Received January 6, 2021, accepted January 27, 2021, date of publication January 29, 2021, date of current version February 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055738

Secure Opto-Audio Cryptosystem Using XORing Mask and Hartley Transform

OSAMA S. FARAGALLAH[1] **AND HALA S. EL-SAYED**[2]
[1]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 21944, Saudi Arabia
[2]Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom 32511, Egypt

Corresponding author: Osama S. Faragallah (o.salah@tu.edu.sa)

This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/08), Taif University, Taif, Saudi Arabia.

ABSTRACT This research paper proposes a secure opto-audio cryptosystem using XORing mask and Hartley transform (HT). The digital one dimensional (1D) plainaudio data is converted into two dimensional plainaudio map (2D PAM) and after that, the 2D PAM is divided into 2D plainaudio blocks (2D PABs). The basic idea of the proposed opto-audio encryption system depends on XORing each block of the 2D PABs with a single image selected from a personal image database that can be viewed as a secret key in the proposed opto-audio cryptosystem. Each block of the mixed 2D PABs is then transposed using the chaotic logistic adjusted sine map (LASM) and optically encrypted with HT. The XOR and LASM are implemented digitally while HT implemented optically. An additional XORing mask step helps to remove residual intelligibility from the 2D PABs, fill in speechless gaps in spoken conversations, and destroy both the pitch and format details. The utilization of chaotic LASM allows efficient noise immunity. A comparative study is held between the proposed opto-audio encryption system and other related audio encryption systems in terms the standard well known encryption metrics. The results have confirmed the efficiency of the introduced opto-audio encryption system. The proposed opto-audio encryption system security is explored from an accurate encryption point of view, and tests confirmed the superiority of the proposed opto-audio encryption system from the encryption point of view.

INDEX TERMS Optical encryption, DRPE, hartley transform.

I. INTRODUCTION

Due to the fast evolution of recent telecommunication systems, the field of information security has raised a lot of serious challenges. Multimedia cryptosystems make use of various mathematical tools and techniques with the potential of modifying both statistical and perceptual properties of multimedia file to look like random [1]–[7]. Such techniques may be classified into optical, chaotic and hybrid chaotic-optical techniques.

With respect to the optical domain, optical information security schemes attract a lot interests and become increasingly very important due to their distinct merits like arbitrary parameter selection and handling 2D complex data in parallel at high computational speed [8]. So, it has been concluded that the optical information processing concept will result an efficient data encryption methodology [9], [10]. Optical audio cryptosystem techniques are employed using Fourier transforms, fractional Fourier transforms and random phase encoding. [9]–[11]. The double random phase encoding (DRPE) optical ciphering has become a significant topic in optical information security field since introduced by Refregier and Javidi in 1995 [12]. The DRPE is considered as a well-known optical encryption technique which relays on the 4-F optical correlator for encrypting a plainimage as a stationary white noise cipherimage. The random phase masks serve as ciphering keys are employed in image/Fourier planes. Since then, several optical image cryptosystems have been considered like holography [13], optical transforms [1]–[5], [8]–[15], and interference [18]. In [19], the authors present a virtual optics scheme to encrypt digital audio using the virtual optical scheme parameters. This scheme is based on position sensitivity and virtual wavelength of discrete Fresnel diffraction in addition to the complex valued random coverage mask. In [20], the authors present a digital holography (DH)-based optical voice encryption scheme. The hologram, containing audio information is optically encrypted using Fourier transform (FT)-based DRPE. The DH decryption can reconstruct the plainaudio using the correct parameters. The scheme is proved to an efficient potential security

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

tool for voice and useful for other security applications. In [21], the authors present an optical voice encryption that employs DRPE in different optical domains like fractional Fourier, Fresnel, and gyrator transforms. An optical setup using off-axis digital hologram is applied for recording the holograms time-series representing the audio wave. After that, the DRPE in different transforms is applied for encrypting audio information. It is noted that employing DRPE with different domains improves the security level. In [22], the authors present an audio cryptosystem using the cosine number transform (CNT). The CNT is recursively employed to blocks of non-compressed digital audio samples. A secret key is utilized to determine the iteration numbers the transform is employed for each block. The proposed method is proved to be immune against chosen-plaintext, known-plaintext, and differential attacks.

With respect to chaotic domain, chaotic maps have high sensitive to initial conditions. So, they are commonly utilized in audio cryptosystems [23]. Encryption of audio can be employed using several ways and implemented to scenarios with manifold needs. In [24], the authors present audio encryption based on chaotic transposition and a multiplicative non-binary system. In [25], the authors utilize high dimensional chaotic map for improving the security and key space of iterative audio encryption scheme. In [26], an audio encryption package for TV cloud computing is presented. The encryption of audio is employed using chaotic and multiple keys with discrete transforms. In [40], the authors present a speech cryptography scheme based on 2D Zaslavsky and 2D Cat transforms. The speech signal is compressed using discrete cosine transform (DCT), and then hidden using random numbers generated from the 2D Zaslavsky map, and finally transformed using the 2D Cat map. The proposed method is proved to give larger key space, good SNR and more complex dynamical features proofed with good randomness. In [41], the authors present a lossless dual channel speech encryption using one time keys. The speech signal is handled using confusion and diffusion operations through applying chaotic system with modified multi scroll and one-time keys. The proposed method is proved to give good statistical properties and large key space that makes exhaustive key search impractical, good SNR and more complex dynamical features proofed with good randomness. The authors in [42] have introduced a design for stream cipher encryption using one-time keys and chaotic maps. The proposed stream encryption uses the piecewise linear chaotic mapping for generating a pseudo random key stream sequence. The scheme is applied for color images and the test results confirm its sufficient security level. Also, it is demonstrated that the encrypted image is immune with respect to noise, and the scheme is sufficient for color image encryption applications. The authors in [43] have proposed a color image cipher based on bit-level transposition using piecewise linear chaotic map (PWLCM) and high dimension chaotic mapping using Chen system. Experiment tests of the proposed scheme demonstrated a good encryption result and enough large key space to be resistant against various attack types. The authors in [44] have introduced a proposal for a confusion/diffusion encryption scheme for grayscale images. The grayscale image rows and columns are transposed using the piecewise linear chaotic map (PWLCM)-based arrays. The grayscale image pixels are transformed into four nucleotides using the deoxyribonucleic acid (DNA). Experiment tests of the proposed scheme achieved a satisfactory encryption result and enough large key space to be resistant against various attack types. The authors in [45] have proposed an image cipher system using high-dimension Lorenz chaotic mapping and neural network perceptron model. The proposed method is analyzed and experimental tests demonstrated its strong security and resistance against various existing attacks.

The authors in [46] introduced a fast transposition-diffusion image encryption scheme combined with cyclic shift and sorting permutation. The proposed scheme can guarantee good transposition performance with low time and space complexity. Also, the scheme utilizes a parallel diffusion for achieving a qualitative efficiency enhancement compared to conventional diffusion schemes. The authors in [47] introduced a chaotic image encryption scheme using a matrix semi-tensor product (STP) with a complex secret key. The plainimage pixels are split four blocks at random. Then, the pixels of each block are processed using Arnold transform and the four blocks are mixed together to create the scrambled image. This is followed by designing a complex secret key. The STP is employed to both the scrambled image and chaotic sequences to get the encrypted image. The achieved results demonstrated that the proposal is secure and efficient compared to other encryption schemes. The authors in [48] introduced an image cipher using the chaotic technology, matrix semi-tensor product theorem, and a Boolean network. A random key stream is produced based on a two dimensional LASM. The Boolean network is encoded and the Boolean matrix is produced. After that, the plainimage is scrambled with the aid of three random position transposing and the encrypted image is generated using the matrix semi-tensor product theorem also, a new Boolean network may be produced through encoding the ciphered image. The experiment tests ensured that the scheme allows greater security features in comparison to other encryption schemes. The authors in [49] introduced a secure image cipher based on the fractal sorting matrix (FSM) and chaotic pixel diffusing with two chaotic sequences. The experimental comparisons confirmed that the proposed scheme is fast and provides a high pass rate of local Shannon. So, the scheme ensured grater security and immunity against several attacks.

With respect to chaotic-optical methods [1], [27], chaotic domain methods are mixed with optical domain methods. In [1], authors introduce a method to encrypt audio with a mixture of baker or cat maps and opto encryption. In [27], the authors transform the digital audio's data into 2D matrix digital audio termed the sound map (SM). Then the SM Arnold transformed and encrypted in optics using DRPE.

In [50], the authors present a speech encryption scheme using Collatz conjecture based variable-length encoding. The proposed method gives good entropy results and larger key space with higher key sensibility.

The 2D Hartley transform (2D HT) [26] corresponds arithmetically to a pair of Fourier transformations (FTs), and results in real valued. Both of 2D HT direct/inverse phases are correspondent. The 2D HT includes amplitude data, which spatially illuminated either incoherent or coherent and listed on intensity medium which is straightforward than the FT scheme [29]–[31].

In some applications like audio evidence in court and commercial secret talks, digital audio is required to be hidden and encrypted. The digital sound begins with sampling the input plain-sound in arranged discrete time intervals and followed by quantizing the sampled estimations into a discrete spaced levels number. The standard rate of sampling is 8-48 kHz [27]. The standard bits number/sample employed for digital sound is 8-16 bits. Digital sound may be considered like a digital data stream, it can be represented like 1D data matrix. The paper presents an efficient optical audio cryptosystem approach using XORing mask, LASM, and HT-based optical encryption. The audio is considered like a digital data stream and represented like 1D data matrix. Here, the 1D data matrix of digital plainaudio is converted into 2D data matrix of PAM termed as 2D PAM. the 2D PAM is divided into 2D PABs. The size of each block of 2D PABs is 4*4 byte. The XORing mask procedure is performed by XORing each block of the 2D PABs with a single image selected from a private database. The selected image can be considered as an extra key. Each block of mixed 2D PABs resulted from the XORing mask procedure is scrambled using LASM and optically encrypted with HT. Both of XOR and LSLM are implemented digitally while HT implemented optically. So, the proposed opto-audio cryptosystem has two stages; the confusion and diffusion stages. The confusion stage is performed using the chaotic LASM. The diffusion stage is performed in terms of XORing mask between each block of the 2D PABs and a single image selected from a personal image database and optical HT. At the destination, a HT-based optical deciphering procedure is followed by the inverse of LASM and the XORing mask procedures to extract the original 2D PABs.

The main advantages of proposed optical audio cryptosystem using XORing mask, LASM, and HT can be summarized as follows. Firstly, the XORing mask procedure achieves good diffusion and hence increases the security level. Secondly, the employment of the chaotic LASM as a pre-processing transposing phase gives the optical audio cryptosystem the advantage of the noise immunity. Thirdly, the 2D HT-based optical encryption provides and increases the proposed opto-audio cryptosystem physical security. Fourthly, the chosen image from the private image database can be considered as an extra secret key in conjunction to initial parameters of LASM and the main encoding keys of the 2D HT-based optical encryption. Finally, the 2D PABs do not provide any visual impact. Table 1 compares between the proposed opto-audio cryptosystem and other state-of-the-art methods [19]–[22], [26], [27], [40]–[45], [50].

The paper rest includes the following sections. Sect. II overviews and introduces the necessary preliminaries regarding the LASM and the 2D HT. Sect. III explains in details of the proposed opto-audio cryptosystem. Sect. IV presents the test results. Sect. V presents a comparison study between the proposed opto-audio cryptosystem and the related state-of-the-art methods. Conclusions are given in Sect. VI.

II. PRELIMINARIES

A. LOGISTIC-ADJUSTED-SINE MAP (LASM)

A Logistic adjusted Sine map (LASM) is a 2D chaotic map which is used to scramble the pixels in the 2D PABs. It is expressed as follows [26]:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} \sin\left[\pi\mu(y_i+3)x_i(1-x_i)\right] \\ \sin\left[\pi\mu(x_{i+1}+3)y_i(1-y_i)\right] \end{bmatrix} \quad (1)$$

where $\mu \in [0, 1]$. The LASM is a combination between Sine and Logistic maps. First, the logistic formula $x_i(1-x_i)$ is multiplied by μ then it is inserted into the Sine map. After that, the phase matrix is stretched from 1D to 2D. In the LASM, two inputs are interactively manipulated and the result (x_{i+1}, y_{i+1}) spread into the 2D phase matrix. It is more complex in comparison with sine and logistic maps. But the results are much harder to anticipate [28]. The LASM is a 2D chaotic system that can exhibit and offer a quite complex chaotic dynamic state and is extremely utilized in encryption applications. The LASM can exhibit a chaotic behavior if $\mu \in \{1\} \cup [0.44,\ 0.93] \cup [0.4,\ 0.42] \cup [0.37,\ 0.38]$, and the resulted $\{x_n, y_n\}, n = 0, 1, 2, 3, \ldots.\}$ sequence becomes non-periodic and so sensible with respect to the input primary initial values [28], [48]. In this paper, $\mu = 0.91$.

B. THE TWO DIMENSIONAL HARTLEY TRANSFORM (2D HT)

This section is dedicated for reviewing the optical encryption scheme with the HT. The HT is introduced in 1942 by Hartley [33] and considered as substitution to the FT. It may be optically performed without needing the phase and supplies just the FTs intensity view [29]. The 2D HT for a real function $F(x_i, y_i)$ can be computed as [30-32]:

$$\mathrm{HT}(\mathrm{x}_0,\mathrm{y}_0) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \mathrm{F}(\mathrm{x}_\mathrm{i},\mathrm{y}_\mathrm{i})\mathrm{cas}\left[2\pi\left(\mathrm{x}_0\mathrm{x}_\mathrm{i}+\mathrm{y}_0\mathrm{y}_\mathrm{i}\right)\right]\mathrm{dx}_\mathrm{i}\mathrm{dy}_\mathrm{i} \quad (2)$$

The Inverse 2D Hartley transform (HT^{-1}) is computed as:

$$\mathrm{HT}^{-1}(\mathrm{x}_\mathrm{i},\mathrm{y}_\mathrm{i}) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \mathrm{HT}(\mathrm{x}_0,\mathrm{y}_0)\,\mathrm{cas}\left[2\pi\left(\mathrm{x}_0\mathrm{x}_\mathrm{i}+\mathrm{y}_0\mathrm{y}_\mathrm{i}\right)\right]\mathrm{dx}_0\mathrm{dy}_0 \quad (3)$$

where cas = cos + sin.

TABLE 1. Comparison of the proposed opto-audio cryptosystem using and XORing mask and Hartley transform (HT) and other state-of-the-art methods [19]–[22], [26], [27], [40]–[45], [50].

Cryptosystem	Keys No.	Classification type		Dimensions	Implementation	Advantage	Disadvantage
		Diffusion	Confusion				
Proposed optical audio cryptosystem	6	Yes	No	2D & 3D	Optical Or Digital	Strong encryption	There is no compression and authenticity verification schemes
Arnold-DRPE optical audio cryptosystem [27]	3	Yes	Yes				
Virtual optics audio cryptosystem [19]	3	Yes	No			Less complexity	
Chaotic-based audio cryptosystem [26]	1	No	Yes	2D	Digital	Simple	
Optical DH-based Audio Cryptosystem [20]	2	Yes	No	2D	Optical Or Digital	Strong encryption	
Optical transform-based DRPE Audio Cryptosystem [21]	2	Yes	No	2D	Optical Or Digital	Strong encryption	
CNT-based Audio Cryptosystem [22]	1	Yes	No	2D	Digital	Simple	
Zaslavsky-based Audio Cryptosystem [40]	9	Yes	Yes	2D	Digital	Strong encryption	
Confusion-diffusion based Audio Cryptosystem [41]	1	Yes	Yes	2D	Digital	Simple	
on one-time keys and robust chaotic maps-based Color image encryption [42]	4	Yes	Yes	1D	Digital	Simple	
Spatial bit-level permutation and high dimension chaotic-based Color image encryption [43]	13	Yes	Yes	1D & 3D	Digital	Strong encryption	
DNA complementary rule and chaotic maps-based Image encryption [44]	10	Yes	Yes	1D	Digital	Strong encryption	
perceptron model-based chaotic image encryption [45]	8	Yes	Yes	3D	Digital	Strong encryption	
Collatz conjecture-based Audio Cryptosystem [50]	1	Yes	Yes	2D	Digital	Strong encryption	

As a result for the 2D HT definition, it may be estimated from two Fourier transforms (FTs) as [29]:

$$\begin{aligned} \mathrm{HT}(x_0,y_0) &= \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \mathrm{F}(x_i,y_i)\mathrm{cas}\left[2\pi\left(x_0x_i+y_0y_i\right)\right]dx_i dy_i \\ &= \frac{\exp(\frac{i\pi}{4})}{\sqrt{2}}\left\{\begin{array}{l}\mathrm{FT}\left[\mathrm{F}(x_i,y_i)\right] \\ +\exp(\frac{-i\pi}{2})\mathrm{FT}\left[\mathrm{F}(-x_i,-y_i)\right]\end{array}\right\} \end{aligned} \tag{4}$$

where $\mathrm{FT}\left[\mathrm{F}(x_i,y_i)\right]$ represents the FT of $\mathrm{F}(x_i,y_i)$. The fixed constant $\frac{\exp(\frac{i\pi}{4})}{\sqrt{2}}$ may be ignored within the 2D HT procedure since the HT squared modulus is estimated the output plane. Finally, it can be seen that the 2D HT can be estimated through employing two FTs with a $\exp(\frac{-i\pi}{2})$ phase.

III. THE PROPOSED OPTO-AUDIO CRYPTOSYSTEM

The idea of the proposed opto-audio encryption system depends on XORing mask by XORing each block of 2D PABs with a single image selected from a personal image database that can be viewed as an extra secret key in the proposed opto-audio cryptosystem. As the utilized personal image database that contains images of 4*4 byte size and since we perform XORing mask by XORing each block of 2D PABs with a single image of 4*4 byte size selected from the personal image database, So, the size of each block of 2D PABs must be the same and equivalent as the size the selected image from the personal image database. This is the reason why PAM is segmented into blocks of 4*4 byte 2D PABs. The mixed 2D PABs is then transposed using the chaotic LASM and optically encrypted with HT.

A. PROCESS OF RESHAPING THE 1D DIGITAL PLAINAUDIO INTO 2D PAM

If $S(i),i = 1,2,....k$ represents the 1D plainaudio of k samples $[S(1), S(2),.....S(k)]$ where, $S(1), S(2),.....S(k)$ denote each block of 2D PAM. Assume that $F(M,N)$ is the 2D PAM of $M \times N$ size. Then, $F(M,N)$ can be defined as:

$$F(M,N) = \begin{bmatrix} F(1),.....F(M) \\ .. \\ .. \\ .. \\ .F((M-1)\times N+1),.....F(M\times N) \end{bmatrix} \tag{5}$$

If each block of 2D PAM $S(i),i = 1,2,....k$ assigns to 2D PAM, then this can be represented as:

$$F(m,n) = S((m-1)\times M+n) \tag{6}$$

11001110	10010111	10101001	11010010
10011111	00001101	10000011	11100011
11110001	11001011	00001101	10010011
10100110	10110010	11100111	10111011

(a)

11011011	01101111	11011111	00001111
10001110	10001110	11011111	00001101
10101110	10110110	11010111	10000111
01110001	01100110	11010010	11001010

(b)

00010101	11111000	01110110	11011101
00010001	10000011	01011100	11101110
01011111	01111101	11011010	00010100
11010111	11010100	00110101	01110001

(c)

FIGURE 1. Preprocessing phase steps of XORing the 4 × 4 byte 2D PAB with the chosen image from the secret image database. (a) Original 4 × 4 byte 2D PAB. (b) The 128-bit selected image. (c) The mixed 2D PAB after XORing with the 128-bit selected image.

where $F(m, n)$ represents each pixel in the 2D PAM, $1 \leq m \leq M$,$1 \leq n \leq N$, and $k \leq M \times N$. The 2D PAM after the assignment process can be represented as:

$$F(M,N) = \begin{bmatrix} S(1),...,...,...,S(M) \\ .. \\ .. \\ .. \\ .S((M-1)\times N+1),...,S(M)...,S(M\times N) \end{bmatrix} \tag{7}$$

The 2D PAM looks like 2D image and is known as the audio map.

B. PRE-PROCESSING STAGE

In the pre-processing stage, a secret database image of 1024 images is used. Each selected image $I(m, n)$ is 128-bit size. Initially, the user chooses a given image $I(m, n)$, and then every block of 2D PABs is 128-bit (4*4 byte size) is XORed with the chosen image. The preprocessing steps are described in Fig 1. Fig. 1(a) illustrates a 2D PAB.

Fig. 1(b) shows the chosen image of 128-bit. Fig. 1(c) shows the mixed 2D PAB after XORing with the chosen image. As illustrated in Fig. 1(c), the mixed 2D PAB contains the chosen image that is XORed with the 2D PAB.

C. ENCRYPTION OF THE OPTO-AUDIO CRYPTOSYSTEM

Now, each 2D PAB is firstly masked by XORing with the chosen secret image. The mixed 2D PAB is then scrambled using LASM and optically encrypted with 2D HT. The two random phase diffusers of the 2D HT serve as main encoding keys. Also, the selected image from the private database and parameters of LASM can be considered as extra additional secret keys.

The encryption steps of the proposed opto-audio cryptosystem are arranged as:

1. Reshape the 1D plainaudio into 2D PAM $F(m, n)$.
2. Divide the 2D PAM into k blocks of 4×4 byte 2D PABs $F_i(m, n)$, where $i = 1, 2, 3, ...k$. Each block i of 2D PABs is termed $F_i(m, n)$.
3. Choose an image $I(m, n)$ from the user secret image database.
4. Employ XORing mask between the chosen image $I(m, n)$ and each block i of 2D PABs $F_i(m, n)$.

$$X_i(m,n) = F_i(m,n) \oplus I(m,n) \tag{8}$$

5. Each of the resulted mixed 2D PABs $X_i(m, n)$ is transposed using LASM.

$$LASM[X_i(m,n)] = LASM[F_i(m,n) \oplus I(m,n)] \tag{9}$$

6. Employ 2D-HT opto encryption for each of the resulted LASM transposed mixed 2D PABs using the two random phase diffusers of the 2D HT that serve as the main two encoding keys.

$$C_i(m,n) = \mathrm{HT}^{-1}[\mathrm{HT}[LASM[F_i(m,n) \oplus I(m,n)] \times exp(j2\pi\theta(m,n))] \times exp(j2\pi\omega(m,n))] \tag{10}$$

7. Collect all encrypted k blocks of 2D cipheraudio blocks (CABs) $C_i(m, n)$, where $i = 1, 2, 3, ...k$ to produce the encrypted audio map $C(m, n)$.

$$C(m,n) = (C_1(m,n), C_2(m,n), ..., C_k(m,n)) \tag{11}$$

8. Reshape the encrypted audio blocks $C(m, n)$ into 1D encrypted audio.

D. DECRYPTION OF THE OPTO-AUDIO CRYPTOSYSTEM

The steps of decryption for the proposed opto-audio cryptosystem can be detailed as follows:

1. Reshape the 1D encrypted audio into 2D cipher audio map (CAM) $C(m, n)$.
2. Divide the 2D CAM into k blocks of 4×4 byte 2D CABs $C_i(m, n)$, where $i = 1, 2, 3, ...k$. Each block i of 2D CABs is termed $C_i(m, n)$.
3. Employ 2D-HT opto decryption for each of the 2D CABs $C_i(m, n)$ using the conjugate of two random phase diffusers of the 2D HT that serve as the main two encoding keys.

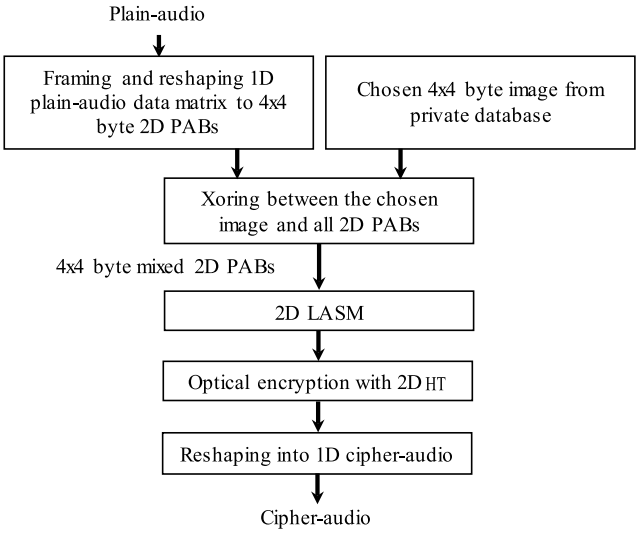
$$Y_i(m,n) = \mathrm{HT}^{-1}[\mathrm{HT}[C_i(m,n) \times exp(-j2\pi\omega(u,v))] \times exp(-j2\pi\theta(m,n))] \tag{12}$$

4. Each of the Hartley transformed 2D CABs $Y_i(m, n)$ is transposed using the inverse of LASM.

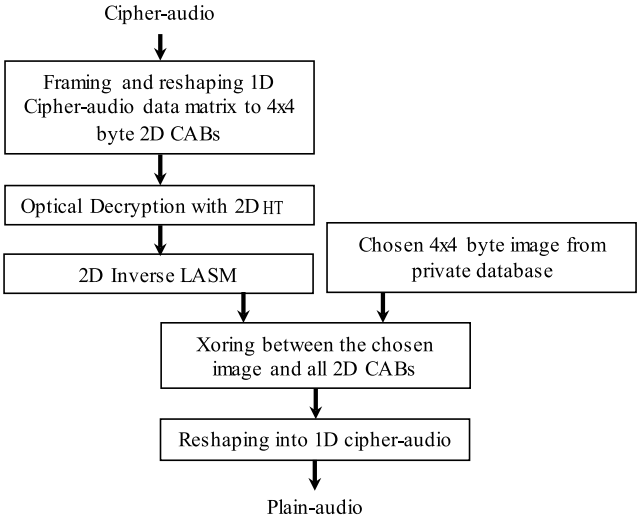
$$LASM^{-1}[Y_i(m,n)] = LASM^{-1}[\mathrm{HT}^{-1}[\mathrm{HT}[C_i(m,n) \times exp(-j2\pi\omega(u,v))] \times exp(-j2\pi\theta(m,n))]] \tag{13}$$

5. Employ XORing mask between the chosen image $I(m, n)$ and each block i of inverse LASM transposed audio blocks $LASM^{-1}[Y_i(m, n)]$.

$$F_i(m,n) = LASM^{-1}[\mathrm{HT}^{-1}[\mathrm{HT}[C_i(m,n) \times exp(-j2\pi\omega(u,v))] \times exp(-j2\pi\theta(m,n))]] \tag{14}$$



(a) The Proposed Opto-audio Cryptosystem Encryption



(b) The Proposed Opto-audio Cryptosystem Decryption

FIGURE 2. The proposed opto-audio cryptosystem using XORing mask and Hartley transform (HT).

6. Collect all decrypted k blocks of audio (2D PABs) $F_i(m, n)$, where $i = 1, 2, 3, ...k$ to produce the 2D PAM $F(m, n)$.

$$F(m, n) = (F_1(m, n), F_2(m, n), ..., F_k(m, n)) \quad (15)$$

7. Reshape the decrypted audio blocks $F(m, n)$ into 1D audio.

Fig. 2 shows the proposed opto-audio cryptosystem using XORing mask, LASM, and Hartley transform (HT).

IV. EXPERIMENTAL TESTS

In this section, we also know that 2D HT based opto-audio encryption is secure and effective encryption. Therefore, we are primarily interested in exploring the effect of XOR's quality improvement on the 2D PABs when mixed with chosen secret images as a pre-processing step prior to LASM scrambling, and 2D HT based opto encryption. In addition, we would like to study the quality degradation effects presented in decrypted audio. This part is sectioned into two subcategories; the first one is to inquire about the encrypted audio quality, and the other is to inquire about the decrypted audio quality. Simulation experiments were conducted on the Matlab R2017b with Windows 10 environment. The experiments have been conducted using nine collections of audio samples classified into several types of audio such as Female-Male, Female, Artificial Frog voice, people, animal, piano, alarm, music and chimes.

A. QUALITY OF ENCRYPTED AUDIO

The encrypted audio is examined to demonstrate and confirm the quality improvements introduced by the pre-processing mask phase by XORing each block of 2D PABs with a chosen secret image prior to LASM scrambling and 2D HT-based opto encryption. The proposed opto-audio cryptosystems security is tested against a number of attacks, such as statistical and differential attacks, known and chosen plaintext attacks, occlusion attack, additive white Gaussian noise (AWGN) and multiplicative white Gaussian noise (MWGN) Attacks, and compression attack. Test results confirm the dominance of the proposed opto-audio cryptosystem from a cryptographic perspective.

1) THE RESIDUAL INTELLIGIBILITY

The Female source audio depicted in Fig. 3(a) is ciphered using DRPE [12], chaotic-DRPE [1], 2D HT-based optical encryption, and the proposed opto-audio cryptosystem. The outcomes are illustrated in Figs. 3(b-e). Figs. 4(a-e) show the Female plainaudio spectrogram, Female cipheraudio spectrograms using DRPE, chaotic-DRPE, 2DHT-based optical encryption, and the proposed opto-audio cryptosystem using XORing mask, LASM scrambling, and Hartley transform (HT). Audio encryption looks like random sound without audio streams. This eliminates plainaudio tones and ensures that the rest of the intelligence is not valuable to the attackers in the communication channel.

2) STATISTICAL TESTS

Statistical tests were performed on the proposed opto-audio cryptosystem to test its effectiveness, which can resist statistical attacks [51]. The statistical experiments are employed in terms of the spectral distortion (SD) and correlation coefficient (r_{PACA}) of the cipheraudio with respect to the plainaudio.

a: CORRELATION COEFFICIENT METRIC

Correlation coefficient evaluation between 2D PABs and associated 2D CABs is considered a good estimate to assess the proposed opto-audio cryptosystem encryption quality. It is calculated as [34], [35]:

$$r_{PACA} = \frac{cov_v(PA, CA)}{\sqrt{D(PA)}\sqrt{D(CA)}} \quad (16)$$

where cov_v(PA,CA) is the covariance between the original plainaudio PA and the cipheraudio CA. $D(PA)$ and $D(CA)$ are

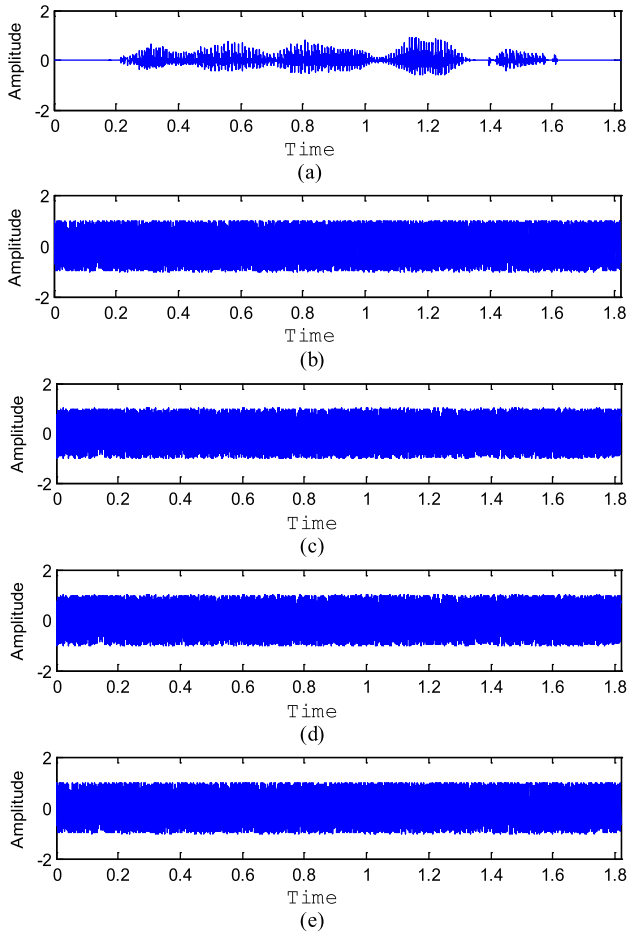


FIGURE 3. Female source audio encryption. (a) Female source audio. (b) Encrypted female audio using DRPE [12]. (c) Encrypted female audio using chaotic-DRPE [1]. (d) Encrypted female audio using the 2D HT-based optical encryption. (e) Encrypted female audio using the proposed opto-audio cryptosystem.

the plainaudio PA and cipheraudio CA variances. In addition to numerical calculations, the following formulas are utilized [34]–[35]:

$$E(PA) = \frac{1}{N_s}\sum_{i=1}^{N_s} PA(i) \tag{17}$$

$$D(PA) = \frac{1}{N_s}\sum_{i=1}^{N_s} (PA(i) - E(PA))^2 \tag{18}$$

$$cov_v(PA, CA) = \frac{1}{N_s}\sum_{i=1}^{N_s} (PAg(i) - E(PA))(CA(i) - E(CA)) \tag{19}$$

where N_s represents the number of audio samples used in the evaluations. Low correlation coefficient r_{PACA} values indicate excellent encryption quality.

The correlation coefficient results of plainaudio and cipheraudio signals using DRPE [12], chaotic-DRPE [1], 2D-HT based opto encryption and the proposed opto-audio cryptosystem for the nine test audio samples are given in Table 2. It is observed that the correlation coefficients of proposed

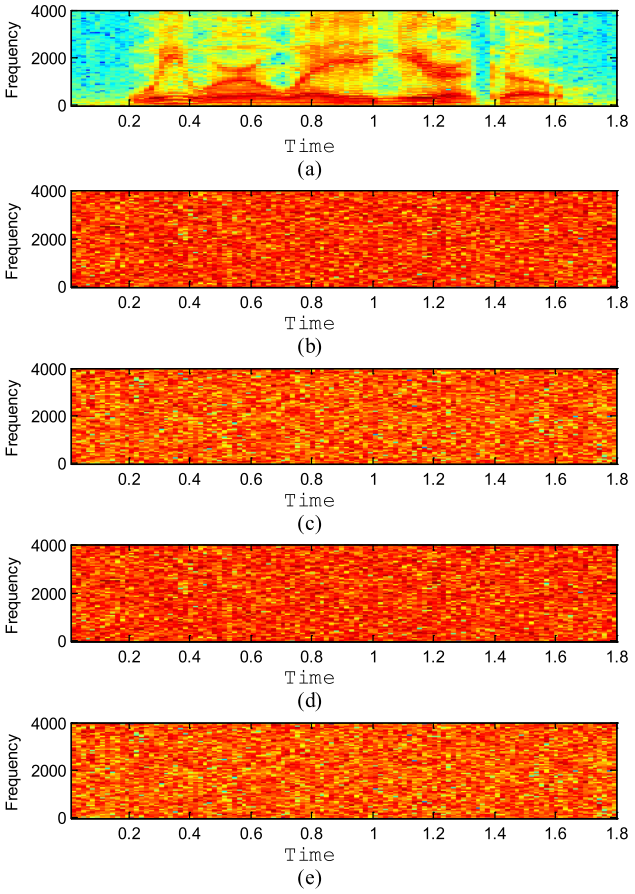


FIGURE 4. Spectrogram of encrypted female plainaudio. (a) Female plainaudio spectrogram. (b) Encrypted female audio spectrogram using DRPE [12]. (c) Encrypted female audio spectrogram using chaotic-DRPE [1]. (d) Encrypted female audio spectrogram using the 2DHT-based optical encryption. (e) Encrypted female audio spectrogram using the proposed opto-audio cryptosystem.

TABLE 2. Correlation Coefficients of DRPE [12], chaotic-DRPE [1], 2DHT-based opto encryption and the proposed opto-audio cryptosystem for different audio samples.

Audio	Encryption Method			
	DRPE [12]	Chaotic-DRPE [1]	2D HT-based opto-audio encryption	The proposed opto-audio cryptosystem
Female-Male	0.0079	0.0075	0.0046	0.0039
Female	0.0081	0.0078	0.0048	0.0042
Artificial Frog voice	0.0083	0.0076	0.0044	0.0038
People	0.0085	0.0077	0.0047	0.0040
Animal	0.0082	0.0072	0.0050	0.0043
Piano	0.0080	0.0073	0.0052	0.0044
Alarm	0.0081	0.0075	0.0051	0.0045
Music	0.0079	0.0074	0.0045	0.0040
Chimes	0.0084	0.0079	0.0051	0.0038

opto-audio cryptosystem are the smallest ones and almost zero compared to other encryption schemes.

b: SPECTRAL DISTORTION (SD)

The SD is computed in the frequency domain for both the plainaudio frequency spectrum and cipheraudio

TABLE 3. The SD of DRPE [12], chaotic-DRPE [1], 2DHT-based opto encryption and the proposed opto-audio cryptosystem for different audio samples.

Audio	SD			
	DRPE [12]	Chaotic-DRPE [1]	2D HT-based opto-audio encryption	The proposed opto-audio cryptosystem
Female-Male	28.4877	26.5862	32.4753	34.8224
Female	27.8954	26.9512	31.8521	34.5462
Artificial Frog voice	27.6541	26.7854	31.5624	34.3658
People	28.2156	27.1498	32.0256	34.6547
Animal	28.1125	27.0264	31.9862	33.8542
Piano	27.9542	26.9824	31.7245	33.4235
Alarm	27.7745	26.3251	31.5489	33.9754
Music	28.1145	27.6528	31.2586	33.7546
Chimes	27.9621	26.8524	30.9957	33.8256

frequency spectrum. The SD determines how the cipheraudio spectrum is far from its corresponding plainaudio. It can be estimated as [36]:

$$SD = \frac{1}{M}\sum_{m=0}^{M-1}\sum_{i=Nm}^{Nm+N-1}|S_a(i) - S_b(i)| \tag{20}$$

Here, $S_a(i)$, $S_b(i)$ are the plainaudio spectrum and cipheraudio spectrum specified in dB for a specific block in the time domain. M and N are the block number and block size in the audio.

High SD values indicate excellent encryption quality. The SD results of plainaudio and cipheraudio using DRPE [12], chaotic-DRPE [1], 2D-based opto encryption, and the proposed opto-audio cryptosystem for the nine test audio samples are given in Table 3. The results illustrated in Table 3 conclude that the plainaudio XORing with the pre-selected image prior to LASM scrambling and opto encryption improves the encryption quality and increases SD between the plainaudio and the cipheraudio. Also, it is observed that the SD values of proposed opto-audio cryptosystem are the largest ones compared to other encryption schemes. This demonstrates and ensures the dominance of the proposed opto-audio cryptosystem with respect to other encryption schemes.

3) PLAINAUDIO SENSITIVITY TESTS

The perfect feature of any audio cryptosystem is the critical sensitivity to small changes in the input plainaudio such as bit editing of input plainaudio. In general, attackers can only make a small change, such as changing a bit from the plainaudio and notifying the effect. In this manner, the attacker may deduce the important relationship between the input plainaudio and the output cipheraudio. Small changes in the input plainaudio can result in significant changes in the cipheraudio, making the differential attack inefficient and practically useless [52].

The sensitivity of the proposed opto-audio cryptosystem, to slight modifications is tested through changing just one bit value in the chosen plainaudio and notifies the output of

TABLE 4. NPCR of DRPE [12], chaotic-DRPE [1], 2DHT-based opto encryption and the proposed opto-audio cryptosystem for different audio samples.

Audio	NPCR			
	DRPE [12]	Chaotic-DRPE [1]	2D HT-based opto-audio encryption	The proposed opto-audio cryptosystem
Female-Male	99.62	99.66	99.71	99.75
Female	99.62	99.65	99.68	99.70
Artificial Frog voice	99.60	99.61	99.63	99.66
People	99.58	99.59	99.60	99.64
Animal	99.60	99.63	99.68	99.72
Piano	99.57	99.58	99.60	99.62
Alarm	99.60	99.61	99.67	99.71
Music	99.57	99.58	99.59	99.60
Chimes	99.59	99.60	99.62	99.67

the proposed opto-audio cryptosystem. To test the effect of a single bit modification of the chosen plainaudio on the whole cipheraudio, we use two known measures; the number of pixel changing rate (NPCR) and the unified average changing intensity (UACI). If we have two cipheraudio signals defined as G1(x,y) and G2(x,y) correspond to their selected plainaudios that have just only a single bit difference, then a bipolar array T similar to G1 and G2 is defined. Therefore, T(x,y) is estimated by G1(x,y) and G2(x,y). If G1(x,y) = G2(x,y), then T(x,y) = 1; Alternatively, T(x,y) = 0. The NPCR can be calculated as [37]–[39]:

$$\text{NPCR} = \frac{\sum_{i,j} T(x,y)}{MN} x100\% \tag{21}$$

where M defines the height of G1and N defines the width of G2. The NPCR calculates the different pixel number ratio to the total pixel number in G1 and G2. The UACI is evaluated as [37]–[39]:

$$\text{UACI} = \frac{1}{MN}\left[\sum_{x,y}\frac{G1(x,y) - G2(x,y)}{255}\right] x100\% \tag{22}$$

It calculates the difference average intensity between G1 and G2. High NPCR and UACI values ensure good encryption quality and high sensitivity with respect to small changes in either the input plainaudio or the chosen image. The NPCR and UACI results of DRPE [12], chaotic-DRPE [1], 2D-HT based opto encryption and the proposed opto-audio cryptosystem for the nine test audio samples are tabulated in Table 4 and Table 5. The results illustrated in Table 4 and Table 5 indicate that the NPCR and UACI values of proposed opto-audio cryptosystem are the largest ones compared to other encryption schemes. This confirms and ensures the sensitivity of the proposed opto-audio cryptosystem with respect to small changes in either the input plainaudio or the chosen image. Also, the obtained results demonstrate the efficiency of the proposed opto-audio cryptosystem with respect to other encryption schemes.

TABLE 5. UACI of DRPE [12], chaotic-DRPE [1], 2DHT-based opto encryption and the proposed opto-audio cryptosystem for different audio samples.

Audio	UACI			
	DRPE [12]	Chaotic-DRPE [1]	2D HT-based opto-audio encryption	The proposed opto-audio cryptosystem
Female-Male	27.5547	29.986	32.8754	33.2145
Female	27.6982	29.3568	32.7894	33.1456
Artificial Frog voice	27.3456	29.3658	32.6547	33.2265
People	26.9856	28.8654	31.9875	33.1425
Animal	26.8754	28.9546	31.9654	33.2287
Piano	27.3258	29.5324	32.8547	33.3215
Alarm	27.6597	29.1256	31.9964	33.1475
Music	26.9853	29.9852	32.3689	33.1597
Chimes	26.5687	28.7856	31.8566	33.3217

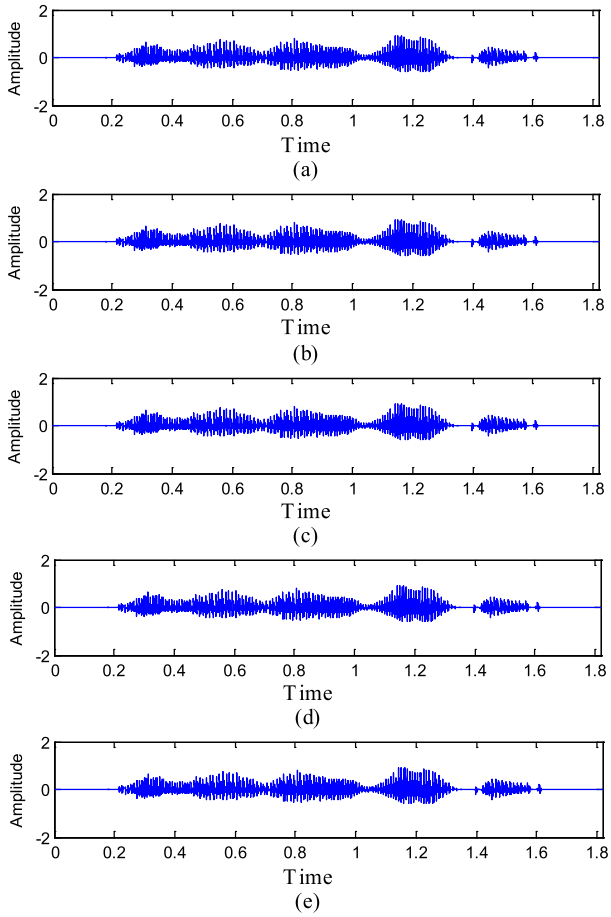


FIGURE 5. Decryption of female audio. (a) Female plainaudio. (b) Decrypted female audio using DRPE [12]. (c) Decrypted female audio using chaotic-DRPE [1]. (d) Decrypted female audio using the 2DHT-based optical encryption. (e) Decrypted female audio using the proposed optical audio cryptosystem.

B. QUALITY OF DECRYPTED AUDIO

The decrypted audio is examined to demonstrate its quality with respect to the original plainaudio. The Female plainaudio is encrypted with DRPE [12], chaotic-DRPE [1], 2D HT-based optical encryption and the proposed opto-audio cryptosystem. After that, the Female cipheraudio signal is deciphered using DRPE [12], chaotic-DRPE [1], 2D HT-based optical encryption and the proposed opto-audio cryptosystem. The decryption results are depicted in Figs. 5(b-e). Figs. 6(a-e) show the decrypted Female cipheraudio spectrograms using DRPE [12], chaotic-DRPE [1], 2D HT-based optical encryption and the proposed opto-audio cryptosystem.

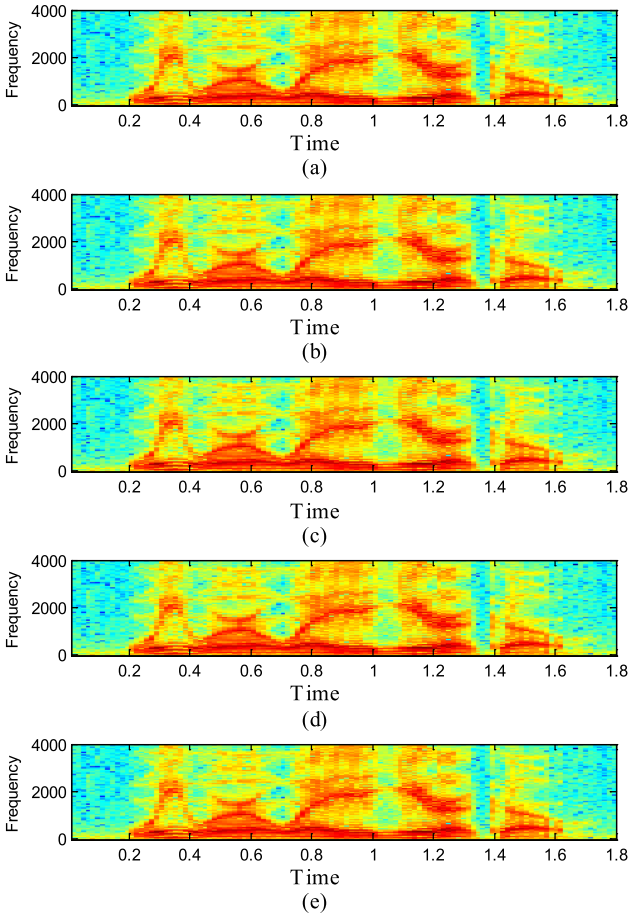


FIGURE 6. Spectrogram of decrypted female audio. (a) Female plainaudio spectrogram. (b) Decrypted female audio spectrogram using DRPE [12]. (c) Decrypted female audio spectrogram using chaotic-DRPE [1]. (d) Decrypted female audio spectrogram using the 2DHT-based optical encryption. (e) Decrypted female audio spectrogram using the proposed opto-audio cryptosystem.

To estimate the semantic quality of decrypted audio, two metrics are used to assess the quality of the decrypted audio signal; correlation coefficient and SD. So, the decrypted audio is compared to plainaudio in terms of SD and correlation coefficient. High correlation coefficient and low SD values can ensure and guarantee the superiority of the audio cryptosystem. The SD and correlation coefficient results of decrypted audio using DRPE [12], chaotic-DRPE [1], 2D HT-based opto-audio encryption and the proposed opto-audio cryptosystems for the nine collections of audio samples are shown in Table 6 and Table 7. The results illustrated in Table 6 and Table 7 indicates that the decrypted audio has better quality in terms of low SD values that equal zero and high

TABLE 6. The SD of the decrypted audio using DRPE [12], chaotic-DRPE [1], 2DHT-based opto encryption and the proposed opto-audio cryptosystem for different audio samples.

Audio	SD			
	DRPE [12]	Chaotic-DRPE [1]	2D HT-based opto-audio encryption	The proposed opto-audio cryptosystem
Female-Male	0	0	0	0
Female	0	0	0	0
Artificial Frog voice	0	0	0	0
People	0	0	0	0
Animal	0	0	0	0
Piano	0	0	0	0
Alarm	0	0	0	0
Music	0	0	0	0
Chimes	0	0	0	0

TABLE 7. Correlation coefficients of the decrypted audio using DRPE [12], chaotic-DRPE [1], 2DHT-based opto encryption and the proposed opto-audio cryptosystem for different audio samples.

Audio	SD			
	DRPE [12]	Chaotic-DRPE [1]	2D HT-based opto-audio encryption	The proposed opto-audio cryptosystem
Female-Male	1	1	1	1
Female	1	1	1	1
Artificial Frog voice	1	1	1	1
People	1	1	1	1
Animal	1	1	1	1
Piano	1	1	1	1
Alarm	1	1	1	1
Music	1	1	1	1
Chimes	1	1	1	1

correlation coefficient values that equal 1. The achieved outcomes shown in Figs. 5-6 and Tables VI-VII ensure and guarantee the dominance of the proposed opto-audio cryptosystem.

C. THE EFFECT OF KNOWN PLAINTEXT, CHOSEN PLAINTEXT, CIPHERTEXT ONLY, AND CHOSEN CIPHERTEXT ATTACKS

The robustness of the proposed opto-audio cryptosystem using XORing mask, LASM, and Hartley transform (HT) is examined against both known plaintext, chosen plaintext, ciphertext only, and chosen ciphertext attacks using the impulse function. The Female plainaudio and the artificial plainaudio for Frog voice are shown in Figs. 7(a) and (b) are encrypted with the proposed opto-audio cryptosystem and their corresponding cipheraudio signals are illustrated in Figs. 7(c) and (d). It is supposed that the original Female plainaudio and its respective cipheraudio are attacked and the artificial cipheraudio for Frog voice is attacked. The results of both known plaintext and chosen plaintext attacks are illustrated in Figs. 7(e) and (f), respectively. The results demonstrate and ensure the robustness of the proposed opto-audio

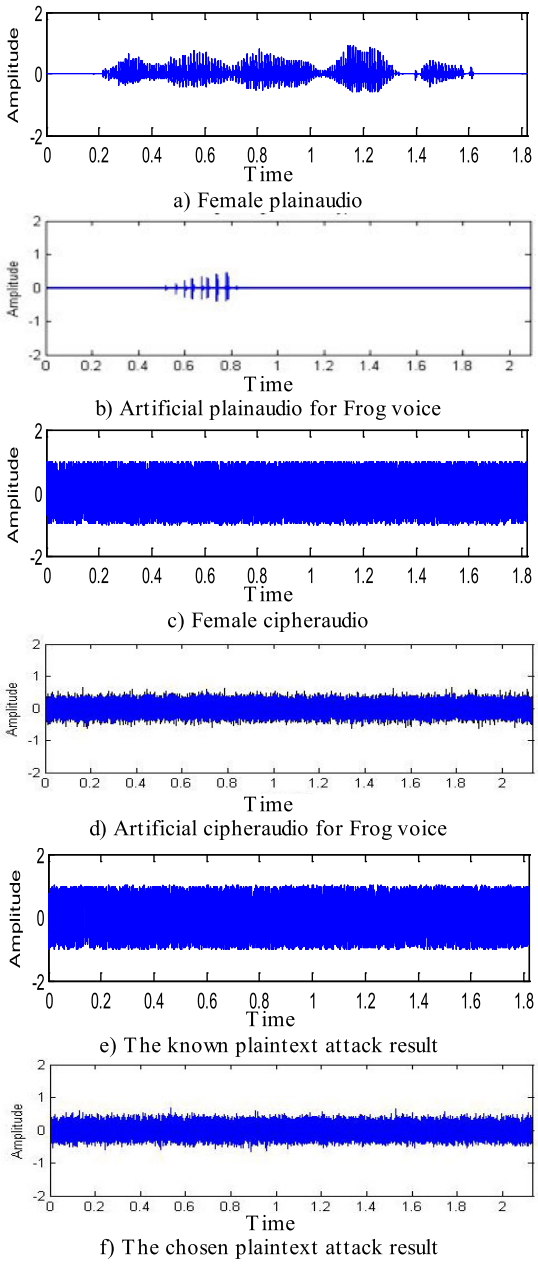


FIGURE 7. The resistance of the proposed opto-audio cryptosystem against both known plaintext and chosen plaintext attacks.

cryptosystem with respect to both known plaintext and chosen plaintext attacks. Also, in [53], it is shown that the chosen plaintext attack is the utmost strong attack. When the proposed opto-audio cryptosystem has the power of resisting such type of attack, it is surly that it has the ability to withstand all other attack types. The proposed opto-audio cryptosystem is so sensitive with respect to LASM initial parameters, encoding keys of the 2D HT-based optical encryption, and the chosen image from the private image database. If any one of these parameters is modified, the output of the proposed opto-audio cryptosystem would be completely different. Also, in the optical 2D HT diffusion procedure, the ciphered value is not just based on its plain value and the keys but also based on the former plain and

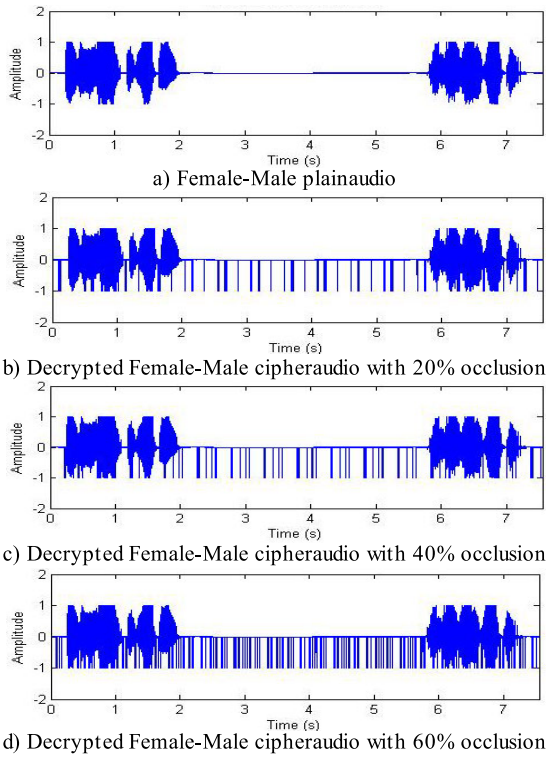


FIGURE 8. Robustness of the proposed opto-audio cryptosystem against occlusion attack.

cipher values. Such findings indicate that various encrypted images have various former plain and cipher values. Hence, the proposed opto-audio cryptosystem can withstand the chosen ciphertext attack.

D. THE EFFECT OF OCCLUSION ATTACK

The resistance of the proposed opto-audio cryptosystem using XORing mask, LASM, and Hartley transform (HT) against the occluding attack is investigated. The decryption is performed on the occluded Female-Male cipheraudio with 20%, 40% and 60% occlusion percentages. The respected deciphered Female-Male audio-audio results with 20%, 40% and 60% occlusion percentages are depicted in Figs. 8(b), (c), and (d). The obtained results indicate that the main skeleton of the Female-Male plainaudio can be recovered and ensure the robustness of the proposed opto-audio cryptosystem against occlusion attack.

E. THE EFFECT OF AWGN AND MWGN ATTACKS

The immunity of the proposed opto-audio cryptosystem using XORing mask, LASM, and Hartley transform (HT) against AWGN and MWGN is examined during the deciphering phase. The peak signal to noise ratio (PSNR) is utilized for evaluating the quality of different decrypted audio samples in the presence of both AWGN and MWGN with different variances. In all different audio samples, the decryption process has been employed with the right keys. The PSNR results of the proposed opto-audio cryptosystem for different decrypted audio samples in the presence of both AWGN and MWGN with different variances are shown in Table 8 and Table VIV. The results demonstrated that the different decrypted audio samples using proposed opto-audio cryptosystem in the presence of both AWGN and MWGN with different variances have good PSNR results. The presence of the original plain-audio can be recognized in all the examined audio samples. The obtained results ensure the robustness of the proposed opto-audio cryptosystem against certain amount of both AWGN and MWGN degradation in the encrypted audio.

TABLE 8. The PSNR of the proposed opto-audio cryptosystem for different decrypted audio samples in the presence of AWGN with different variances.

Audio	PSNR				
	σ =0.01	σ = 0.05	σ = 0.1	σ = 0.15	σ =0.20
Female-Male	18.572	13.847	10.958	9.855	8.568
Female	18.165	13.755	10.855	9.675	8.467
Artificial Frog voice	17.457	12.995	10.654	9.375	8.256
People	17.265	13.116	10.259	9.654	8.015
Animal	16.852	12.854	9.875	8.985	7.892
Piano	16.564	12.567	9.542	8.542	7.784
Alarm	17.658	13.015	10.526	9.542	8.425
Music	16.254	12.584	9.742	8.775	7.854
Chimes	18.358	13.885	10.955	9.774	8.498

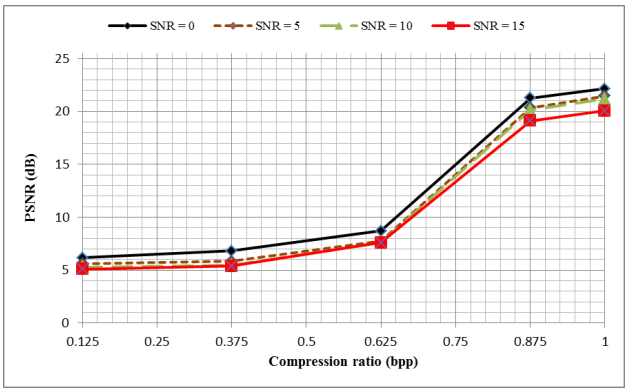


FIGURE 9. The Impact of compression on the decrypted audio with various SNR.

F. THE EFFECT OF COMPRESSION ON THE DECRYPTED AUDIO

The effect of compression on the robustness of the proposed opto-audio cryptosystem using XORing mask, LASM, and Hartley transform (HT) is inspected.

This is done by investigating the effect of compression on the cipheraudio with noise existence in the decryption process. The procedure begins with performing audio encryption using the proposed opto-audio cryptosystem and followed by employing audio compression using various compression ratios with various SNR. Fig. 9 illustrates the compression effect on the decrypted audio with various SNR. The results demonstrated that the PSNR of decrypted audio increases with increasing the compression ratio with different SNR.

TABLE 9. The PSNR of the proposed opto-audio cryptosystem for different decrypted audio samples in the presence of MWGN with different variances.

Audio	PSNR				
	σ =0.01	σ = 0.05	σ = 0.1	σ = 0.15	σ =0.20
Female-Male	16.425	12.689	10.547	9.598	8.1425
Female	16.584	13.142	10.145	9.542	8.112
Artificial Frog voice	16.236	12.129	10.362	8.852	7.879
People	16.456	12.116	9.548	8.875	7.454
Animal	15.235	12.118	9.215	8.118	7.351
Piano	15.745	11.362	8.113	7.985	7.116
Alarm	16.623	13.259	9.223	8.442	7.887
Music	15.116	11.365	9.118	8.127	7.105
Chimes	16.659	12.554	10.113	8.996	7.987

TABLE 10. Comparison between the proposed opto-audio cryptosystem and the other related state-of-the-art methods [22], [40]–[42] for Female-Male audio.

Method	SD	r_{PACA}	NPCR	UACI
Ref. [22]	32.9542	0.0068	99.42	28.24
Ref. [40]	32.8452	0.0081	99.37	27.82
Ref. [41]	33.6587	0.0059	99.52	28.75
Ref. [42]	33.2584	0.0048	99.66	28.84
Proposed opto-audio cryptosystem	34.8224	0.0039	99.75	29.12

V. COMPARISON STUDY BETWEEN THE PROPOSED OPTO-AUDIO CRYPTOSYSTEM AND THE RELATED STATE-OF-THE-ART METHODS

To ensure and confirm the effectiveness of the proposed opto-audio cryptosystem using XORing mask, LASM, and Hartley transform (HT), it is compared with the recent state-of-the-art methods [22], [40], [41], [42] in terms of various metrics like SD, correlation coefficient, NPCR, and UACI. The comparison study between the proposed opto-audio cryptosystem and the related state-of-the-art methods [20], [38]–[40] are employed on the Female-Male audio.

Table 10 shows the results of comparison between the proposed opto-audio cryptosystem and the related state-of-the-art methods [22], [40]–[42] for Female-Male audio. Form the relative results shown in Table VIVI, it is noted that the proposed opto-audio cryptosystem has the best SD value. So, the proposed opto-audio cryptosystem is appreciated and recommended compared to the related state-of-the-art methods [22], [40]–[42]. With respect to the similarity between the plainaudio and cipheraudio signals, the proposed opto-audio cryptosystem correlation coefficient is the lowest one and nearly almost zero compared to the related state-of-the-art methods [22], [40]–[42]. Also, It is observed that the proposed opto-audio cryptosystem gives high NPCR and UACI values compared to the related state-of-the-art methods [22], [40]–[42].

VI. CONCLUSION

This paper has introduced an effective secure opto-audio cryptosystem that protects audio data. The proposed opto-audio cryptosystem is based on the XORing mask process, LASM scrambling, and the optical encryption using 2D-HT. Experimental investigations confirmed the vulnerability of the proposed opto-audio cryptosystem system with respect to statistical and differential attacks, known and chosen plaintext attacks, occlusion attack, AWGN and MWGN Attacks, and compression attack. The proposed scheme introduces a specific XORing mask process that enhances the security of the proposed opto-audio cipher. A standalone image database is used to improve data security, provide additional keys and monitor authentication. Experimental tests have confirmed that the proposed opto-audio cryptosystem have no effect on the quality of the decrypted audio.

REFERENCES

[1] E. M. Elshamy, E.-S.-M. El-Rabaie, O. S. Faragallah, O. A. Elshakankiry, F. E. Abd El-Samie, H. S. El-sayed, and S. F. El-Zoghdy, "Efficient audio cryptosystem based on chaotic maps and double random phase encoding," *Int. J. Speech Technol.*, vol. 18, no. 4, pp. 619–631, Dec. 2015.

[2] M. H. Elhoseny, S. O. Faragallah, E. H. H. Ahmed, B. H. Kazemian, S. H. El-sayed, and E. F. A. El-Samie, "The effect of fractional Fourier transform in encryption quality for digital images," *Optik-Int. J. Light Electron Opt.*, vol. 127, no. 1, pp. 315–319, 2016.

[3] H. M. Elhoseny, H. E. H. Ahmed, A. M. Abbas, H. B. Kazemian, O. S. Faragallah, S. M. El-Rabaie, and F. E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," *Signal, Image Video Process.*, vol. 9, no. 3, pp. 611–622, Mar. 2015.

[4] F. I. Elashry, S. O. Faragallah, M. A. Abbas, S. El-Rabaie, and E. F. A. El-Samie, "Homomorphic image encryption," *J. Electron. Imag.*, vol. 18, no. 3, 2009, Art. no. 033002.

[5] A. M. Elshamy, A. N. Z. Rashed, A. E.-N.-A. Mohamed, O. S. Faragalla, Y. Mu, S. A. Alshebeili, and F. E. El-Samie, "Optical image encryption based on chaotic baker map and double random phase encoding," *J. Lightw. Technol.*, vol. 31, no. 15, pp. 2533–2539, Aug. 1, 2013.

[6] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[7] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

[8] K. N. Nishchal, *Optical Cryptosystems*. Bristol, U.K.: IOP, 2019.

[9] M. A. Elshamy, E. F. A. El-Samie, S. O. Faragallah, M. S. Elshamy, S. H. El-Sayed, S. F. El-Zoghdy, N. Z. A. Rashed, A. A. El-Naser Mohamed, and Q. A. Alhamad, "Optical image cryptosystem using double random phase encoding and arnold's cat map," *Opt. Quantum Electron.*, vol. 48, no. 3, pp. 1–18, 2016.

[10] O. S. Faragallah and A. Afifi, "Optical color image cryptosystem using chaotic baker mapping based-double random phase encoding," *Opt. Quantum Electron.*, vol. 49, no. 3, pp. 1–28, Mar. 2017.

[11] X. Wang and D. Zhao, "Image encryption based on anamorphic fractional Fourier transform and three-step phase-shifting interferometry," *Opt. Commun.*, vol. 268, no. 2, pp. 240–244, Dec. 2006.

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

[13] L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Opt. Exp.*, vol. 14, no. 19, pp. 8552–8560, 2006.

[14] Z. Liu, J. Dai, X. Sun, and S. Liu, "Color image encryption by using the rotation of color vector in hartley transform domains," *Opt. Lasers Eng.*, vol. 48, nos. 7–8, pp. 800–805, Jul. 2010.

[15] J. Dou, Q. He, Y. Peng, Q. Sun, S. Liu, and Z. Liu, "A convolution-based fractional transform," *Opt. Quantum Electron.*, vol. 48, no. 8, pp. 400–407, Aug. 2016.

[16] N. Singh and A. Sinha, "Gyrator transform-based optical image encryption, using chaos," *Opt. Lasers Eng.*, vol. 47, no. 5, pp. 539–546, May 2009.

[17] M. Singh, A. Kumar, and K. Singh, "Encryption by using matrix-added, or matrix-multiplied input images placed in the input plane of a double random phase encoding geometry," *Opt. Lasers Eng.*, vol. 47, no. 11, pp. 1293–1300, Nov. 2009.

[18] Y. Zhang and B. Wang, "Optical image encryption based on interference," *Opt. Lett.*, vol. 33, no. 21, pp. 2443–2445, Nov. 2008.
[19] X. Peng, Z. Cui, L. Cai, and L. Yu, "Digital audio signal encryption with a virtual optics scheme," *Optik*, vol. 114, no. 2, pp. 69–75, 2003.
[20] S. K. Rajput and O. Matoba, "Optical voice encryption based on digital holography," *Opt. Lett.*, vol. 42, no. 22, pp. 4619–4622, 2017, doi: 10.1364/OL.42.004619.
[21] S. K. Rajput and O. Matoba, "Security-enhanced optical voice encryption in various domains and comparative analysis," *Appl. Opt.*, vol. 58, no. 11, pp. 3013–3022, 2019.
[22] J. B. Lima and E. F. da Silva Neto, "Audio encryption based on the cosine number transform," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8403–8418, Jul. 2016.
[23] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.
[24] K. Raghunandhan, D. Radhakrishna, K. Sudeepa, and A. Ganesh, "Efficient audio encryption algorithm for online applications using transposition and multiplicative non-binary system," *Int. J. Eng. Res. Technol.*, vol. 2, no. 6, pp. 472–477, 2013.
[25] R. Gnanajeyaraman, K. Prasadh, and D. Ramar, "Audio encryption using higher dimensional chaotic map," *Int. J. Recent Trends Eng.*, vol. 1, no. 2, pp. 103–107, 2009.
[26] S. M. S. Eldin, S. A. Khamis, A.-A.-I. M. Hassanin, and M. A. Alsharqawy, "New audio encryption package for TV cloud computing," *Int. J. Speech Technol.*, vol. 18, no. 1, pp. 131–142, Mar. 2015.
[27] X. Lu, Y. Cao, P. Lu, and A. Zhai, "Digital audio information hiding based on arnold transformation and double random-phase encoding technique," *Optik*, vol. 123, no. 8, pp. 697–702, Apr. 2012.
[28] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.
[29] J. D. Villasenor, "Optical hartley transforms," *Proc. IEEE*, vol. 82, no. 3, pp. 391–399, Mar. 1994.
[30] H.-E. Hwang, "An optical image cryptosystem based on Hartley transform in the fresnel transform domain," *Opt. Commun.*, vol. 284, no. 13, pp. 3243–3247, Jun. 2011.
[31] M. R. Abuturab, "Color image security system based on discrete Hartley transform in gyrator transform domain," *Opt. Lasers Eng.*, vol. 51, no. 3, pp. 317–324, Mar. 2013.
[32] Z. Liu, J. Dai, X. Sun, and S. Liu, "Optical color image hiding scheme based on chaotic mapping and Hartley transform," *Opt. Laser Eng.*, vol. 51, no. 8, pp. 967–972, 2013.
[33] R. N. Bracewellm, *The Hartley Transform*. Oxford, U.K.: Oxford Univ. Press, 1986.
[34] O. S. Faragallah, H. S. El-sayed, A. Afifi, and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Opt. Lasers Eng.*, vol. 137, Feb. 2021, Art. no. 106333.
[35] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, M. A. Alzain, J. F. Al-Amri, and F. E. A. El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," *IEEE Access*, vol. 8, pp. 103200–103218, 2020.
[36] P. Hedelin, F. Nordén, and J. Skoglund, "SD optimization of spectral coders," in *Proc. IEEE Workshop Speech Coding*, Jun. 1999, pp. 28–30.
[37] M. Alajmi, I. Elashry, H. S. El-Sayed, and O. S. Faragallah, "A password-based authentication system based on the CAPTCHA AI problem," *IEEE Access*, vol. 8, pp. 153914–153928, 2020.
[38] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-Sayed, E. A. Naeem, M. A. Alzain, J. F. Al-Amri, B. Soh, and F. E. A. El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," *IEEE Access*, vol. 8, pp. 42491–42503, 2020.
[39] M. Alajmi, I. Elashry, H. S. El-Sayed, and O. S. Farag Allah, "Steganography of encrypted messages inside valid QR codes," *IEEE Access*, vol. 8, pp. 27861–27873, 2020.
[40] F. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," *Procedia Comput. Sci.*, vol. 93, pp. 816–823, Jan. 2016.
[41] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, 2016.
[42] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.
[43] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.
[44] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012.
[45] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Nov. 2010.
[46] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
[47] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci.*, vol. 539, pp. 195–214, Oct. 2020.
[48] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.
[49] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.
[50] D. Renza, S. Mendoza, and D. M. Ballesteros L., "High-uncertainty audio signal encryption based on the collatz conjecture," *J. Inf. Secur. Appl.*, vol. 46, pp. 62–69, Jun. 2019.
[51] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[52] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft Comput.*, vol. 26, pp. 10–20, Jan. 2015.
[53] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.

OSAMA S. FARAGALLAH received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently a Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator, from 1997 to 2002, and has been an Assistant Lecturer, from 2002 to 2007. Since 2007, he has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. In 2015, he joined the Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya, Saudi Arabia. His current research interests include network security, cryptography, the Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, remote sensing, chaos theory, and mobile communications.

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