} \tag{5}$$

Moreover, these subband features are encoded to construct phase mask keys, where phases are uniformly distributed in the region $[0, 2\pi]$. Using a horizontal subband, the phase mask that is produced is indicated as

$$CEDPM_H = exp(i2\pi CM_{LH}) \tag{6}$$

It is noticed from Eq. (6) that the resultant phase mask as shown in Figure 3 has a speckle pattern and randomness, and is referred to as a chaotic encoded directional phase mask ($CEDPM_H$). In a similar manner, vertical (HL) and diagonal (HH) subbands are employed in the construction of the $CEDPM_V$ and $CEDPM_D$ keys. The algorithm's parameters are crucial during the key generation process and would be needed during the decryption stage. It is also mentioned that these parameters might be enough to produce numerous directional encryption keys that aid in minimizing storage space. With this in mind, optical encryption for color images aims to provide increased security and resilience. The next part goes into more detail about the color encryption design process.

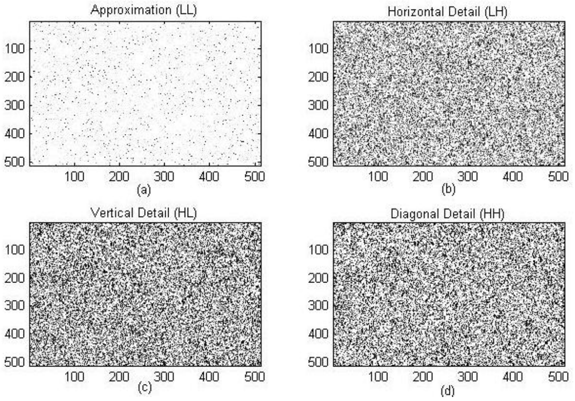

FIGURE 2. Subbands representation (a) Low frequency (LL) (b) Horizontal (LH) (c) Vertical (HL) (d) Diagonal (HH).

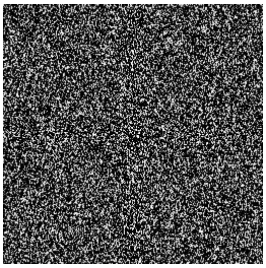

FIGURE 3. Obtained chaotic encoded directional phase mask ($CEDPM_H$).

B. ENCRYPTION SCHEME

Figure 4 describes the encrypting mechanism of the color image. In a color image, each pixel element is represented by three coordinates, which are linked to each color component. In the system, the color image $I(x, y)$ is decomposed into the R, G, and B components which are denoted by $I_R(x, y)$, $I_G(x, y)$, and $I_B(x, y)$, respectively.

$$I(x, y) = [I_R(x, y), I_G(x, y), I_B(x, y)] \tag{7}$$

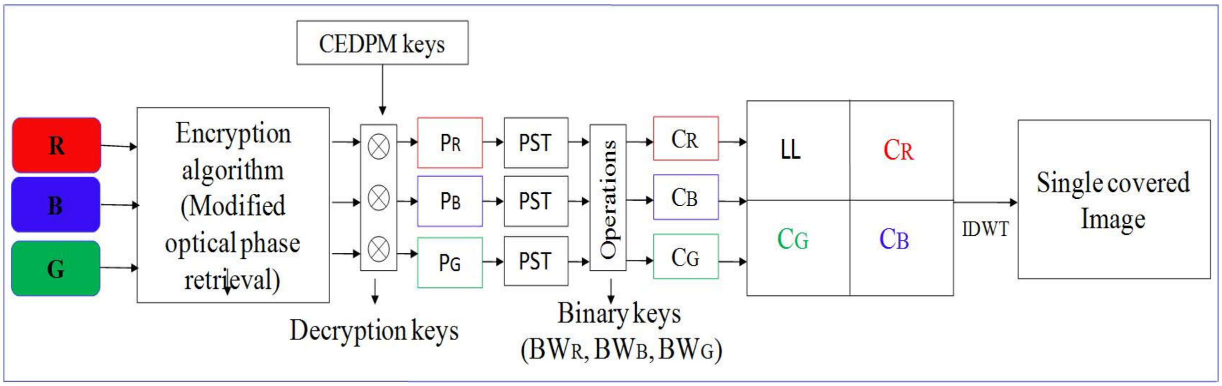

FIGURE 4. Flow diagram of the encryption process.

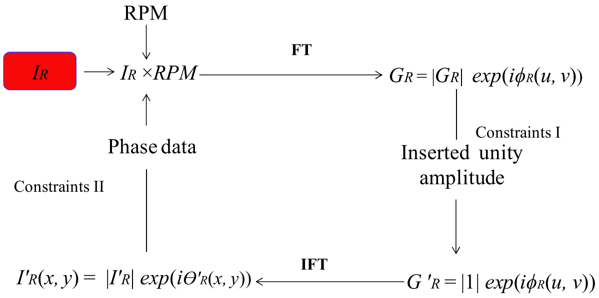

FIGURE 5. Encoding of color components using optical phase retrieval algorithm

In the idea, each color component is encoded by using modified phase retrieval algorithms. As shown in Figure 5, the algorithm implements iteratively by applying known constrain at the object plane and the frequency plane, respectively [23], [24]. At the beginning of the process, each color component is first combined by an arbitrarily selected RPM. It is then iteratively alternates between the Fourier domain and the spatial domain. First, the constraints are applied in the Fourier domain by changing the Fourier intensity by one factor while keeping the phase distribution constant. After executing the inverse Fourier transform (IFT), the data in the spatial domain is obtained. After performing several iterations, each color component is transformed into a Fourier phase function. For demonstration, the encoding steps of the phase retrieval algorithm for a red color plane "$I_R\,(x, y)$" can be mathematically given as:

Step 1: Initially, the Fourier transform (*FT*) of combined the red color component $I_R\,(x, y)$ with RPM is calculated as

$$G_R(u, v) = FT\,(I_R\,(x, y) \times RPM(x, y)) \tag{8}$$

$$G_R(u, v) = |G_R\,(u, v)|\, exp[i\emptyset_R\,(u, v)] \tag{9}$$

It gives complex distribution in the Fourier domain in terms of amplitude ($|G_R\,(u, v)|$) and phase part ($\exp[i\emptyset_R\,(u, v)]$) with respect to the R plane as represented Eq. (9). Here, (*x*, *y*) and (*u*, *v*) show coordinates in the spatial and Fourier domains, respectively.

Step 2: Reported that the Fourier transform, which is employed by the phase retrieval algorithm, has followed the linearity characteristics. To interrupt the linearity of the procedure, the amplitude specified in Eq. (9) is substituted with unity while keeping maintain Fourier phase part unchanged, and the inverse Fourier transform (IFT) is then performed as follows:

$$I'_R(x, y) = IFT\,(|1|\, exp[i\emptyset_R\,(u, v)]) \tag{10}$$

Step 3: As demonstrated in Eq. (10), information in the object domain is obtained. It has a mathematical expression in Eq. (11). In this stage, the amplitude $I'_R(x, y)$ is modified by using the second constraint which is the initial amplitude of the red color $I_R\,(x, y)$ component. These operations can be expressed mathematically as

$$I'_R\,(x, y) = \left|I'_R\,(x, y)\right| exp[i\theta'_R\,(x, y)] \tag{11}$$

$$I'_R\,(x, y) = |I_R\,(x, y)|\, exp[i\theta'_R\,(x, y)] \tag{12}$$

Step 4: The steps outlined in Equations (8)–(12) must be implemented through a number of iterations. Thus, the red color component is transformed into the Fourier phase using this procedure [24], [28], which has the following mathematical expression

$$P_R = exp[i\emptyset_R\,(u, v)] \tag{13}$$

The term "P_R" refers to the encoded phase data of the initial R color component, which is combined with the $CEDPM_H$ key. Furthermore, pixel scrambling transform (PST) procedures are applied to jumble by altering the pixel location of the resultant phase data to further increase the nonlinearity and difficulty of the encryption process [10], which is represented mathematically as

$$\begin{aligned} T_{PST} &= PST(P_R \cdot CEDPM_H) \\ &= \exp\,[i\emptyset_{RPST}\,(u, v)] \end{aligned} \tag{14}$$

As obtained information from Eq. (14), we divide it into two parts (i) angle part and (ii) sign part.

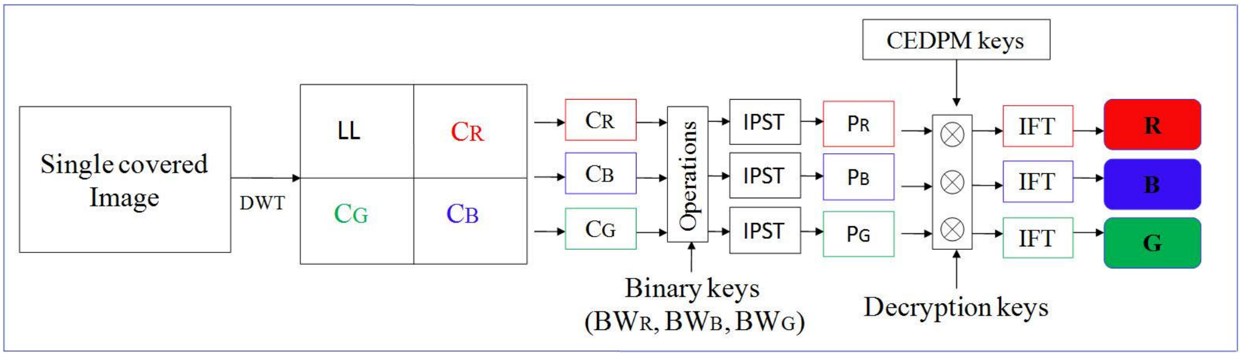

FIGURE 6. Flow diagram of the decrypting color components.

(i) The angle component has undergone digital processing to provide information to depict the absolute distribution as

$$C_R = abs[\emptyset_{\mathrm{RPST}}\,(u, v)] \tag{15}$$

(ii) To protect sign distribution, this can be encoded in terms of binary key (BW) as

$$BW_R = \begin{cases} 1, & if\ \emptyset_{\mathrm{RPST}}\,(u, v) \geq 1 \\ 0, & if\ \emptyset_{\mathrm{RPST}}\,(u, v) < 0 \end{cases} \tag{16}$$

Similarly, the processes listed in Equations (8)–(16) are carried out for green $I_G\,(x, y)$ and blue $I_B\,(x, y)$ combined with the $CEDPM_V$, and $CEDPM_D$, respectively. Using these steps, the encoded components for green and blue are given as

$$C_G = abs[\emptyset_{\mathrm{GPST}}\,(u, v)] \tag{17}$$

$$BW_G = \begin{cases} 1, & if\ \emptyset_{\mathrm{GPST}}\,(u, v) \geq 1 \\ 0, & if\ \emptyset_{\mathrm{GPST}}\,(u, v) < 0 \end{cases} \tag{18}$$

$$C_B = abs[\emptyset_{\mathrm{BPST}}\,(u, v)] \tag{19}$$

$$BW_B = \begin{cases} 1, & if\ \emptyset_{BPST}\,(u, v)) \geq 1 \\ 0, & if\ \emptyset_{BPST}\,(u, v) < 0 \end{cases} \tag{20}$$

It is important to note that the BW_R, BW_G, and BW_B keys are necessary required for the decryption procedure, as the aforementioned stages make clear. Furthermore, the PTFT operation is performed to the encoded color components (C_R, C_G, and C_B) obtained from Eqs. ((15), (17), and (19)) to generate the ciphertext. The phase truncation (PT) and phase reservation (PR), as detailed in Ref. [14], can be mathematically represented for the R color plane as follows to create ciphertext and decryption keys during the PTFT operation:

$$E_R = PT\{FT[C_R \times RPM]\} \tag{21}$$

$$E_R = PT\{FT\ [E_R\,(u, v)]\} \tag{22}$$

$$D_R = PR\{FT\ [E_R\,(u, v)]\} \tag{23}$$

Similarly, the processes given in Equations (21)–(23) are carried out for green for G and B color components and expressed as

$$E_G = PT\{FT\ [E_G\,(u, v)]\} \tag{24}$$

$$D_G = PR\{FT\ [E_G\,(u, v)]\} \tag{25}$$

$$E_B = PT\{FT\ [E_B\,(u, v)]\} \tag{26}$$

$$D_B = PR\{FT\ [E_B\,(u, v)]\} \tag{27}$$

From the above steps, the "D_R", "D_G", and "D_B" work as decryption keys corresponding to the R, G, and B color components while the terms "E_R", "E_G", and "E_B" shows real-valued cipher images of respective color components. The ciphertext corresponding to the R, G, and B planes are positioned at horizontal, vertical, and diagonal subband locations and fused with a low-frequency subband to achieve a single covered image by performing inverse wavelet operation that conceals encrypted color information.

$$E = [CM_{LL}, E_R, E_G, E_B] \tag{28}$$

$$W'(x, y) = IDWT[E] \tag{29}$$

This covered image $[W'(x, y)]$ serves as a carrier image, ensuring it secure and reliable transmission to the recipient across digital media. The PST order, BW, CEDPM, and D keys of the corresponding color components are needed for decryption. Any modifications or variances will result in an incorrect decryption of the input color component data.

C. DECRYPTION PROCESS

The procedure of decrypting color information is shown in Figure 6, which is the reverse operation of the encryption stage. The wavelet and chaotic parameters are also needed to produce the CEDPM keys as explained in Section II that help in decoding the color components. The first step in the decryption process is to provide a covered image, from which the encrypted color information for the R, G, and B channels is extracted by performing wavelet operation.

$$\begin{aligned} E &= DWT[W'(x, y)] \\ &= [CM_{LL}, E_R, E_G, E_B] \end{aligned} \tag{30}$$

Moreover, the following steps are carried out for decoding the R color component. This can be seen from decoding the cipher red (E_R) color information as retrieved in Eq. (30) that encoded phase color components (C_R) are obtained through a phase truncation operation on the product of the encrypted data (E_R) and the D_R key. This result is then combined the result with BW_R key to obtain the scrambling phase (T_{PST}). To extract the R color component, combining the conjugate of the $CEDPM_H$ key with the findings from the IPST data is also analyzed using an inverse Fourier transform.

$$C_R = PT\{FT\,(E_R \cdot D_R)\} \tag{31}$$

$$T_{PST} = \exp\{iC_R BW_R\} \tag{32}$$

$$P_R = IPST(T_{PST}) \times conj\,(CEDPM_H) \tag{33}$$

$$I_R = IFT(P_R) \tag{34}$$

Similar to this, the color content information in the G and B color planes can be decrypted by processing the E_G and E_B.

In the last step of the decryption procedure, the input color information $I(x, y)$ is obtained by merging information that has been acquired in the red, blue, and green color planes, respectively. The decryption step can be mathematically expressed as:

$$I(x, y) = [I_R\,(x, y)\,, I_G\,(x, y)\,, I_B\,(x, y)] \tag{35}$$

IV. RESULT AND DISCUSSION

This section includes the results of decryption against key combinations and unauthorized attacks, as well as analyses of key sensitivity, statistical tests, noise, and occlusion attacks, security, and comparative performance. To do this, a series of numerical experiments are performed on MATLAB 2014 set up on Windows 7 with 4 GB RAM and a core i5 processor. Any common or standard color test image can be used with our idea. For demonstration purposes, two color photographs are chosen: one is a traditional color image, and the other is a snapshot of a flower captured with the iPhone 8 Plus and used in computer simulations.

A. INPUT DATA

In order to analyze the proposed idea, test color images of 256 × 256 pixels are shown in Figures 7(a) and 7(e). These images are then divided into R, G, and B color components, as indicated in Figures 7(b)–7(d) and Figures 7(f)–7(h).

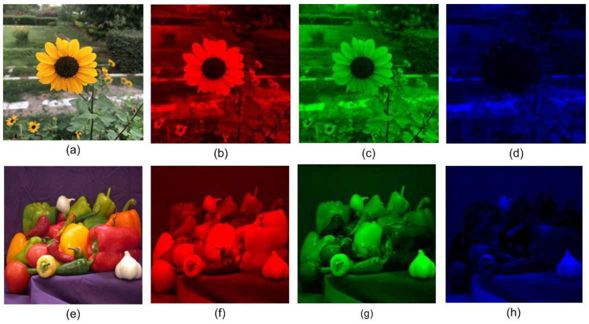

FIGURE 7. Test color images: (a) Input flower image (b) R plane of flower image (c) G plane of flower image (d) B plane of flower image (e) Input pepper image (f) R plane of pepper image (g) G plane of pepper image (h) B plane of pepper image.

In our simulations, the logistic map parameters form simulation are $x = 0.32$ and $r = 3.82$ for generating a chaotic sequence of samples = 262144. These samples are resized with size 512 × 512 pixels and then utilized to decompose by applying the 'Haar' wavelet in horizontal, vertical, and diagonal subbands of size 256 × 256 pixels as displayed in Figure 2, which are encoded as $CEDPM_H$, $CEDPM_V$,and $CEDPM_D$ as shown in Figures 8(a)–8(c) and then applied to encrypt R, G, and B color components, respectively. These keys are used to measure the encryption efficacy of the proposed concept for the selected two-color image as indicated in Figure 7.

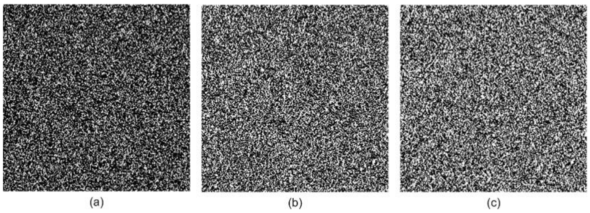

FIGURE 8. Generated chaotic encoded directional phase mask (CEDPM) keys (a) $CEDPM_H$ (b) $CEDPM_V$(c) $CEDPM_D$.

Using the encryption process for the selected two-color image as indicated in Figures 7(b)–7(d) and Figures 7(f)–7(h), the R, G, and B color components are encoded in a cipher image as indicated in Figures 9(a)–9(c) and Figures 9(d)–9(f), respectively. This encryption process also generates decryption keys corresponding to R, G, and B color components as shown in Figure 10. Finally, cipher images of R, G, and B color domains are fused with low-frequency components using wavelet operation. The result of this operation is a single covered image that, as seen in Figures 11(a) and 11(b), respectively, corresponds to Figures 7(a) and 7(e). It can be noticed that the covered image doesn't carry any visual resemblance with the original information and acts as noisy data.

B. DECRYPTION RESULTS

To recover color components, the covered image is provided to the decryption stage and then cipher color components are

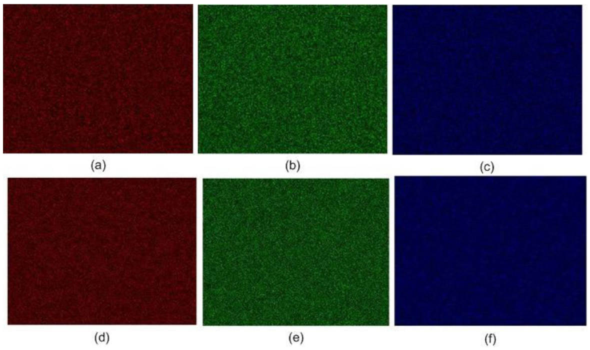

FIGURE 9. Cipher color components (E_R, E_G, and E_B) (a) encrypted R plane of flower image (b) encrypted G plane of flower image (c) encrypted B plane of flower image (d) encrypted R plane of pepper image (e) encrypted G plane of pepper image (f) encrypted B plane of pepper image.

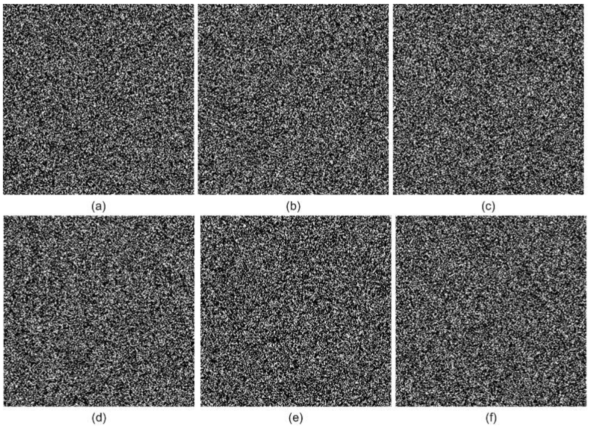

FIGURE 10. The decryption keys (D_R, D_G, and D_B) (a) decryption key for R plane of flower image (b) decryption key for G plane of flower image (c) decryption key for B plane of flower image (d) decryption key for R plane of pepper image (e) decryption key for G plane of pepper image (f) decryption key for B plane of pepper image.

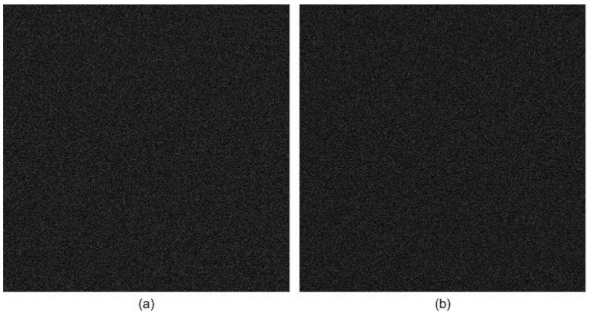

FIGURE 11. Single covered image [$W'(x, y)$] yielded for (a) the flower image, (b) the pepper image.

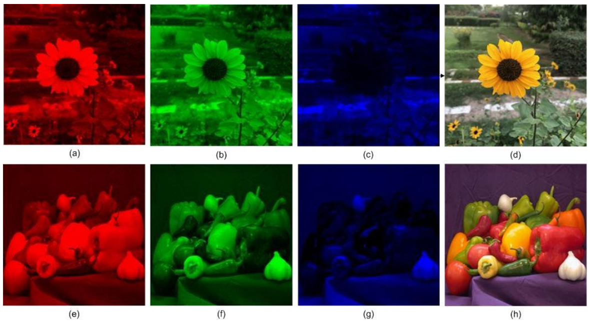

FIGURE 12. Decryption results (a) R plane of flower image (b) G plane of flower image (c) B plane of flower image (d) Input flower image (e) R plane of pepper image (f) G plane of pepper image (g) B plane of pepper image (f) Input pepper image.

extracted by using a wavelet operation. Moreover, decryption keys such as PST order, BW, CEDPM, and D keys are necessarily required to correspond to the R, G, and B color components. Any change in keys and parameters leads to a wrong decryption of the color components. So, the decryption steps using the possible key combinations are investigated, and the results are given in Figures 12–13. Figures 12(a)–12(c) and 12(e)–12(g) decrypt the input color component in the R, G, and B domains, respectively, when all keys are correctly entered into the decryption procedure. These figures' color components look the same as those for the selected image in Figures 7(b)–7(d) and 7(f)–7(h) respectively. Figures 12(d) and 12(h) display a truly obtained input color image for the selected two-color image, as shown in Figures 7(a) and 7(e).

To determine the accuracy of the recovered color components, the mean squared errors (MSE) and correlation coefficient (CC) between the input color component and the retrieved color component, respectively are evaluated [23], [24].

$$MSE = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} \left| I_R(x, y) - I'_R(x, y) \right|^2}{M \times N} \tag{36}$$

TABLE 1. Performance evaluation for flower image.

S. No.	Decrypted Color components	CC	MSE
1	$I_R(x,y)$	0.99	1.2026e-04
2	$I_G(x,y)$	0.99	2.7049e-05
3	$I_B(x,y)$	0.99	3.9092e-05
4	$\frac{(I_R(x,y) + I_G(x,y) + I_B(x,y))}{3}$	0.99	6.2134e-05

TABLE 2. Performance evaluation for pepper image.

S. No.	Decrypted Color components	CC	MSE
1	$I_R(x,y)$	0.99	1.2026e-04
2	$I_G(x,y)$	0.99	2.7049e-05
3	$I_B(x,y)$	0.99	3.9092e-05
4	$\frac{(I_R(x,y) + I_G(x,y) + I_B(x,y))}{3}$	0.99	6.2134e-05

where M and N are the size of the color image. The terms "$\bar{I}_R$" and "$\bar{I}'_R$" show the mean of the input red color component ($I_R(x, y)$) and the retrieved red color component ($I'_R(x, y)$), respectively. For full-color image information, performance is also shown in terms of the average of MSE and CC values as mentioned in Table 1 and 2 for the selected two images as shown in Figure 7.

Additionally, several unauthorized attempts have been demonstrated to retrieve the R color component for the selected two-color image. In the case of the R color component of the flower image, Figures 13(a)–13(d) represent the decrypted image. The recovered result is shown in Figure 13(a) when the $CEDPM_H$ key is excluded from the decryption process. The recovered result, when the D_R and the $CEDPM_H$ keys are positioned incorrectly,

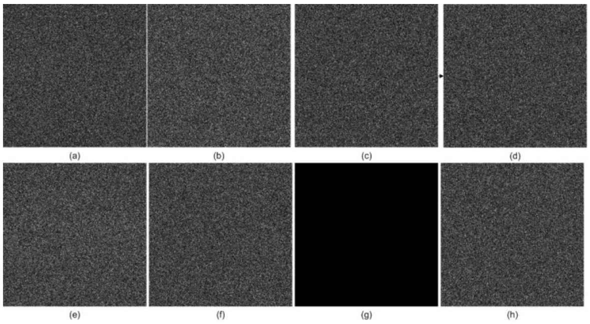

FIGURE 13. Decryption results for R color component: for flower image (a) no $CEDPM_H$ keys (b) wrongly placed D_R and $CEDPM_H$ key (c) $CEDPM_H$ replaced by arbitrarily RPM key (d) incorrect order of the PST keys for peppers image (e) no $CEDPM_H$ keys (f) wrongly placed D_R and $CEDPM_H$ key (g) $CEDPM_H$ replaced by arbitrarily RPM key (h) incorrect order of the PST keys.

is shown in Figure 13(b). When PST keys are used incorrectly, the retrieved content of the R color component is depicted in Figure 13(c). The recovered information is shown in Figure 13(d), where the CEDPM$_\text{H}$ key has been replaced with arbitrarily selected RPM keys. The estimated mean square error (MSE) between Figures 13(a)–13(d) and Figure 7(b) is determined to be 0.1137, 0.1103, 0.1142, and 0.1145. The results for the peppers image, as displayed in Figures 13(e)–13(h), also demonstrate that the recovered R color component solely contains noise information. Moreover, similar decryption results for G and B color components have been found for a subset of two color images against unauthorized attempts.

C. HISTOGRAM RESULTS

An image's histogram primarily shows the distribution of pixels with respect to intensity [1]. The histogram of the input image and the encryption image should be different.

The input color component histograms for the R, G, and B planes are shown in Figures 14(a)–14(c) and Figures 15(a)–15(c), as shown in Figures 7(b)–7(d) and Figures 7(f)–7(h), respectively. The encrypted color component histograms are shown in Figures 14(d)–14(f) and Figures 15(d)–15(f), as indicated in Figures 9(a)–9(c) and 9(d)–9(f). It is impossible to infer information about color components from the histogram analysis results.

D. SENSITIVITY TEST OF THE CEDPM KEY

To obtain information on color components, we assess the sensitivity of the CEDPM key by looking at minute deviations or modifications. The key parameters involved in decrypting the color components, such as [$x = 0.320000000000001$ and $r = 3.82$] and [$x = 0.32$ and $r = 3.8200000001$], are altered to confirm this. Figures 16(a)–16(c), 16(d)–16(f), as well as 17(a)–17(c), and Figures 17(d)–17(f), illustrate that the decoded color components of pepper and flower do not represent the original color components in any way or provide any useful information. As a result, even little adjustments or departures from the logistic map parameters will cause the CEDPM keys to be changed.

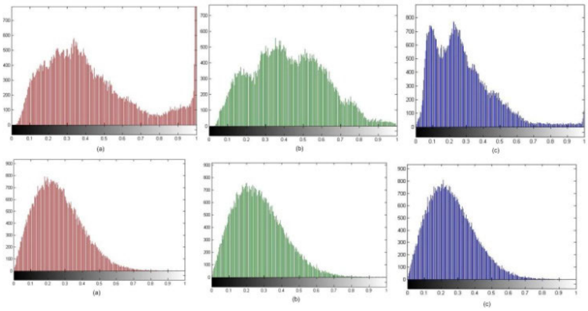

FIGURE 14. Histograms of the color components of the flower image (a) input R plane (b) input G plane (c) input B plane (d) encrypted R plane (e) encrypted G plane (f) encrypted B plane.

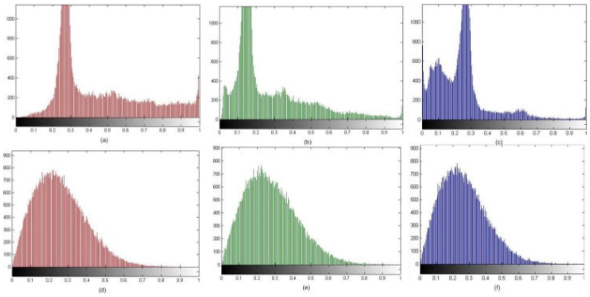

FIGURE 15. Histograms of the color components of the pepper image (a) input R plane (b) input G plane (c) input B plane (d) encrypted R plane (e) encrypted G plane (f) encrypted B plane.

E. OCCLUSION AND NOISE EFFECT

We investigate the effects of occlusion and noise on digital media during data storage or transfer [28]. When the covered image pixels of the flower and pepper, as shown in Figures 11(a)–11(b), have been occluded with 12.50% and 23.43% of pixels, the recovered color picture is displayed in Figures 18(a)–18(b) and Figures 18(c)–18(d), as well as Figures 19(a)–19(b) and Figures 19(c)–19(d). When the pepper and flower-covered picture pixels, as seen in Figures 11(a)–11(b), are corrupted with many noise types present, including Gaussian and Salt & Pepper noise, the decrypted color image is displayed in Figures 20–21. The outcomes of the experiment demonstrate how resilient the suggested system is to occlusion and noise attacks.

$$CC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_R(x,y)-\bar{I}_R\right)\left(I'_R(x,y)-\bar{I}'_R\right)}{\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_R(x,y)-\bar{I}_R\right)^2}\sqrt{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I'_R(x,y)-\bar{I}'_R\right)^2}} \tag{37}$$

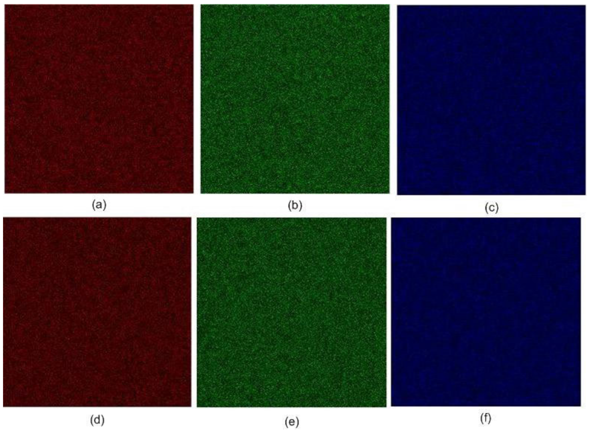

FIGURE 16. Decrypted results when the key parameters slightly change, $x = 0.320000000000001$, and $r = 3.82$ (a) R plane of flower image (b) G plane of flower image (c) B plane of flower image (d) R plane of pepper image (e) G plane of pepper image (f) B plane of pepper image.

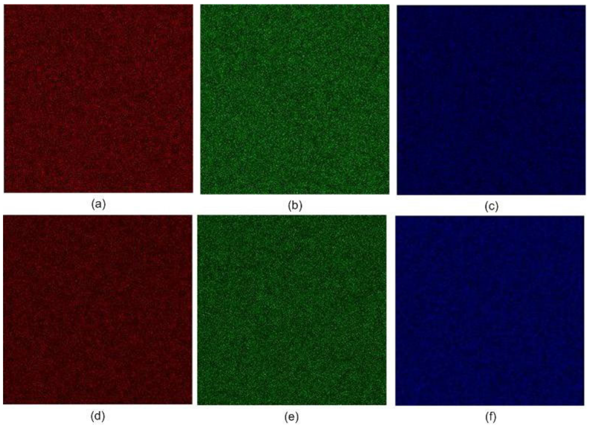

FIGURE 17. Decrypted results when the key parameters slightly change, $x = 0.32$, and $r = 3.8200000001$ (a) R plane of flower image (b) G plane of flower image (c) B plane of flower image (d) R plane of pepper image (e) G plane of pepper image (f) B plane of pepper image.

F. SECURITY ANALYSES

To evaluate security strength, the proposed color encryption scheme is tested against known plaintext attacks and special attacks [11], [15]. In our idea, the test color image segregated into R, G, and B planes is utilized to convert in the phase-only function at the Fourier domain using the phase retrieval algorithm. Moreover, the operation of pixel scrambling in the Fourier domain is applied and then digitally divided into binary keys (BW_R, BW_G, and BW_B) and amplitude distribution (C_R, C_G, and C_B) in R, G, and B color planes, respectively. To encrypt the amplitude distribution, the PTFT processes are combined to produce the cipher color images in R, G, and B color planes, respectively. To secure and reliable transmission, the color cipher images are efficiently hidden involving the wavelet process. In the process, several transforms are involved to increase the complexity and nonlinearity of the encryption process. In the case of unauthorized access to the color content, inherent noise increases at each iterative step using a phase retrieval algorithm. Hence, the proposed color image encryption leads to high robustness and immunity against known plaintext and special attacks.

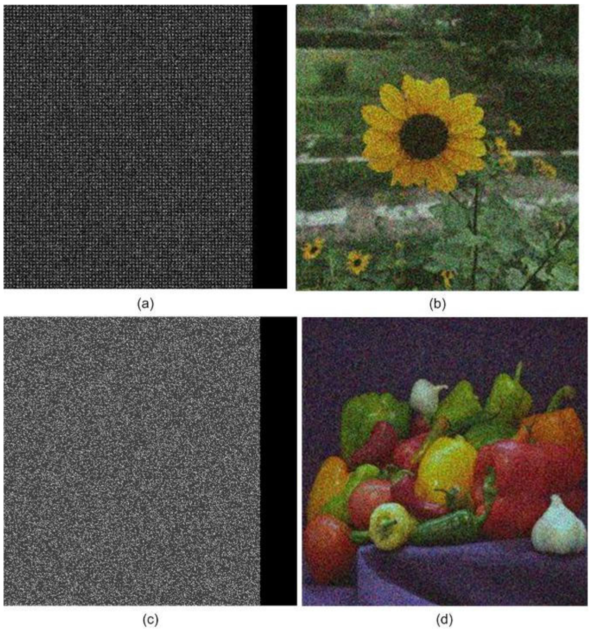

FIGURE 18. Occlusion attack results (a) occluded with 12.50% pixels of covered image for flower (b) Retrieved image for flower (c) occluded with 12.50% pixels of covered image of peppers (d) Retrieved image for pepper.

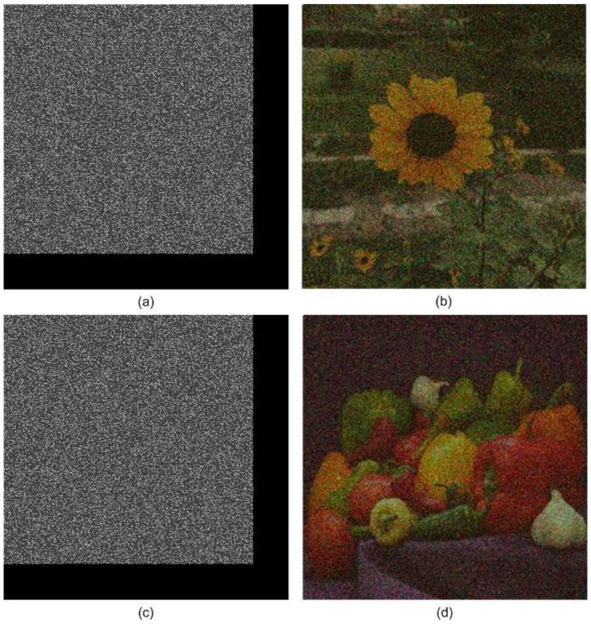

FIGURE 19. Occlusion attack results (a) occluded with 23.43% pixels of covered image for flower (b) Retrieved image for flower (c) occluded with 23.43% pixels of covered image of peppers (d) Retrieved image for pepper.

G. COMPARATIVE ANALYSIS

This section presents the comparative performance of our proposed scheme with some of the previously published schemes for color images. In the reported methods [37], [38],

TABLE 3. Comparative performance of the proposed color image encryption.

Performance Features	Ref.[37]	Ref.[38]	Ref.[39]	Ref.[40]	Ref.[41]	Ref.[42]	Ref.[43]	Ref.[44]	Proposed work
Robustness of decryption keys	√	√	√	√	√	√	√	√	√
statistical analyses	√	√	√	√	√	√	√	√	√
Sensitivity to initial condition and key	√	√	√	√	×	√	√	√	√
Robust to noise attacks	×	×	√	√	√	√	√	√	√
Robust to occlusion attacks	×	×	√	√	√	√	√	√	√
Robust to attacks such as known plaintext attacks,	√	√	√	√	×	√	√	√	√
Adds an extra layer of security	×	×	×	×	√	×	×	×	√

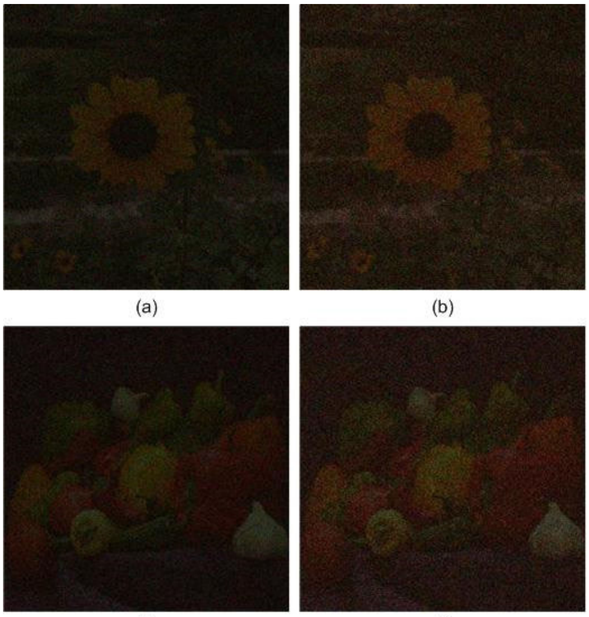
(a) (b) (c) (d)

FIGURE 20. Noise (Gaussian) impact results for covered image (a) recovered image (0.01var) of flower (b) recovered image (0.05var) of flower (c) recovered image (0.01var) of pepper (d) recovered image (0.05var) of pepper.

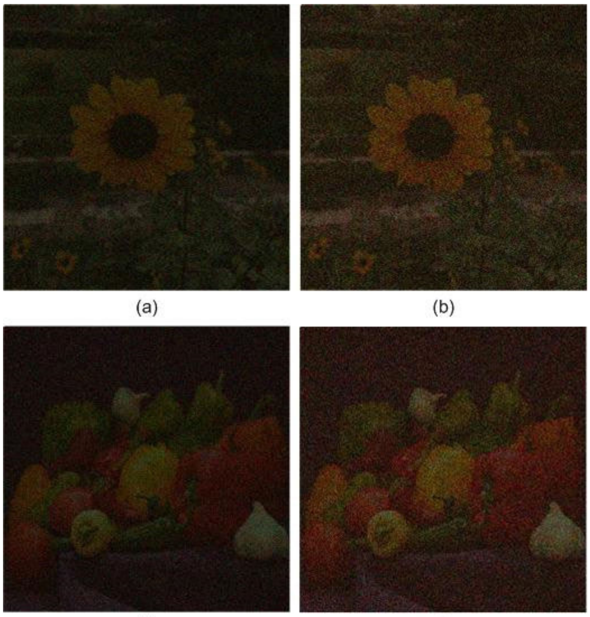
(a) (b) (c) (d)

FIGURE 21. Noise (Salt & Pepper) impact results for covered image (a) recovered image (0.01var) of flower (b) recovered image (0.05var) of flower (c) recovered image (0.01var) of pepper (d) recovered image (0.05var) of pepper.

[39], [40], [41], [42], [43], [44], color image encryptions can resist existing several types of attacks and perform well in noise and occlusion attacks. It can be seen from Table 3 shows that these methods are reliable and safe in terms of security performance.

However, these schemes involve several transforms to attain robustness and higher security against potential attacks. In Ref. [41], a method for producing random phase masks using the chaotic Henon map parameters and fingerprint biometrics is described. This key applies to encrypting color images in the domains of the Fourier transform, fractional Fourier transform (FrFT), Fresnel transform (FrT), and Gyrator transform (GT). It is noted that in comparison to other domains, results of the GT domain report better performance while keeping user authentication. Above all, there is no examination of this strategy for potential attacks. Furthermore, an investigatio of the reported cryptosystem against

TABLE 4. Provides the running time.

Color components	Time in seconds (flower)	Time in seconds (peppers)
R encoding	11.617214	11.257966
G encoding	12.927456.	10.363334
Blue encoding	13.492815	12.886273
Embedding cipher R, G, and B image to make single cover image	1.594112	0.614461
R decoding	1.820281	1.545786
G decoding	1.663955	1.559970
B decoding	1.350808	1.532809
Combining R, G, and B color planes to form True RGB image	1.472096	1.468652

tests of occlusion and noise attacks is not provided in Refs. [37] and [38].

Table 4 provides the running time of the proposed strategy for encrypting and decrypting the color components of both images. The chaotic and wavelet scheme parameters in our system are adequate to provide the CEDPM keys needed for both encryption and decryption. This will assist in using less storage space. Furthermore, our scheme provides an additional security layer to secure color material, and it is a pioneer in key distribution for encryption and decryption. As a result, our plan is effective and comparable in this regard. We will investigate our notion for multi-image and multimedia data encryption in the future.

V. CONCLUSION

This study suggests an innovative technique for generating CEDPM keys to secure color photographs. The different CEDPM keys are constructed by first combining the chaotic map with the DWT to produce pseudo-random sequences. For data encryption, these keys' enticing statistical characteristics include discriminability and randomness. Additionally, color images are encrypted using PTFT and optical phase retrieval techniques to investigate the potential applications of the CEDPM key. The cipher color components are then successfully incorporated into a covered image to enhance security against unauthorized assaults and ensure trustworthy transmission throughout the transfer of digital material. Computer simulations verify the robustness and efficacy of the proposed method for encrypting color information. Furthermore, our proposed scheme outperforms the others in terms of potential attack types including noise and occlusion, and performs better in terms of possible key combinations, key sensitivity, mean square error, and correlation coefficient. It is also comparable to the newly published research in this field.

Conflict of interest: The authors declare that they have no conflict of interest.

REFERENCES

[1] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," *Proc. IEEE*, vol. 97, no. 6, pp. 1128–1148, Jun. 2009.

[2] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Process.*, vol. 164, pp. 163–185, Nov. 2019.

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

[4] W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," *Adv. Opt. Photon.*, vol. 6, pp. 120–155, Apr. 2014.

[5] Z. Yun-Peng, L. Wei, C. Shui-Ping, Z. Zheng-Jun, N. Xuan, and D. Wei-Di, "Digital image encryption algorithm based on chaos and improved DES," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, San Antonio, TX, USA, Oct. 2009, pp. 474–479.

[6] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in *Multimedia Security Handbook*, B. Furht and D. Kirovski, Eds. Boca Raton, FL, USA: CRC Press, Dec. 2004, pp. 67–133.

[7] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, pp. 767–769, Apr. 1995.

[8] N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Opt. Lasers Eng.*, vol. 46, no. 2, pp. 117–123, Feb. 2008.

[9] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 29, pp. 1584–1586, Jul. 2004.

[10] Q. Wang, Q. Ding, Z. Zhang, and L. Ding, "Digital image encryption research based on DWT and chaos," in *Proc. 4th Int. Conf. Natural Comput.*, Jinan, China, Nov. 2008, pp. 494–498.

[11] 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, pp. 1044–1046, Jan. 2006.

[12] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.*, vol. 31, pp. 3261–3263, Oct. 2006.

[13] N. Saini and A. Sinha, "Biometrics based key management of double random phase encoding scheme using error control codes," *Opt. Lasers Eng.*, vol. 51, no. 8, pp. 1014–1022, Aug. 2013.

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

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

[16] W. He, S. Pan, M. Liao, D. Lu, Q. Xing, and X. Peng, "A learning-based method of attack on optical asymmetric cryptosystems," *Opt. Lasers Eng.*, vol. 138, Mar. 2021, Art. no. 106415.

[17] A. Alarifi, M. Amoon, M. H. Aly, and W. El-Shafai, "Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system," *IEEE Access*, vol. 8, pp. 221246–221268, 2020.

[18] G. Verma and A. Sinha, "Optical image encryption system using nonlinear approach based on biometric authentication," *J. Mod. Opt.*, vol. 64, pp. 1321–1329, Feb. 2017.

[19] D. Souza, A. Burlamaqui, and G. Souza Filho, "Improving biometrics authentication with a multi-factor approach based on optical interference and chaotic maps," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2013–2032, Jan. 2018.

[20] T. Nomura and B. Javidi, "Optical encryption using a joint transform correlator architecture," *Opt. Eng.*, vol. 39, pp. 2031–2035, Aug. 2000.

[21] B. Javidi and N. Takanori, "Securing information by use of digital holography," *Opt. Lett.*, vol. 25, pp. 28–30, 2000.

[22] I. Mehra and N. K. Nishchal, "Asymmetric cryptosystem for securing multiple images using two beam interference phenomenon," *Opt. Laser Technol.*, vol. 60, pp. 1–7, Jan. 2014.

[23] G. Verma and A. Sinha, "Securing information using optically generated biometric keys," *J. Opt.*, vol. 18, no. 11, Oct. 2016, Art. no. 115701.

[24] 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, May 2019.

[25] G. Verma, W. He, and X. Peng, "A novel four image encryption approach in sparse domain based on biometric keys," *Multimedia Tools Appl.*, vol. 82, no. 15, pp. 22889–22904, Feb. 2023.

[26] D. Lu, M. Liao, W. He, Q. Xing, G. Verma, and X. Peng, "Experimental optical secret sharing via an iterative phase retrieval algorithm," *Opt. Lasers Eng.*, vol. 126, Mar. 2020, Art. no. 105904.

[27] I. Mehra and N. K. Nishchal, "Fingerprint image encryption using phase retrieval algorithm in gyrator wavelet transform domain using QR decomposition," *Opt. Commun.*, vol. 533, Apr. 2023, Art. no. 129265.

[28] G. Verma, W. He, D. Lu, M. Liao, X. Peng, J. Healy, and J. Sheridan, "Securing multiple information using bio-chaotic keys," *IEEE Photon. J.*, vol. 13, no. 1, pp. 1–17, Feb. 2021.

[29] S. Q. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," *Microw. Opt. Technol. Lett.*, vol. 21, pp. 318–323, Apr. 1999.

[30] D. Amaya, M. Tebaldi, R. Torroba, and N. Bolognini, "Digital color encryption using a multi-wavelength approach and a joint transform correlator," *J. Opt. A, Pure Appl. Opt.*, vol. 10, no. 10, Oct. 2008, Art. no. 104031.

[31] L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Opt. Exp.*, vol. 14, pp. 8552–8560, Sep. 2006.

[32] W. Chen, C. Quan, and C. J. Tay, "Optical color image encryption based on Arnold transform and interference method," *Opt. Commun.*, vol. 282, no. 18, pp. 3680–3685, Sep. 2009.

[33] W. Chen and X. Chen, "Optical color image encryption based on an asymmetric cryptosystem in the Fresnel domain," *Opt. Commun.*, vol. 284, pp. 3913–3917, Aug. 2011.

[34] X. Deng and D. Zhao, "Single-channel color image encryption based on asymmetric cryptosystem," *Opt. Laser Technol.*, vol. 44, pp. 136–140, Feb. 2012.

[35] A. Momeni Asl, A. Broumandnia, and S. J. Mirabedini, "Scale invariant digital color image encryption using a 3D modular chaotic map," *IEEE Access*, vol. 9, pp. 102433–102449, 2021.

[36] X. Ding and G. Chen, "Optical color image encryption using position multiplexing technique based on phase truncation operation," *Opt. Laser Technol.*, vol. 57, pp. 110–118, Apr. 2014.

[37] M. Yildirim, "Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit," *Chaos, Solitons Fractals*, vol. 155, Feb. 2022, Art. no. 111631.

[38] M. R. Abuturab, "Securing multiple-single-channel color image using unequal spectrum decomposition and 2D-SLIM biometric keys," *Opt. Commun.*, vol. 493, Aug. 2021, Art. no. 127034.

[39] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A color image encryption technique using block scrambling and chaos," *Multimedia Tools Appl.*, vol. 81, pp. 505–525, Sep. 2022.

[40] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106040.

[41] Y. Su, W. Xu, J. Zhao, L. Chen, and X. Tian, "Optical color image encryption based on chaotic fingerprint phase mask in various domains and comparative analysis," *Appl. Opt.*, vol. 59, no. 2, pp. 474–483, Jan. 2020.

[42] M. Chen and C. Tang, "Optical single-channel color image cryptosystem based on vector decomposition and three-dimensional chaotic maps," *Appl. Opt.*, vol. 57, no. 32, pp. 9690–9698, Nov. 2018.

[43] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020.

[44] M. G. A. Malik, Z. Bashir, N. Iqbal, and Md. A. Imtiaz, "Color image encryption algorithm based on hyper-chaos and DNA computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020.

[45] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 60, pp. 12–32, Jul. 2018.

[46] M. Rafiq Abuturab, "Multiple color image cryptosystem based on coupled-logistic-map-biometric keys, QR decomposition with column pivoting and optical Fresnel transform," *Opt. Laser Technol.*, vol. 161, Jun. 2023, Art. no. 109109.

[47] S. Agarwal, "A review of image scrambling technique using chaotic maps," *Int. J. Eng. Technol. Innov.*, vol. 8, no. 2, pp. 77–98, Mar. 2018.

[48] S. Zhou, X. Wang, M. Wang, and Y. Zhang, "Simple colour image cryptosystem with very high level of security," *Chaos, Solitons Fractals*, vol. 141, Dec. 2020, Art. no. 110225.

[49] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61334–61345, 2021.

[50] T. Lin, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dyn.*, vol. 105, pp. 1859–1876, Jul. 2021.

[51] B. Sun, C. Zhang, Q. Peng, and B. Du, "Color image encryption algorithm based on 5D memristive chaotic system and group scrambling," *Optik*, vol. 287, Sep. 2023, Art. no. 171132.

[52] Q. Liu and L. Liu, "Color image encryption algorithm based on DNA coding and double chaos system," *IEEE Access*, vol. 8, pp. 83596–83610, 2020.

GAURAV VERMA received the M.Tech. degree in optoelectronics specialization in optical communication from the Shri G. S. Institute of Technology and Science, Indore, India, and the Ph.D. degree in optical information security and authentication from the Indian Institute of Technology Delhi, New Delhi, India, in 2017. He was with the College of Applied Physics and Optoelectronics Engineering, Shenzhen University, China, as a Postdoctoral Researcher. He is currently an Assistant Professor with the B. K. Birla Institute of Engineering and Technology, Pilani, Rajasthan, India. His research interests include optical information processing, optical security, image encryption and decryption, biometrics, and optical imaging techniques.

WENQI HE received the B.S. degree in optoelectronic information engineering from South China Normal University, in 2007, and the M.S. degree in physical electronics and the Ph.D. degree in optical engineering from Shenzhen University, China, in 2010 and 2012, respectively. He is with the College of Physics and Optoelectronic Engineering, Shenzhen University. He has authored more than 50 articles in peer-reviewed professional journals. His current research interests include computational optical imaging and machine vision.

XIANG PENG received the B.S., M.S., and Ph.D. degrees from Tianjin University, in 1981, 1984, and 1989, respectively, all in optical engineering.

In 1984, he was with Tianjin University, as an Assistant Professor. From July 1985 to July 1986, he was a Visiting Scholar with the Department of Electrical and Electronic Engineering, University of Huston, TX, USA. From 1990 to 1992, he was with the Institute of Applied Optics, University of Stuttgart, as an Alexander von Humboldt Fellow. He was with Tianjin University, as an Associate Professor, in 1996, and a Full Professor, in 1998. Since 2003, he has been a Full Professor with Shenzhen University. He is also the Director of the Engineering Laboratory for 3-D Imaging and Modeling, Shenzhen Government; and a Principal Scientist with ESUN Company Ltd., College of Optoelectronics Engineering, Shenzhen University. He is leading a research group to conduct research in the areas of 3-D imaging and modeling, optical security, optical metrology, and the phase-optics based imaging and display. He has authored or coauthored over 100 refereed journal articles and holds over 20 patents. His current research interests include optical imaging, metrology, and optical security.

DAJIANG LU (Member, IEEE) received the B.S. and Ph.D. degrees in optical engineering from Shenzhen University, China, in 2011 and 2016, respectively. He was a Research Scientist with Shenzhen University, from 2017 to 2022, where he is currently an Assistant Professor with the College of Mechatronics and Control Engineering. His research interests include computational imaging, optical information processing and security, and machine learning.