An asymmetric audio watermarking cryptosystem based on Fresnel transform

NEELAM[1], A. K. YADAV[2,*]
[1]*Department of Mathematics, Amity School of Applied Sciences, Amity University Haryana, Gurugram-122043, India*
[2]*Department of Mathematics, School of Basic Sciences, Central University of Haryana, Mahendergarh-123031, India*

In this paper, we present a secure audio watermarking scheme based on Fresnel transform. An input audio file is first converted to an image and then bonded with a random amplitude mask (RAM) followed by a Fresnel transform. The transformed image is subjected to phase truncation (PT) and phase reservation (PR) operation. Thereafter, 3D Lorenz chaotic system is applied on the PT part, and the PR part serves as the first decryption key. The resulting image is bonded with a random phase mask (RPM) followed by another Fresnel transform. The transformed image is subjected to another PT and PR operation. Finally, the phase truncated part is embedded in a host image to produce watermarked image, and the phase reserved part serves as the second decryption key. Fresnel transform parameters add to security of the proposed system. The proposed scheme is tested for its feasibility, and it shows robustness against known-plaintext attack (KPA), chosen-plaintext attack (CPA), and occlusion attack.

(Received May 17, 2022; accepted October 7, 2024)

Keywords: Fresnel propagation, Lorenz transform, Audio watermarking, Asymmetric cryptosystem

1. Introduction

With the rapidly growing information systems in the digital age, data security assumes critical importance. Cryptography allows us to design suitable algorithms for information security. In cryptography, encryption schemes to encrypt and decrypt data are generally classified as symmetric or asymmetric. In the last few decades, numerous image encryption systems have been developed. Double random phase encoding (DRPE) is the first optical image encryption scheme given by Refregier and Javidi in 1995 [1], in which an input image is encrypted into a white noise using Fourier transform. DRPE is a symmetric scheme in which encryption and decryption keys are the same. Thereafter, many symmetric schemes were developed based on mathematical transforms such as Fresnel transform [2], Gyrator transform [3-5], fractional Mellin transform [6], fractional Hartley transform [7]. But later on, it was found that due to its linearity, DRPE is vulnerable to known-plaintext attack (KPA), chosen-plaintext attack (CPA), chosen-ciphertext attack (CCA), ciphertext only attack (COA) [8-10]. To overcome linearity of the symmetric schemes, phase truncated Fourier transform (PTFT) based scheme was proposed as the first asymmetric (nonlinear) scheme, in which encryption and decryption keys are different [11]. After that, many asymmetric schemes have been developed using mathematical transforms such as fractional Hartley transform [12], Gyrator transform [13-15], and Fourier transform [16]. But later it was found that some asymmetric schemes are vulnerable to special attack [17,18]. Many symmetric and asymmetric schemes have also been proposed for watermarking in the past few years [19-24].

Digital watermarking is a process of hiding information. There are mainly two processes in watermarking: embedding and extraction. Watermarking is a technique in which watermark data is embedded into digital multimedia such as audio, video and images. In 1992, 'Digital Watermark' was first created by Andrew Tirkel and Charles Osborne [25]. Digital watermarking is used for purposes such as data authentication and identification, broadcast monitoring, copyright protection, and temper detection. Watermarking schemes are desired to have large capacity, robustness and good imperceptibility. Several symmetric and asymmetric watermarking schemes have been reported in the literature. Singh et al. [26] proposed a DRPE-based digital watermarking scheme using gyrator transform and chaotic random phase masks. Vashisth et al. [27] proposed an asymmetric watermarking scheme in gyrator domain. A number of watermarking schemes, reported in the literature, are based on various mathematical transforms such as discrete cosine transform (DCT), fractional Fourier transform (FrFT), Fresnel transform (FrT). Arora et al. [28] have used jigsaw transform in discrete cosine transform to watermark an image. Li et al. [29] designed a watermarking algorithm based on DCT and FrFT in an invariant wavelet domain. Yadav et al. [30] proposed a watermarking scheme in gyrator domain for phase images using devil's vortex Fresnel lens (DVFL). Kang et al. [31] presented a watermarking technique based on Fresnel transform. The usage of Fresnel transform helps to increase the number of keys and provides extra security. James et al. [32] proposed a linear Fresnel transform and its applications. There are a number of schemes based on FrT. Yadav et al. [33] proposed an asymmetric cryptosystem based on Fresnel transform and Arnold transform using structured phase mask. Abuturab [34] presented a colour image encryption

scheme based on high- dimension chaotic random phase mask in Fresnel domain.

In digital communication, massive amount of data gets transferred, out of which a significant amount is in the form of audio. That is why audio encryption is essential for security purposes. Recently, a few schemes have been reported on audio encryption techniques. Anjana et al [35] proposed an asymmetric audio encryption scheme based on Arnold transform and random decomposition in Fourier domain. Faragallah [36] proposed a secure audio watermarking scheme using LSB watermarking and AES (Advanced Encryption Standard) or RC6. Suresh et al [37] proposed an audio watermarking scheme based on discrete wavelet transform (DWT), discrete cosine transform (DCT) and singular value decomposition (SVD). Farzaneh and Toroghi [38] presented an audio watermarking algorithm using graph-based transform and SVD.

The present work reported in this paper deals with asymmetric audio watermarking scheme in Fresnel transform domain. First, we take an audio file and convert it into a phase image of size 256x256 pixels bonded with Random Amplitude Mask (RAM). In the watermarking process an input image is converted to a phase image which gives better security to the proposed scheme. After that, to obtain watermarked image we applied the Fresnel transform and 3D Lorenz chaotic system and embeded the resulting encrypted image into a host image. The parameters of Fresnel transform provide extra security to our scheme. All the simulation results are performed on MATLAB R2021a.

The proposed work assumes importance due to asymmetry in the watermarking cryptosystem for audio signals. Such an approach in Fresnel domain has not been reported so far. Application of 3D Lorenz transform, based on chaos theory provides additional security. This adds to the attempts to develop a secure cryptosystem for audio watermarking.

2. Background

2.1. Fresnel transform

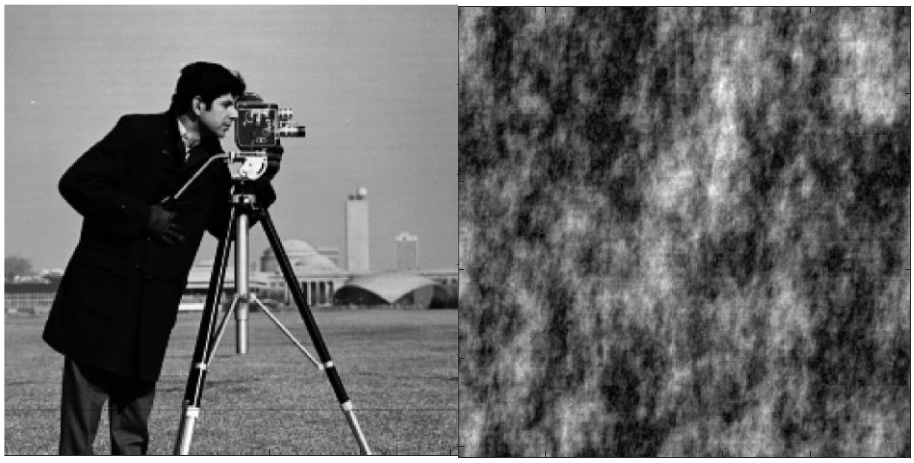
Fresnel transform is a two-dimensional linear canonical transform [33,34]. The Fresnel transform (FrT) of an input image I (x, y) is mathematically defined as [31]

$$\mathrm{f}\,(x_0, y_0) = FrT_{\lambda,z}\ \{\mathrm{I}\ (\mathrm{x},\ \mathrm{y})\} = \iint_{-\infty}^{+\infty} I(x,y)\ h_{\lambda,z}(x_0, y_0, x, y)dxdy \tag{1}$$

where $FrT_{\lambda,z}$ denotes the Fresnel transform, λ is wavelength, and z is the propagation distance. Coordinates of the input image and the output (transformed) image are denoted by (x, y) and (x_0, y_0) respectively. The kernel $h_{\lambda,z}$ of the Fresnel transform is expressed as

$$h_{\lambda,z}(x_0, y_0, x, y) = \frac{\exp\left(\frac{i2\pi z}{\lambda}\right)}{\sqrt{i\lambda z}} \exp\left[\frac{i\pi}{z\lambda}(x_0 - x)^2 + (y_0 - y)^2\right] \tag{2}$$

In Fresnel transform, λ and z are the two parameters which will serve as extra keys in the proposed scheme. Such additional parameters enhance the security of the system.



(a) *(b)*

Fig. 1. (a) Grayscale cameraman image of size 256 x256 pixels, (b) Fresnel transformed image (λ = 632.8nm, propagation distance d_1 = 20mm and d_2 = 30mm)

2.2. 3D Lorenz chaotic system

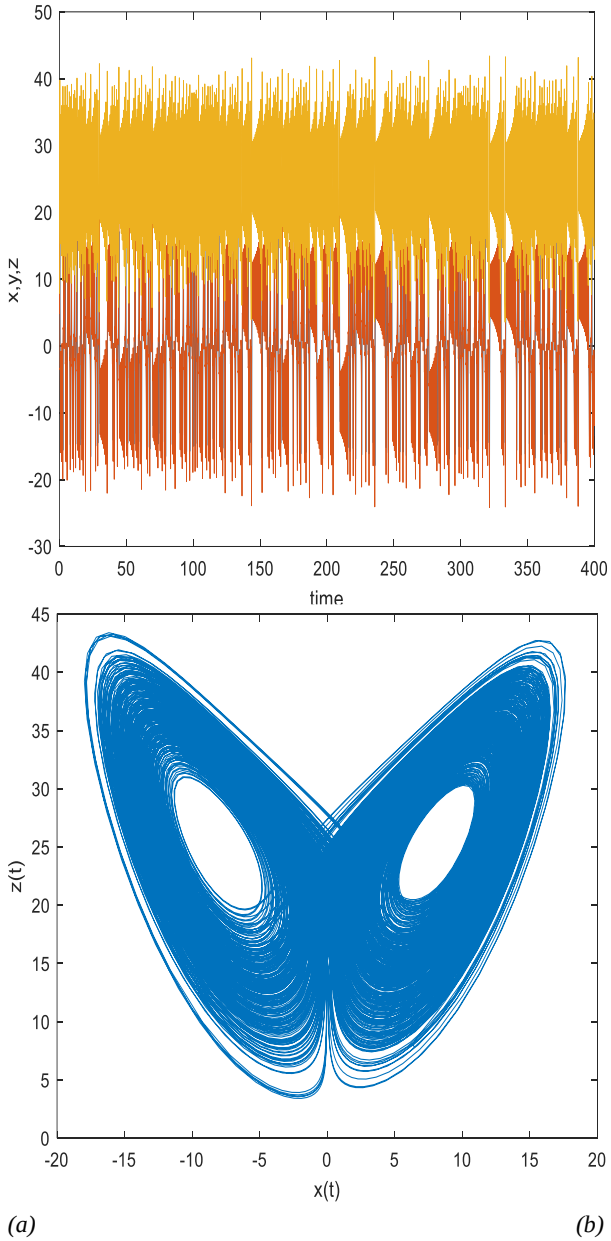
The basic principle of 3D Lorenz chaotic system is described here. In 1963, Edward N Lorenz proposed three coupled ordinary differential equations [39]

$$\frac{dx}{dt} = \sigma(y\text{-}x) \tag{3}$$

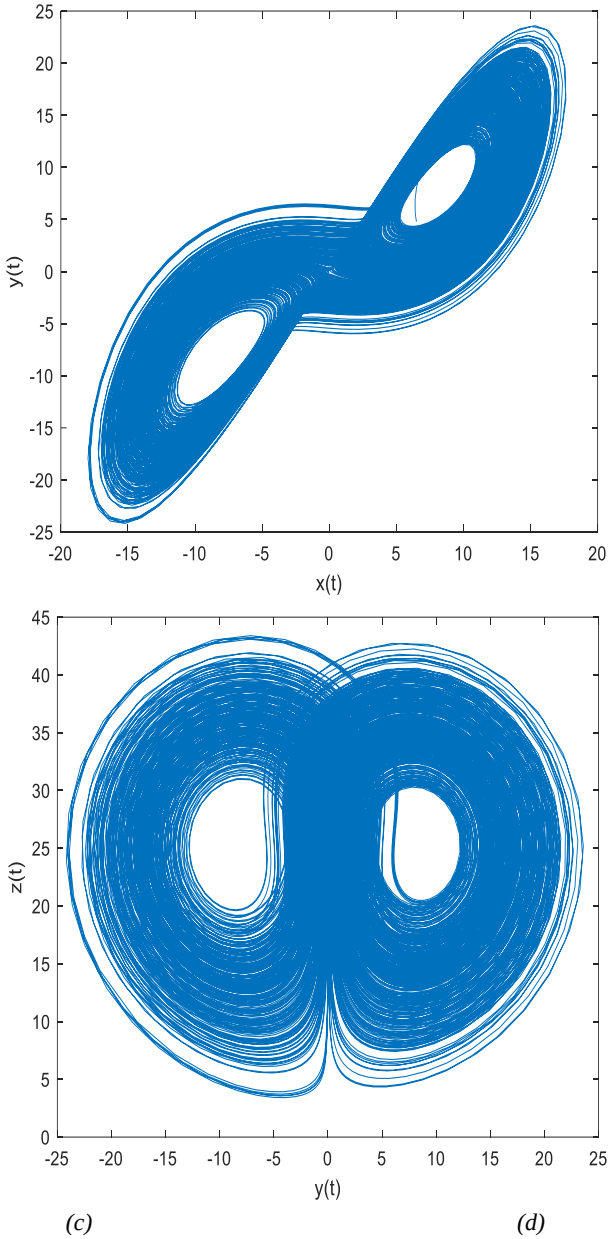
$$\frac{dy}{dt} = rx - y - xz \tag{4}$$

$$\frac{dz}{dt} = xy - bz \tag{5}$$

where σ, r, and b are Lorenz parameters with initial conditions $x_0, y_0, and\ z_0$. The values of Lorenz parameters are taken as σ = 26.456, r = 10, b = 8/3, and initial values of x, y, and z serve as secret keys [40-42].



(a) (b)



(c) (d)

Fig. 2. (a) Time series of x, y, and z plane; (b) projection of phase plot in x-z plane; (c) x-y plane; (d) y-z plane with σ = 26.456, r = 10 and b = 8/3 (color online)

3. Watermarking scheme

The watermarking scheme proposed in this paper is shown as a flowchart in Fig.3. The corresponding encryption and decryption processes are described in section 3.1 and 3.2 respectively.

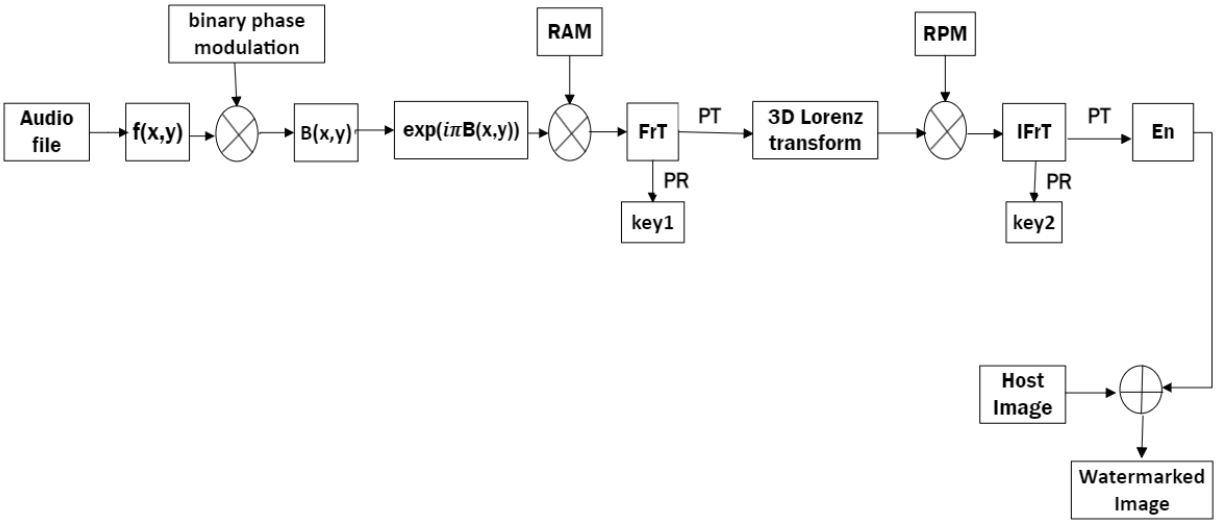


Fig. 3. Flowchart of encryption process

3.1. Encryption process

The encryption process for an input audio file is illustrated with the following steps:

Step 1. First, we capture an audio file of size Nx1 and convert it to a 2D image f (x, y) of size a x b pixels, where a x b =N. Simultaneously, a matrix A is constructed whose elements take a value -1 if the corresponding pixel value of f (x, y) is less than zero, otherwise take a value 1. This process is referred to as binary phase modulation. Thereafter, we multiply the matrix A(x,y) and f(x,y) to obtain B(x,y). Image B(x,y) will serve as the input image in the scheme. It is converted to a phase image and then bonded with random amplitude mask (RAM) to give a complex image I(x,y).

$$I(x,y) = RAM.* \exp(i\pi B(x,y)) \quad (6)$$

Step 2. Fresnel transform (FrT) is applied on the resulting complex image I(x,y). The transformed image is subjected to phase truncation (PT) and phase reservation (PR) operations. PR will provide the first decryption key (key1).

$$I1 = PT\{FrT(I(x,y))\} \quad (7)$$

$$key1 = PR\{FrT(I(x,y))\} \quad (8)$$

Step 3. Apply 3D Lorenz transform on the phase truncated part, and the resulting image is bonded with a random phase mask (RPM).

$$I2 = \{(3D\ Lorenz\ transform\ (I1)).*RPM\} \quad (9)$$

Step 4. Inverse Fresnel transform (IFrT) is applied on the resulting image of step 3. This is followed by another phase truncation operation. The phase truncated part (PT) gives the encrypted image and the phase reserved (PR) will serve as the second decryption key (key2).

$$En = PT\{IFrT(I2)\} \quad (10)$$

$$key2 = PR\{IFrT(I2)\} \quad (11)$$

Step 5. The resulting encrypted image (En) is embedded in a host image A (x, y) with an attenuation factor α to give a watermarked image E. The attenuation factor α is chosen arbitrarily.

$$E = A\ (x, y) + \alpha.En \quad (12)$$

3.2. Decryption process

The steps of the decryption process are described as follows:

Step 1. The decryption process starts with extraction of host image A (x, y) from the watermarked image E using the equation

$$D = (E - A\ (x, y))\ /\alpha \quad (13)$$

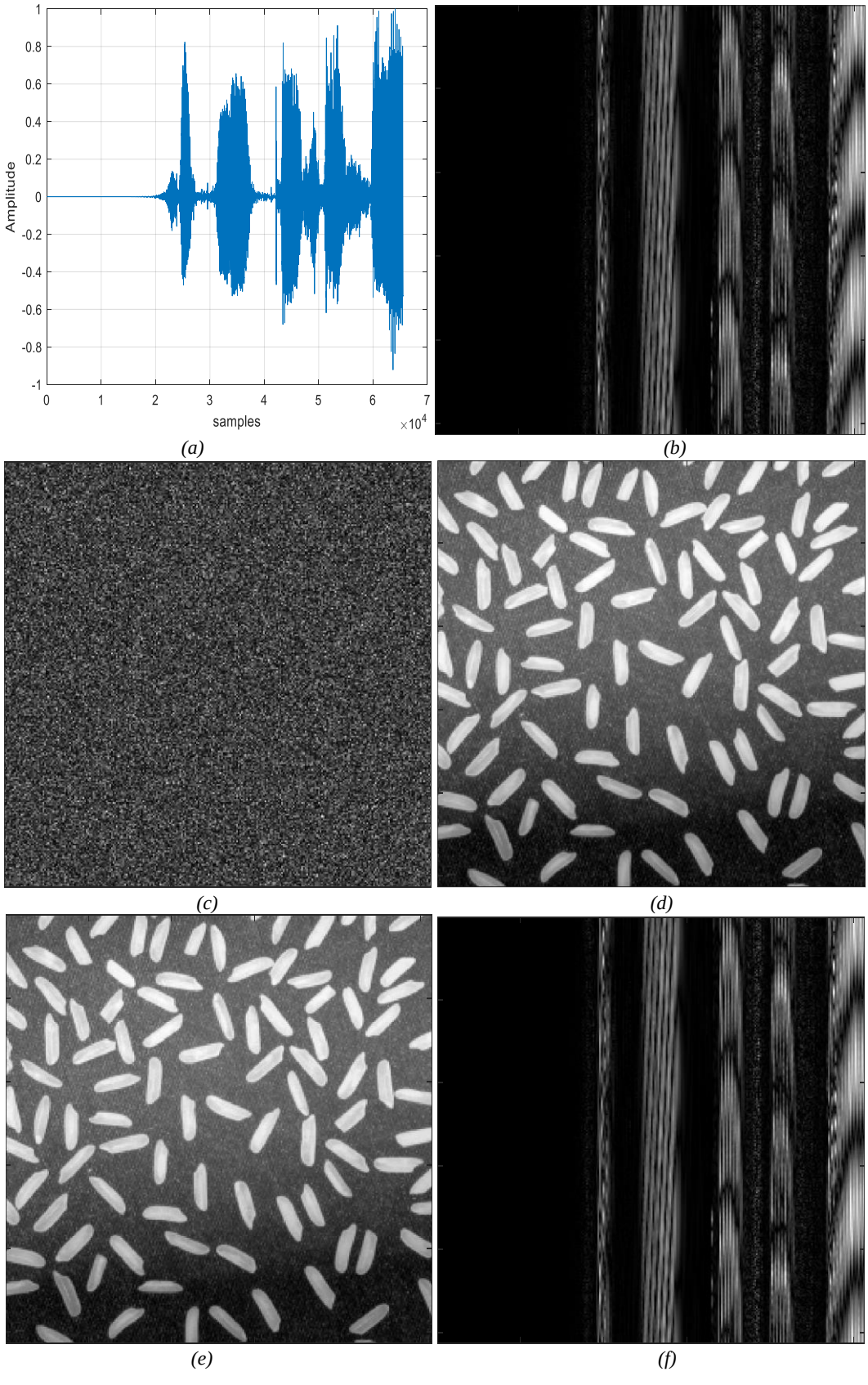
Step 2. The second private key (key2) is combined with D which is then subjected to Fresnel transform to give

$$D1 = abs\ (FrT(D.*key2)) \quad (14)$$

Step 3. In this step, inverse 3D Lorenz transform is applied on D1. Thereafter, the first private key (key1) is combined with it and followed by taking inverse Fresnel transform. The phase part of the resulting image provides the original input image.

F = angle {IFrT ((Inverse 3D Lorenz (D1)).*key1) (15)

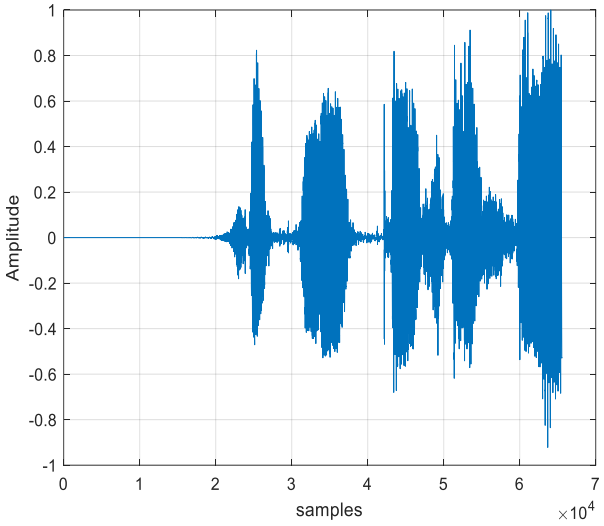
Step 4. Finally, the recovered image is subjected to reverse operations to get the original audio file.



(a) *(b)*

(c) *(d)*

(e) *(f)*

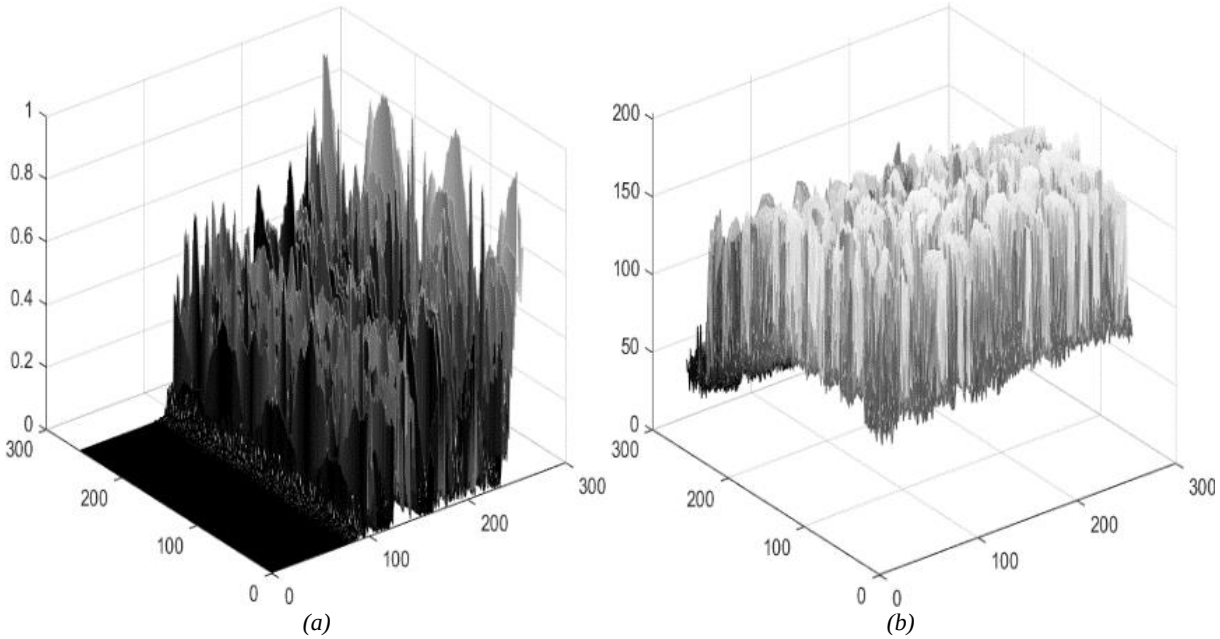


(g)

Fig. 4. Encryption and decryption process of audio watermarking algorithm; (a) Input audio signal; (b) Image corresponding to input audio converted to a ✗ b image; (c) Encrypted image (En); (d) Host image; (e) Watermarked image; (f) Recovered input image; (g) Recovered audio signal (color online)

4. Results and discussion

Numerical simulation of the proposed watermarking scheme is performed using MATLAB R2021a. In the scheme, first we consider an audio file (Fig. 4a) which is converted into an image of size a $\times$ b pixels (Fig. 4b). All the simulation results are performed on the input image (Fig. 4b). For watermarking, we take a host image of size 256 $\times$ 256 pixels (Figure 4d). The values of parameters of Fresnel transform are taken as follows: wavelength λ = 632.8nm, propagation distance d_1= 20mm and d_2= 30mm. Performance of the proposed watermarking scheme is evaluated through statistical metrices such as correlation coefficient, information entropy, histogram analysis, and peak signal-to-noise ratio (PSNR). The robustness of the system is tested against occlusion attack and recovery attack.



(a) *(b)*

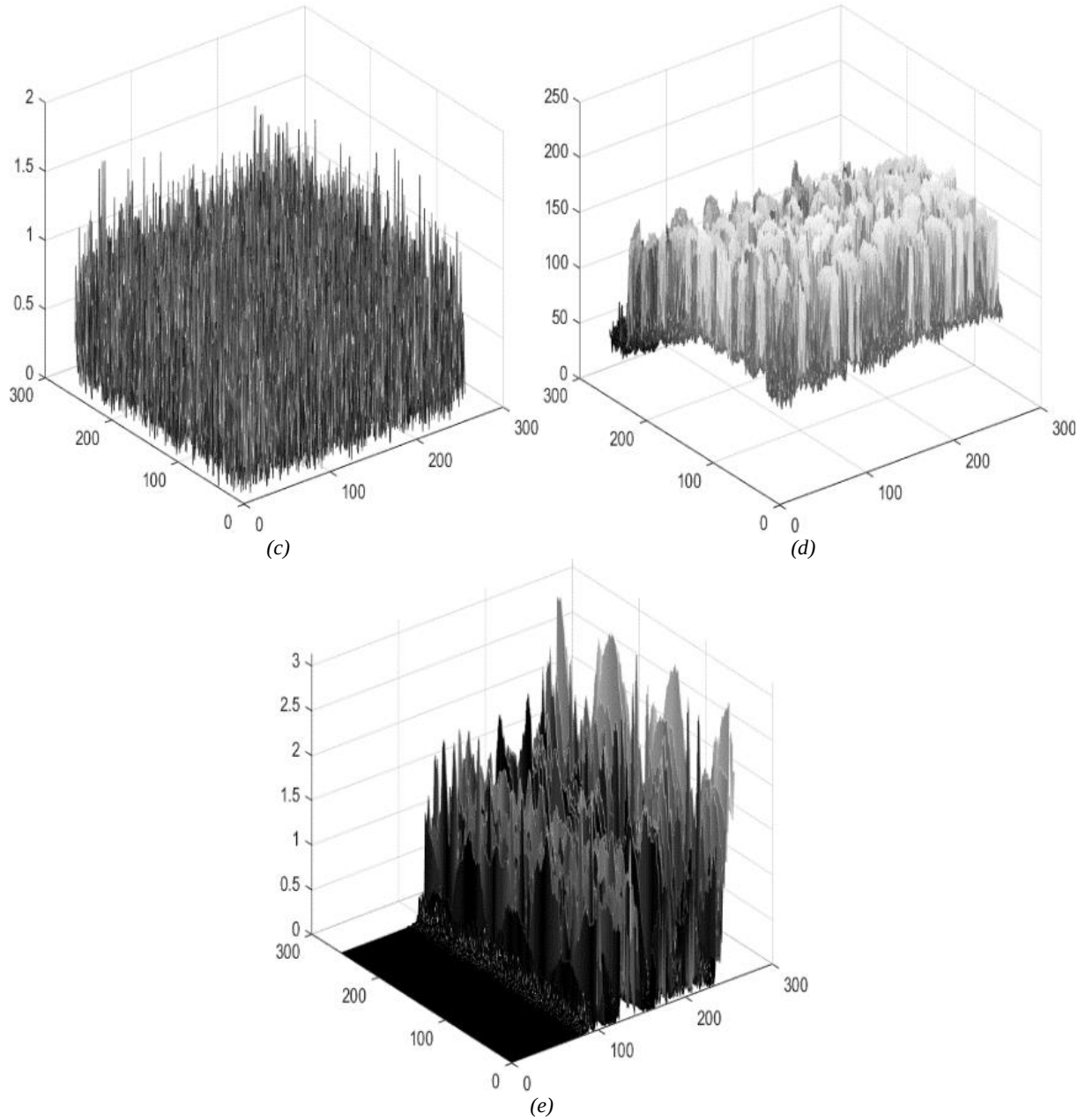


Fig. 5. 3D plots of (a) Input image; (b) Host image; (c) Encrypted image; (d) Watermarked image; (e) Recovered original image

4.1. Information entropy (IE)

Information Entropy [42] is used to determine the randomness of the information stored in the given data. The value of entropy for grayscale images lies in the range [0, 8], the ideal value for encrypted image being 8. If the value of entropy is high, it is very difficult to recover the information by an attacker. Mathematically, it is defined as

$$E(x) = -\sum_{i=1}^{M} P(x_i) log_2 P(x_i) \quad (16)$$

where E(x) denotes the entropy of source 'x' and $P(x_i)$ is the probability of x_i.

In our proposed scheme, entropy of the input image is 5.3827 and entropy of the corresponding encrypted image is 7.7284 which is very close to 8. This value shows the randomness of the encrypted image, which is very high and signifies high quality of encryption. This indicates that the proposed system is robust and the randomness of pixels is quite apparent in the encrypted image.

4.2. Histogram plots

Analysis of histograms and 3D plots [43] have been performed to check the effectiveness of the proposed audio watermarking scheme. Fig. 5 (a-d) shows the 3D plots of the input image (which is converted from the audio file), host image, encrypted image, watermarked image, recovered the image. From Fig. 5(a) and 5(e), it is observed that plots of the input image and the recovered image are quite similar. Fig. 5(d) shows 3D plot of the watermarked image which is completely different from Fig. 5(a). It may be noted that 3D plots represent both the position and the pixel values.

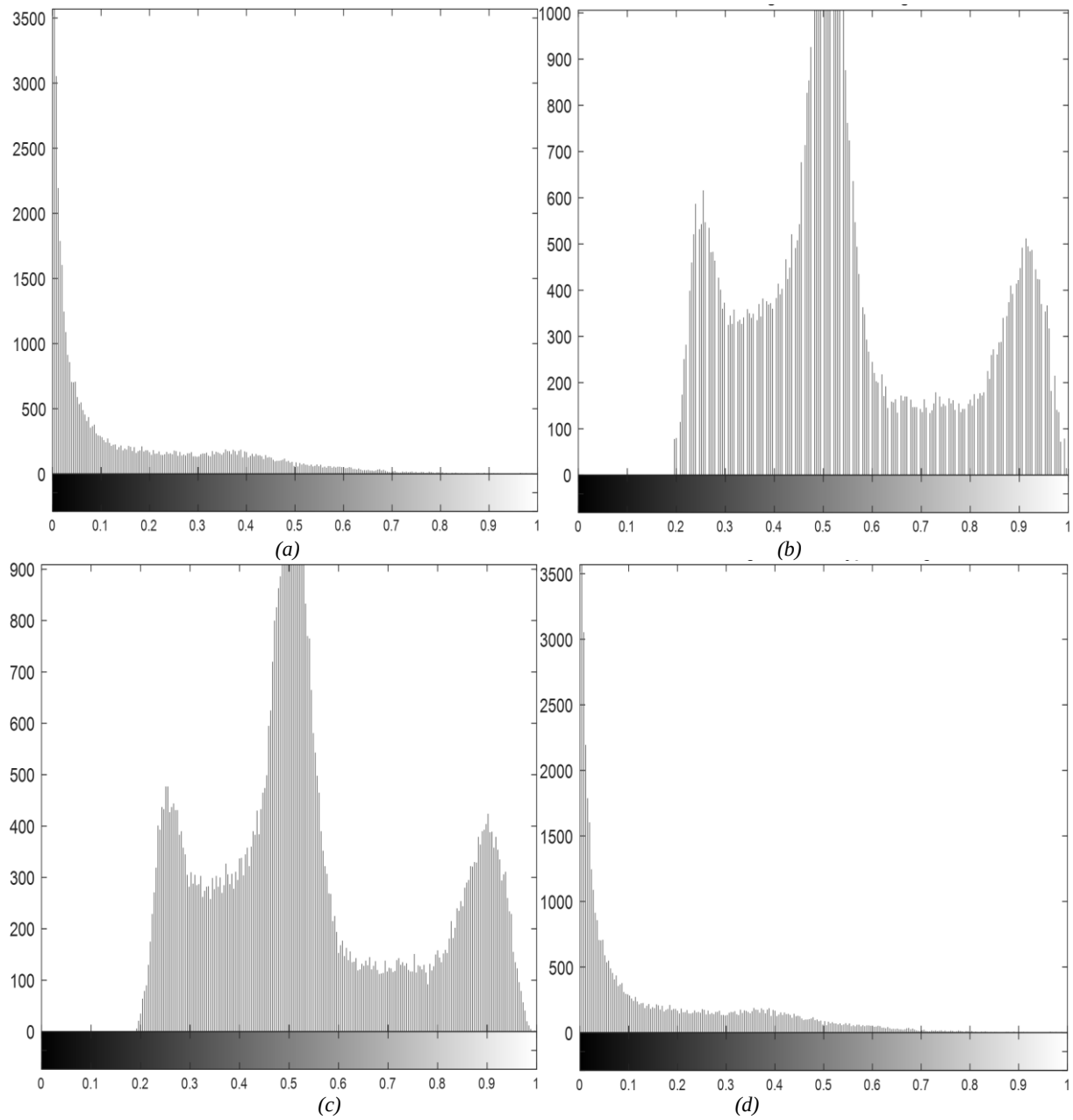


Fig. 6. Histogram plots of (a) input image; (b) host image; (c) watermarked image; (d) recovered image

Fig. 6(a-d) shows the histogram plots of the input image (corresponding to the input audio file), host image, watermarked image, recovered image. Fig. 6(a) and 6(d) show that both the histograms are quite similar. Fig. 6(a) and 6(c) show that the histograms of the input image and the corresponding encrypted image are quite different, showing the quality of encryption obtained from the proposed watermarking scheme. Due to complete dissimilarity in histograms of the input image and its encrypted image, it is nearby impossible to get any hint of the input image from the corresponding encrypted image. Thus, attackers cannot get any information about the input image from the histogram analysis.

4.3. Correlation coefficient

Correlation coefficient is a commonly used statistical metric to determine correlation between adjacent pixels of an image in horizontal, vertical or diagonal directions. In the present watermarking scheme, we have randomly selected a pair of 15000 adjacent pixels in the horizontal direction. Mathematically, correlation coefficient (CC) is defined as

$$\mathrm{CC} = \frac{cov(x,y)}{\sigma(x)\sigma(y)} \tag{17}$$

$$\text{cov(x,y)} = \frac{1}{N}\sum_{i=1}^{N}[(x_i - \bar{x})(y_i - \bar{y})] \quad (18)$$

$$\sigma(\text{x}) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2} \quad (19)$$

$$\sigma(\text{y}) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2} \quad (20)$$

where cov(x, y) is the covariance between samples x and y, which represent coordinates of an image. N is the number of pixel pairs (x_i, y_i). Here, σ(x) and σ(y) are the standard deviation of x and y, $\bar{x}$ and $\bar{y}$ denote the mean of x_i and y_i pixel values.

Fig. 7(a) shows the plot of correlation distribution of randomly selected 15000 pairs of adjacent pixels of the input image in horizontal direction. A high degree of correlation is observed in the plot. Fig. 7(b) shows the corresponding plot of correlation distribution of the encrypted image, which is clearly different from the correlation distribution of the input image. Fig. 7(d) shows the correlation plot of the watermarked image which is weakly correlated with pixels spread out in both the directions. The proposed watermarking scheme is providing highest CC value which is 1. From the plots of correlation-distribution we can see that the pixels in the watermarked image are weakly correlated and shows resistance against statistical attack. Further, it is worth observing similarity in correlation distribution plots of the host image and the watermarked image in Fig. 7(c) and Fig. 7(d) respectively.

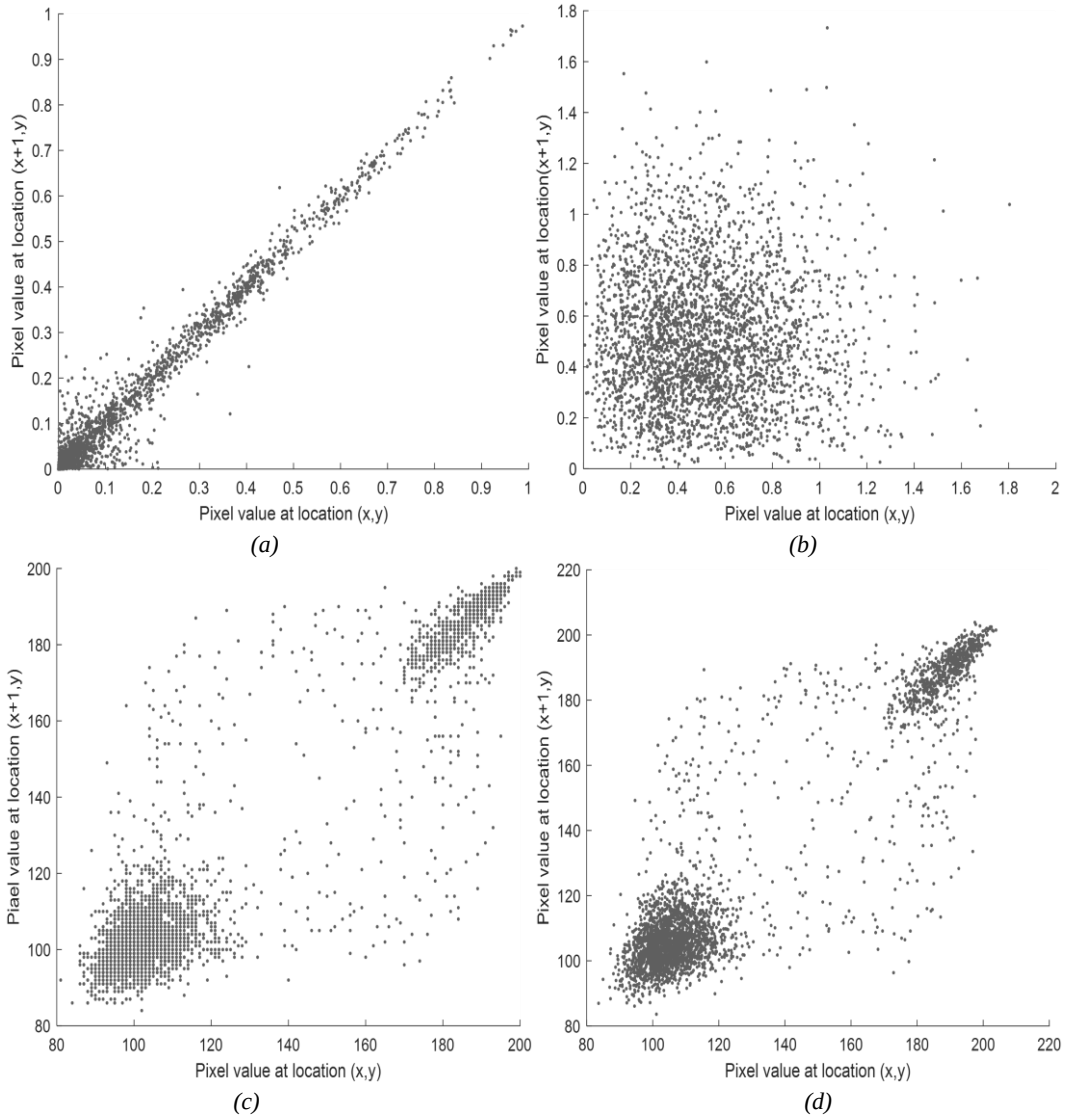


Fig. 7. Correlation distribution plots in horizontal direction of (a) Input image, (b) its corresponding encrypted image, (c) Host image and (d) Watermarked image

4.4. Peak signal-to-noise ratio (PSNR)

PSNR (Peak Signal-to-Noise Ratio) [44] is used to check the pixel quality measurement between input image and decrypted image. Mathematically, it is defined as

$$\text{PSNR}=10*log_{10}x\left\{\frac{255^2}{\frac{1}{MxN}\sum_{x=1}^{M}\sum_{y=1}^{N}|I(x,y)-E(x,y)|^2}\right\} \quad (21)$$

where I(x,y) and E(x,y) are the input and the decrypted images respectively. PSNR value of the proposed watermarking scheme is 55.4406.

4.5. Occlusion attack

Occlusion attack analysis is performed to check the robustness of the scheme against occlusion attack on the watermarked image. In the occlusion attack some part of the watermarked (encrypted) image is made unavailable by occluding it and then we analyse the impact of loss of information on retrieval of the input image. Fig. 8 shows PSNR plot versus occluded area. It is observed that as the area of occlusion increases the value of PSNR decreases [45,46]. Smaller value of PSNR shows that the loss of information is large. The variation of PSNR clearly indicates the robustness of the scheme to the occlusion attack.

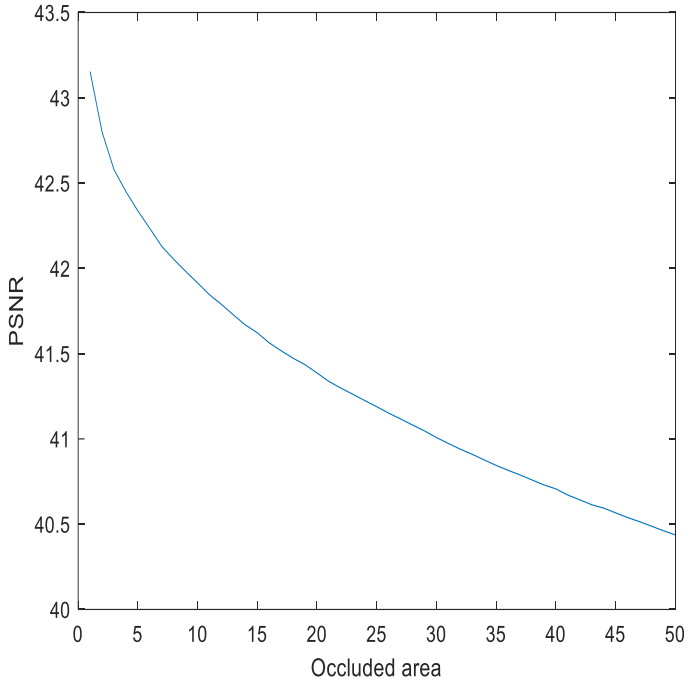


Fig. 8. A plot of PSNR versus occluded area (color online)

4.6. Comparison with other schemes

The present scheme is primarily developed for audio watermarking in Fresnel domain and is assymetric in structure. Thus, it is fair to attempt its comparison with similar schemes at least with the same objective of audio watermarking. However, a broad comparison of recently reported audio encryption and watermarking schemes with the proposed scheme is presented in the Table 1.

Table 1. Comparison of the proposed scheme with other similar schemes

S.No.	Scheme	Features
1	Anjana et al. [35]	Asymmetric, Arnold, Random Decomposition, Fourier Transform
2	Faragallah [36]	LSB Watermarking, Advanced Encryption Standard, RC6
3	Suresh et al. [37]	Discrete Wavelet Transform, Discrete Cosine Transform, Singular Value Decomposition
4	Faragallah and Toroghi [38]	Graph Based Transform, Singular Value Decomposition
5	Present Scheme	Fresnel Transform, 3D Lorenz Transform

5. Conclusions

In this study, we have proposed an asymmetric audio watermarking scheme using Fresnel transform. Also, the scheme has used chaos theory based 3D Lorenz transform in the frquency domain. The validity, feasibility and security analysis of the scheme is performed through the numerical simulations using MATLAB R2021a. The proposed scheme shows resistance against statistical attacks as seen from entropy analysis, histogram analysis, correlation distribution and 3D plots. The asymmetric nature of proposed watermarking scheme makes it immune to other attacks like KPA and CPA. This scheme also resists occlusion attack, thus indicating robustness of the watermarking scheme. A comparison of the proposed scheme with existing audio watermarking/encryption schemes has been presented. The Fresnel transform parameters provides extra security to the system by increasing the keyspace.

References

[1] P. Refregier, B. Javidi, Optics Letters **20**, 767 (1995).
[2] G. Situ, J. Zhan, Optics Letters **29**, 1584 (2004).
[3] J. A. Rodrigo, T. Alieva, M. L. Calvo, Optics Express **15**, 2190 (2007).
[4] H. Li, Optics and Lasers in Engineering **47**, 45 (2009).
[5] M. R. Abuturab, Applied Optics **51**, 3006 (2012).
[6] N. R. Zhou, Y. Wang, L. Gong, Optics Communication **284**, 3234 (2011).
[7] C. Jimenez, C. Torres, L. Mattos, Journal of Physics: Conference Series **274**, 012041 (2011).
[8] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, Optics Express **15**, 10253 (2007).
[9] X. Peng, P. Zhang, H. Wei, B. Yu, Optics Letters **31**(8), 1044 (2006).
[10] H. Tashima, M. Takeda, H. Suzuki, T. Obi, M. Yamaguchi, N. Ohyama, Optics Express **18**(13), 13772 (2010).
[11] W. Qin, X. Peng, Optics Letters **35**, 118 (2010).
[12] A. K. Yadav, P. Singh, I. Saini, K. Singh, Journal of Modern Optics **66**(6), 629 (2018).
[13] M. R. Abuturab, Optics and Lasers in Engineering **58**, 39 (2014).
[14] H. Chen, C. Tanougast, Z. Liu, L. Sieler, Optics and Lasers in Engineering **93**, 1 (2017).
[15] M. R. Abuturab, Optics and Lasers in Engineering **69**, 49 (2015).
[16] S. Anjana, I. Saini, P. Singh, A. K. Yadav, Advances in Intelligent Systems and Computing **706**, 29 (2018).
[17] X. Wang, D. Zhao, Optics Communications **285**(6), 1078 (2012).
[18] X. Wang, Y. Chen, C. Dai, D. Zhao, Applied Optics **53**(2), 208 (2014).
[19] N. Jayashree, R. S. Bhuvaneswaran, Computers Materia and Continua **58**(1), 263 (2019).
[20] O. P. Singh, A. K. Singh, G. Srivastava, N. Kumar, Multimedia Tools and Applications **80**(20), 30367 (2020).
[21] S. Yuan, D. A. Magayane, X. Liu, X. Zhou, G. Lu, Z. Wang, H. Zhang, Z. Li, Optics Communications **482**, 126568 (2021).
[22] G. Qu, X. Meng, X. Yang, H. Wu, P. Wang, W. He, H. Chen, Optics and Lasers in Engineering **137**, 106376 (2021).
[23] P. Singh, A. K. Yadav, K. Singh, I. Saini, Journal of Optoelectronics and Advanced Materials **21**, 484 (2019).
[24] Q. Guo, Z. Liu, S. Liucora, Optics Communications **284**, 3918 (2011).
[25] A. Z. Tirkel, G. A. Rankin, R. M. Van Schyndel, W. J. Ho, N. R. A. Mee, C F Osborne, DICTA 93, Macquarie University, 666 (1992).
[26] N. Singh, A. Sinha, Optik **121**, 1427 (2010).
[27] S. Vashisth, A. K. Yadav, H. Singh, K. Singh, Proceedings of SPIE - The International Society for Optical Engineering **9654**, 96542E (2015).
[28] M. Arora, M. Khurana, Optical and Quantum Electronics **52**, 59 (2020).
[29] Y. M. Li, D. Wei, L. Zhang, Information Sciences **551**, 205 (2021).
[30] A. K. Yadav, S. Vashisth, H. Singh, K. Singh, Optics Communications **344**, 172 (2015).
[31] S. Kang, Y. Aoki, Proceedings IEEE International Conference on Multimedia Computing and Systems **1**, 625 (1999).
[32] D. F. V. James, G. S. Agarwal, Optics Communications **126**, 207 (1996).
[33] S. Yadav, H. Singh, IET Image Processing, **15**(5), (2021).
[34] M. R. Abuturab, Optics and Lasers in Engineering **129**, 106038 (2020).
[35] S. Anjana, P. Singh, A. K. Yadav, K. Singh, Asian Journal of Physics **27**, 637 (2018).
[36] O. S. Faragallah, Wireless Personal Communications **98**, 2009 (2018).
[37] G. Suresh, N. V. Lalitha, Ch. S. Rao, V. Sailaja, International Conference on Devices, Circuits and Systems, IEEE 177 (2012).
[38] M. Farzaneh, R. M. Toroghi, International Symposium on Telecommunications (IST) IEEE, 137 (2020).
[39] Edward N. Lorenz, Journal of the Atmospheric Sciences **20**, 130 (1963).
[40] H. Singh, Optics and Lasers in Engineering **81**, 125 (2016).
[41] N. Sharma, I. Saini, A. K. Yadav, P. Singh, 3D Research **8**, 39 (2017).
[42] V. Kumar, A. Girdhar, Multimedia Tools and Applications **80**(3), 3749 (2020).
[43] P. Yadav, H. Singh, 3D Research **9**, 20 (2018).
[44] M. Kaur, V. Kumar, Archives of Computational Methods in Engineering **27**(1), 15 (2020).
[45] P. Rakheja, R. Vig, P. Singh, Optik **176**, 425 (2019).
[46] E. Kumari, S. Mukherjee, P. Singh, R. Kumar, Results in Optics **1**, 100009 (2020).

*Corresponding author: akyadav@cuh.ac.in