Hindawi
Security and Communication Networks
Volume 2022, Article ID 7857975, 14 pages
https://doi.org/10.1155/2022/7857975

Research Article

Robust Authentication System with Privacy Preservation of Biometrics

Sonali D. Patil,[1] Roshani Raut,[1] Rutvij H. Jhaveri,[2] Tariq Ahamed Ahanger,[3] Pallavi V. Dhade,[4] Atul B. Kathole,[1] and Kapil N. Vhatkar[1]

[1] *Information Technology Department, Pimpri Chinchwad College of Engineering, Pune 411044, India*
[2] *Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Gandhinagar, India*
[3] *College of Computer Engineering and Sciences, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia*
[4] *Computer Engineering Department, Pimpri Chinchwad College of Engineering, Pune 411044, India*

Correspondence should be addressed to Rutvij H. Jhaveri; rutvij.jhaveri@sot.pdpu.ac.in

Received 20 December 2021; Revised 10 March 2022; Accepted 22 March 2022; Published 2 May 2022

Academic Editor: Luigi Catuogno

IoT-based multi-biometric system is a blend of multiple biometric templates that can be used for user authentication/verification using sensors. The leakage of the biometric trait information may cause critical privacy and security issues. It is expected to protect the privacy details of individuals through the irreversibility, unlinkability, and renewability of multi-biometric templates used in the authentication system. This study presents a robust authentication system with secure multi-biometric template protection techniques based on discrete cosine transform feature transformation and Lagrange's interpolation-based image transformation. Three biometric traits namely iris, fingerprint, and palm print are recorded using sensors to validate the proposed multi-biometric template protection system. The fusion of all traits used is giving an average of 95.42% genuine acceptance rate and an average of 4.57% false rejection rate. Despite any number of biometric templates used for authentication, the proposed image transformation techniques keep the size of the final storage requirement as 8 X 8, which achieves constant space complexity (O(1)). The stored template is not linked with original templates; it is irreversible and renewable as new enrolment of the same individual will produce a new template every time. Overall, the proposed technique provides a secure authentication system with high accuracy, a constant size database, and the privacy preservation of biometric traits.

1. Introduction

Access to private or sensitive information has always been an integral part of our daily routine in the modern world. A fast-moving trend that affects more people every day raises significant security concerns. Authentication is a broadly agreed solution to the above. Biometric authentication is the most effective way of identifying and authenticating individuals securely and quickly. It enables the authentication of an individual based on unique biological characteristics, which are distinctive and relevant only to them. It is an assessment of a person's identity, where the goal is to capture that unique biometric piece of data. It could be an image of their face, a recording of their voice, fingerprint, palm print image, finger vein, handwriting, etc. Several concerns have evolved with traditional unimodal biometric identification, including notable intercontinental variants—anti-universal and fast-paced invasions [1]. Therefore, the unimodal biometric method is less effective and less secure. Due to the combination of multiple traits, multimodal biometric systems are much more reliable and safer. Multi-biometric authentication techniques outperform unimodal biometric systems due to the presence of several modalities. Computationally efficient multiple biological trait hybridization technology has been introduced gradually to adequately address the flaws [2]. A malicious user could indeed begin producing a fabricated snippet to access biometric system [3]. In multimodal biometric authentication, a person must have been present physically, and attempting to make obfuscation is a big challenge [4]. The prime objective of the evolution of multiple traits is to strengthen protection because security measures are more crucial, and therefore, multiple biometric traits are saved in multimodal systems. When publicly revealed, the biometric multimodal template would invoke many such security breaches, particularly in comparison with the biometric unimodal template, so protecting the multimodal biometric template seems to be most essential [5].

The multimodal biometric system has many advantages that include the following:

(1) **Precision:** multimodal biometrics stores data from two or more biometric characteristics (e.g., a fingerprint and a face; or a face and an iris), while unimodal biometric arrangements store data from a single biometric characteristic [6, 7].

(2) **Increased and Reliable Recognition:** numerous characteristics are accessible, increasing the reliability of the multimodal system. A multimodal biometric method enables greater precision in identifying and verifying processes [6, 7].

(3) **Enhanced Security:** the employment of various documentation and acknowledgment techniques allows an arrangement to identify several biometric characteristics to reach a greater grade of threshold acknowledgment, and a structure administrator may choose the exact security level required [6, 7]. It enhances the privacy and security of user data.

(4) **User Reception:** as previously mentioned, multimodal biometric structures are much more dependable, precise, and secure, and many nations invest significantly in this kind of infrastructure.

To enhance protection for multi-biometric traits, biometric template protection strategy (BTP) will be used where the biometric data of an end user are taken. This is often unique, so any violation of data security could result in catastrophic results. As per the European Union (EU) General Data Protection Regulations (GDPR) 2016/679, biometrics are sensitive and private data of the person, which implies that the use of such data automatically leads to privacy rights. Biometric templates should therefore be protected to prevent any leaking of top-secret information. This is permitted by the biometric template protection (BTP) strategic approach. Under such a strategy, the sensitive C pattern is retrieved from the biometric M trait, probably using a secret key, and saved through memory.

To be precise, there are three primary criteria for these kinds of templates laid down in the ISO/IEC 24745 standard as detailed as follows:

(1) **Irreversibility:** biometric sensitive data must be analysed before storage through irreversible transitions.

(2) **Unlinkability:** stored biometric responses should not be linked through networks and databases.

(3) **Renewability:** when one template has been lost or stolen, new ones should be issued that do not meet the old template. This is because biometric features cannot even be replaced.

While multi-biometric validation schemes are more protected, specific concerns have been raised about the high precision of biometric information. This adds to privacy concerns, the huge size of databases, and the unified structure, which may introduce dangers to security and privacy. Data leakage may result in severe privacy and security concerns since it always involves private and sensitive data. By increasing the number of biometric traits, we can achieve a high level of protection for templates. However, the use of several biometric traits can cause an increase in the size of the database, and sometimes, the protected templates might not always meet all the requirements of ISO/IEC 24745.

Multi-biometric template authentication suffers from the following difficulties:

(1) Privacy preservation

(2) ISO 24745 standard requirements

(3) Single point failure of the database.

In this study, a secured multi-biometric template protection technique using irreversible, unlinkable, and renewable image transformation techniques based on Lagrange's interpolation is proposed and critically analysed through extensive experimentation.

The significant contribution of this research is as follows:

(1) Multi-biometric template protection through privacy preservation.

(2) ISO 24745 standard requirements achieved.

(3) Single point failure of the database.

(4) Size of the database.

The organization of this article is offered as follows. Section 2 contains the literature review. Section 3 describes the proposed scheme. The result and discussion are analysed in section 4. Lastly, in Section 5, the conclusion is presented.

2. Literature Review

This section gives a detailed overview of existing work and approaches used by different researchers.

2.1. Related Work. According to the study, there are three significant kinds of multi-biometric template protection: biometric cryptosystem, feature transformation, and image transformation. Many researchers have proposed various multi-biometric template protection schemes. The underlying techniques of these schemes are, namely, homomorphic stochastic encryption and user identity problem-solving method—to increase the security of a private information-protected preservation network, homomorphic stochastic encoding is employed. As a result, the encryption method used in this case efficiently reduces computing time and framework evaluated for fingerprint recognition and employs a discrete cosine transformation technique for attribute retrieval (DCT). The suggested scheme's objective is to provide very secure validation via the use of secret delivery, a pattern security method based on DNA encoding for multimodal biometric recognition. The suggested method employs DNA encrypting to combine changes in the biometric features of several templates into DNA planning. It first generates a cacophonous succession before being converted to a DNA alliance. Following the acquisition of DNA sequences, it conducts DNA enclosure on the two DNA provisions, a pattern defense technique based on a feature transformation approach for multimodal biometric identification. This approach utilizes the mixture of high points obtained by mixing DCT coefficients from face and palm print pictures [7], a mechanism for merging characteristics at the trait level, and an RSA methodology for securing multiple traits. Real-time biometric modality cryptosystems also received a security assessment due to their fingerprint, finger vein, and retina usage. This significantly improves the efficacy of RSA-based multimodal biometric cryptosystems [8]. By defining cross-figures and using the composite investigation concept, the finger vein and the signature image are extracted and the associated features are acquired. After that, the stocks are produced using the graphic cryptographic method on the biometric models. The stocks are kept in separate sources, ensuring that no data are exposed [9], and the unified network has enhanced the security architecture. The system is composed of two modules: enrolment and authentication [10–13]. The literature demonstrates the need for a more robust way of protecting multi-biometric template data. The research demonstrated the multimodal biometric concept of bio-hashing facial and fingerprint features while ensuring anonymity. The suggested scheme's findings are enhanced by including face and fingerprint characteristics and testing them on two paradoxical bimodal datasets. Secrecy requirements apply to multi-biometric authentication systems, which exacerbates concerns about data leaking [14].

A multi-biometric model used bin-based classifiers based on score-level fusion. It effectively enhances the authentication rate and reduces the error rate. The optimized PSO was used to reduce unnecessary details after combining iris and face features. As far as speed and memory requirements are concerned, PSO in this scheme is more computationally inexpensive [15]. The comparative study of the different fusion methods with their results has been described [16]. The three fusion plans feature-level, score-level, and decision-level mergers with the security pattern are projected as multibiometric cryptosystem to handle the challenges in the multibiometric finger scheme. It focuses only on irreversibility, no observation on renewability and memory but is a time-efficient method [17]. Permutation of score convergence and engagement methods employing two modalities (fingerprint and finger vein) are used to evaluate which one makes the most progress [18]. Privacy and security concerns are not taken into consideration.

The study presented unlinkable multi-instance iris biometric cryptographic algorithms obtained with the proposed fuzzy vault system. The designed methodology locks biometric-selected features retrieved from binary iris biometric datasets, i.e., iris codes, of conservative and liberal irises in some kind of a fuzzy model vault [19]. A multi-template secure system that relies on bloom filters and binary statistical image features (BSIF) collects information from either the face and both periorbital areas, and templates guarded by bloom filters and match score aggregation are used to maximize recognition rate [20]. Irreversibility and unlinkability of the system are assessed in terms of the referenced protection evaluation criteria. A method of privacy policy-preserving iris verification employing completely homomorphic encryption further guarantees privacy and security of templates and prohibits data leaks from templates. It fulfills all of the criteria set out in ISO/IEC 24745 [21]. To address privacy problems in template matching, template security methods, such as cancelable biometrics, have been implemented. It carried out an ISO/IEC standard 24745 compatible evaluation of block remapping and distorting, focusing mainly on recognizing technical problems and security and unlinkability facets. The authors have presented the first research to implement and assess cancellable template protection mechanisms within VIS/NIR 2D face, iris, and per orbital biometric domain [22]. A multimodal biometric pattern defense technique ensures the security of deposited biometric patterns in the record. The recommended method is watermarking, shuffling, a Hadamard matrix, and a chaotic map. An approach for predicting the main components of the multibiometric protection template focused on bloom filters has been proposed [23]. This demonstrates the irreversibility and unlinkability. A cancelable multibiometric authentication of users in which a unique bitwise encryption approach is used to convert a biometric template to a protected template. The implementations have been described by cryptographic blocks, cipher-based encryption, and critical hashing algorithms. The study provides an empirical formula that the framework assures confidentiality and irreversibility.

A method for archiving protected iris templates, which essentially seeks to minimize tasks in computationally intensive verification mode, is proposed [24]. It also focused on using arbitrary permutations in iris code rows and corresponding indexing employing bloom filters and binary search trees. The inconsistency, irreversibility, and renewability have been experimentally demonstrated [24]. The issue of unavoidable biometric error rates using a unique cuckoo filtering solution is overcome that combines both steady bits and discriminatory bits at the same time to obtain a bigger and more powerful template protection system [25]. Gomez-Barrero and Galbally [26] proposed a technique to assess the multiple perspectives of inverse biometrics by implementing reconstruction algorithms with distinct biometric traits, which reduces the effect of the security breaches. A detailed study of the biometric template protection strategies mainly focuses exclusively on cancellable biometric technologies, like using the bio-hashing method to achieve cancellable ventral finger templates [27]. Sarkar and Singh [28] discussed the review of the performance, security, and different biometric template protection schemes for biometric authentication systems to understand the challenges and threats of the multibiometric authentication system. A technique is implemented in [29] to develop a solid 3-dimensional template using the individual's fingerprint. From much of the minutiae point of the fingerprint, the minutiae triplets are calculated to produce a secure user template. The user template formed using the presented approach has been proven reliable and has good revocability, diversity, security, and performance [29]. Block SBL (BSBL) algorithm is proposed to estimate the channel performance by exploiting the block-sparse structure of the sparse multipath channel model [30]. The biometric templates are protected from attacks using cancellable biometrics. The sensitivity analysis is carried out in different network conditions by taking packet delivery ratio and normalized routing overhead as the performance metrics and varying the values of distrust threshold, trust component's weight, and trust update interval [31]. It has been suggested that it is highly beneficial to alter them before actually storing them in databases through one of those cancellable and non-invertible breakthroughs. A novel procedure integrates fingerprints and behavioral biometrics to enhance user authentication security while maintaining functionality and confidentiality [32]. A secure multi-biometric pattern protection method is based on the hybridizing of the transformation of structures and the transformation of images where the discrete cosine transform (DCT) is used for the conversion of systems, and the polynomial secret sharing scheme (SSS) is used for hybridizing resultant in the guard of multi-biometric patterns. The scheme uses a client server-based network model, which can be enhanced with different network models such as user gateway sensor, used in sensor networks and the Internet of things [33]. The cancellable biometric concept was used to protect biometric templates. It achieved iris image protection by performing a repeatable, nonreversible transformation in the image domain prior to extracting the features. Two traditional transformations, block remapping and texture warping, have been applied to iris textures acquired from the CASIA-V3 Iris database. The paper presented the results on the matching performance using different block sizes for block remapping and mesh-warping transformation. The key sensitivity of a popular iris recognition method is also provided [34]. An enterprise rights management system is proposed, which ensures "on-site" information confidentiality protection. Strong multi-biometric verification schemes are being used to authenticate operator identities, while their biometrics are protected using cancellable biometrics. The fusion of face and voice biometrics is used to evaluate cancellable biometrics. Local data encryption and minimal data transfers are standard features of system. A secure key management protocol is being used by on-site devices and the remote manufacturer's support centre to ensure the efficient and dynamic enforcement of arbitrary data provider-defined access policies [35]. Cancelable biometrics is being used as viable solution to the privacy and security concerns associated with biometric authentication. A patch-based representation that is localised and does not require registration is presented. In [36], a method is developed for making the new representation of cancelable trait and demonstrated that it is resistant to adversarial attacks.

2.2. Review. Table 1 portrays the performance/accuracy and limitations in the state-of-the-art multi-biometric authentication systems with different biometrics. This work showcases the research gaps as mentioned as follows:

(1) The existing schemes in the literature have no mechanism to control the increase in the size of the database as the number of biometric traits increases. The addition of biometric features increases the size of the database.

(2) The existing work fails to handle the leakage of private data.

(3) Irreversibility, unlinkability, and renewability are not followed.

Thus, the proposed secured multi-biometric template protection technique using irreversible, unlinkable, and renewable image transformation based on Lagrange's interpolation provides multi-biometric template protection with constant space complexity despite any number of biometric traits used for authentication.

3. Proposed Scheme

Protection of biometric data is critical as it is a person's private information. Multi-biometric authentication is necessary as a disadvantage to a unimodal biometric authentication system. This work provides a secure multi-biometric template protection method based on feature and image transformation.

Three biometric traits, namely iris, palm print, and fingerprint, are captured using different sensors and input for DCT. DCT converts all 512 X 512 size biometric templates into the feature vectors of size 8 X 8. These 8 X 8 feature vectors are converted into a single 8 X 8 size secret template using the proposed LI-based image transformation technique. The generated secret template is irreversible, unlinkable, and renewable concerning the original biometric traits of an individual.

The feature transformation uses the DCT technique, and for image transformation, Lagrange's interpolation (LI)-based reverse secret sharing is used.

3.1. Discrete Cosine Transform (DCT). DCT's first step is to transform potential raw image data features, i.e., fingerprint, iris, and palm print, from a spectral domain to a frequency domain. The derived input images are reconstructed for one of the most pertinent information. The first chosen feature throughout the transformed image is rearranged in a lengthy vector feature. The form of that whole coefficient seems to be quite valuable since it includes crucial information about the image. It maintains only a few coefficients for compression. For this reason, the DCT coefficients are extracted from all the 2D images of fingerprint, iris, and palm print.

(1) states the 2D-DCT for the m X m matrix, which is the primitive form of the matrix aspect. The computational complexity of DCT is also lower. First, a block of size 8 X 8 is obtained from the entire image, whereby using 2D-DCT, each block is transformed independently. We can thus go off

Table 1: Comparison of state-of-the-art multi-biometric authentication systems with different biometrics.

Reference	Methodology	Performance/accuracy	Irreversibility	Unlinkability	Renewability	Limitations
Gomez-Barrero 2017 [2]	Protection of multi-biometric templates via homomorphic encryption	High accuracy rates, reaching EERs as low as 0.12%, and requiring protected templates comprising 200 KB	√	√	---	Renewability needs to attain
Dong, J., Meng, X., Chen, M. and Wang, Z., 2017 [6]	For multimodal biometric identification, pattern defense based on DNA coding is required	ERR of the presented algorithm is 3.6%	---	---	√	Unlinkability and irreversibility standards are not taken into consideration
Ahmad, M., Mohamad, N., Md Isa, M., Ngadiran, R. and Darsono, A., 2017 [7]	Fusion of DCT image low-frequency coefficients for multimodal biometrics using face and palm print	The recognition rate is 95%	---	---	---	Not focused on ISO standards
Jagadiswary, D. and Saraswady, D., 2016 [8]	Using fused multimodal biometrics for biometric authentication	Performance of multimodal biometrics with RSA has GAR of 95.3% and FAR of 0.01%	---	---	---	-
Nandhinipreetha, A. and Radha, N., 2016 [9]	Visual cryptography validates multimodal biometric templates such as the finger vein and signature	The system is increased with a low FAR of 2%, FRR of 1.3%, and accuracy of 98.2%	---	---	---	-
M. K., Prasad, M. V. N. K. and Raju, U. S. N. (2020) [21],	Using completely homomorphic encryption, privacy-preserving iris authentication	(EER = 0.19%, 0.39%, 0.99%, and 0.28% for CASIA-V 1.0, CASIA-V3-Interval, IITD, and SDUMLA-HMT iris databases)	√	√	√	All ISO standards are satisfied
Gupta, A. et al. (2014) [37]	We can combine face, palm vein, and palm print modalities at the feature level using the discrete cosine transform	This methodology has 0% FAR with 100% GAR with Canberra distance	---	---	---	---
Peng, J. et al. (2014) [17]	Multi-biometric fingerprint cryptosystems: a fusion approach and template security	Three fusion strategies, feature-level, score-level, and decision-level mergers with the corresponding template protection technique, are proposed as multi-biometric finger cryptosystems	√	---	---	Huge memory required
Vishi, K. and Mavroeidis, V. (2018) [18]	A comparison of methods for fusing fingerprint and finger vein biometric data at the score level	Evaluated permutations of score convergence and ways of engaging using two modalities	---	---	---	Privacy and security concerns are not taken into consideration
Rathgeb, C. et al. (2016) [19]	Improved multi-biometric fuzzy iris vault that is unlinkable	An unlinkable multi-instance iris biometric cryptographic algorithms were obtained with the presented fuzzy vault system	---	---	---	Privacy and security concerns are not taken into consideration

Table 1: Continued.

Reference	Methodology	Performance/accuracy	Irreversibility	Unlinkability	Renewability	Limitations
Stokkenes, M. et al. (2016) [20]	Protection against multiple biometric templates—an study of the security implications of binarized statistical characteristics used in bloom filters for cellphones	Presented system based on bloom filters and binary statistical image features (BSIFs)	√	√	---	Renewability is not being attained
Morampudi, M. K., Prasad, M. V. N. K., &Raju, U. S. N. (2020) [21]	Using completely homomorphic encryption to protect the privacy of iris authentication	Introduced a method of privacy policy-preserving iris verification employing completely homomorphic encryption	√	√	√	All ISO standards are taken into consideration
Kirchgasser, S. et al. (2020) [22]	Multiple face biometrics in the visible and near-infrared light domain are protected using templates	Introduced template security mechanisms, including cancellable biometrics	---	√	---	One ISO standard is attained
Nafea, O. et al. (2016) [38]	Watermarking is used to secure hybrid multi-biometric templates	The scheme is based on a watermarking process, a shuffling process, and a Hadamard matrix	---	---	---	---
Gomez-Barrero, M. et al. (2018) [23]	Protection of several biometric templates using bloom filters	Presented an approach for predicting the principal components of the multi-biometric protection template focusing on bloom filters	√	√	---	Renewability is not being attained
Chang, D. et al. (2020) [24]	A cancelable multi-biometric method is possible using a fuzzy separator and innovative bitwise encoding	Presented a cancellable multi-biometric authentication of users in which a unique bitwise encryption method was used	√	---	---	All ISO standards not attained
Drozdowski, P. et al. (2018) [24]	Indexing iris codes using cancelable bloom filter-based exploration assemblies while maintaining privacy	Presented the first-ever method for archiving protected iris templates, which essentially seeks to minimize tasks in computationally intensive verification mode	√	---	---	All ISO standards not attained
S. S. et al. (2020) [29]	Biometric identification solution that is both robust and safe	Presented a technique in which a strong 3-dimensional template was developed using the fingerprint of the individual	---	---	---	Revocability, diversity is attained

Table 1: Continued.

Reference	Methodology	Performance/accuracy	Irreversibility	Unlinkability	Renewability	Limitations
Jutta H¨ammerle-Uhl.et.al (2009) [34]	Cancelable iris biometrics using block remapping and image warping	Presented cancelable biometric protection technique where two classical transformations, block remapping and texture warping, were applied to iris textures	√	---	---	One ISO standard is attained
LUIGI CATUOGNO et. al. (2016) [35]	An enterprise rights management system for on-the-field maintenance facilities	A secure multi-biometric authentication scheme is used to identify operators while guaranteeing system usability and user privacy	---	---	---	Security is attained but not all ISO standards
Sharat Chikkerur et.al. (2008) [36]	Generating registration-free cancelable fingerprint templates	A secure, registration-free construction of cancelable fingerprint templates is proposed. New fingerprint representation and from that cancelable biometrics constructed	√	---	---	Non-invertible variations achieved

to DCT to retrieve data contained inside this frequency response and employ it even during the phase of identification.

The equation of DCT for pixel at location (u, v) is given as follows:

$$F(u,v) = \alpha(v)\alpha(u)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\ldots\ldots\ldots\ldots\ \cos\left[\frac{u\pi(2x+1)}{2}\right]\cos\left[\frac{v\pi(2y+1)}{2N}\right], \tag{1}$$

where

$$0 \le u \le N-1,$$

$$\alpha(u,v) = \begin{cases} \dfrac{1}{\sqrt{N}} \text{for}\,(u,v) = 0, \\[2ex] \sqrt{\dfrac{2}{N}}\, for\ 1 \le (u,v) \le N-1. \end{cases} \tag{2}$$

In the proposed work, 8 X 8 size feature vector is generated using DCT for each biometric template.

3.2. Lagrange's Interpolation (LI)-Based Image Transformation. Each biometric trait's 8 X 8 size feature vectors are used as input for the proposed image transformation. The secret template S is computed using generated 8 X 8 size feature vectors T_1, T_2, $T_3 \ldots T_n$, T_{n+1}.

$$S = LI\left(T_1, T_2, T_3 \ldots T_n, T_{n+1}\right). \tag{3}$$

3.3. Lagrange Interpolation. Nth degree polynomial equations P(x) are constructed using values of n+1 feature vectors. The two functions *f(x)* and *g(x)* are computed. *f(x)* is the appropriate function of computed *N*+1 discrete values which are later used to interpolate or approximate the *g(x)* function. The *g(x)* will continue moving through all *N*+1 interpolation points.

The interpolation points or nodes are given as per equation (2).

$$\begin{aligned} x_0 f(x_0) &\equiv f_0, \\ x_1 f(x_1) &\equiv f_1, \\ x_2 f(x_2) &\equiv f_2, \\ &\ldots\ldots, \\ x_N f(x_N) &\equiv f_N. \end{aligned} \tag{4}$$

(5) is a polynomial and can be formed using the Lagrange interpolation formula with different vectors. Only one Nth degree polynomial moves through the given set of (N+ 1) points. Its part is demonstrated here as a sequence of powers shown through.

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_N x^N, \tag{5}$$

where a_i is the ith position value of 8 X 8 feature vector.

In our proposed method, the following polynomial-based equation shown in (6) is generated with degree 2, and the number of biometric traits is 3.

$$P(x) = a_0 + a_1 x + a_2 x^2. \tag{6}$$

A g(x) should therefore fit f(x) only at a chosen data point, and it is as follows:

$$\begin{gathered} g\left(x_0\right) = f_0 \Rightarrow a_0 + a_1 x_0 + a_2 x_0^2 + \ldots.. + a_N x_0^N = f_0, \\ g\left(x_1\right) = f_1 \Rightarrow a_0 + a_1 x_1 + a_2 x_1^2 + \ldots.. + a_N x_1^N = f_1, \\ \ldots.., \\ g\left(x_N\right) = f_N \Rightarrow a_0 + a_1 x_N + a_2 x_N^2 + \ldots.. + a_N x_N^N = f_N. \end{gathered} \tag{7}$$

Soling these sets of simultaneous equations, one secret template is created.

As discussed above, the low-frequency features collected by DCT from palm print, iris, and fingerprint are integrated into series to introduce a unique fusion vector. A new feature-level fusion is created using the limited information provided in fingerprint, iris, and palm print vectors. The generated irreversible secret biometric template protects the user's private biometric data. The generated template gets stored in the database.

3.4. The Operational Flow of the System.

3.4. The Operational Flow of the System. There are two phases associated with the process of the authentication system:

1. Enrolment process
2. Authentication process

3.4.1. Steps of the Enrolment Process. The steps of the enrolment process are as follows:

Step 1. Input biometric traits—fingerprint, iris, and palm print using sensors.

Step 2. Apply preprocessing steps to get apparent 512x512 size biometric traits.

Step 3. Apply DCT to all accepted biometric traits to obtain 8X8 feature vectors.

Step 4. Apply LI-based image transformation technique to form unique 8X8 size fusion vector.

Step 5. Store secret unique fusion vector in the database.

In the enrolment process, biometric traits are captured using a sensor. After considering the images of the fingerprint, iris, and palm print, the data are normalized to eliminate the noise. The transform domain is used to obtain relevant information from the images, and also, the feature vector is created. Next, the LI-based image transformation on these feature vectors is applied to get a unique fusion vector. The steps of the enrolment process are illustrated in Figure 1.

The sensor collects the user's fresh fingerprint, palm, and iris during user authentication. Using the transform domain, features are recovered after picture capture. The obtained feature pattern is assessed by comparing the acquired feature pattern to the pattern in the shared database. The two templates are compared using similarity tests, which validate the user's authorization. Figure 2 illustrates the authentication procedure. The steps for the authentication process are as follows.

3.4.2. Steps for the Authentication Process. The steps of the authentication process are given as follows:

Step 1. Input biometric traits—fingerprint, iris, and palm print using sensors.

Step 2. Apply preprocessing steps to get apparent 512 X 512 size biometric traits.

Step 3. Apply DCT to all accepted biometric traits to obtain 8 X 8 feature vectors.

Step 4. Apply LI-based image transformation technique to form unique 8 X 8 size fusion vector.

Step 5. Fetch and store a unique fusion vector from the database.

Step 6. Compare both the fusion vectors obtained in step 4 and step 5.

Step 7. Decide whether a person is authorized or unauthorized.

Experimentation is performed on a sample fingerprint, iris, and palm print with a DCT, and then, three traits are fused into a single template with LI-based image transformation.

3.5. Performance Measures

3.5.1. Genuine Acceptance Rate (GAR). This refers to the total number of genuine clients with whom the model has an agreement. It is provided as follows: GAR = 100-FRR. The genuine acceptance ratio (GAR) is computed for each fingerprint vector, iris, palm print templates, and the fusion of all characteristics.

3.5.2. False Rejection Rate (FRR). Due to the low excellence of the obtained biometric signal, the recorded user continually refused entry and is excluded for validation. The proportion of genuine users rejected by the biometric system is the rejection rate. The formula is given in (8), which defines FRR. FR is the number of untruthful rejections, whereas P denotes the maximum quantity of identification authentication.

$$\mathrm{FRR} = \frac{\mathrm{FR}}{P} * 100, \tag{8}$$

where FR=number of untruthful rejections and P = maximum quantity of identification authentication.

3.5.3. Root-Mean-Square Error (RMSE). The root-mean-square error has become a widely used measure of the difference between the model's or estimator's predicted values (sample and population) and the observed values. The root-mean-square error is calculated as follows:

$$\mathrm{RMSE} = \sqrt{\frac{\sum\left(p_i - o_i\right)^2}{n}}, \tag{9}$$

where p = predicted values, o = observed values, and n = number of observations.

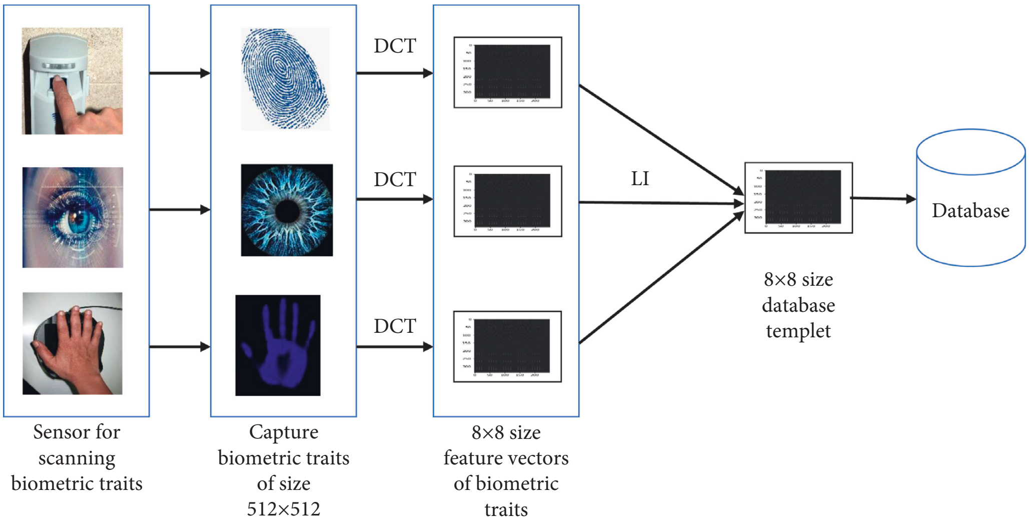


Figure 1: Enrolment process.

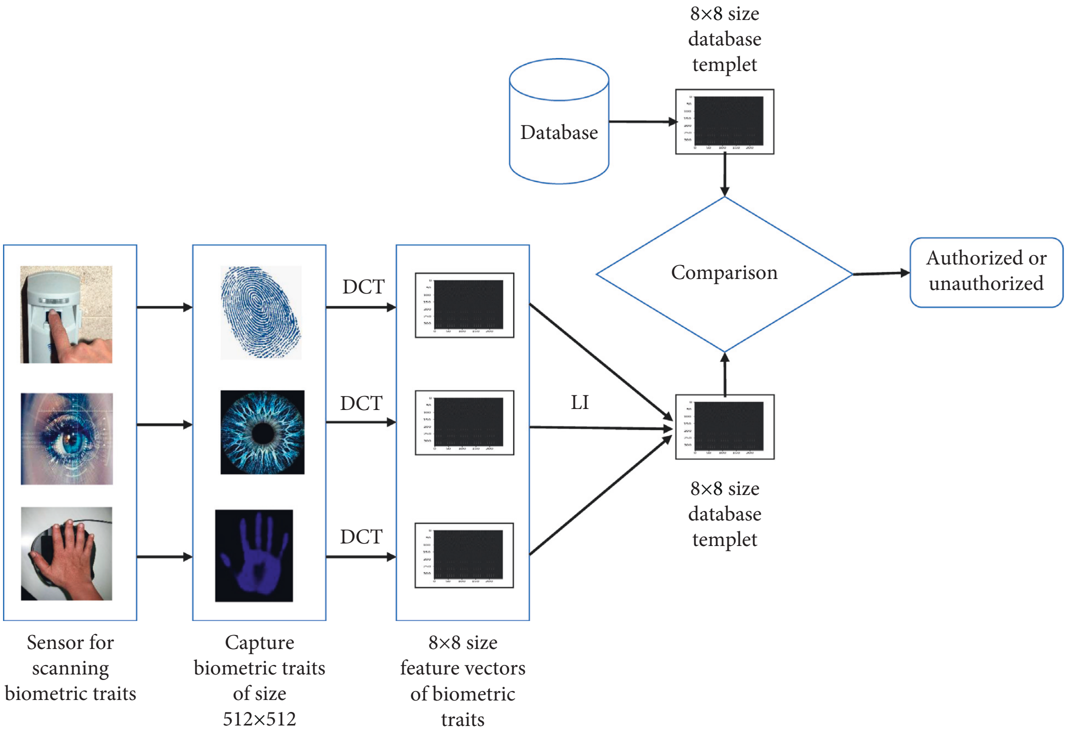


Figure 2: Authentication process.

3.5.4. Standard Deviation (SD). The standard deviation (SD) measures how often data within a range vary or scatter. A dataset's standard deviation equals the square root of its variance, as defined as follows:

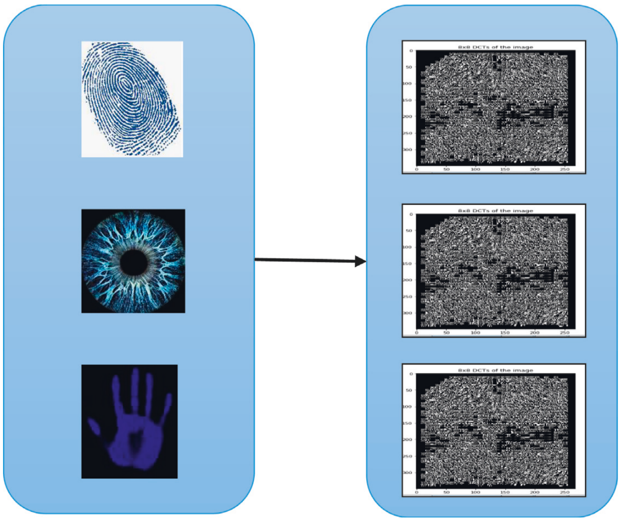
$$SD = \sqrt{\frac{\sum |x_i - \mu|^2}{N}}, \tag{10}$$

where X_i = the value of ith particle in the population, μ = the mean value of the population, and N=size of the population.

Python's proposed scheme uses a testbed comprising 500 fingerprint, iris, and palm print samples, which were taken from 100 people. The results are discussed in the following section.

4. Results and Discussion

Three biometric traits, namely iris, fingerprint, and palm print, are considered of size 512 X 512. The discrete cosine transform (DCT) is applied on these original templates of size 512 X 512.



Fingerprint, iris and palmprint templates

Feature vectors of biometric traits

Figure 3: Fingerprint, iris, and palm print templates with their DCT.

4.1. Vector Size Threshold. To decide the vector size, various experiments are done on original biometric templates of size 512 X 512. The discrete cosine transform is applied on test fingerprint, iris, and palm print images. All original biometric traits are converted into 4 X 4, 8 X 8, and 16 X 16 feature vectors. Figure 3 shows original biometric templates and their corresponding DCT.

The tests are evaluated on feature vectors of different sizes such as 4 X 4, 8 X 8, 16 X 16, and 32 X 32. Discrete cosine transformation (DCT) is used on every 512 X 512 size template to transform it into 4 X 4, 8 X 8, and 16 X 16 feature vectors. This process compresses the size of the original image. Fusion of these 4 X 4, 8 X 8, and 16 X 16 fingerprint, iris, and palm print images is used.

To decide the better compressed vector size threshold, root-mean-square error (RMSE) is used. The calculated RMSE values of the same individual and different individuals are described in Tables 2 and 3.

Table 2 shows that the maximum RMSE value for the same individual is 1209.238.

Table 3 shows that the minimum RMSE value for the different individuals is 5577.564.

This difference in maximum and minimum RMSE value supports better results for GAR and FRR.

First, the GAR and FRR results are calculated individually for the entire biometric template for fingerprint, iris, and palm print. There are various threshold values taken for computing GAR and FRR. The threshold is computed using the least error in the reconstruction of the template, which Min gives, and the constant factor multiplied with standard deviation (SD). At last, the GAR and FRR are computed to fuse all three biometric templates.

The GAR and FRR are computed for 4 X 4, 8 X 8, and 16 X 16 feature vector sizes. Table 4 shows the GAR and FRR results for feature vector size 4 X 4 for various threshold values. From Table 4, it has been observed that the fusion of biometric traits achieved the highest authentication accuracy of 91.07% for 4 X 4 feature vector size.

Table 5 shows the GAR and FRR results for feature vector size 8 X 8 for various threshold values. For the 8 X 8 feature vector, the fusion of biometric traits achieved the highest authentication accuracy of 95.42%, shown in Table 5.

Table 6 shows the GAR and FRR results for feature vector size 16 X 16 for various threshold values. The fusion achieves the highest authentication accuracy of 93.40% for the 16 X16 feature vector, shown in Table 6.

As shown in Figure 4, GAR results show that the highest accuracy is achieved for feature vector of size 8 X 8. The fusion of biometric traits achieves the highest accuracy of 95.42% for size 8 X 8.

The proposed Lagrange-based image transformation reduces original size 512 X 512 to the secret template of size 8 X 8. This reduces database size to a great extent, which saves storage requirements.

4.2. Space Complexity Results. In the first experimentation test, the number of traits used was 2 (fingerprint and iris) and gradually increased with 512 X 512. The proposed hybridization of feature and image transformation technique will generate a single secure template of size 8 X 8. As we increase the number of traits by 1, each of which is 512 X 512, it still generates a single secure template of the same size of 8 X 8. Hence, there will not be an increase in the size of the database, as shown in Table 7.

As observed in Table 7, 99.98% size reduction is achieved despite any number of biometric templates used for authentication.

4.3. Renewability. The new enrolment of the same individual will produce a new template every time. The new index is generated and used to compute a database template of size 8 X 8.

Table 2: RMSE values of the same individual.

Shared reconstructed image	Original image samples				
	1	2	3	4	5
1	0.0	1073.203	940.346	998.435	1022.112
2	1073.203	0.0	**1209.238**	1123.342	970.671
3	940.346	1209.238	0.0	1095.781	1027.998
4	998.435	1123.342	1095.781	0.0	973.873
5	1022.112	970.671	1027.998	973.873	0.0

The bold value represents maximum RMSE value for the same individual.

Table 3: RMSE values for different individuals.

Shared reconstructed image	Image samples of different individuals				
	6	7	8	9	10
1	5753.467	5742.036	**5577.564**	5765.231	5822.876
2	5827.785	5731.899	5626.132	5812.561	5791.435
3	5881.271	5819.497	5708.537	5623.771	5582.402
4	5598.231	5781.652	5632.871	5623.876	5623.123
5	5587.234	5679.792	5587.776	5578.755	5781.998

The bold value represents minimum RMSE value for the different individual.

Table 4: GAR 4 X 4 feature vector size.

Feature vector size		
GAR result for feature vector size 4 X 4		
Threshold	Fusion GAR (%)	Fusion FRR (%)
Mean + SD	79.54	20.54
Mean + 2∗SD	81.52	18.48
Mean + 0.75∗ (Max-Min)	84.34	15.66
Mean + 3∗SD	85.15	14.44
Mean + 4∗SD	89.56	10.44
Mean + 5∗SD	**91.07**	8.93

The bold value highest authentication accuracy %.

Table 5: GAR 8 X 8 feature vector size.

Feature vector size		
GAR result for feature vector size 8 X 8		
Threshold	Fusion GAR (%)	Fusion FRR (%)
Mean + SD	89.54	10.45
Mean + 2∗SD	91.50	8.49
Mean + 0.75∗ (Max-Min)	88.23	11.76
Mean + 3∗SD	92.15	7.84
Mean + 4∗SD	93.89	6.11
Mean + 5∗SD	**95.42**	4.57

The bold value highest authentication accuracy %.

Table 6: GAR 16 X16 feature vector size.

Feature vector size		
GAR result for feature vector size 16 X 16		
Threshold	Fusion GAR (%)	Fusion FRR (%)
Mean + SD	81.54	18.46
Mean + 2∗SD	85.50	14.50
Mean + 0.75∗ (Max-Min)	88.23	11.77
Mean + 3∗SD	91.15	8.85
Mean + 4∗SD	92.89	7.58
Mean + 5∗SD	**93.40**	6.60

The bold value highest authentication accuracy %.

In Table 8, it is observed that the enrolments of the same individual at different instances are generating completely new database templates. The high RMSE values show dissimilarity to the stored template and prove renewability.

Also, the stored template is not linked with any of the original templates used for authentication. The generated secure template is irreversible, unlikable, and also renewable.

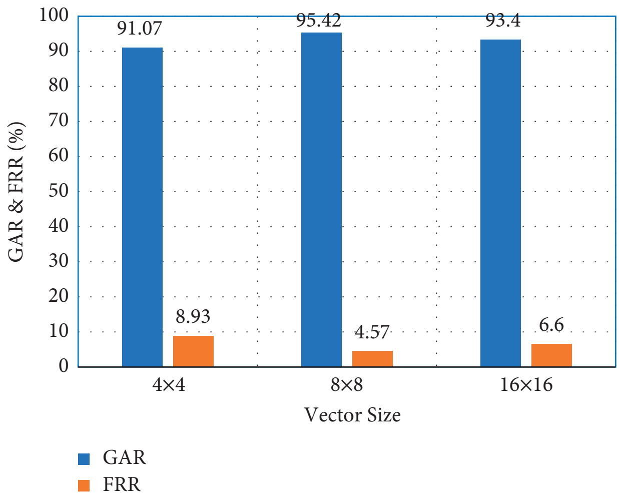


Figure 4: GAR for 4 X 4, 8 X 8, and 16 X 16 feature vector size.

Table 7: Space complexity for no. of traits.

Traits	No. of traits used	Original size	Size in the database
Fingerprint, iris	2	2 ∗ 512 X 512	8 X 8
Fingerprint, palm print, iris	3	3 ∗ 512 X 512	8 X 8
Two different fingerprints, palm print, iris	4	4 ∗ 512 X 512	8 X 8
Fingerprint, palm print, iris, face	5	5 ∗ 512 X 512	8 X 8
"*n*" no. of traits	*n*	*n* ∗ 512 X 512	8 X 8

Table 8: RMSE values of the biometric template of the same individual.

Sr. No.	RMSE values of the biometric template of the same individual
1	5589.982
2	5677.534
3	5627.536
4	4873.231
5	5644.982

5. Conclusion

In this work, we have addressed the problem of a secured authentication system with privacy preservation of biometrics. An irreversible, unlinkable, and renewable image transformation technique is implemented based on Lagrange's interpolation and discrete cosine transform (DCT) feature transformation for user authentication. The proposed system provides a secure authentication system with high accuracy, a constant size database, and protection of multi-biometric traits. The original multi-biometric traits of size 512 X 512 are reduced to a secure database template of size 8 X 8. This reduces the database size to a great extent, which results in saving storage requirements. The addition of a number of biometric traits used for authentication keeps the size of the final storage requirement as 8X8, which achieves constant space complexity. The generated secure template is irreversible, unlikable, and also renewable. The proposed system gives an average of 95.42% GAR and an average of 4.57% FRR. These obtained GAR and FRR validate the high accuracy of the proposed multi-biometric authentication technique. In future work, the authentication process can be expedited with parallel processing. The proposed system can be extended to various sensor-based biometric applications such as Aadhar cards, e-passports, and similar applications.

Nomenclature

LI:	Lagrange's interpolation
DCT:	Discrete cosine transform
GAR:	Genuine acceptance rate
FRR:	False rejection rate
BTP:	Biometric template protection
EU:	European Union
GDPR:	General data protection regulation
BSIF:	Binarized/binary statistical image features
IFO:	Indexing first one
SHA:	Single hash attack
RMA:	Record multiplicity attack
SSS:	Secret sharing scheme
RMSE:	Root-mean-square error
SD:	Standard deviation
IoT:	Internet of things

Data Availability

Dataset Used: The Hong Kong Polytechnic University, http://www.comp.polyu.edu.hk/~biometrics/HRF/HRF.htm.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] M. Ahlawat and C. Kant, “An introduction to multimodal biometric system: an overview,” *IJSRD-International J.*vol. 3, no. 02, pp. 1150–1154, 2015.

[2] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, “Multi-biometric template protection based on Homomorphic Encryption,” *Pattern Recognition*, vol. 67, pp. 149–163, 2017.

[3] R. S. Patil, S. D. Patil, and S. D. Thepade, “Performance evaluation of fingerprint trait authentication system,” *Advances in Intelligent Systems and Computing*, vol. 632, pp. 143–151, 2018.

[4] R. S. Patil, “An explication of multifarious secret sharing schemes,” *International Journal of Computers and Applications*, vol. 46, no. 19, 2012.

[5] S. Patil, K. Tajane, and J. Sirdeshpande, “Secret sharing schemes for secure biometric authentication,” *International Journal of Scientific Engineering and Research*, vol. 4, no. 6, pp. 2890–2895, 2013.

[6] J. Dong, X. Meng, M. Chen, and Z. Wang, “Template protection based on DNA coding for multimodal biometric recognition,” in *Proceedings of the 2017 4th 2017 4th International Conference on Systems and Informatics (ICSAI)*, pp. 1738–1742, Hangzhou, China, November 2017.

[7] M. I. Ahmad, N. Mohamad, M. N. Md Isa, R. Ngadiran, and A. M. Darsono, “Fusion of low frequency coefficients of DCT transform image for face and palmprint multimodal biometrics,” in *Proceedings of the 2017 3rd IEEE International Conference on Cybernetics (CYBCONF)*, Exeter, UK, June 2017.

[8] D. Jagadiswary and D. Saraswady, “Biometric authentication using fused multimodal biometric,” *Procedia Computer Science*, vol. 85pp. 109–116, Cms, 2016.

[9] A. Nandhinipreetha and N. Radha, “Multimodal biometric template authentication of finger vein and signature using visual cryptography,” in *Proceedings of the 2016 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 7–10, Coimbatore, India, January 2016.

[10] S. Patil, K. Bhagat, S. Bhosale, and M. Deshmukh, “Intensification of security in 2-factor biometric authentication system,” in *Proceedings of the 2015 2015 International Conference on Pervasive Computing (ICPC)*, Pune, India, January 2015.

[11] R. Patil, S. Patil, and S. Thepade, “Secret sharing based secure authentication system,” *International Journal of Computer Application*, vol. 118, no. 22, pp. 8–11, 2015.

[12] G. Kumar and P. K. Bhatia, “A detailed review of feature extraction in image processing systems,” in *Proceedings of the 2014 Fourth International Conference on Advanced Computing & Communication Technologies*, Rohtak, India, February 2014.

[13] A. Meraoumia, S. Chitroub, and A. Bouridane, “Robust multimodal biometric identification system using Finger-Knuckle-Print features,” in *Proceedings of the 2015 3rd International Conference on Control, Engineering & Information Technology (CEIT)*, Tlemcen, Algeria, May 2015.

[14] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-factor authentication: a survey,” *Cryptography*, vol. 2, no. 1, pp. 1–31, 2018.

[15] S. Kumar, S. Modak, and V. K. Jha, “A novel technique to enhance performance of multibiometric framework using Bin based classifier based on multi-algorithm score level fusion,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 3, pp. 2156–2166, 2020.

[16] E. Balraj and T. Abirami, “A multi-biometric authentication system using fusion level techniques,” *Int. J. Sci. Technol. Res.*vol. 9, no. 1, pp. 3332–3335, 2020.

[17] J. Peng, Q. Li, A. A. Abd El-Latif, and X. Niu, “Finger multibiometric cryptosystems: fusion strategy and template security,” *Journal of Electronic Imaging*, vol. 23, no. 2, p. 023001, 2014.

[18] K. Vishi and V. Mavroeidis, “An evaluation of score level fusion approaches for fingerprint and finger-vein biometrics,” no. Nisk,” 2018, http://arxiv.org/abs/1805.10666.

[19] C. Rathgeb, B. Tams, J. Wagner, and C. Busch, “Unlinkable improved multi-biometric iris fuzzy vault,” *EURASIP Journal on Information Security*, vol. 2016, no. 1, 2016.

[20] M. Stokkenes, R. Ramachandra, M. K. Sigaard, K. Raja, M. Gomez-Barrero, and C. Busch, “Multi-biometric template protection - a security analysis of binarized statistical features for Bloom filters on smartphones,” in *Proceedings of the 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, Oulu, Finland, December 2016.

[21] M. K. Morampudi, M. V. N. K. Prasad, and U. S. N. Raju, “Privacy-preserving iris authentication using fully homomorphic encryption,” *Multimedia Tools and Applications*, vol. 79, no. 27-28, pp. 19215–19237, 2020.

[22] S. Kirchgasser, L. Debiasi, R. Schraml et al., “Template protection on multiple facial biometrics in the signal domain under visible and near-infrared light,” in *Proceedings of the 2020 8th International Workshop on Biometrics and Forensics (IWBF)*, Porto, Portugal, April 2020.

[23] M. Gomez-Barrero, C. Rathgeb, G. Li, R. Ramachandra, J. Galbally, and C. Busch, “Multi-biometric template protection based on bloom filters,” *Information Fusion*, vol. 42, pp. 37–50, 2018.

[24] P. Drozdowski, S. Garg, C. Rathgeb, M. Gomez-Barrcro, D. Chang, and C. Busch, “Privacy-preserving indexing of iris-codes with cancelable bloom filter-based search structures,” in *Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO)*, pp. 2360–2364, Rome, Italy, September 2018.

[25] K. B. Raja, R. Raghavendra, and C. Busch, “Towards reducing the error rates in template protection for Iris recognition using custom Cuckoo filters,” in *Proceedings of the 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, pp. 1–8, Hyderabad, India, January 2019.

[26] M. Gomez-Barrero and J. Galbally, “Reversing the irreversible: a survey on inverse biometrics,” *Computers & Security*, vol. 90, p. 101700, 2020.

[27] A. Singh, A. Arora, G. Jaswal, and A. Nigam, “Comprehensive survey on cancelable biometrics with novel case study on finger dorsal template protection,” *Journal of Banking and Financial Technology*, vol. 4, no. 1, pp. 37–52, 2020.

[28] A. Sarkar and B. K. Singh, “A review on performance,security and various biometric template protection

schemes for biometric authentication systems," *Multimedia Tools and Applications*, vol. 79, no. 37-38, pp. 27721–27776, 2020.

[29] S. S. Ali, V. S. Baghel, I. I. Ganapathi, and S. Prakash, "Robust biometric authentication system with a secure user template," *Image and Vision Computing*, vol. 104, Article ID 104004, 2020.

[30] H. Wang, X. Li, and R. H. Jhaveri, "Sparse Bayesian learning based channel estimation in FBMC/OQAM industrial IoT networks," *Computer Communications*, vol. 176, pp. 40–45, 2021.

[31] R. H. Jhaveri, N. M. Patel, Y. Zhong, and A. K. Sangaiah, "Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT," *IEEE Access*, vol. 6, pp. 20085–20103, 2018.

[32] A. Ninassi, S. Vernois, and C. Rosenberger, "Privacy compliant multi-biometric authentication on smartphones," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy*, pp. 173–181, Funchal, Portugal, January 2018.

[33] C. Patel, D. Joshi, N. Doshi, A. Veeramuthu, and R. Jhaveri, "An enhanced approach for three factor remote user authentication in multi - server environment," *Journal of Intelligent and Fuzzy Systems*, vol. 39, no. 6, pp. 8609–8620, 2020.

[34] J. Hämmerle-Uhl, E. Pschernig, and A. Uhl, "Cancelable Iris biometrics using block Re-mapping and image warping," in *Proceedings of the ISC '09: Proceedings of the 12th International Conference on Information Security*, pp. 135–142, Pisa, Italy, September 2009.

[35] L. Catuogno, C. Galdi, and D. Riccio, "An enterprise rights management system for on-the-field maintenance facilities," *IEEE Access*, vol. 8, pp. 95987–95996, 2020.

[36] S. Chikkerur, N. K. Ratha, J. H. Connell, and R. M. Bolle, "Generating registration-free cancelable fingerprint templates," in *Proceedings of the 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*, Washington, DC, USA, October 2008.

[37] A. Gupta, A. Malage, D. More, P. Hemane, P. Bhautmage, and D. Dhandekar, "Feature level fusion of face, palm vein and palm print modalities using Discrete Cosine Transform," in *Proceedings of the 2014 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014)*, pp. 1–5, Unnao, India, Auguest 2014.

[38] O. Nafea, S. Ghouzali, W. Abdul, and E.-u.-H. Qazi, "Hybrid multi-biometric template protection using watermarking," *The Computer Journal*, vol. 59, no. 9, pp. 1392–1407, 2016.