Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.024375
Article

Tech Science Press

Optical Ciphering Scheme for Cancellable Speaker Identification System

Walid El-Shafai[1,2], Marwa A. Elsayed[1], Mohsen A. Rashwan[3], Moawad I. Dessouky[1], Adel S. El-Fishawy[1], Naglaa F. Soliman[4], Amel A. Alhussan[5,*] and Fathi E. Abd El-Samie[1]

[1]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[2]Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh, 11586, Saudi Arabia
[3]Department of Electronics and Communications, Faculty of Engineering, Cairo University, Cairo, Egypt
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, 11671, Saudi Arabia
[5]Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
*Corresponding Author: Amel A. Alhussan. Email: aaalhussan@pnu.edu.sa
Received: 15 October 2021; Accepted: 23 March 2022

Abstract: Most current security and authentication systems are based on personal biometrics. The security problem is a major issue in the field of biometric systems. This is due to the use in databases of the original biometrics. Then biometrics will forever be lost if these databases are attacked. Protecting privacy is the most important goal of cancelable biometrics. In order to protect privacy, therefore, cancelable biometrics should be non-invertible in such a way that no information can be inverted from the cancelable biometric templates stored in personal identification/verification databases. One methodology to achieve non-invertibility is the employment of non-invertible transforms. This work suggests an encryption process for cancellable speaker identification using a hybrid encryption system. This system includes the 3D Jigsaw transforms and Fractional Fourier Transform (FrFT). The proposed scheme is compared with the optical Double Random Phase Encoding (DRPE) encryption process. The evaluation of simulation results of cancellable biometrics shows that the algorithm proposed is secure, authoritative, and feasible. The encryption and cancelability effects are good and reveal good performance. Also, it introduces recommended security and robustness levels for its utilization for achieving efficient cancellable biometrics systems.

Keywords: Cancellable biometrics; jigsaw transform; FrFT; DRPE; speaker identification

1 Introduction

Speech is the principal mode of communication among human beings and the most natural and efficient way of exchanging information between human beings. Speaker identification is the process of recognizing an individual from voice biometrics. Unlike other biometrics, voice-based biometric traits cannot be captured without the speaker's awareness. The best-known commercialized form of voice biometrics is speaker recognition.

The speaker recognition system has various applications [1], such as voice dialing, voice mail, IM services, confidential information security, and web access control. More security is needed because of the wide range of speaker recognition applications. Speech signals are therefore required to be encrypted. Password and identification cards are well-known traditional security systems that can be broken easily. Using biometric features has added many benefits to traditional verification methods and it avoids many threats. Biometrics is the oldest known document in the history of China, Egypt, and Ancient Babylon. Recently, biometric recognition systems have become a significant processing field for many applications, especially in security [2–4].

Biometric recognition refers to the automatic identification of persons based on their biological and behavioral features (for example, face, fingerprints, iris, palm/finger vein, voice) [5]. Biometrics are the main reliable solution for some applications, such as border checking, forensics, covert surveillance, and deduplication of identity). Furthermore, in applications that require claimed identity verification, such as access control, financial transactions, etc., biometrics is compatible with or complements traditional authentication mechanisms. At the same time, the growth of biometric systems in authentication applications is hampered by different attack factors [6].

A template comprises a compact representation of the sensitive biometric features containing the most important discriminatory data necessary for person recognition [7]. The fact that biometrics are irreplaceable in nature obscures this threat. Unlike passwords, the exposed template cannot be discarded, and the user can be re-enrolled based on the same trait. This may seriously affect the privacy of individuals enrolled in biometric systems. Biometric authentication systems have been widely deployed due to the usability of identity management. For example, biometric information disclosure can result in the exposure of sensitive personal data. A parametric, irreversible, and revocable transformation is used to safeguard the confidentiality and security of the biometric templates [8–11].

Security systems based on biometric cryptosystems create a secure token by generating a key from biometric information called Helper Data [12]. Therefore, most biometric cryptosystems require a database to store helper data used in the verification process. According to how helper data are obtained, these systems are categorized as Key-Binding and Key-Generation systems [13,14]. The idea to protect the biometric template is to use the cancelable biometric techniques [15] to transform it into a transform domain before it is stored in the database. This modified information is sometimes referred to in the literature as renewable biometric references (RBRs) [16]. An important feature of these schemes is producing a new protected template on request by modifying/issuing a new key.

In order to become effective, each biometric template scheme must meet certain fundamental requirements for security and privacy. These are listed below [17–20]:

- **Irreversibility.** It can be technically stated that no personal information on the initial biometric patterns is to be leaked from the stored data. However, due to certain limitations in the design of the plans or the lack of appropriate theoretical evaluations, this strict binding has not been practically met.
- **Unlinkability/Diversity**. This property provides several major cryptographic attacks. This requires that the data stored by the same user in the different databases are not identical. If not, the personal data can be exploited statistically to filter user information.
- **Revocability**. Revocability requirement states that new templates from raw biometric data should be generated if the database is compromised.

- **Usability**. Due to different transformations or constraints, the resulting system performance (e.g., high error rates) has been significantly limited in protecting biometric template schemes. Biometric cryptosystems (referred to by their entropy S) have achieved reverse security levels related to their False Accept Rate (FAR).

An intentional and repeatable distortion of a biometric signal based on a selected transformation can be defined as cancelable biometric transformation [21]. This could allow the same biometric template to be used in different applications by applying different transformations. A transformation is referred to as revocable when it is possible to cancel or replace the stored template with a new template on the base of the same biometric data [8] [22–24]. A specific transformation parameter is used to get its transformed version of a biometric vector [25], while a hybrid biometric cryptosystem [26–30] combines different security algorithms.

Before the original biometric or extracted features have been stored, they are altered by cryptosystems. Cancellable biometric approaches enhance problems of unlinkability and diversity. In addition, cancelable biometric approaches are revokable if the kept template can be replaced with identical biometric data by a new template [31]. The discrete Fourier transform and a random projection on the original template can also achieve cancellability [32]. This transformation converts the original template into a complicated form, making it harder for an attacker to break its security. In [33], a non-invertible template transformation based on hash code is employed to ensure its linkability and revocability.

The outlines of the paper are organized as follows. Section 2 contains related work on cancelable biometrics. Section 3 provides the proposed cancellable biometric-based hybrid encryption system. Section 4 gives the results of simulation and comparative analysis of results. Finally, the concluding remarks are presented in Section 5.

2 Related Works

Cancelable biometrics is used to achieve template protection based on transformation [34]. The cancelable biometric concept helps to create a cancelable biometric template. The biometric template contains a distorted version that allows for high privacy levels by using the same biometric data for several templates.

Fingerprint recognition is the most commonly available technology in biometrics [35,36]. The biometric fingerprint protection scheme based on cryptographic hatching was presented by Sadhya and Singh [37]. The core of this scheme focuses mainly on using cryptographic hash functions that ensure adequate security. The proposed framework was tested on different fingerprint databases and the results were comparable with other current cancelable systems (EERs of 5.8%, 5.3%, 15.8%, and 14.5%).

DRPE method [38] for irreversibly encrypted iris codes is used in the FrFT area. In the cancelable approach, the RPM1, encryption keys, and RPM2 are used. This prevents the need for transmitted keys and improves the confidentiality of authentication by the cancelable system because every user has a unique key to obtain scrambled iris templates. Bultheel et al. [39] proposed a cancelable, probabilistic random projection-based voice-biometric system. The problem with voice biometrics is that speakers are recognized based on the user's statistical models. Recent papers introduce binarization methods in the integrated protection system of speaker models.

Kaur et al. [40] introduced a multi-bit allocation binarization template to deal with this problem. In addition, the proposed methods for extracting binary discriminatory features are applicable to template protection. Because biometric cryptosystems have restrictions like generating several non-related templates, the proposal to eliminate these limitations was a hybrid approach. Different cryptosystems are combined with a hybrid biometric cryptosystem, such as a key-binding scheme with bio-hashing and a non-invertible transformation with a fuzzy vault scheme [41]. The hybrid biometric cryptosystem benefits from cancelable biometric properties while ensuring enhanced security [42].

To secure speech signals, Sadhya [43]. proposed different signal processing algorithms to have cancellable transformations. On the other hand, strict analysis demonstrates the resistance of the proposed cancelable speech technique to various serious attacks, while other biometric template protection criteria are required. The main contributions of the proposed hybrid cryptosystem for cancellable biometrics are as follows:

- It has a non-invertible transform that ensures high revocability and diversity to provide additional security.
- Achieving high and recommended security outcomes for all tested evaluation metrics.
- To measure the performance of the suggested optical 3D Jigsaw transform, additional comparative analyses have been performed.

3 Proposed Hybrid Cryptosystem for Cancellable Biometrics

The general diagram of the proposed cancellable biometric-based hybrid ciphering system is revealed in Fig. 1. First, we convert the speech signal to a spectrogram gray-level image. The detailed steps of the proposed cancellable biometric system include:

1. The original image $f(x, y)$ is separated into different planes.
2. Every plane $f_i(x, y)$ is converted into $J[f_i(x, y)]$ using 3D Jigsaw transformation.
3. The transformed template obtained from the 3D Jigsaw is also ciphered with the FrFT with an order (α_x, α_y).
4. The first stage output is multiplied with a secret mask $R_1(x, y)$ which is chosen to be a phase function $\exp[i\ \psi(x, y)]$.
5. The final encrypted biometric template is then obtained by encrypting the resulting ciphered template with another ciphering phase of the FRFT with an order (β_x, β_y).

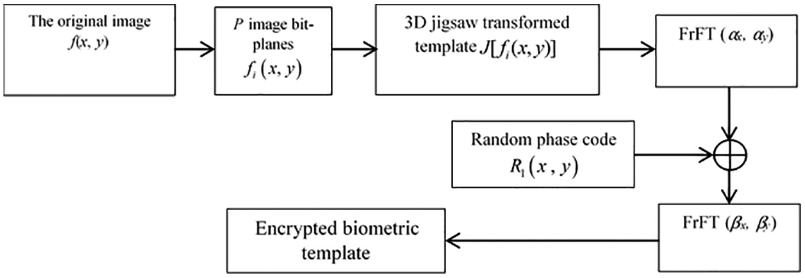

The original image $f(x, y)$
P image bit-planes $f_i(x, y)$
3D jigsaw transformed template $J[f_i(x,y)]$
FrFT (α_x, α_y)
Random phase code $R_1(x, y)$
FrFT (β_x, β_y)
Encrypted biometric template

Figure 1: Proposed cancellable biometric-based hybrid encryption system

The suggested technique includes two template plans: a non-invertible cancellable biometric system and two phases of the FrFT algorithm. Firstly, The input template is transformed with a 3D Jigsaw transformation algorithm as a non-invertible cancellable biometric scheme, more definitions, discussions, and details about Jigsaw transform can be found in [44–50]. Next, a random phase code $R_1(x, y)$ is multiplied with the output of this encryption stage. Finally, a second ciphering phase of the FrFT is used to obtain the ciphered template. The basis for the encrypted biometric template is a Jigsaw transformation algorithm, different fractional parameters, and random phase codes. This increases the encryption system robustness.

Therefore, the suggested scheme uses image ciphering, which utilizes two 2D-FrFT cascaded phases of a function *f(x, y)*. The employed 2D-FrFT is exploited in our proposed cancelable biometric system to encrypt the biometric templates represented mathematically as in Eq. (1).

$$F^{\alpha_x\alpha_y}[f(x,\ y)](u,\ v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K_{\alpha_x\alpha_y}(x,\ y;\ u,\ v)f(x,\ y)dx\,dy \tag{1}$$

with the kernel

$$K_{\alpha_x\alpha_y}(x,\ y;\ u,\ v) = K_{\alpha_x}(x,\ u)K_{\alpha_y}(y,\ v)$$

where

$$K_{\alpha_x}(x,\ u) = \begin{cases} A_{\phi_x}\exp[i\pi(x^2\ \cot\phi_x - 2xu\ \cos\ ec\phi_x + u^2\ cot\phi_x)] & \text{if}\alpha_x \neq n\pi \\ \delta(x-u) & \text{if}\ \alpha_x = 2n\pi \\ \delta(x+u) & \text{if}\ \alpha_x = (2n+1)\pi \end{cases}$$

and

$$A_{\phi_x} = \frac{\exp\{-i[\pi\ \mathrm{sgn}(\phi_x)/4 - \phi_x/2]\}}{[|\sin(\phi_x)|]^{\frac{1}{2}}}$$

where $\delta(.)$ is the delta function, $K_{\alpha_y}(y,\ v)$ is the angle along the x axis, and $K_{\alpha_y}(y,\ v)$ is the angle along the y axis [50,51].

The proposed cancellable biometric-based hybrid encryption system schematic diagram is displayed in Fig. 2. First, the user template is divided into P planes. Let $f(x, y)$ be the input biometric template with size $N \times N$ and $f_i(x, y)$ represent the P bit-planes where $i = 1$ to P and $P = 8$ planes.

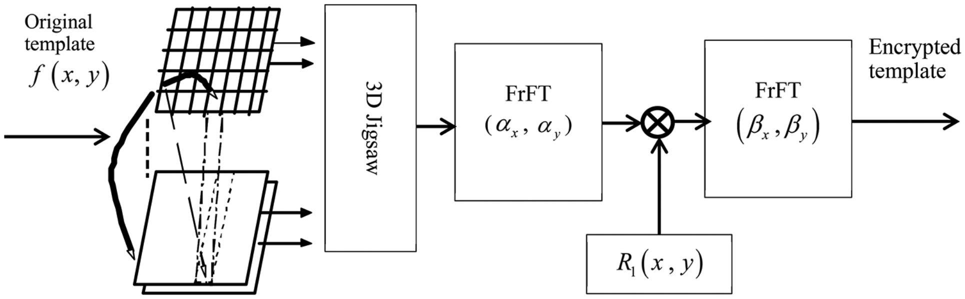


Figure 2: Steps of 3D Jigsaw and FrFT ciphering system

4 Simulation Results

To elucidate the impact of utilizing the suggested scheme, we examine two different samples datasets of speech signals. An important parameter in analyzing ciphered biometrics is visual inspection in which hidden features represent high cancelability benefits and good ciphering performance. Therefore, the strength of the cancellable biometric system is evaluated with different metrics such as Receiver Operating Characteristic (ROC), False Positive Fraction (FPF), True Positive Fraction (TPF), Probability of False Distribution (PFD), and Probability of True Distribution (PTD) [52–62]. In addition, the correlation scores between biometric templates are also employed. Only when a score to a test person exceeds a certain level the system is accessible.

The two testing datasets of the utilized speech samples in simulation tests are shown in Figs. 3 and 5. Figs. 4 and 6 show the biometric images for the tested nine biometric speech of the two datasets. In the simulations, nine biometric images are chosen for the two data samples for encryption using the proposed encryption scheme. To check the cancelability performance of the proposed hybrid encryption scheme, a number of random simulation tests have been performed. We compare the performance of the proposed FrFT + Jigsaw scheme-based cancellable biometric system with the DRPE encryption technique-based cancellable biometric system [44]. Figs. 7 and 8 show a comparison between the encryption outputs of the proposed FrFT + Jigsaw scheme and the state-of-the-art DRPE technique [44] for the two tested biometric samples. The simulation outcomes show that the proposed scheme performs efficiently compared to other related DRPE schemes [44].

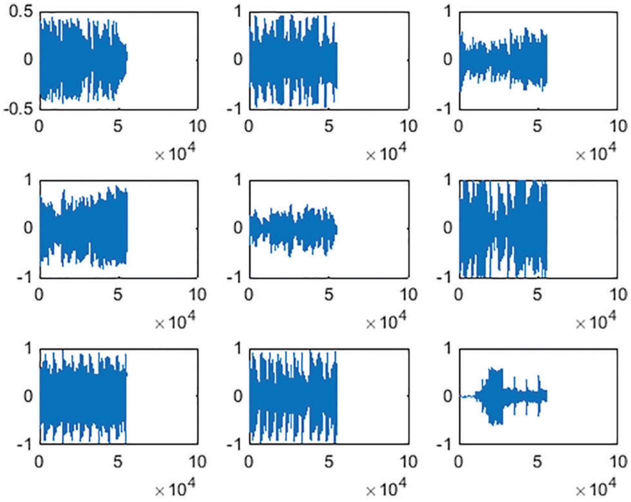


Figure 3: The tested nine speech samples of the 1st dataset

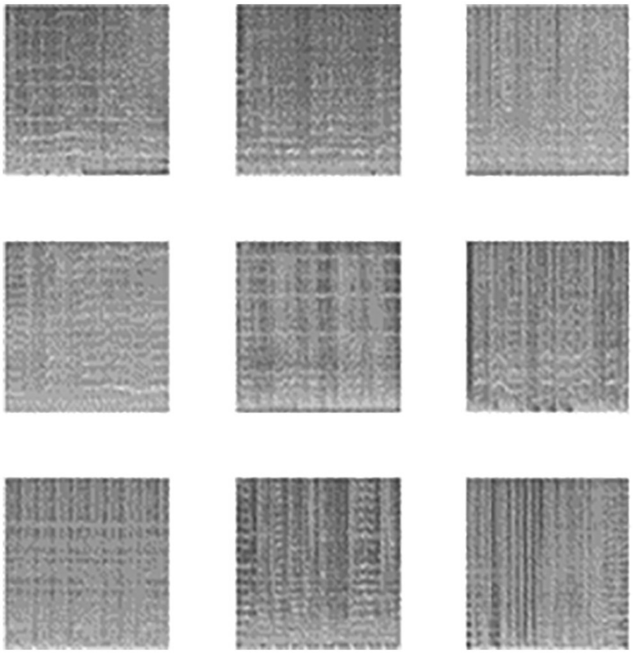


Figure 4: The biometric images of the tested nine speech samples of the 1st dataset

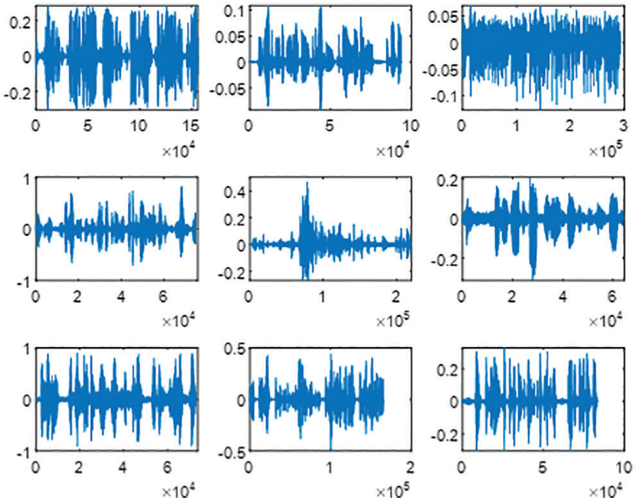


Figure 5: The tested nine speech samples of the 2^{nd} dataset

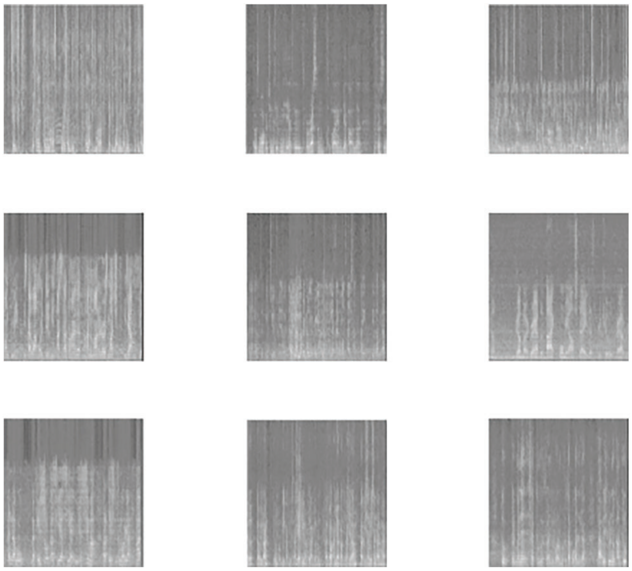


Figure 6: The biometric images of the tested nine speech samples of the 2^{nd} dataset

Figs. 9 and 10 show the PTD, PFD, and ROC as the comparison curves of the output authentication stage between the conventional DRPE scheme and the proposed FrFT + Jigsaw scheme for the nine biometric data samples of the sample datasets. These curves determine the threshold and probability of error in the authentication stage. Depending on the threshold value, the intersection point determines whether or not this user is an authorized user. Figs. 11 and 12 show the histograms for the tested schemes. It is observed that the suggested scheme provides better flat histograms, which means achieving efficient ciphering performance compared to the related DRPE scheme.

Tabs. 1 and 2 present the correlation scores of the examined schemes for the tested datasets. These achieved scores prove that the suggested ciphering scheme can secure the stored speech signal compared to other related ciphering schemes [44].

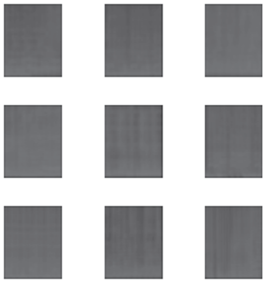
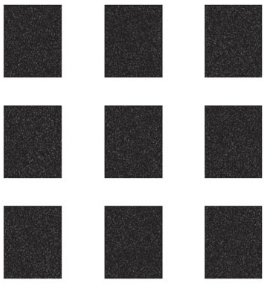
Encryption stage output using DRPE scheme [44]	
Encryption stage output using FrFT + Jigsaw scheme (Proposed)	

Figure 7: Encryption outcomes of 1st dataset

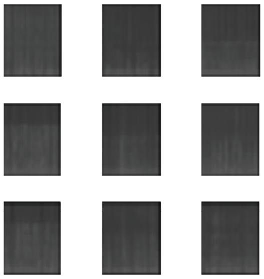
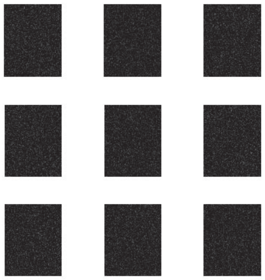
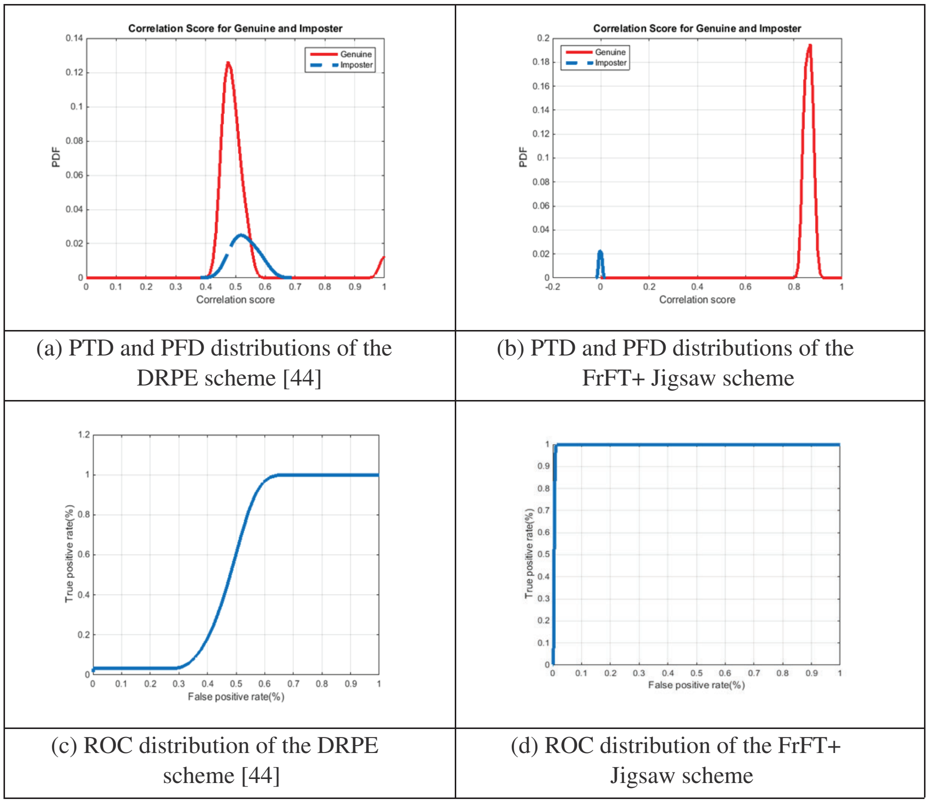
Encryption stage output using DRPE scheme [44]	
Encryption stage output using FrFT + Jigsaw scheme (Proposed)	

Figure 8: Encryption outcomes of the 2nd dataset



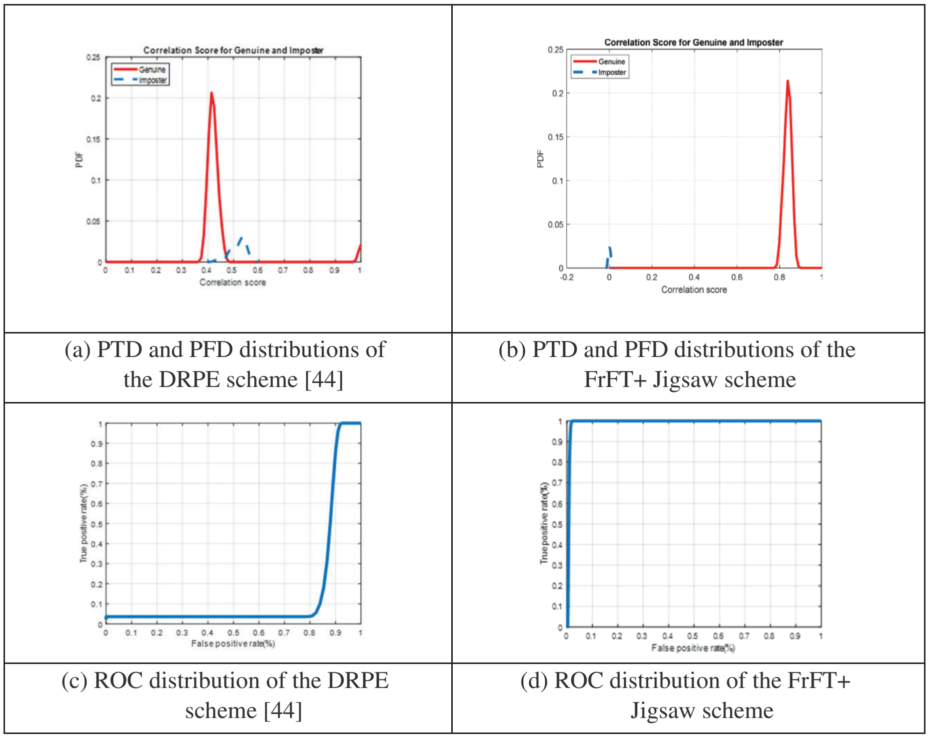
(a) PTD and PFD distributions of the DRPE scheme [44]

(b) PTD and PFD distributions of the FrFT+ Jigsaw scheme

(c) ROC distribution of the DRPE scheme [44]

(d) ROC distribution of the FrFT+ Jigsaw scheme

Figure 9: The PTD, PFD, and ROC outcomes of the 1st dataset



(a) PTD and PFD distributions of the DRPE scheme [44]

(b) PTD and PFD distributions of the FrFT+ Jigsaw scheme

(c) ROC distribution of the DRPE scheme [44]

(d) ROC distribution of the FrFT+ Jigsaw scheme

Figure 10: The PTD, PFD, and ROC outcomes of the 2nd dataset

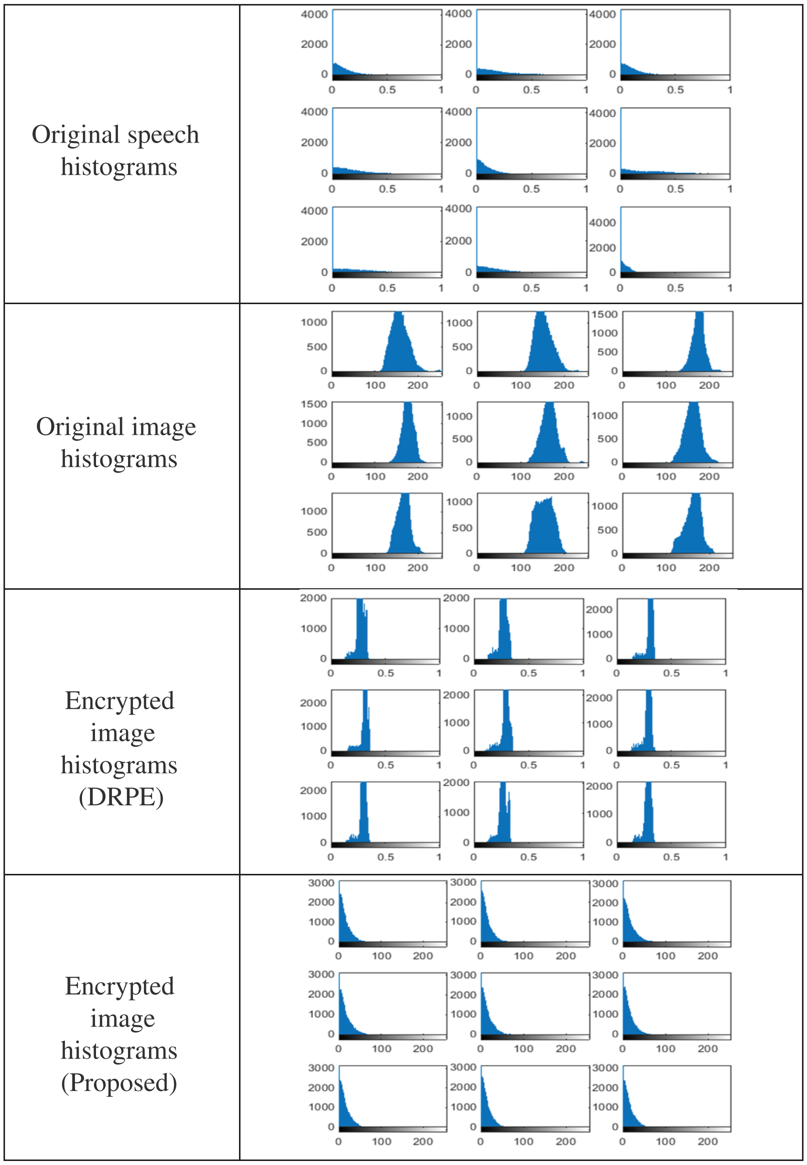


Figure 11: Histograms of the 1st dataset

Additional experimental tests in terms of EER, FAR (False Accept Rate), FRR (False Reject Rate), and AROC metrics are performed to compare the proposed scheme with recent related schemes [34,44,51,57–62], as shown in Tab. 3. These acquired outcomes prove the cancelability efficiency and high ciphering performance of the proposed scheme compared to other conventional schemes.

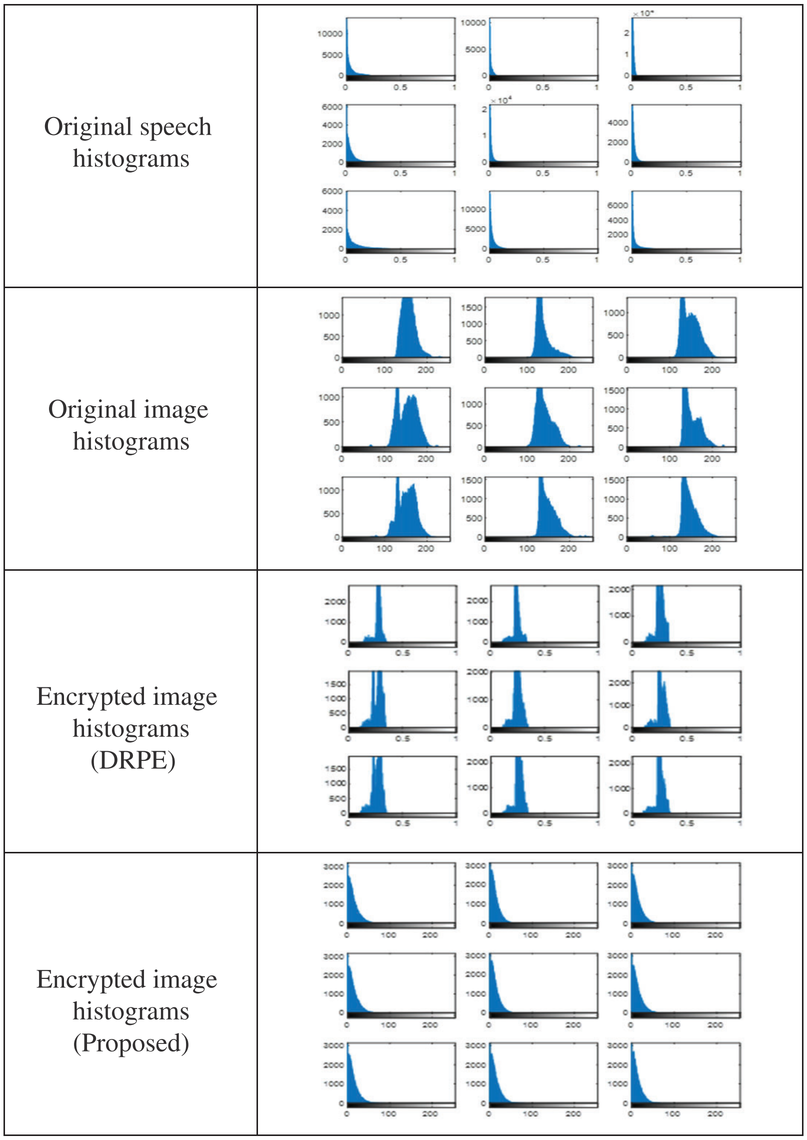


Figure 12: Histograms of the 2nd dataset

Table 1: Correlation scores of the 1st dataset

Speech sample	Correlation score with false speech		Correlation score with true speech	
	DRPE [44]	Proposed	DRPE [44]	Proposed
speech1	0.5699	−0.0036	1	0.8586
speech2	0.5818	−0.0020	0.5199	0.8462
speech3	0.4898	−7.9868e−04	0.4776	0.8827
speech4	0.5224	0.0041	0.4840	0.8853
speech5	0.5024	0.0030	0.4719	0.8721
speech6	0.4924	−4.0540e−04	0.4454	0.8642

(Continued)

Table 1 (continued)

Speech sample	Correlation score with false speech		Correlation score with true speech	
	DRPE [44]	Proposed	DRPE [44]	Proposed
speech7	0.5335	−0.0077	0.4905	0.8708
speech8	0.5306	9.9378e−05	0.5086	0.8516
speech9	0.4972	−0.0044	0.4727	0.8640

Table 2: Correlation scores of the 2nd dataset

Speech sample	Correlation score with false speech		Correlation score with true speech	
	DRPE [44]	Proposed	DRPE [44]	Proposed
speech1	0.4392	−0.0051	1	0.8570
speech2	0.4941	0.0058	0.4213	0.8086
speech3	0.5423	−0.0031	0.4248	0.8411
speech4	0.5328	0.0101	0.4093	0.8505
speech5	0.5211	−0.0025	0.4213	0.8130
speech6	0.5433	−7.1928e−04	0.4296	0.8442
speech7	0.5463	−0.0068	0.4320	0.8461
speech8	0.5306	0.0044	0.3973	0.8363
speech9	0.5475	9.1537e−04	0.4552	0.8293

Table 3: The statistical evaluation security analysis results for cancellable templates for the proposed cancellable system and the cancellable literature systems

Scheme	EER	FAR	FRR	AROC
Proposed	0.0035	0.0106	0.0038	0.9958
[44]	0.0740	0.4885	0.6759	0.5146
[51]	0.0224	0.0607	0.0447	0.9744
[34]	0.0215	0.0305	0.0424	0.9864
[57]	0.0219	0.0946	0.2983	0.8920
[58]	0.0862	0.0359	0.0129	0.9274
[59]	0.0622	0.0741	0.0667	0.9343
[60]	0.0436	0.0632	0.0279	0.9592
[61]	0.0351	0.0497	0.2836	0.9583
[62]	0.0096	0.0263	0.0192	0.9673

5 Conclusions

This paper introduced an improved encryption scheme that is more secure against hackers for an efficient cancelable speaker recognition system. The major contribution of this work is to integrate FrFT with the 3D Jigsaw transformation to achieve efficient cancellability for biometric speech templates. Therefore, the proposed encryption scheme simultaneously enhances diffusion in the ciphered biometric speech. The experimental simulation outcomes have confirmed that the suggested ciphering system ensures the efficient encryption of stored biometric templates. As a result, compared to traditional techniques, it is better qualified for secure biometric templates. Moreover, it provides highly-valued PFD, PTD, ROC, histogram, and correlation. Furthermore, the simulation outcomes expounded the eminence of executing the suggested 3D Jigsaw ciphering scheme for cancelable speaker identification with the traditional encryption schemes to reinforce the cancellability of the stored speech signals, likewise acquiring considerable subjective and objective results.

Acknowledgement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R66), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding Statement: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R66), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Furui, “An overview of speaker recognition technology,” *The Kluwer International Series in Engineering and Computer Science*, vol. 6, no. 3, pp. 31–55, 1996.

[2] G. Raho, M. Al-Ani, A. Al-Hamami and R. Kanaan, “Universal developing of persons identification based on RFID,” *Journal of Emerging Trends in Computing and Information Sciences*, vol. 6, no. 10, pp. 592–597, 2015.

[3] R. Prasad, M. Al-Ani and S. Nejres, “Hybrid fusion of two human biometric features,” *International Journal of Business and ICT*, vol. 2, no. 1, pp. 19–27, 2016.

[4] A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie *et al.,* “Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security application,” *Entropy*, vol. 22, no. 12, pp. 1–32, 2020.

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

[6] S. Ibrahim, M. Egila, H. Shawky, M. Elsaid, W. El-Shafa *et al.,* “Cancelable face and fingerprint recognition based on the 3D jigsaw transform and optical encryption,” *Multimedia Tools and Applications*, vol. 13, pp. 1–26, 2020.

[7] N. Soliman, M. Khalil, A. Algarni, S. Ismail, R. Marzouk *et al.,* “Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication,” *Multimedia Tools and Applications*, vol. 8, pp. 1–35, 2020.

[8] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon *et al.,* “Novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications,” *IEEE Access*, vol. 8, pp. 128548–128573, 2020.

[9] O. Faragallah, A. Afifi, W. El-Shafai, H. El-Sayed, E. Naeem *et al.,* “Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications,” *IEEE Access*, vol. 8, pp. 42491–42503, 2020.

[10] O. Faragallah, H. El-sayed, A. Afifi and W. El-Shafai, “Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform,” *Optics and Lasers in Engineering*, vol. 137, pp. 1–15, 2021.

[11] O. Faragallah, M. Alzain, H. El-Sayed, J. Al-Amri, W. El-Shafai *et al.,* “Block-based optical color image encryption based on double random phase encoding,” *IEEE Access*, vol. 7, pp. 4184–4194, 2018.

[12] K. Al-Afandy, W. El-Shafai, E. El-Rabaie, F. Abd El-Samie, O. Faragallah *et al.,* "Robust hybrid watermarking techniques for different color imaging systems," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25709–25759, 2018.

[13] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Security of 3D-HEVC transmission based on fusion and watermarking techniques," *Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27211–27244, 2019.

[14] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Efficient hybrid watermarking schemes for robust and secure 3D-MVC communication," *International Journal of Communication Systems*, vol. 31, no. 4, pp. 1–23, 2018.

[15] O. Faragallah, M. AlZain, H. El-Sayed, J. Al-Amri, W. El-Shafai *et al.,* "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2495–2519, 2020.

[16] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Encoder-independent decoder-dependent depth-assisted error concealment algorithm for wireless 3D video communication," *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13145–13172, 2018.

[17] W. El-Shafai, "Pixel-level matching based multi-hypothesis error concealment modes for wireless 3D H. 264/MVC communication," *3D Research*, vol. 6, no. 3, pp. 1–11, 2015.

[18] F. Abd El-Samie, R. Nassar, M. Safan, M. Abdelhamed and W. El-Shafai, "Efficient implementation of optical scanning holography in cancelable biometrics," *Applied Optics*, vol. 60, no. 13, pp. 3659–3667, 2021.

[19] O. Faragallah, E. Naeem, W. El-Shafai, N. Ramadan and F. El-Samie, "Efficient chaotic-baker-map-based cancelable face recognition," *Journal of Ambient Intelligence and Humanized Computing*, vol. 3, no. 9, pp. 1–39, 2021.

[20] I. Badr, A. Radwan, E. EL-Rabaie, I. Said and F. Abd El-Samie, "Cancellable face recognition based on fractional-order lorenz chaotic system and haar wavelet fusion," *Digital Signal Processing*, vol. 11, no. 6, pp. 1–24, 2021.

[21] H. El-Hameed, N. Ramadan, W. El-Shafai, A. Khalaf and F. El-Samie, "Cancelable biometric security system based on advanced chaotic maps," *The Visual Computer*, vol. 2, no. 7, pp. 1–17, 2021.

[22] M. Savvides, B. Kumar and P. Khosla, "Cancelable biometric filters for face recognition," in *Proc. of the 17th Int. Conf. on Pattern Recognition (ICPR)*, Cairo, Egypt, pp. 922–925, 2004.

[23] P. Tekade and P. Shende, "Enhancement of security through fused multimodal biometric system," in *Proc. Int. Conf. on Computing, Communication, Control and Automation (ICCUBEA)*, Pune, India, pp. 1–5, 2017.

[24] E. Tarif, S. Wibowo, S. Wasimi and A. Tareef, "A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system," *Multimedia Tools and Applications*, vol. 77, no. 2, pp. 2485–2503, 2018.

[25] M. Khan, L. Xie and J. Zhang, "Chaos and NDFT-based spread spectrum concealing of fingerprint-biometric data into audio signals," *Digital Signal Processing*, vol. 20, no. 1, pp. 179–190, 2010.

[26] M. Ao and S. Li, "Near infrared face based biometric key binding," in *Proc. Int. Conf. on Biometrics*, Springer, Berlin, Heidelberg, pp. 376–385, 2009.

[27] Y. Feng, P. Yuen and A. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 103–117, 2010.

[28] S. Sree and N. Radha, "Cancellable multimodal biometric user authentication system with fuzzy vault," in *Proc. IEEE Int. Conf. on Computer Communication and Informatics (ICCCI)*, Cairo, Egypt, pp. 1–6, 2016.

[29] L. Wu and S. Yuan, "A face based fuzzy vault scheme for secure online authentication," in *Proc. IEEE Second Int. Symp. on Data, Privacy, and E-Commerce*, Alexandria, Egypt, pp. 45–49, 2010.

[30] Z. Jin, A. Teoh, B. Goi and Y. Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," *Pattern Recognition*, vol. 56, no. 8, pp. 50–62, 2016.

[31] D. Rachapalli and H. Kalluri, "A survey on biometrie template protection using cancelable biometric scheme," in *Proc. 2th Int. Conf. on Electrical, Computer and Communication Technologies (ICECCT)*, Cairo, Egypt, pp. 1–4, 2017.

[32] B. Alam, Z. Jin, W. Yap and B. Goi, "An alignment-free cancelable fingerprint template for bio-Cryptosystems," *Journal of Network and Computer Applications*, vol. 115, no. 5, pp. 20–32, 2018.

[33] Z. Jin, J. Hwang, S. Kim, S. Cho, Y. Lai *et al.,* "A cancellable ranking based hashing method for fingerprint template protection," in *Proc. Int. Conf. on Mobile Networks and Management*, Springer, Cham, Madrid, Spain, pp. 378–389, 2017.

[34] P. Kumar, J. Joseph and K. Singh, "Optical image encryption using a jigsaw transform for silhouette removal in interference-based methods and decryption with a single spatial light modulator," *Applied Optics*, vol. 50, no. 13, pp. 1805–11, 2011.

[35] S. Mitra, "Digital signal processing a computer based approach," *MCGrawhill*, vol. 5, no. 3, pp. 1–33, 2001.

[36] H. Ozaktas, Z. Zalevsky and M. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing*, John Wiley, Chichester, New York, USA, vol. 3, no. 9, pp. 1–201, 2001.

[37] R. Jacob, T. Thomas and A. Unnikrishnan, "Applications of fractional Fourier transform in sonar signal processing," *IETE Journal of Research*, vol. 55, no. 1, pp. 16–27, 2009.

[38] E. Sejdic, I. Djurovic and J. Stankovic, "Fractional Fourier transform as a signal processing tool: An overview of recent developments," *Signal Processing*, vol. 91, no. 6, pp. 1351–1369, 2011.

[39] A. Bultheel and H. Sulbaran, "Recent developments in the theory of the fractional Fourier and linear canonical transforms," *The Bulletin of the Belgian Mathematical Society*, vol. 13, no. 5, pp. 971–1005, 2007.

[40] H. Kaur and P. Khanna, "Biometric template protection using cancelable biometrics and visual cryptography techniques," *Multimedia Tools and Applications*, vol. 75, no. 23, pp. 16333–16361, 2016.

[41] N. Ratha, S. Chikkerur, J. Connell and R. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[42] F. Quan, S. Fei, C. Anni and Z. Feifei, "Cracking cancelable fingerprint template of ratha," in *Proc. Int. Symp. on Computer Science and Computational Technology*, Madrid, Spain, pp. 572–575, 2008.

[43] D. Sadhya and S. Singh, "Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions," *Multimedia Tools and Applications*, vol. 77, no. 3, pp. 15113–15137, 2018.

[44] R. Soliman, M. Amin and F. El-Samie, "A double random phase encoding approach for cancelable iris recognition," *Optical and Quantum Electronics*, vol. 50, no. 8, pp. 326–340,2018 ,.

[45] A. Teoh and L. Chong, "Secure speech template protection in speaker verification system," *Speech Communication*, vol. 52, no. 2, pp. 150–163, 2010.

[46] M. Paulini, C. Rathgeb, A. Nautsch, H. Reichau and H. Reininger, "Multi-bit allocation: Preparing voice biometrics for template protection," in *Proc. the Speaker and Language Recognition Workshop*, Shenzen, China, pp. 291–296, 2016.

[47] E. Chandra and K. Kanagalakshmi, "Cancelable biometric template generation and protection schemes: A review," in *Proc. Int. Conf. on Electronics Computer Technology (ICECT)*, Tokyo, Japan, pp. 15–20, 2011.

[48] H. Zhu, Q. He and Y. Li, "A Two-step hybrid approach for voiceprint-biometric template protection," in *Proc. Int. Conf. on Machine Learning and Cyber- Netics (ICMLC)*, Cairo, Egypt, pp. 560–565, 2012.

[49] K. Chee, Z. Jin, D. Cai, M. Li and W. Yap, "Cancellable speech template via random binary orthogonal matrices projection hashing," *Pattern Recognition*, vol. 76, no. 5, pp. 273–287, 2018.

[50] A. Sinha and K. Singh, "Image encryption using fractional Fourier transform and 3D jigsaw transform," *Optical Engineering*, vol. 9, no. 2, pp. 158–166, 2013.

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

[52] E. Volte, J. Patarin and V. Nachef, "Zero knowledge with rubik's cubes and non-abelian groups," in *Proc. Int. Conf. on Cryptology and Network Security*, Springer, Cham, Sapin, Madrid, pp. 74–91, 2013.

[53] J. Wu, Z. Zhu and S. Guo, "A quality model for evaluating encryption-as-a-service," in *Proc. Int. Conf. on Security, Privacy and Anonymity in Computation, Communication and Storage*, Springer, Cham, Sapin, Madrid, pp. 557–569, 2017.

[54] M. Tarek, O. Ouda and T. Hamza, "Pre-image resistant cancelable biometrics scheme using bidirectional memory model," *Network Security*, vol. 19, no. 4, pp. 498–506, 2017.

[55] Y. Lai, Z. Jin, A. Teoh, B. Goi and W. Yap, "Cancellable iris template generation based on indexing-first-one hashing," *Pattern Recognition*, vol. 64, no. 4, pp. 105–117, 2017.

[56] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, no. 5, pp. 242–251, 2018.

[57] H. Kaur and P. Khanna, "Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing," *Future Generation Computer System*, vol. 102, no. 5, pp. 30–41, 2020.

[58] W. Yang, S. Wang, G. Zheng, J. Chaudhry and C. Valli, "ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures," *Journal of Supercomputing*, vol. 74, no. 10, pp. 4893–4909, 2018.

[59] N. Kumar, "On generating cancelable biometric templates using visual secret sharing," in *Proc. Science Information*, Cham, Springer, Cairo, Egypt, pp. 532–544, 2020.

[60] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition*, vol. 47, no. 3, pp. 1321–1329, 2014.

[61] W. He, X. Peng, W. Qin and X. Meng, "The keyed optical hash function based on cascaded phase-truncated Fourier transforms," *Optics Communications*, vol. 283, no. 11, pp. 2328–2332, 2010.

[62] D. Chang, S. Garg, M. Hasan and S. Mishra, "Cancelable multi-biometric approach using fuzzy extractor and novel bit-wise encryption," *IEEE Transactions on Information Forensics and Security*, vol. 15, no. 5, pp. 3152–3167, 2020.