Received: 19 July 2023 | *Revised:* 10 September 2023 | *Accepted:* 30 November 2023
DOI: 10.37917/ijeee.20.2.14 *Vol. 20 | Issue 2 | December 2024*

Iraqi Journal for Electrical and Electronic Engineering
Original Article

Open Access

Design of High-Secure Digital/Optical Double Color Image Encryption Assisted by 9D Chaos and DnCNN

Rusul Abdulridha Muttashar*, Raad Sami Fyath
Department of Computer Engineering, Al-Nahrain University, Baghdad, Iraq

Correspondance
*Rusul Abdulridha Muttashar,
Department of Computer Engineering,
Al-Nahrain University, Baghdad, Iraq
Email: Rsusl97.abd@gmail.com

Abstract
With the rapid development of multimedia technology, securing the transfer of images becomes an urgent matter. Therefore, designing a high-speed/secure system for color images is a real challenge. A nine-dimensional (9D) chaotic-based digital/optical encryption schem is proposed for double-color images in this paper. The scheme consists of cascaded digital and optical encryption parts. The nine chaotic sequences are grouped into three sets, where each set is responsible for encryption one of the RGB channels independently. One of them controls the fusion, XOR operation, and scrambling-based digital part. The other two sets are used for controlling the optical part by constructing two independent chaotic phase masks in the optical Fourier transforms domain. A denoising convolution neural network (DnCNN) is designed to enhance the robustness of the decrypted images against the Gaussian noise. The simulation results prove the robustness of the proposed scheme as the entropy factor reaches an average of 7.997 for the encrypted color lena-baboon images with an infinite peak signal-to-noise ratio (PSNR) for the decrypted images. The designed DnCNN operates efficiently with the proposed encryption scheme as it enhances the performance against the Gaussian noise, where the PSNR of the decrypted Lena image is enhanced from 27.01 dB to 32.56 dB after applying the DnCNN.

Keywords
Hybrid digital/optical encryption, 9D chaotic system, Double color image encryption, DnCNN, Chaotic-based image encryption.

I. Introduction

As of advances in communication and networking technology, research has been conducted on transmitting images securely in real-time [1–3]. Generally, secure transmission can be achieved by applying image encryption algorithms at the transmitter side and related decryption algorithms at the authorized receiver side [4–6]. Recently, there has been increasing interest in using optical technology for encrypting gray and color images to achieve a high-speed encryption process [3, 4, 7]. The optical encryption (OE) process treats the image directly as a two-dimensional (2D) object. Therefore, it does not use image digitization as done in the digital encryption (DE) counterpart. Further, OE methods have some characteristic features due to the optical devices [8, 9]. For example, the amplitude and phase information of all image pixels can be processed simultaneously. Further, image encryption can be processed in various matrix spaces such as phase and polarization, which offers additional security level and reliability. The general structure of OE schemes consists of lasers, spatial light modulators (SLMs), lenses, beam splitters, and detectors [8]. A spatial light modulator is a general term describing devices that are used to modulate the amplitude, phase, or polarization of light waves. The SLM produces transparency controlled by the computer according to the image or mask required to modulate the light beam [10]. It is worth mentioning here that the operation of the OE scheme may be assisted by DE algorithms to support certain functions which cannot be implemented using the available optical and/or photonic

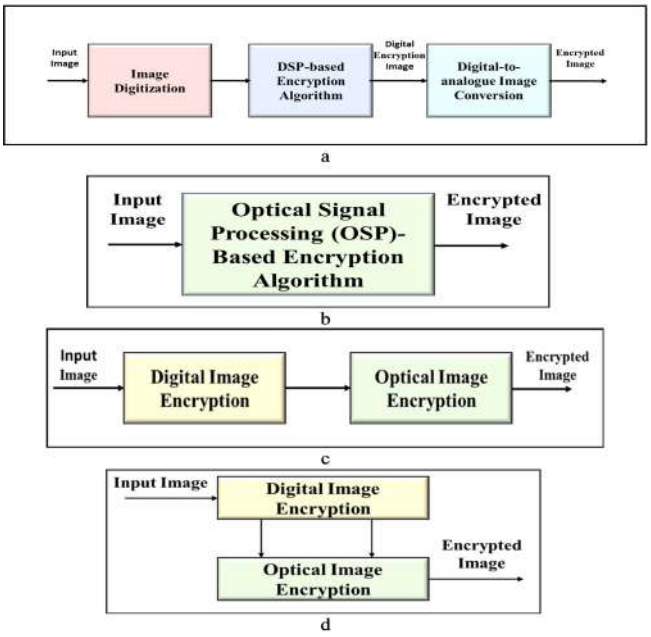


Fig. 1. Block diagrams of different image encryption schemes (a) Digital encryption (b) Optical encryption (c) Cascaded hybrid digital/optical encryption (d) Hybrid image encryption using correlated digital and optical subschemes.

techniques [5, 11]. In this case, the system is called a hybrid digital/optical encryption (HDOE) scheme. Fig. 1a-d briefly illustrate the main concepts of these different image encryption schemes using block diagram description. Note that the DE scheme needs an introductory stage where the image is digitized before going to the DSP-based algorithms Fig. 1a. In contrast, the OE scheme deals directly with the 2D image Fig. 1b. The hybrid encryption scheme is generally based on cascaded DE and OE parts Fig. 1c. However more efficient hybrid encryption scheme has been proposed in the literature where DE is used to control different parts of the OE scheme Fig. 1d.

Recently, there has been increasing interest in using chaotic dynamic systems in the design of image encryption/decryption schemes to increase the level and robustness of security. The dynamic of a chaotic system is very sensitive to initial conditions. To ensure a successful image decryption, two identical chaotic sources with the same initial conditions are used, one on the encryption side and the other on the authorized user decryption side. Different chaotic-based algorithms have been proposed for DE [4, 12], OE [10, 13], and hybrid HDOE [14, 15]. Increasing the dimension (i.e., order) of the chaotic system plays a key role to enhance the encryption process's efficiency. For example, Kumar et al. proposed in 2020 an HDOE encryption algorithm for a double-color image using a three-dimensional (3D) chaotic map and 2D-multiple parameter fractional Fourier transform (FrFT) [14]. In 2021, Faragallah et al. presented an OE algorithm for color images using 2D logistic-based FrFT [5].

The main challenge facing researchers working in optical image encryption is how to design efficient OE and HDOE schemes incorporating the following issues (which have been usually suggested as future work in their publications).

1)

Developing the existing designs or suggesting new designs to support multiple color image encryption. Most of the related work reported in the literature has been concerned mainly with single-color image [16] and to less extent for double-color image [15]. Very few works have been reported on multiple color images [17].

2)

Incorporating advanced encryption-assisted techniques such as deep learning (DL) and chaos. These two techniques have already been adopted in digital image encryption and need to be modified for OE. Few publications have been appeared in the literature describing the design of DL-assisted OE schemes, which concerned mainly with single-color images [18, 19]. Although chaotic dynamic systems have already been adopted in OE, the dimension (order) of these dynamics does not exceed five. This is also true for DE counterparts. A higher-order chaotic system is expected to play a key role in increasing the encryption level and robustness.

II. Related work

This section presents a brief literature survey on double and multiple-image optical encryption methods. Due to the limited number of published articles using deep learning on this topic, the survey is extended to cover deep learning-assisted single-image optical encryption.

In 2018, Huo et al. [20] suggested a double random phase encoding (DRPE) and compressive sensing (CS)-based multiple image binary and grayscale optical encryption method. The multiple-image compressed sample data were integrated and extracted using orthogonal encoding and used CS to sample each plaintext image during the encryption process. The results revealed that the hybrid multiple-image encryption approach minimizes key data while maintaining system security.

In 2019, Chen et al. [21] proposed a method to increase the robustness of 2D/3D optical image encryption using dilated deep CNN. They adopted DRPE in the FrFT domain and introduced the pixel position scrambling method to increase the security of the encryption system. A fast and effective denoising convolution neural network (DnCNN) based on the DL concept was employed to overcome the problem that

encrypted images are susceptible to attacks in practical applications.

In 2020, Kumar et al. [14] demonstrated the 2D multiple parameters fractional discrete cosine transform (2D-MPFrDCT) and the 3D-chaotic logistic map (3D-LCM) to present a new encryption and decryption method for optical and digital double color images. A random phase mask (RPM) produced by 3D-LCM was multiplied by the second scrambled image.

In 2021, Man et al. [15] proposed a double grayscale image encryption algorithm based on dynamic adaptive diffusion, five-dimensional (5D) chaos, and CNN. The algorithm used a two-channel (optical channel/digital channel) encryption method supported by a novel image bit-level split-fusion scheme, which depends on the amount of information it holds. Further, a chaotic sequence was employed as a convolution kernel of CNN to generate a plaintext-related chaotic pointer to control the scrambling operation of two images. The optical encryption channel used DRPE scheme.

In 2021, Liao et al. [22] introduced a two-step DL strategy for ciphertext image-only attacks (COA) on a classical DRPE system. In particular, they built a virtual DRPE system to collect the training data. In Addition, the inverse problem in COA was split into two more specific inverse problems. Two deep neural networks (DNNs) were used after training to respectively learn the removal of speckle noise in the autocorrelation domain and the de-correlation operation to retrieve the plaintext image.

In 2021, Ni et al. [23] suggested a multiple image encryption approach based on CS and DL in the optical gyrator transform (GT) domains. Various measurements were obtained after compression of the images using CS, then the pixels of each measure were scrambled using a chaotic system. The scrambled measurements were combined into a matrix and diffused by XOR operation with a chaotic matrix. Later, the diffused matrix was encoded with an RPM and an optical gyrator transform to obtain a complex-valued matrix, which was taken as the ciphertext.

In 2022, Abuturab et al. [17] investigated using CS, chaotic-biometric keys, and optical FrFT for multiple-color image fusion, compression, and encryption. The original four-color images were split into four sub bands in the proposed cryptosystem. Four sub bands were merged to create a single image separated into R, G, and B channels, where CS compresses each channel. The measurement matrix was a circulant matrix based on a logistic map's random sequence. The compressed R and G channels produce the first chaotic-biometric phase mask (CBPM), while the compact B channel produces the second CBPM. The resulting complex image is modulated by a second CBPM, then FrFT. The final encrypted image was a phase- and amplitude-truncated.

In 2022, Zhang et al. [24] proposed a secure double grayscale image encryption scheme based on a novel fusion application of CS and DRPE optical transformation technology. The method not only realizes the compression and encryption of two images into one image but also realizes image authentication.

In 2022, Zhang et al. [25] evaluated the use of DL to create a single-exposure phase-only optical image encryption and hiding (POIEH) technique. The original image and corresponding encrypted hidden interferogram acquired with POIEH were used to train an end-to-end designed U-net. Once the relationship between the encrypted hidden interferogram and the reconstructed image was learned, only a single-frame encrypted hidden interferogram was needed to reconstruct POIEH.

The main conclusions drawn from this survey as related to double and multiple image encryption are

1)

The maximum dimension of the used chaotic system is 5D. It is expected that going to higher-dimensional chaos will increase the level of encryption security and open new space keys to support further the quality measures of the encryption process.

2)

The optical transform (such as Fourier transform (FT), FrFT, and GT)-based encryption methods used a double random phase encoding approach. It is interesting to investigate these optical transform-based methods using double chaotic (or hybrid chaotic/random) phase-encoding approaches.

3)

The use of DL to enhance double and multiple-image optical inception is limited in the open literature. This issue needs further investigation to enhance the optical encryption capability.

This paper aims to design a high-secure optical scheme for multiple color image encryption incorporating deep learning techniques for performance enhancement. This aim may be achieved through the following steps

A.

Proposing a chaotic-based HDOE scheme to make use of the advantages behind both digital and optical encryption algorithms.

B.

Using a high-order chaotic system such as a 9D system to enhance the security level and robustness of the proposed HDOE algorithm.

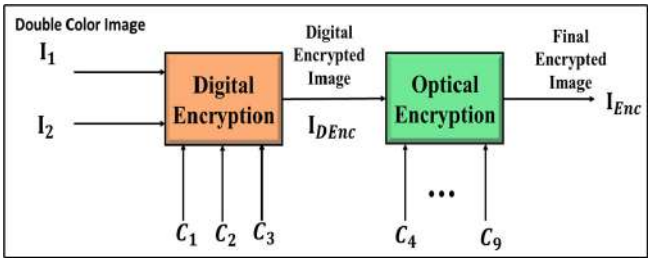


Fig. 2. A simplified block diagram of the proposed double-color image encryption scheme using hybrid digital/optical algorithms.

C.

Using deep learning DnCNN to reduce the noise level of the received encrypted images.

III. Proposed Double-Color Image Encryption/Decryption Scheme

This section describes a hybrid digital / optical encryption / decryption scheme for a double-color image (DCI). The scheme is based on a 9D chaotic system and assisted by DL for denoising the decrypted images. The proposed HDOE scheme uses a double chaotic phase encoding technique implemented in the Fourier transform domain. The contribution behind the design of the process is also reported.

A. Proposed Encryption Scheme

The proposed DCI scheme is based on an HDOE algorithm implemented with a 9D chaotic system. The scheme contains several steps, as shown in the following subsections. A simple block diagram of the DCI-HDOE scheme is shown in Fig. 2, and a detailed description of the system is given in Fig. 3. The encryption scheme consists mainly of cascading a digital encryption sub scheme (DEsS) controlled by three outputs of the chaotic system $(C_1, C_2,$ and $C_3)$ and an optical encryption subscheme (OEsS) controlled by the rest six outputs of the chaotic system $(C_4, ..., C_9)$. The two-color images are first applied to the DEsS to produce a single digital encrypted image I_{DEnc} which then passes through the OEsS to yield the final encrypted image I_{Enc}.

1) Nine-dimensional Chaotic System

In this work, two-color image encryption subschemes are designed, one for the digital domain and the other for the optical domain. The 9D chaotic dynamical system adopted to control the two subschemes is based on reference [26]. This system has two Lyapunov exponent (LE), which indicates the generation of hyper-chaotic dynamics. As a result, the system is suitable as the key generator of image encryption.

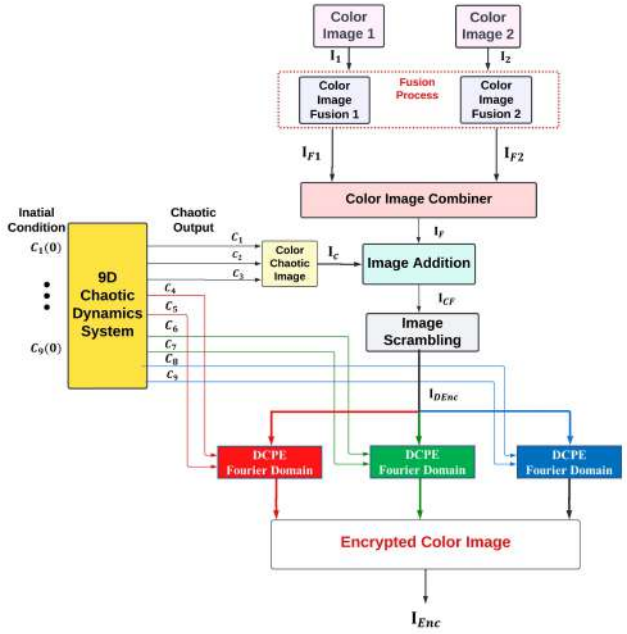


Fig. 3. Block diagram of the proposed DCI-HDOE scheme.

The chaotic dynamics is described by

$$
\begin{aligned}
C_1 &= \sigma b_1 C_1 - C_2 C_4 + b_4 C_4^2 + b_3 C_3 C_5 - \sigma b_2 C_7 \\
C_2 &= -\sigma C_2 + C_1 C_4 - C_2 C_5 + C_4 C_5 - \sigma C_9/2 \\
C_3 &= -\sigma b_1 C_3 + C_2 C_4 + b_4 C_2^2 - b_3 C_1 C_5 + \sigma b_2 C_8 \\
C_4 &= -\sigma C_4 - C_2 C_3 - C_2 C_5 + C_4 C_5 + \sigma C_9/2 \\
C_5 &= -\sigma b_5 C_5 + C_2^2/2 - C_4^2/2 \\
C_6 &= -b_6 C_6 + C_2 C_9 - C_4 C_9 \\
C_7 &= -b_1 C_7 - r C_1 + 2 C_5 C_8 - C_4 C_9 \\
C_8 &= -b_1 C_8 + r C_3 - 2 C_5 C_7 + C_2 C_9 \\
C_9 &= -C_9 - r C_2 + r C_4 - 2 C_2 C_6 + 2 C_4 C_6 + C_4 C_7 - C_2 C_8.
\end{aligned}
\tag{1}
$$

The control parameters σ, r, b_1, b_2, b_3, b_4, b_5 and b_6 are time-independent parameters used to control the chaotic dynamics. The phase space projections of the 9D attractor is shown in Fig. 4, assuming σ = 0.5, b_1 = 10/3, b_2 = 5/3, b_3 = 6/5, b_4 = 1/5, b_5 = 4/3, b_6 = 8/3 and r = 24.00 . The used initial conditions are $C_1(0)$ = 0.01, $C_2(0)$ = 0, $C_3(0)$ = 0.01, $C_4(0)$ = 0, $C_5(0)$ = 0, $C_6(0)$ = 0, $C_7(0)$ = 0, $C_8(0)$ = 0 and $C_9(0)$ = 0.1.

2) Digital Encryption Subscheme

Two-color images I_1 and I_2 each of size M×N is applied to this subscheme to yield a single-color encrypted image I_{DE}. M and N are the numbers of rows and columns, respectively, in each image's R, G, and B channels. The algorithm of DEsS consists of four steps: fusion process, image combining, XOR

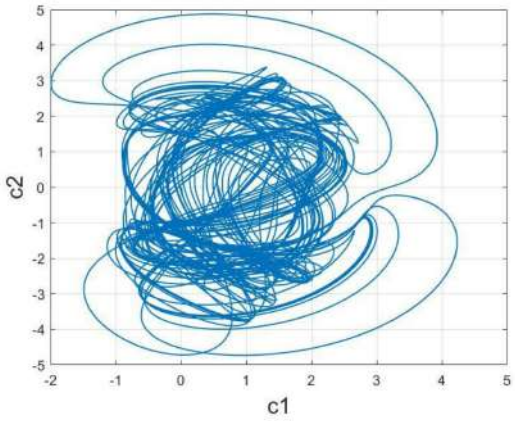


Fig. 4. Examples of the 9D-chaotic attractor for the $C_1 - C_2$ plane.

operation with RGB chaotic image, and scrambling. The procedures for these steps are as follows

i. A fusion process is applied to the input double-color image, yielding two new color images I_{F1} and I_{F2}. This method is adopted according to the amount of information carried by various binary bits of image pixels and reflects scrambling at the bit-slice levels. Fig. 5 shows the process of the fusion method used in this work.

ii. The image combiner gathers the two-color fusion images I_{F1} and I_{F2}, each of size M×N, one above the other, to produce a single fusion image I_F with a size of 2M×N.

iii. A chaotic color image I_C of size, 2M×N is constructed as an encryption key by three of the nine chaotic system outputs (C_1, C_2 and C_3, where each output is responsible for one of the RGB channels. The chaotic image I_C is XORing with the color fusion image I_F to get a chaotic fusion image I_{CF}. The chaotic gray images I_{CR}, I_{CG} and I_{CB}, corresponding to the RGB channels, are constructed based on the sequence C_1, C_2 and C_3, respectively. This is done after using integer sequencing according to (2)

$$\begin{aligned} I_{CR}(i) &= fix(mod(C_1(i)10^{15}, 255) \\ I_{CG}(i) &= fix(mod(C_2(i)10^{15}, 255) \\ I_{CB}(i) &= fix(mod(C_3(i)10^{15}, 255), \end{aligned} \tag{2}$$

where $fix(C)$ rounds each element of C to the nearest integer and $mod(a,m)$ returns the remainder after dividing a by m. Here, a and m represent the dividend and the divisor, respectively.

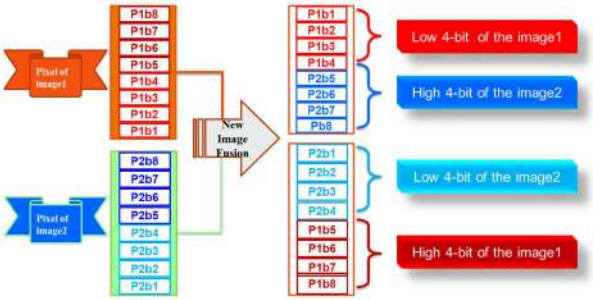


Fig. 5. Brief description of the fusion process.

iv. Finally, a random scrambling technique is applied to the image I_{CF} to produce the encrypted digital image I_{DEnc}. Note that the scrambler arranges the array pixels randomly without altering their values.

3) Optical Encryption Subscheme

The optical encryption subscheme is based on double chaotic phase encoding (DCPE) implemented in the 2D optical Fourier transform (FT) domain for each RGB channel of the received digital encrypted image, as shown in Fig. 6. Note that the 2D optical FT can be implemented using a single lens. The lens produces an FT image at the back focal plane for an image located at the front focal plane. For each color channel, the optical encryption (OE) consists of two cascaded FTs supported by two chaotic phase masks (CPMs). Each CPM is generated by one output of the chaotic system. One CMP is bonded with the primary image, and another is placed in the Fourier domain, as shown in Fig. 7.

The mathematician framework describes the operation of DCPE-based FT encryption, which can be adopted from after replacing the DRPE with double chaotic phase masks (DCPMs). Consider the red channel as an example; the CPMs can be explained as follow [27]

$$C_{PM1\_R}(x,y) = exp(j\phi_1(x,y)) = exp(j2\pi C_4(x,y)), \tag{3}$$

$$C_{PM2\_R}(x,y) = exp(j\phi_2(x,y)) = exp(j2\pi C_5(x,y)), \tag{4}$$

where C_4 and C_5 are the fourth and fifth chaotic. The same operations are applied to green and blue channels. The first step is to bound the input image whose electric field E_{in} with C_{PM1}, the combined function is FT, leading to An electric field $E_1(u,v)$

$$\begin{aligned} E_1(u,v) &= FT[E_{in}(x,y)C_{PM1\_R}(x,y)] \\ &= \iint [E_{in}(x,y)epx(2\pi jC_{CPM1\_R}(x,y)) \\ &\quad exp(-2\pi j(ux+uv))]dxdy \end{aligned} \tag{5}$$

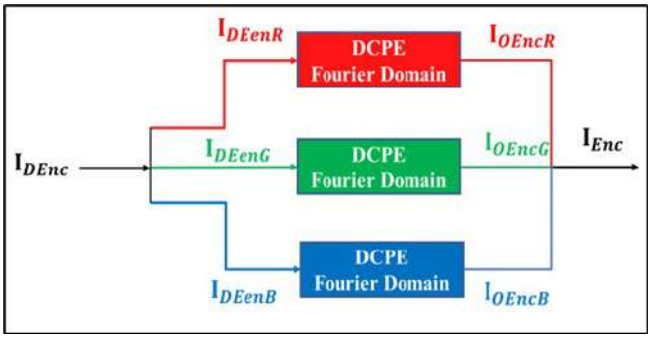


Fig. 6. Optical encryption process.

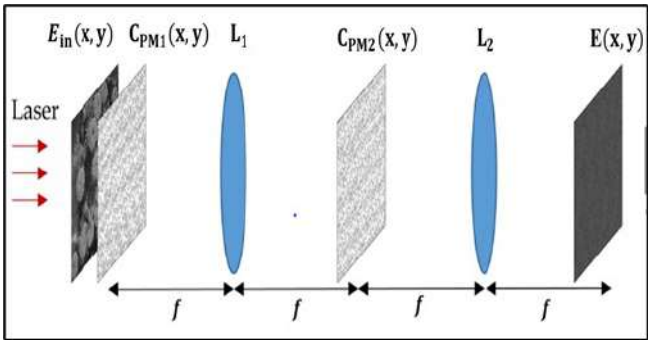


Fig. 7. Schematic diagram of the DCPE-based encryption scheme.

Here, (x,y) and (u,v) represent the image plane and Fourier plane coordinates, respectively. The second step is to bound the obtained Fourier spectrum with a statistically independent C_{PM2}, $exp(2\pi jC_{PM2})$, and retrieve the resulting spectrum once more FT

$$\begin{aligned} E(x,y) &= FT[E_1(u,v)C_{PM2\_R}(u,v)] \\ &= \iint [E_1(u,v)exp(2\pi jC_{CPM2\_R}(u,v)) \\ &\quad exp(-2\pi j(ux+uv))]dudv \end{aligned} \tag{6}$$

where $E(x,y)$ is the field of the final encryption image.

B. Proposed Decryption Scheme

Decryption is the inverse process of encryption and its aim is to recover the input images from the encrypted image. Fig. 8 shows a block diagram of the proposed hybrid digital / optical decryption (HDOD) scheme. The encryption and decryption keys are identical, and the chaotic sequence generated during decryption is consistent with that generated during encryption.

C. Denoising Convolution Neural Network

A quick and efficient denoiser convolution neural network (DnCNN) based on the DL principle is used in this work to address the issue that encrypted images are susceptible to some assaults in real applications. The resolution of the reconstructed images is increased by applying CNN, which also increases the algorithm's security robustness. The structure of DnCNN consists of an input image layer with a patch size (50) and four "convolutional layers + ReLU"; for each one of the first three layers, 64 filters (kernels) of size 3x3 are used to generate 64 feature maps. Each layer produces a feature map except the fourth layer, which does not have a ReLU but a stride = one and a "Regression layer." The zero padding is implemented to ensure that the feature map and input image have the same size. In order to distinguish the difference between a noisy and a clean image, the DnCNN is used in our system. Fig. 9 illustrates the architecture of the used DnCNN.

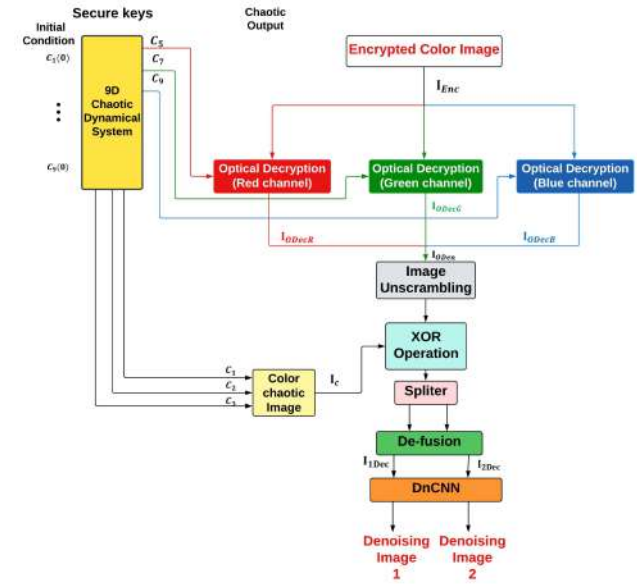


Fig. 8. Block diagram for hybrid optical / digital decryption scheme.

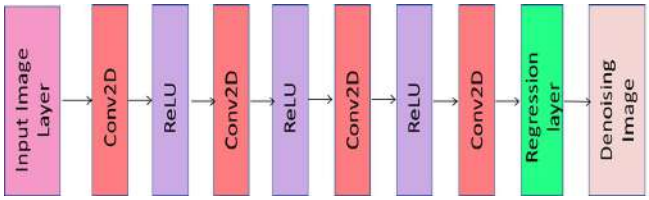


Fig. 9. Architecture of the DnCNN.

IV. Simulation Results

This section presents simulation results for the proposed encryption / decryption algorithms described in Section III. The performance is evaluated using conventional encryption qual-

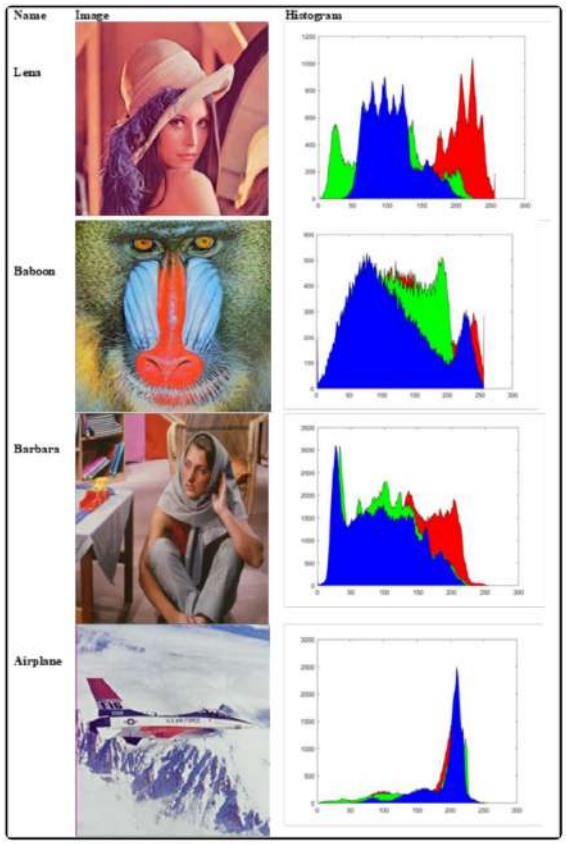


Fig. 10. The original color images and their histograms.

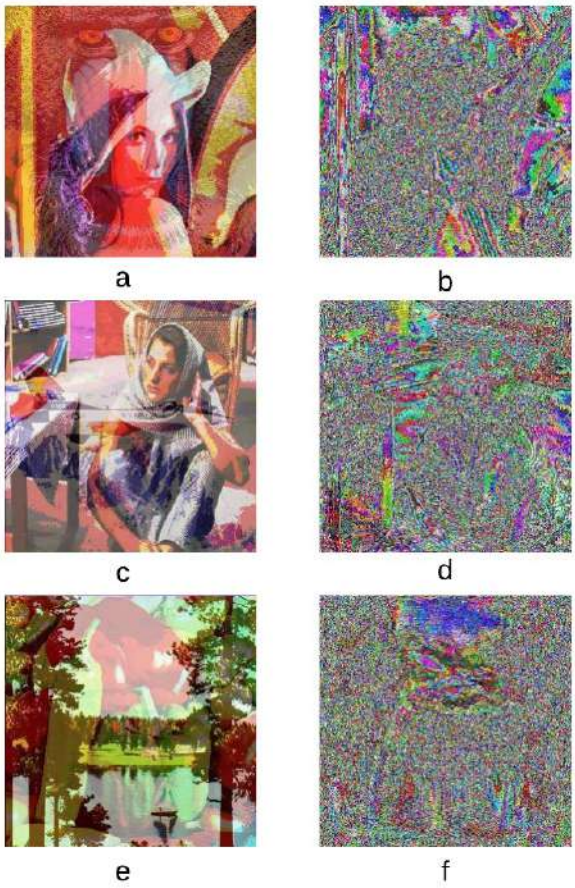


Fig. 11. Resultant fusion images correspond to the input double-color image. (a), (c), and (e) high-bit image I_{F1} , (b), (d), and (f) low-bit image I_{F2}.

ity measuring techniques. In this work, six color images are used for testing: Lena, baboon, airplane, Barbara, peppers, and sailboat, each of dimensions 256×256, are used as the input for the proposed HDOE scheme. Fig. 10 shows the input images and their histograms. For space limitation, most of the results are reported for the double image of Lena and Baboon.

A. Digital Encryption Results

1) Fusion Process Resul

The two-color images are applied to the fusion process, which is the first step of DEsS, and the obtained images at different points are given in Fig. 11. Parts a and b of this figure show the resultant high-bit and low-bit fusion images I_{F1} and I_{F2} for Leana and baboon. Parts (c and d) and (e and f) present the results corresponding to (Barbara and airplane) and (sailboat and peppers), respectively.

2) Color Images Combiner Results

The image combiner gathers the two fusion images Lena and Baboon I_{F1} and I_{F2}, each of size 256×256, one above the other to produce a single image I_F with a size of 512×256. The same process is applied for other images. Fig. 12 shows the results of the combiner output image.

3) Chaotic Fusion Image Results

Fig.13 displays the results describing the XOR operation of the generated chaotic image I_C with the color fusion image I_F to get a chaotic fusion image I_{CF}.

4) Scrambling Image Results

A random scrambling operation is applied to the chaotic fusion image I_{CF} and the result is given in Fig. 14, corresponding to the Lena-baboon case.

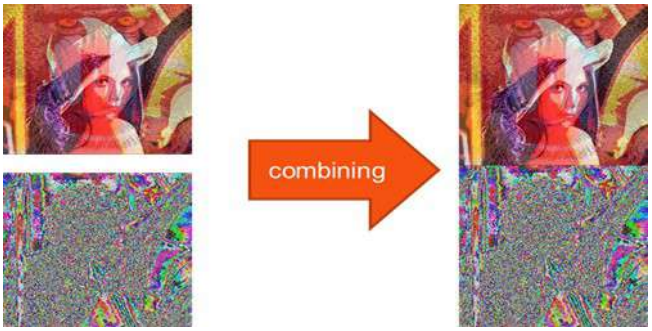


Fig. 12. Images corresponding to the generation of the combined fusion image in the DEsS.

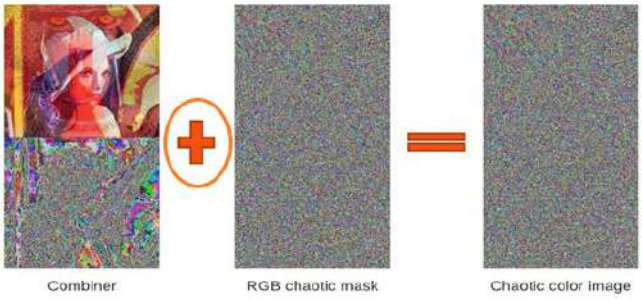


Fig. 13. XOR operation fusion images with RGB chaotic image.

B. Optical Encryption Results

The simulation results of the OEsS are displayed in Fig. 15. The scrambled image (part (a) of this figure) is used as the input of this OEsS. The cipher images after optical mask1, after optical mask2, and the final result I_{Enc} are presented in parts (b) to (d) of this figure, respectively. The output of the HDOE scheme describes the final cipher image, which will be applied to the security evaluation tester later in this subsection.

C. Decryption Results

The decryption algorithm is processed as done in the encryption algorithm but in reverse order. The decryption scheme consists of an optical decryption subscheme (ODsS) followed by a digital decryption subscheme (DDsS). Fig. 16 presents the results related to the final stage of the decryption process, namely the DDsS. Parts a-d of the figure shows the unscrambled, de-fusion, and decrypted images, respectively.

V. Performance Evaluation Metrics For The HDOE Scheme

A security analysis is provided to evaluate the algorithm's performance. The test images used to assess the efficiency and security level are given in Fig. 10.

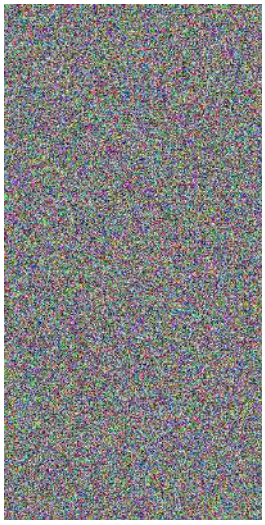


Fig. 14. Scrambled image I_{DEnc}.

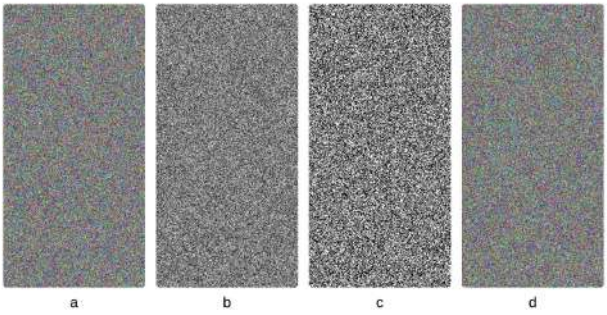


Fig. 15. Optical encryption results (Lena and Baboon). (a) scrambled image, (b) cipher image after optical mask1, (c) cipher image after optical mask2, (d) final cipher image.

A. Information Entropy

The performance of the proposed HDOE scheme is tested through entropy measures. The entropy for the three-color channels of the final optical encrypted color images I_{Enc} are presented in Table I. The values in this table are very close to 8, which corresponds to the entropy of an ideal encryption; $log_2 256 = 8$.

B. Histogram Analysis

The histograms of the encrypted images corresponding to the images of Lena-baboon, Barbara-airplane, and sailboat-peppers are shown in Fig. 17. It can be seen that the histogram of the encrypted image is quite uniform and significantly dissimilar to the histogram of the plaintext image. This prevents an attacker from learning anything about the plain image from its encrypted version. Note that the histograms of the decrypted images match that of the original input images given

Fig. 16. Results of the decrypted subscheme. (a) unscrambled image, (b) de-fusion image, (c) decrypted Lena, (d) decrypted baboon images.

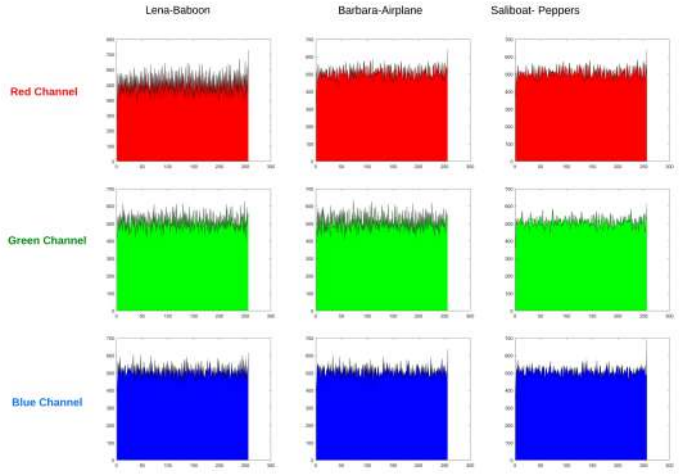


Fig. 17. Histograms of the RGB encrypted images.

TABLE I.
ENTROPY FOR VARIOUS COLOR IMAGES IN THE THREE COLOR CHANNELS USED IN THE HDOE SCHEME.

Entropy			
RGB Channels	Lena-Baboon	Barbara-Airplane	Sailboat-Peppers
Red	7.9987	7.9978	7.9982
Green	7.9984	7.9971	7.9975
Blue	7.9986	7.9976	7.9961

in Fig. 10, as shown in Fig. 18.

C. Correlation Coefficient Analysis

A correlation coefficient measures the similarity or dissimilarity between adjacent image pixels along the vertical, horizontal, and diagonal directions. The correlation coefficient's value falls between -1 and 1, with -1 denoting a negative correlation, +1 a positive correlation, and 0 denoting no correlation. In order to withstand statistical attacks, the encrypted image must have a correlation coefficient between neighboring pixels nearly equal to zero in all directions. The results are depicted in Figs. 19 and 20, which present the three-channel correlation coefficients for the original images of Lena and Baboon, respectively. As can be observed, the adjacent pixels in the three directions (horizontal (HD), vertical (VD), and diagonal (DD)) have a linear correlation characteristic. This is in contrast to the correlation characteristics of the encrypted images Lena-baboon as displayed in Fig. 21. Table II lists the three-direction correlation coefficient for the used original images. The encrypted image's horizontal, vertical, and diagonal correlation coefficients are also given in Table III. Investigation of these results reveals that the encrypted images' correlation coefficients are almost zero. This highlights the effectiveness of the encryption process adopted in this work.

D. Noise Attack Analysis

During transmission, noise significantly impacts the quality of the encrypted image. The results show that the noise attack with various noise levels on the encrypted image yields decrypted images that still maintain noise resistance and image retrieval well. This is illustrated in Fig. 22 where the decrypted images of Lena, Baboon, sailboat, and peppers are displayed when the corresponding encrypted images are affected by a Gaussian noise of standard deviation σ. The results are presented for σ = 0.5, 5, 10, 15, and 20 in columns a-e, respectively. The results show that the proposed scheme resists noise attacks.

E. Cropping Attack Analysis

To test the effectiveness of the proposed method against cropping attacks, one can examine the performance of the encrypted image after the cropped with various formats, as shown in Fig. 23. Parts a-d of this figure show the encrypted image cropped with size 32×32 from the upper left, with size 64×64, with size 128×128 from the upper left, and with size 128×128 from the middle image right, respectively. The decrypted versions of the corresponding images are displayed in parts (e)-(l) of the figure and show that the deciphered images are still recognizable and keep the majority of the original visual information. This indicates that the proposed method of encryption is resistant to occlusion attacks.

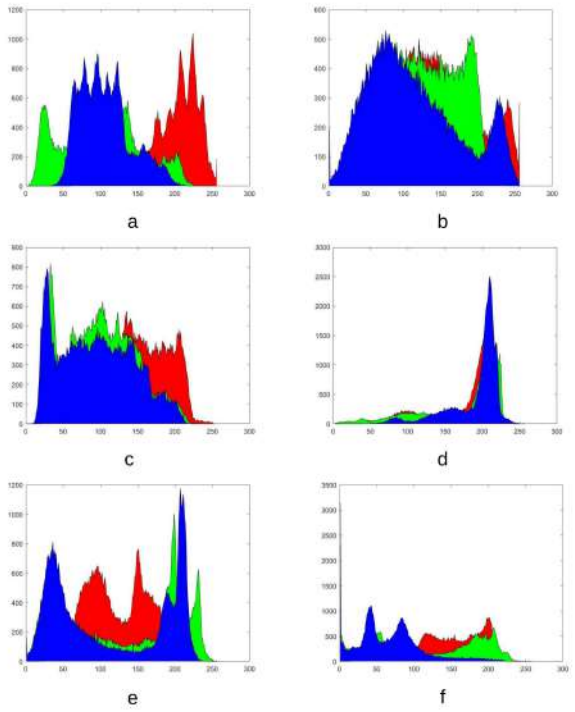


Fig. 18. Histograms of the decrypted images (a) Lena (b) baboon (c) Barbara (d) airplane (e) sailboat and (f) peppers.

F. Key Sensitivity Analysis

The sensitivity of the encryption process to the initial conditions of the chaotic parameters used to generate the chaotic phase masks are examined here. Lena and baboon images are used as examples to test the sensitivity to the initial conditions of the key. As depicted in Fig. 24 even if a tiny deviation is made for one of the deciphering key parameters (chaotic initial condition), the decryption process fails. This indicates that the key of the proposed technique is extremely sensitive. Investigation of the results also indicate that the maximum allowable variation in the initial condition value to yield successful decryption is 10^{-17}.

G. Key Space Analysis

A key space analysis is performed to determine the number of distinct keys that can be used in the encryption procedure. The proposed image encryption scheme assumes that the transmitter and receiver share the secret keys and variables via a secure channel. seventeen keys are involved here: $\alpha, r, b_1, b_2, b_3, b_4, b_5, b_6, C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8$, and C_9. Because the calculation precision of the double precision number is 10^{-16}, the key space of the algorithm will be more than $(10^{16})^{17} = 2^{903} > 2^{100}$ which is sufficiently large to resist all types of brute force attacks.

TABLE II.
THREE-DIRECTION CORRELATION COEFFICIENTS FOR VARIOUS ORIGINAL COLOR IMAGES.

Images	Channel	VD	HD	DD
Lena	Red	0.9477	0.9733	0.9259
	Green	0.9474	0.9736	0.9270
	Blue	0.9078	0.9486	0.8360
Baboon	Red	0.8360	0.7723	0.7765
	Green	0.7523	0.6643	0.6604
	Blue	0.8498	0.8007	0.7937
Barbara	Red	0.9423	0.9736	0.9239
	Green	0.9295	0.9681	0.9072
	Blue	0.9417	0.9738	0.9234
Airplane	Red	0.8906	0.8832	0.8180
	Green	0.9099	0.9035	0.8497
	Blue	0.8464	0.8237	0.7500
Sailboat	Red	0.8773	0.8654	0.8188
	Green	0.9404	0.9379	0.9072
	Blue	0.9426	0.9428	0.9137
Peppers	Red	0.9350	0.9394	0.8987
	Green	0.9642	0.9704	0.9425
	Blue	0.9292	0.9381	0.8919

H. DnCNN Results

A four-layer DnCNN is designed in this work. Fig. 25 shows the root mean square error (RMSE) and loss function curve for training using a dataset of 931 images dataset. After 37240 iterations, the RMSE decreases significantly and somewhat settles between 1% and 2% RMSE values. While there is a decrease in the curve of the loss function with respect to the number of iterations, which is about 0.4. This means that the proposed DnCNN structure does well despite the insufficient data set, and there is no overfitting in the training process. The PSNR measurement is used for the validation of this design. Table IV illustrates the PSNR values before and after

TABLE III.
CORRELATION COEFFICIENTS IN THE THREE DIRECTIONS FOR VARIOUS COLOR-ENCRYPTED IMAGES.

Images	Channels	VD	HD	DD
Lena-Baboon	Red	-0.0012	-0.0013	-0.0002
	Green	0.0018	-0.0004	0.0020
	Blue	0.0010	-0.0000	0.0005
Barbara-Airplane	Red	0.0032	0.0038	-0.0019
	Green	-0.0052	0.0029	-0.0013
	Blue	0.0004	-0.0024	0.0047
Sailboat-Peppers	Red	-0.0041	0.0053	-0.0013
	Green	0.0004	-0.0013	-0.0000
	Blue	-0.0011	0.0093	-0.0017

TABLE IV.
PSNR VALUE BEFORE AND AFTER APPLIED DNCNN WITH DIFFERENT STANDARD DEVIATION σ OF GAUSSIAN NOISE.

Name of Images	Before DnCNN				
	$\sigma = 0.5$	$\sigma = 5$	$\sigma = 10$	$\sigma = 15$	$\sigma = 20$
Lena	27.01	17.28	15.17	13.91	13.04
Baboon	23.80	15.06	12.97	11.83	11.12
Barbara	26.97	17.37	15.25	13.98	13.17
Airplane	23.95	14.57	12.25	11.22	10.55
Sailboat	27.05	17.24	14.93	13.63	12.74
Peppers	23.67	14.54	12.36	11.27	10.54
After DnCNN					
Lena	32.56	23.72	21.34	19.62	18.48
Baboon	21.86	19.51	17.88	16.79	16.02
Barbara	27.91	23.25	21.32	19.90	18.90
Airplane	28.13	21.80	17.96	16.17	15.01
Sailboat	27.65	22.82	20.76	19.15	17.87
Peppers	29.24	20.64	17.16	16.11	15.19

denoising by DnCNN for noisy images with different values of standard deviation σ. MATLAB R2021b is used to train the denoising model. Fig. 26 shows examples of original peppers images, noisy, and denoised image for different noise values. The parameter values of the training options are as follows.

i. The learning rate is 110^{-4}**.**

ii. The training network sets initial weights.

iii. The number of epochs is 10 for the trained model.

VI. COMPARATION WITH RELATED WORK

This section gives a brief comparison of encryption measures obtained by using the proposed encryption scheme with that reported in related work. The three measures used for comparison are entropy, encryption key sensitivity, and key space. For entropy comparison, the results of this work are compared with that of Refs. [2, 5, 15, 28].The comparison results are listed in Table V along with brief description parameters of the used encryption scheme. Investigation of the results of this table reveals that the proposed scheme in this work offers an entropy that is nearest to the ideal case (entropy = 8) compared with other references.
The proposed scheme offers 10^{-17} key sensitivity and 2^{903} key space. These results indicate that the proposed scheme has higher key sensitivity and a much higher key space dimension.

TABLE V.
COMPARISON OF ENTROPY WITH RELATED WORK FOR DOUBLE AND MULTIPLE IMAGES.

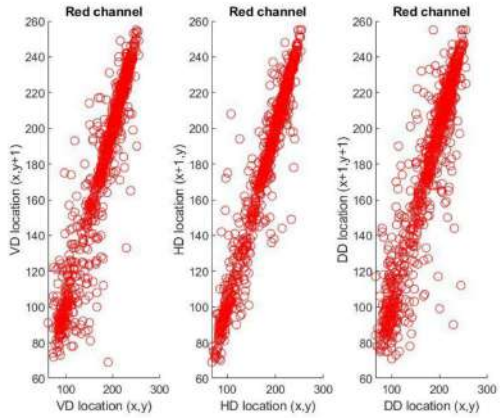
Ref.	Encryption Scheme	No. of Image	Chaotic System	Entropy
[15]	Hybrid	Gray-double	5D	7.9991
[5]	Optical	Color-single	2D-Logisic Map	R-7.7358 G-7.6303 B- 7.5681
[28]	Digital	Color-single	Hyperchaotic	R-7.9974 G-7.9971 B-7.9973
[2]	optical	Color-single	Memristive chaos	R-7.9900 G-7.9969 B-7.9972
This Work	Hybrid	Color-multiple	9D	R-7.9991 G-7.9987 B-7.9991

VII. CONCLUSIONS

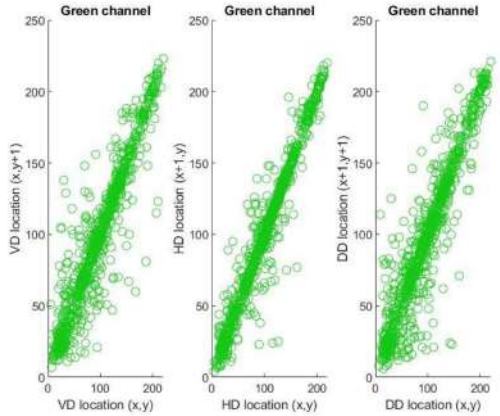
A 9D chaotic-based hybrid digital / optical encryption scheme has been proposed for double-color images. Each of the three chaotic sequences has been used to control the encryption of one of the RGB channels without affecting the other channels. One chaotic sequence controls the channel's fusion, XOR, and scrambling-based digital encryption part. The other two chaotic sequences have been used to construct two chaotic phase masks implemented in the optical FT-based encryption part. A deep learning technique has been used to reduce the effect of Gaussian noise embedded in the received encrypted images. The simulation tests reveal that using a 9D chaotic system to control the operation of the HDOE scheme, with each three sequences, are responsible for one of the RGB channels, increases the security level and robustness of the encryption. The scheme offers 7.9989 entropy for the encrypted color images and an infinite PSNR for the decrypted images. The encryption algorithm successfully resists different attacks, such as noise and cropping attacks. Further, The designed DnCNN operates efficiently with the proposed encryption scheme yielding performance enhancement of the decrypted images against Gaussian noise. The next step in this work is to modify the scheme to deal with more than two color images by adopting compressive sensing techniques.

CONFLICT OF INTEREST

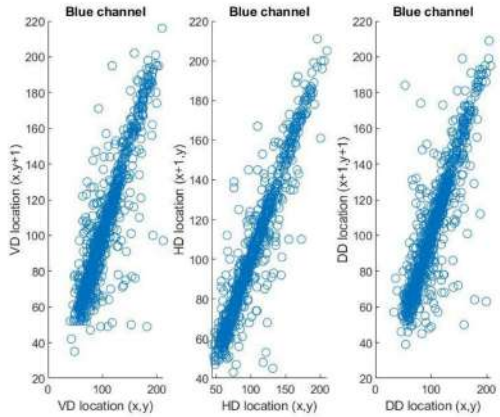
The authors have no conflict of relevant interest to this article.



(a)

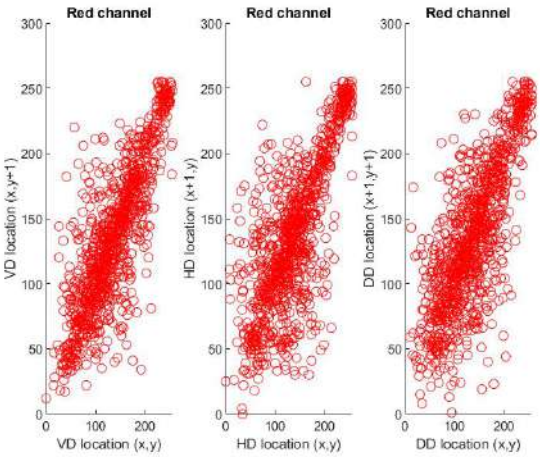


(b)

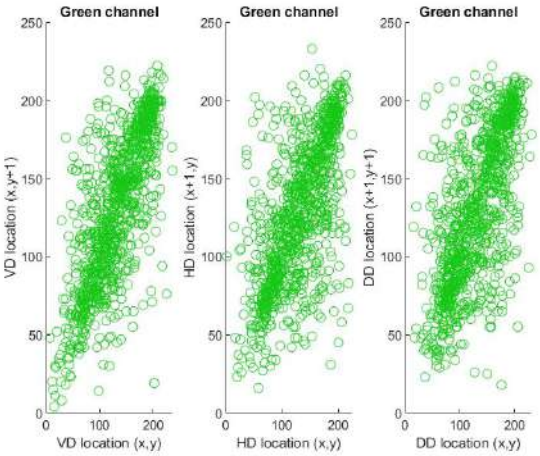


(c)

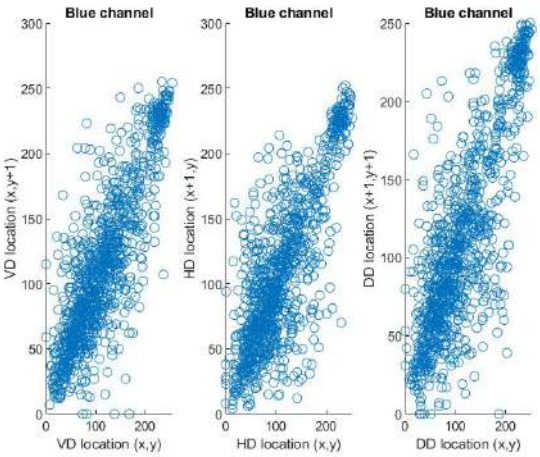
Fig. 19. Correlation coefficient diagram of the original Lena image (a) red channel, (b) green channel, and (c) blue channel.



(a)

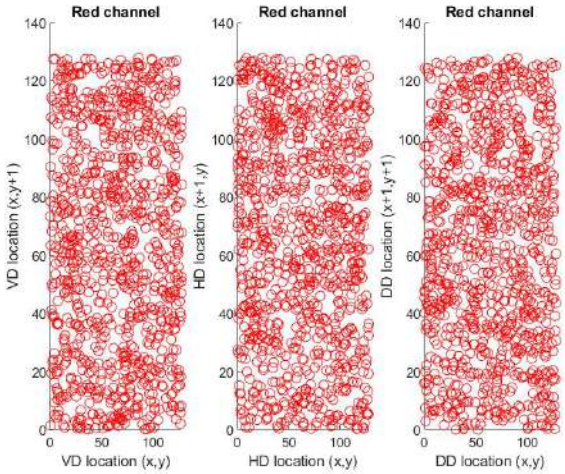


(b)

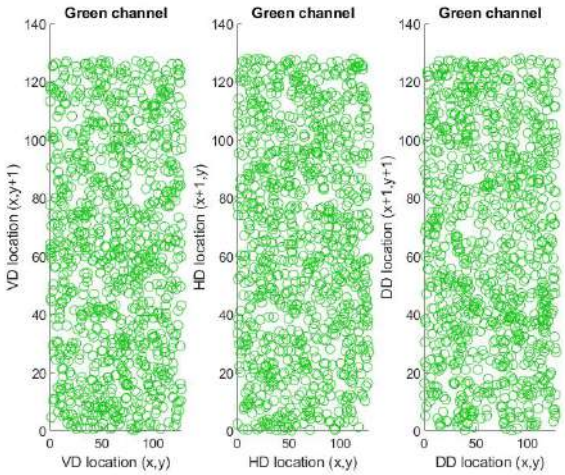


(c)

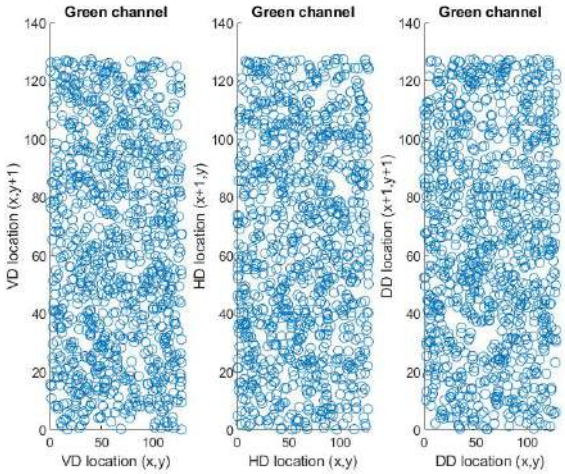
Fig. 20. Correlation coefficient diagram of the original baboon image (a) red channel, (b) green channel, and (c) blue channel.



(a)



(b)



(c)

Fig. 21. Correlation coefficient diagram of the encrypted Lena-baboon images (a) red channel, (b) green channel, and (c) blue channel.

Fig. 22. Decrypted images with different standard deviation values of Gaussian noise. (a) $\sigma = 0.5$, (b) $\sigma = 5$, (c) $\sigma = 10$, (d) $\sigma = 15$ and (e) $\sigma = 20$.

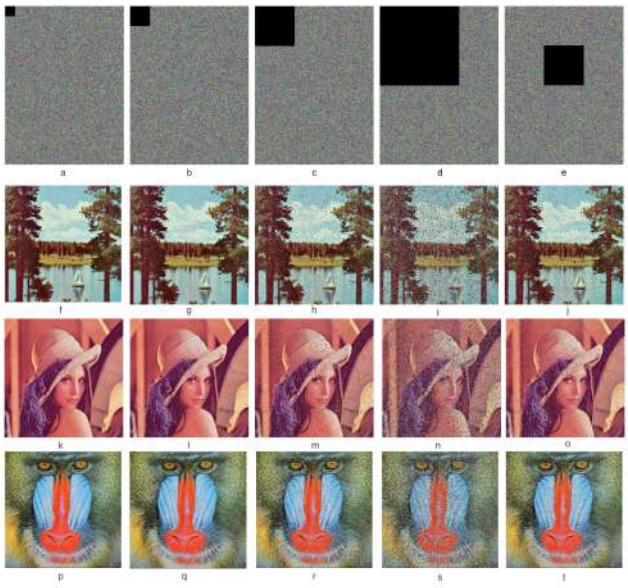


Fig. 23. Experimental results of the cropping attack: first row shows (a-d) cropped images and the remaining rows show corresponding decrypted images.

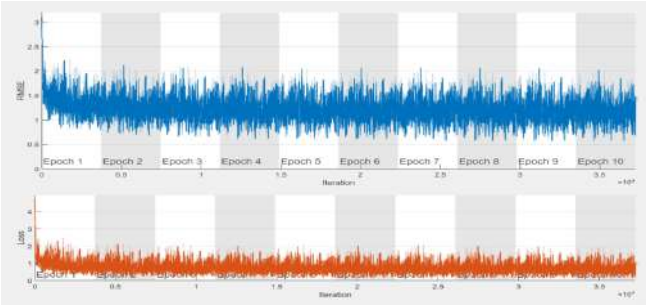


Fig. 25. Training progress of the DnCNN.

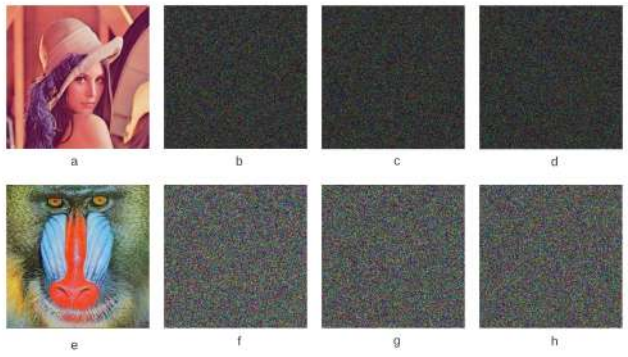


Fig. 24. Key sensitivity. (a) Decrypted Lena image with the correct key, (b) Decrypted image using $C_1(0) = 0.01 + 10^{-17}$, (c) Decrypted image using $C_2(0) = 0 + 10^{-17}$, (d) Decrypted image using $C_3(0) = 0.01 + 10^{-17}$ (e) Decrypted baboon image with correct key (f)-(h) the same incorrect key that used in Lena image.

Fig. 26. Original, noisy, and denoised image for σ=5

REFERENCES

[1] M. Z. J. Wei and X. Tong, "Multi-image compression–encryption algorithm based on compressed sensing and optical encryption," *Entropy*, vol. 24, no. 784, pp. 1–22, 2022.

[2] C. Z. H. Wen and et al, "Secure optical image communication using double random transformation and memristive chaos," *IEEE Photonics Journal*, vol. 15, no. 1, pp. 1–11, 2023.

[3] G. S. Yadav, "A genetic algorithm based image steganography scheme with high embedding capacity and low distortion," *Imaging Science Journal*, vol. 69, no. 4, pp. 143–152, 2023.

[4] Z. A. Abduljabbar and et al, "Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022.

[5] O. S. Faragallah and et al, "Efficient and secure optocryptosystem for color images using 2d logistic-based fractional fourier transform," *Optics and Lasers in Engineering*, vol. 137, no. 106333, pp. 1–15, 2021.

[6] I. Khalid and et al, "An integrated image encryption scheme based on elliptic curve," *IEEE Access*, vol. 11, p. 5483–5501, 2022.

[7] S. S. Yu and et al, "Optical image encryption algorithm based on phase-truncated short-time fractional fourier transform and hyper-chaotic system," *Optics and Lasers in Engineering*, vol. 124, no. 105816, pp. 1–11, 2020.

[8] A. Hazer and R. Yildirim, "A review of single and multiple optical image encryption techniques," *Journal of Optics (United Kingdom)*, vol. 23, no. 113501, pp. 1–93, 2021.

[9] M. Rezai and J. A. Salehi, "Fundamentals of quantum fourier optics," *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1–22, 2022.

[10] Q. Zhou and et al, "Optical image encryption based on two-channel detection and deep learning," *Optics and Lasers in Engineering*, vol. 162, no. 107415, 2022.

[11] Y. Zhao and et al, "High-precision calibration of phase-only spatial light modulators," *IEEE Photonics Journal*, vol. 14, no. 7402508, pp. 1–8, 2022.

[12] M. W. W. Zhou, X. Wang and D. Li, "A new combination chaotic system and its application in a new bit-level image encryption scheme," *Optics and Lasers in Engineering*, vol. 149, no. 106782, 2022.

[13] O. S. Faragallah and et al, "Secure color image cryptosystem based on chaotic logistic in the frft domain," *Multimedia Tools and Applications*, vol. 79, no. 3-4, p. 2495–2519, 2020.

[14] A. B. J. D. Kumar and V. N. Mishra, "Optical and digital double color-image encryption algorithm using 3d chaotic map and 2d-multiple parameter fractional discrete cosine transform," *Results in Optics*, vol. 1, no. 100031, p. 1–16, 2020.

[15] Z. Man and et al, "Double image encryption algorithm based on neural network and chaos," *Chaos, Solitons and Fractals*, vol. 152, no. 111318, pp. 1–16, 2021.

[16] P. Tian and R. Su, "A novel virtual optical image encryption scheme created by combining chaotic s-box with double random phase encoding," *Sensors*, vol. 22, no. 5325, p. 1–24, 2022.

[17] M. R. Abuturab and A. Alfalou, "Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional fourier transform," *Optics and Laser Technology*, vol. 151, no. 108071, pp. 1–13, 2022.

[18] K. Ahmadi and A. Carnicer, "Optical visual encryption using focused beams and convolutional neural networks," *Optics and Lasers in Engineering*, vol. 161, no. 107321, 2023.

[19] K. C. A. K. Singh and A. Singh, "An image security model based on chaos and dna cryptography for iiot images," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, p. 1957–1964, 2022.

[20] D. Huo and et al, "Multiple-image encryption scheme via compressive sensing and orthogonal encoding based on double random phase encoding," *Journal of Modern Optics*, vol. 65, no. 18, p. 2093–2102, 2018.

[21] X. W. L. J. Chen and Q. H. Wang, "Deep learning for improving the robustness of image encryption," *IEEE Access*, vol. 7, p. 181083–181091, 2019.

[22] M. Liao and et al, "Deep-learning-based ciphertext-only attack on optical double random phase encryption," *Opto-Electronic Advances*, vol. 4, no. 5, p. 1–12, 2021.

[23] J. W. R. Ni, F. Wang and Y. Hu, "Multi-image encryption based on compressed sensing and deep learning in optical gyrator domain," *IEEE Photonics Journal*, vol. 13, no. 3076480, p. 1–16, 2021.

[24] R. Zhang and D. Xiao, "Double image encryption scheme based on compressive sensing and double random phase encoding," *Mathematics*, vol. 10, no. 8, p. 1–23, 2022.

[25] Q. Zhang and J. Li, "Single exposure phase-only optical image encryption and hiding method via deep learning," *IEEE Photonics Journal*, vol. 14, no. 7813508, p. 1–8, 2022.

[26] P. Reiterer and et al, "A nine-dimensional lorenz system to study high-dimensional chaos," *Journal of Physics A: Mathematical and General*, vol. 31, no. 34, pp. 7121–7139, 1998.

[27] N. K. Nishchal, *Optical cryptosystems*. IOP Publishing, 2019.

[28] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, pp. 26203–26222, 2019.