IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 9, September 2024

DOI: 10.17148/IJARCCE.2024.13907

Cancellable Biometrics: Trends and Innovations Over the Past Decade

Diptadip Maiti[1], Madhuchhanda Basak[2]

Department of CSE, Techno India University, Kolkata, India[1]

Department of CSE, Brainware University, Barasat, India[2]

Abstract: The paper provides a comprehensive overview and comparative analysis of recent advancements in cancellable biometrics methods. Through an in-depth examination of various studies, the paper showcases a diverse range of techniques and features utilized to enhance the security, privacy, and accuracy of biometric authentication systems. Key findings include the development of robust fingerprint templates using techniques such as Delaunay Triangulation Net and alignment-free templates, as well as the exploration of multi-modal approaches combining different biometric modalities for improved performance. Additionally, privacy-preserving techniques, machine learning-based approaches, and novel integrations with block chain technology are investigated to address concerns about data protection and authentication reliability. The paper highlights the richness and diversity of research efforts in cancellable biometrics, providing valuable insights and advancements to address emerging threats in biometric security.

Keywords: Cancellable biometrics, Template protection, Alignment-free templates, Revocability, Non-invertibility

I. INTRODUCTION

Due to its capacity to provide reliable identity verification, biometric identification techniques have become increasingly popular in today's increasingly digital environment. Biometric systems offer an easy and safe way to regulate access, authorize transactions, and verify identity by using unique physiological or behavioural characteristics like fingerprints, face features, or speech patterns. But in addition to all of its benefits, biometric technologies also present a number of security and privacy issues that should not be disregarded [1]. Biometric data, once compromised, becomes an enduring part of an individual's identity, unlike traditional password-based authentication, where compromised credentials can be readily cancelled or altered. Due to the inability to change or withdraw biometric data, people run serious risks to their personal and financial security and are more susceptible to identity theft and illegal access. Furthermore, the widespread use of biometric systems in many applications has resulted in the accumulation of large databases holding private biometric data, giving rise to worries about privacy violations, monitoring of users, and surveillance. Figure 1 shows the different biometric traits of humans.

Biometric data, once compromised, becomes an enduring part of an individual's identity, unlike traditional password-based authentication, where compromised credentials can be readily cancelled or altered [2].

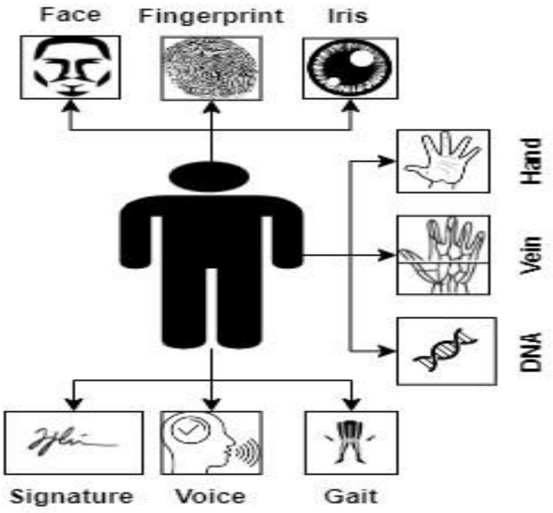

Fig.1. Different Biometric Traits

Due to the inability to change or withdraw biometric data, people run serious risks to their personal and financial security and are more susceptible to identity theft and illegal access. Furthermore, the widespread use of biometric systems in many applications has resulted in the accumulation of large databases holding private biometric data, giving rise to worries about privacy violations, monitoring of users, and surveillance. The goal of this review article is to examine the complexities of cancellable biometrics by offering a thorough examination of the different approaches, strategies, and developments in the subject. The goal of the work is to clarify the advantages, disadvantages, and possible weaknesses of each cancellable biometric methodology by carefully analysing random projections, non-invertible geometric transforms, bio-hashing techniques, and other approaches. Furthermore, the article seeks to identify prospects for additional innovation and improvement in cancellable biometric systems by examining recent research developments and developing trends. The ultimate objective is to promote a better comprehension of cancellable biometrics and its function in resolving the changing privacy and security issues associated with biometric authentication [3].

II. CANCELLABLE BIOMETRICS & ITS PRINCIPALS

In biometric authentication systems, cancellable biometrics is a security and privacy-enhancing technique that converts biometric data into irreversible, non-sensitive representations called cancellable templates [4]. By ensuring that the cancellable template cannot be used to recreate the original biometric data, this transformation procedure protects user privacy and reduces the possibility of illegal access. Users with cancellable biometric systems get control over their biometric data and can handle security issues like identity theft and biometric template theft by being able to revoke and regenerate their biometric templates. Achieving a balance between security and usability is the major objective of cancellable biometrics, which guarantees strong biometric data protection while preserving the efficiency and practicality of biometric authentication 5]. Figure 2 shows the basic block diagram of a cancellable biometric system. The key principles of cancellable biometrics include:

2.1 Irreversibility [4]: The irreversibility principle guarantees that biometric data cannot reasonably be reverse-engineered or reconstructed to obtain the original biometric information once it has been altered. Irreversible transformations theft by securing biometric templates against misuse and unwanted access.

2.2 Non Invertibility [4]: The characteristic of biometric transformations known as" noninvertibility" states that the original biometric data cannot be computationally recovered from its altered representation. Non-invertibility is achieved by using techniques like encryption and cryptographic hashing, which make sure that even if the altered data is intercepted, it cannot be utilized to recreate the original biometric information.

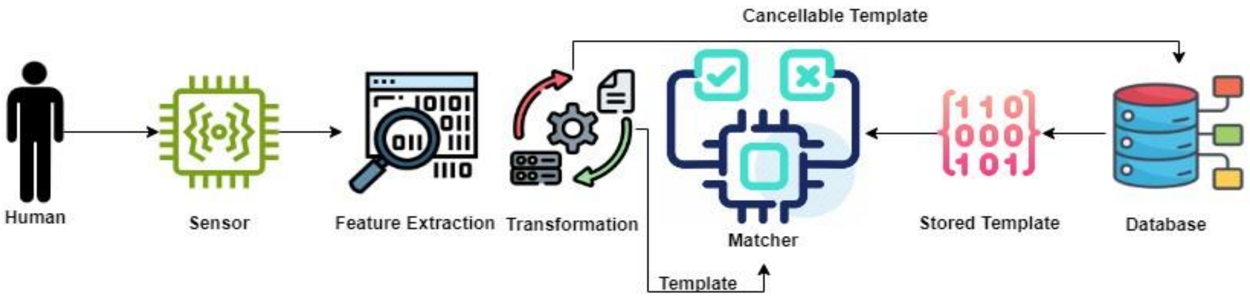

Fig.2. Cancellable Biometric System

2.3 Revocability [4]: Users can revoke and regenerate their biometric templates in the case of a security breach or compromise thanks to revocability. By giving users control over their biometric information, this principle helps individuals reduce the dangers of misuse or unwanted access to their biometric identifiers.

III. TRANSFORMATION TECHNIQUES OF CANCELLABLE BIOMETRIC

In cancellable biometrics, transformation techniques play a crucial role in transforming biometric data into irreversible, non-sensitive representations called cancellable templates. These methods improve security and privacy in biometric authentication systems by making sure that the converted data cannot be reverse engineered to acquire the original biometric information. Figure 3 shows the different transformation techniques used for cancellable biometric. Typical transformation methods include the following:

DOI: 10.17148/IJARCCE.2024.13907

3.1 Feature Transformation Methods [6]:

3.1.1 Random Projection: Using this method, the discriminative information of the biometric feature vectors is preserved while the dimensionality of the data is decreased by projecting them onto a random subspace. Random projection makes it impossible to computationally recover the original data while ensuring that the altered features retain their uniqueness.

3.1.2 Quantization: Each feature vector is assigned to a matching quantized zone by quantization, which divides the continuous feature space into discrete regions. The biometric data is discretized by this procedure, strengthening its defence against reverse engineering.

3.1.3 Salting: Prior to transformation, the biometric feature vectors are salted, or perturbed, by adding random noise. Because of the diversity that this randomization procedure adds to the data, it is harder for attackers to deduce the original biometric information.

3.2 Template Transformation Techniques [7]

3.2.1 Fuzzy Commitment: Fuzzy commitment approaches create cancellable templates that can only be decrypted with the matching keys by binding biometric templates to secret keys using cryptographic techniques. This improves security by guaranteeing that the altered templates cannot be reversed without the key.

3.2.2 Cryptographic Hashing: In order to guarantee that comparable inputs yield different hash values, hashing algorithms use biometric templates to construct fixed-size hash values. The one-way nature of hash functions means that it is computationally impossible to deduce the original template from its hash.

3.2.3 Permutation Methods: Biometric template components can be rearranged using permutation approaches by using a predetermined permutation function. It becomes challenging to recreate the original template as a result of this shuffling process, which modifies the template’s structure while maintaining its discriminatory qualities.

3.3 Hybrid Approaches [8]: To balance security and performance, hybrid systems combine both feature and template transformation techniques. Hybrid approaches can improve the efficacy and resilience of cancellable biometric systems by utilizing the complimentary characteristics of several transformation techniques.

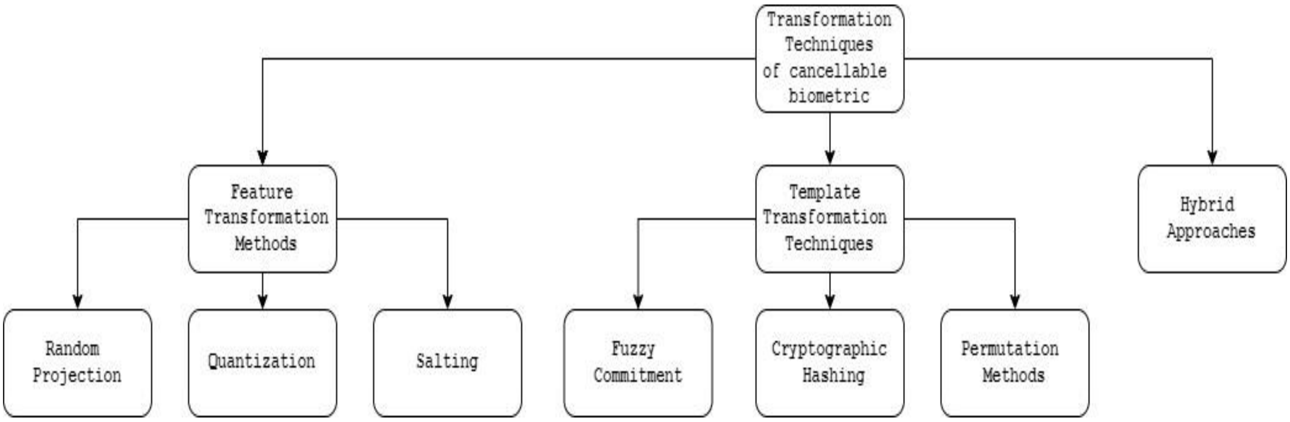
Transformation Techniques of cancellable biometric
Feature Transformation Methods
Template Transformation Techniques
Hybrid Approaches
Random Projection
Quantization
Salting
Fuzzy Commitment
Cryptographic Hashing
Permutation Methods

Fig.3. Transformation Techniques of cancellable biometric

IV. ATTACKS ON CANCELLABLE BIOMETRIC

The purpose of cancellable biometric systems is to improve biometric authentication security and privacy. They are not impervious to some attacks, though [9]. Figure 4 shows the different attacks on cancellable biometric. Among the possible assaults on cancellable biometric systems are:

DOI: 10.17148/IJARCCE.2024.13907

4.1 Template Reconstruction Attacks [10]

4.1.1 Reverse Engineering: In an attempt to recreate the original biometric data, attackers try to reverse-engineer cancellable templates. In order to obtain the original biometric features, this entails dissecting the transformation algorithms and taking use of weaknesses.

4.1.2 Template Matching: In order to find the matching person, attackers can attempt to match cancellable templates with well-known biometric databases or use a brute force search over a sizeable dataset.

4.2 Model-based Attacks [11]:

4.2.1 Model Inversion: By looking at the transformation process’s output, adversaries try to deduce the transformation model employed in cancellable biometric systems. The original biometric data can then be rebuilt using this knowledge to undo the alteration.

4.2.2 Adversarial Learning: Attackers may be able to create artificial cancellable templates or circumvent the system’s security measures by using machine learning techniques to train models that mimic the transformation function.

4.3 Side-channel Attacks [3]:

4.3.1 Timing Analysis: Attackers use differences in the time or processing power needed for various transformation operations as a means of deducing details about the transformation procedure or the cancellable templates.

4.3.2 Power Analysis: In order to obtain sensitive information about the biometric data or cryptographic keys, adversaries keep an eye on patterns of power usage or electromagnetic emissions while the transformation algorithms are being executed.

4.4 Biometric Spoofing [12]:

4.4.1 Presentation Attacks: Attackers attempt to mimic authorized users and obtain illegal access by presenting synthetic or altered biometric samples (e.g., phony fingerprints or face photos) to the biometric system.

4.4.2 Gait Spoofing: Adversaries circumvent cancellable biometric systems that rely on dynamic biometric modalities by imitating the distinct gait patterns or behavioural biometrics of authorized users.

4.5 Cryptographic Attacks [13]:

4.5.1 Key Recovery: By taking advantage of flaws in the encryption or key management systems, attackers try to get secret keys or cryptographic parameters utilized in the transformation techniques.

4.5.2 Collision Attacks: When using cancellable biometric systems, adversaries look for collisions in hash functions or cryptographic primitives to identify different inputs that result in the same output, possibly jeopardizing system security.

4.6 Interference Attacks [14]:

4.6.1 Denial-of-Service (DoS): By flooding cancellable biometric systems with too many authentication requests or by interfering with the biometric data capture procedure, attackers cause disruptions to the system’s functionality.

4.6.2 Jamming: In order to prevent authorized users from accessing the biometric authentication system, adversaries use signal jamming or electromagnetic interference techniques to interfere with the communication channels or sensors used in the system.

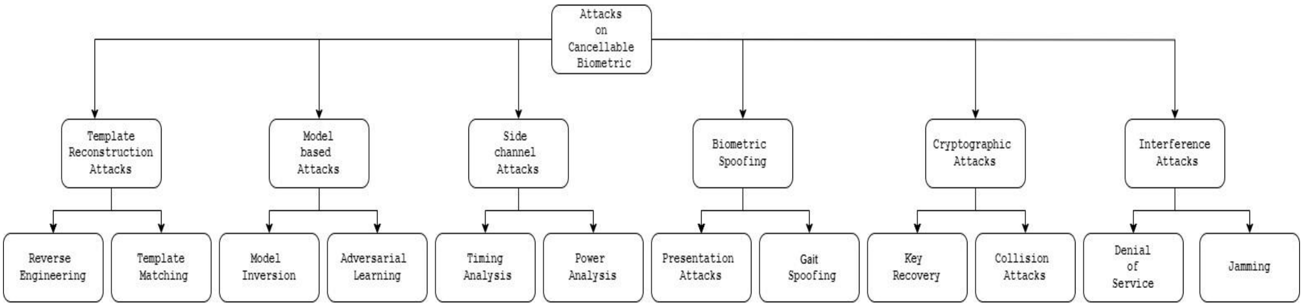

Fig.4. Attacks on Cancellable Biometric

V. DECADE OF CANCELLABLE BIOMETRIC INNOVATION

Al-Assam et al. [15] propose a novel authentication method integrating refundable biometrics and mobile device location to generate one-time authentication tokens, enhancing security. Facial features are extracted using Discrete Wavelet Transform, and the scheme demonstrates effectiveness in reducing identity theft risks in mobile authentication settings. Wong et al. [16] enhance the accuracy and security of cancellable fingerprint templates with the Multi-Line Code (MLC) approach, introducing modifications like dynamically weighted integrated Dice (DWID) similarity. Their method exhibits low Equal Error Rates (EERs) even in stolen key scenarios, as evidenced by evaluations on Fingerprint Verification Competition (FVC) datasets.

Wong et al. [17] introduce a cost-effective cancellable fingerprint template technique, Multi-Line Code (MLC), maintaining performance with low computational complexity. Tested on FVC datasets, it outperforms other distribution-based algorithms, showing promising results with an EER of 4.69% in stolen-key situations on FVC2002 DB1. Wang et al. [18] propose a technique for creating cancellable fingerprint templates without pre-registration, utilizing curtailed circular convolution for efficient one-way transform. Their method demonstrates satisfactory performance across various databases without requiring image realignment, ensuring diversity, revocability, and noninvertibility. Jin et al. [19] present Randomized Graph based Hamming Embedding (RGHE) for creating cancellable fingerprint templates, preserving discriminability in Hamming space and enhancing security against attacks. Evaluation on FVC datasets shows promising results, with low EERs in stolen-token situations. Ferrara et al. [20] address drawbacks of P-MCC templates by introducing 2P-MCC, a two-factor protection system for reversible Minutia Cylinder-Code (MCC) templates. Evaluation on public datasets demonstrates notable improvements over existing techniques in terms of precision and resistance to various attacks.

Rathgeb et al. [21] propose a privacy-preserving biometric authentication framework based on Bloom filters, facilitating feature-level fusion of biometrics while ensuring irreversibility. Evaluation using face and iris databases shows high accuracy and very low equal-error rates, validating the effectiveness of the approach. Sandhya et al. [22] introduce a fingerprint template security technique based on k-Nearest Neighborhood Structure (kNNS), achieving diversity, accuracy, irreversibility, and revocability. Evaluation on FVC 2002 datasets demonstrates improved performance with low EERs across different databases. Kaur et al. [23] propose a method utilizing Gaussian random vectors and one-way modulus hashing for creating cancellable biometric templates, ensuring non-reversibility and simplicity in cancellation. Evaluation on face and palm print modalities shows low Equal Error Rates and non-invertibility of the templates.

Gomez et al. [24] present an irreversible and unlinkable biometric template protection mechanism based on Bloom filters, maintaining accuracy while enhancing security against attacks. Evaluation on face data demonstrates robustness against brute force attacks and cross-matching resistance. Wang et al. [25] propose an innovative technique for creating alignment-free cancellable fingerprint templates based on blind system identification. The method utilizes minutiae-based methods for picture pre-alignment, making it suitable for resource-constrained applications like smart cards and mobile phones. Evaluation on FVC2002 databases demonstrates its effectiveness and comparability with current alignment-free templates.

Wang et al. [26] suggest a technique employing partial Hadamard transform to design cancellable biometrics, preserving binary representations while meeting revocability and diversity requirements. Evaluation on multiple datasets shows competitive recognition performance, particularly in lost-token scenarios, with low Equal Error Rates across different databases.

DOI: 10.17148/IJARCCE.2024.13907

Wang et al. [27] develop a novel technique using local minutia structures for creating alignment-free cancellable fingerprint templates, featuring a computationally efficient partial DFT-based transformation. The approach exhibits robustness against attacks and vulnerability to the ARM, with extensive testing on public databases demonstrating its effectiveness.

Kaur et al. [28] introduce a template protection method utilizing log-Gabor filters to generate reversible binary features, offering strong matching performance across various biometric modalities. The technique proves effective in instances involving stolen tokens and resilient to correlation attacks, ensuring privacy and security. Jin et al. [29] demonstrate Index-of-Max hashing as a two-factor cancellable biometric, providing high accuracy while satisfying non-invertibility, revocability, and non-likability requirements. Experimental results on benchmark fingerprint databases showcase positive accuracy performance and robustness against attacks.

Mukhaiyar [30] presents a cancellable fingerprint system utilizing matrix operations to transform biometric data into abstract representations, demonstrating effectiveness across various databases. The approach offers flexibility in controlling error rates and processing time, suitable for practical implementation. Alam et al. [31] propose an alignment-free cancellable fingerprint template based on noise addition and transformation using Discrete Fourier Transform and random projection. Evaluation on benchmark databases shows robustness against attacks and equivalent accuracy to current approaches. Yang et al. [32] suggest a cancellable multibiometric system utilizing feature-level fusion and noninvertible transformation, achieving consistently low error rates across multiple datasets. Kaur et al. [33] describe the Random Distance Method for producing cancellable biometric characteristics, offering improved efficiency, resistance to attacks, and privacy protection. Experimental evaluation on various datasets demonstrates superior performance compared to original templates.

Kaur et al. [34] introduce the Random Slope approach for creating safe, reversible, and noninvertible cancellable biometric templates, achieving dimensionality reduction and high accuracy across different biometric modalities. Evaluation shows effectiveness in meeting cancelability requirements and preserving user privacy. Dong et al. [35] introduces GASAF, a framework revealing the vulnerability of cancellable biometrics (CB) to similarity-based attacks (SA), especially when possessing a similarity-preserving property. GASAF is evaluated using typical CB methods on iris and face datasets, highlighting its potential risk in real-world scenarios. Jang et al. [36] proposes a cancellable face authentication system employing a Deep Table-based Hashing (DTH) framework, integrating Convolutional Neural Network (CNN)-based features with noise embedding and intra-normalization for enhanced non-invertibility. Evaluation on largescale face datasets demonstrates superior performance in meeting cancelability requirements.

Kim et al. [37] presents a GLRT-based cancellable ECG biometric system utilizing composite hypothesis testing in the compressive sensing domain, coupled with a permutation-based revocation technique for resistance against attacks. The proposed method achieves high detection probability and low false alarm rates, ensuring secure and efficient authentication. Kho et al. [38] introduces a novel alignment-free cancellable fingerprint template design technique based on Partial Local Structure (PLS) descriptor and randomized Non-Negative Least Squares (R-NNLS) optimization, demonstrating improved performance and cancelability across various datasets. Soliman et al. [39] proposes a modified cancellable biometrics system for iris recognition using random projection, featuring iris localization, noise embedding, and segmentation for enhanced security and robustness against attacks. Evaluation on the CASIAIrisV3 dataset showcases impressive identification rates and superior Equal Error Rate (EER).

Walia et al. [40] suggests a real-time, cancellable multimodal biometric system based on deep feature unification, achieving revocability and dimensionality reduction through keys-based feature extraction and non-linear optimum cross diffusion of deep features. Evaluation on benchmark datasets demonstrates favorable performance compared to existing methods. Algarni et al. [41] proposes a cancellable face and fingerprint recognition system using discrete transforms and matrix rotations for enhanced security and simplicity. Evaluation on standard datasets shows improved accuracy and efficiency compared to conventional methods. Li et al. [42] introduces a novel fingerprint template based on local similar image (LSIT) for secure and efficient fingerprint application, achieving cancellability and recognition performance through feature mapping and abstraction. Evaluation on FVC2002 and FVC2004 datasets yields promising results. Yang et al. [43] presents a feature-adaptive random projection-based approach for secure biometric template matching and protection in the encrypted domain, ensuring data security while maintaining competitive performance. Evaluation on publicly accessible databases supports the effectiveness of the proposed method.

Shahzad et al. [44] introduces a novel alignment-free cancellable fingerprint template with dual protection, combining partial discrete wavelet transform (DWT) with a window-shift-XOR model. The approach demonstrates superior performance and increased security across various fingerprint databases, with promising results in terms of equal error

DOI: 10.17148/IJARCCE.2024.13907

rates (EER) and resistance to attacks. Jain et al. [45] proposes a cancellable fingerprint template method utilizing Delaunay Triangulation Net to triangulate points on low-quality fingerprints. Evaluation on benchmark databases shows improved performance compared to existing models, meeting performance metrics such as EER, false acceptance rate (FAR), genuine rejection rate (GRR), and genuine acceptance rate (GAR).

Lee et al. [46] presents Multi-modal Extended Feature Vector (MEFV) hashing, a token less cancellable biometrics approach for face and fingerprint fusion. Evaluation on benchmark datasets demonstrates empirical confirmation of the technique’s effectiveness, showcasing superior matching accuracy and resilience to attacks. Kavati et al. [47] suggests a method for protecting fingerprint templates using elliptical shapes derived from minutiae details, achieving promising results in terms of performance metrics such as false rejection rate (FRR), false acceptance rate (FAR), and equal error rate (EER) across various fingerprint databases.

Wu et al. [48] proposes a cancellable biometric authentication key agreement approach based on the random distance method (RDM) and elliptic curve cryptography (ECC), ensuring privacy protection and resisting various attacks. Experimental evaluation on multiple datasets demonstrates improved biometric authentication accuracy compared to similar techniques. Sperling et al. [49] introduces HEFT, an end-to-end, homomorphically encrypted, non-interactive feature-level fusion and matching system for multi-modal biometrics. Evaluation on voice and face biometric datasets shows significant improvements in matching performance and feature compression compared to uni-biometric representations.

Yin et al. [50] proposes a lightweight cancellable fingerprint template design suitable for Internet of Things (IoT) applications, achieving equivalent authentication performance to state-of-the-art methods while reducing template storage space and computational cost. Kim et al. [51] presents CSMoFN, an end-to-end multi-modal cancellable biometrics method based on deep learning, achieving state-of-the-art verification accuracy on multiple face-periocular multimodal datasets. Elsadai et al. [52] recommends a novel fingerprint recognition method utilizing stylometric features and machine learning techniques, achieving high accuracy and low false acceptance rate (FAR) compared to existing approaches.

Ayoup et al. [53] outlines a cancellable multi-biometric identification scheme demonstrating strong tolerance to noise effects and reduced enrolment procedure runtime, making it suitable for real-time and IoT applications. Ayoup et al. [54] introduces a cancellable multi-biometric system combining encryption techniques, deep-learning-based feature fusion, and selective encryption, providing improved protection and performance metrics such as ROC, AROC, correlation, and entropy.

V. COMPARATIVE ANALYSIS

With a focus on improving security, privacy, and accuracy in biometric authentication systems, the Table 1 offers a thorough summary of current developments in biometric template protection techniques. Numerous features and approaches are used in all the research, such as feature-level fusion, fingerprint template augmentation, cancellable template design, encryption techniques, and authentication token generation.

Specific biometric security issues, like revocability, non-invertibility, attack resistance, and privacy protection, are addressed by each technique. Numerous research endeavors center on enhancing the resilience of fingerprint templates using methods such as partial Hadamard transform, alignment-free templates, Delaunay Triangulation Net, and Gaussian random vectors. In order to improve accuracy and security, several researchers investigate multi-modal techniques that combine various biometric modalities, such as facial and periocular areas.

The use of random projection, permutation-based revocation, and matrix operations to create non-invertible and revocable templates is another notable element of cancellable biometric systems. Concerns regarding data security and confidentiality are addressed by privacy-preserving methods such homomorphically encrypted fusion systems, irreversible representation, and selective encryption.

Furthermore, new techniques for enhancing the precision and dependability of authentication are demonstrated by stylometric features, block chain integration, and machine learning-based methods. The Table 1, taken as a whole, shows the depth and breadth of research endeavors in biometric template protection, with every work making significant contributions to the field’s understanding and progress. Together, these techniques push the limits of biometric security and provide creative answers to new problems and dangers in the quickly changing field of biometric authentication.

DOI: 10.17148/IJARCCE.2024.13907

Table 1. Comparative Analysis of Cancellable Biometric Methods

Study	Method	Techniques/Features	Datasets	Performance
Al-Assam et al. [15]	Authentication token generation	Refundable biometrics, real location, time stamp	Location dataset (London, UK), Extended Yale-B database	Encouraging outcomes for unprotected and mobile authentication settings
Wong et al. [16]	Enhanced MLC-based fingerprint template	Mean modification, binary representation, DWID similarity	FVC datasets	Low EERs in genuine-key and stolen-key scenarios
Wong et al. [17]	Multi-line code fingerprint template	Minutia codes, multi-line code permutation, fingerprint matching	FVC2002 DB1, DB2, FVC2004 DB1	Outperformed other algorithms in stolen-key situation
Wang et al. [18]	cancellable fingerprint templates	Circular convolution, revocability, non-invertibility	FVC2002 DB1, DB2, DB3	Satisfactory performance without image pre-alignment
Jin et al. [19]	Randomized Graph-based Hamming Embedding	Minutiae vicinity decomposition, random projection	FVC2002, FVC2004	Low EERs in stolen-token situation
Ferrara et al. [20]	Two-factor protection system	2P-MCC templates	FVC2002, FVC2004, FVC2006 datasets	Notable improvements in security features
Rathgeb et al. [21]	Privacy-preserving biometric authentication	Irreversible representation, feature-level fusion	BioSecure face corpus, IITD iris database	Very low EER demonstrating privacy protection and biometric performance
Sandhya et al. [22]	k-NNS alignment-free fingerprint template	k-NNS structure, Discrete Fourier Transform	FVC 2002 DB1, DB2, DB3	Better performance in terms of EER
Kaur et al. [23]	Gaussian random vectors for biometric templates	One-way modulus hashing	Face and palmprint biometric modalities	Almost zero EER and simplicity in cancellation and revocation
Gomez et al. [24]	Irreversible and unlinkable biometric template protection	Bloom filters	BioSecure Multi-modal Database (face corpus)	Maintained accuracy with resistance against known attacks
Wang et al. [25]	Blind system identification for alignment-free templates	Minutiae-based methods, resource-constrained applications	FVC2002 DB1, DB2, DB3	Satisfactory performance across databases
Wang et al. [26]	Partial Hadamard transform for cancellable biometrics	Binary biometric representations, revocability, diversity	FVC2002 DB1, DB2, DB3	Favourable recognition performance in lost-token scenario
Wang et al. [27]	Local minutia structures for alignment-free templates	Partial DFT-based non-invertible transformation	FVC2002 DB1-DB3, FVC2004 DB2	Extensively tested with promising performance metrics
Kaur et al. [28]	Log-Gabor filters for reversible binary features	Multi-level modifications, various biometric modalities	Various datasets	Strong matching performance and resistance against attacks
Jin et al. [29]	"Index-of-Max" hashing for two-factor cancellable biometrics	Random parameters, IoM hashing	FVC2002, FVC2004	Positive accuracy performance and meeting security requirements

Mukhaiyar [30]	Matrix operations for cancellable fingerprint system	Kronecker Product, Elementary Row Operation, Inverse Matrix	Various databases	Error rate of 0.063 with influenced processing time
Alam et al. [31]	Alignment-free cancellable fingerprint template	Discrete Fourier transform, random projection	FVC2002, FVC2004	Robustness against attacks with equivalent accuracy
Yang et al. [32]	Feature-level fusion for cancellable multi-biometric system	EP-DFT transformation	Several datasets	Consistently low error rates with enhanced security
Kaur et al. [33]	"Random Distance Method" for cancellable biometric characteristics	Modified domain, smaller revocable templates	Unimodal and multimodal databases	Outperformed original templates in terms of efficiency and privacy
Kaur et al. [34]	"Random Slope" approach for safe, reversible templates	Dimensionality reduction, non-invertible templates	Various biometric modalities	Accuracy scores ranging from 60% to nearly 100%
Dong et al. [35]	GASAF for similarity-based attacks on CB systems	Genetic Algorithm, Similarity-based attacks	CASIA-Iris-Interval, LFW datasets	High potential risk in real-life with quick completion
Jang et al. [36]	Convolutional Neural Network- based face authentication	Deep Table-based Hashing, CNN-based features	YouTube Faces, FaceScrub datasets	Lowest equal error rate on large-scale face image datasets
Kim et al. [37]	GLRT-based approach for cancellable ECG biometric system	Composite hypothesis testing, CS domain	Public ECG-ID data	Up to 93.0% detection probability with satisfactory performance
Kho et al. [38]	Partial Local Structure with R-NNLS optimization	Alignment-free minutiae descriptor, R-NNLS optimization	Five benchmark datasets	Better performance across datasets with EER varying from 0% to 5%
Soliman et al. [39]	Iris recognition via random projection	Random projection, Gabor filter	CASIA-IrisV3 dataset	Impressive identification rates and superior EER
Walia et al. [40]	Real-time cancellable multimodal biometric system	Deep feature unification, revocability	IITD Iris, MMU2 datasets	Favourable performance with unlinkable templates
Algarni et al. [41]	Discrete transforms and matrix rotations for biometric security	Matrix rotations, discrete transforms	Fingerprint and face datasets	Outperformed conventional strategies in accuracy and efficiency
Li et al. [42]	Local-similar image for cancellable fingerprint templates	LSIT mapping, abstracting fingerprint features	FVC2002, FVC2004	Encouraging results in terms of EER
Yang et al. [43]	Feature-adaptive random projection for biometric security	Random projection, encrypted domain	FVC2002 DB1-DB3, FVC2004 DB2	Competitive performance with reserved biometric template data
Shahzad et al. [44]	Dual protection cancellable fingerprint templates	Partial DWT, window-shift-XOR model	Five fingerprint databases	Outperformed current methods with enhanced security and dual protection
Jain et al. [45]	Delaunay Triangulation Net for fingerprint templates	Delaunay's Triangulation Net, 4-dimensional feature set	FVC 2002, FVC 2004	Better performance than current models, with EER ranging from 1.0\% to 2.46\%
Lee et al. [46]	Multimodal Extended Feature Vector hashing	Enhanced XOR encryption, revocability assessment	FVC2002, FVC2004, LFW datasets	Empirically confirmed superior matching accuracy

Kavati et al. [47]	Elliptical shapes for fingerprint templates	Ellipse-based feature vector, DFT-based security	FVC 2002 DB1-DB3	Function rather well with EER from 5.13\% to 12.36\%
Wu et al. [48]	cancellable biometric authentication with RDM and ECC	Random distance method, ECC	FVC2006, CASIA-Face V5, IRIS(LWIR) databases	Improved biometric authentication accuracy
Sperling et al. [49]	Homomorphically encrypted multi-modal fusion system	Homomorphic encryption, feature-level fusion	CPLFW, Google Speech Commands datasets	Significant improvements in matching performance
Yin et al. [50]	Lightweight cancellable fingerprint template design	Length-flexible feature generation, lightweight feature generation	FVC2002 DB1-DB4, FVC2004 DB1-DB4 databases	Equivalent authentication performance with reduced storage and cost
Kim et al. [51]	Cancellable SoftMax Out fusion network	Deep learning-based fusion, permutation SoftMax Out transformation	Multimodal face-periocular datasets	Cutting-edge verification accuracy on evaluated datasets
Elsadai et al. [52]	Stylometric features for fingerprint recognition	Blockchain, machine learning, stylometry	CASIA-FingerprintV5 dataset	Very high accuracy and low false acceptance rate
Ayoup et al. [53]	Cancellable multi-biometric identification scheme	Arnold's Cat Map encryption, selective fusion	Biometric images of various sizes	Good AROC values with reduced over-execution enrolment procedure
Ayoup et al. [54]	Selective encryption for cancellable multi-biometric system	AES encryption, Viola-Jones algorithm	Facial photos dataset	Favourable assessment metrics with faster enrolment time

VI. CONCLUSION

The review paper offers a comprehensive study of several approaches to improve biometric systems security and privacy, from state-of-the-art homomorphically encrypted multi-modal fusion systems to conventional token-based authentication. Researchers have shown a commitment to tackling issues including data integrity in biometric authentication, privacy breaches, and illegal access through thorough evaluation and comparative analysis.

Considerable progress has been made in the direction of obtaining robust and dependable biometric authentication solutions by utilizing techniques such as random projection, encryption, feature fusion, and cancellable biometrics. Although every method has advantages and disadvantages, the basic objective is always the same: making sure biometric systems are reliable and robust in a variety of contexts and use cases.

VII. FUTURE SCOPE

Future studies in the field of biometric template protection may investigate how to improve security and privacy by integrating cutting-edge technology like federated learning and block chain. Biometric templates and authentication records could be safely stored using block chain technology, which provides irreversible and decentralized storage. This lowers the possibility of unwanted access and tampering. Federated learning also offers a privacy-preserving method of biometric authentication by facilitating cooperative model training amongst dispersed devices without exchanging sensitive data.

Furthermore, investigating the use of cutting-edge machine learning methods like adversarial training and deep learning could strengthen the resilience of biometric systems against complex attacks. Standardized evaluation frameworks and standards are also required in order to enable fair comparison and benchmarking of various biometric template protection techniques. Finally, the broad use of safe and privacy-preserving biometric authentication systems in real-world applications will depend on how ethical and legal issues like user consent, data ownership, and regulatory compliance are resolved.

REFERENCES

[1] Anil K Jain, Patrick Flynn, and Arun A Ross. Handbook of biometrics. Springer Science & Business Media, 2007.

[2] Jiankun Hu, David Chek Ling Ngo, and Andrew Beng Jin Teoh. Biometric security. Cambridge Scholars Publishing, 2015.

[3] Mahesh Joshi, Bodhisatwa Mazumdar, and Somnath Dey. Security vulnerabilities against fingerprint biometric system. arXiv preprint arXiv:1805.07116, 2018.

[4] Yan Sui, Xukai Zou, and Yingzi Du. Cancellable biometrics. Biometrics: From fiction to practice, pages 233–252, 2013.

[5] Nalini K Ratha. Privacy protection in high security biometrics applications. In International Conference on Ethics and Policy of Biometrics, pages 62–69. Springer, 2010.

[6] Rima Belguechi, Estelle Cherrier, and Christophe Rosenberger. How to evaluate transformation based cancelable biometric systems? In NIST International Biometric Performance Testing Conference (IBPC), 2012.

[7] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Biometric template transformation: a security analysis. In Media Forensics and Security II, volume 7541, pages 237– 251. SPIE, 2010.

[8] Anne MP Canuto, Fernando Pintro, and Joa˜o C XavierJunior. Investigating fusion approaches in multi-biometric cancellable recognition. Expert Systems with applications, 40(6):1971–1980, 2013.

[9] X Dong, Z Jin, ABJ Teoh, M Tistarelli, and K Wong. On the security risk of cancelable biometrics. arXiv preprint arXiv:1910.07770, 2019.

[10] Tanguy Gernot and Christophe Rosenberger. Robust biometric scheme against replay attacks using one-time biometric templates. Computers & Security, 137:103586, 2024.

[11] Pranab Mohanty, Sudeep Sarkar, and Rangachar Kasturi. From scores to face templates: A model-based approach. IEEE transactions on pattern analysis and machine intelligence, 29(12):2065–2078, 2007.

[12] Tetsuya Izu, Yumi Sakemi, Masahiko Takenaka, and Naoya Torii. A spoofing attack against a cancelable biometric authentication scheme. In 2014 IEEE 28th International Conference on Advanced Information Networking and Applications, pages 234–239. IEEE, 2014.

[13] Arpita Sarkar, Binod Kr Singh, and Ujjayanta Bhaumik. Cryptographic key generation scheme from cancellable biometrics. In Progress in Computing, Analytics and Networking: Proceedings of ICCAN 2017, pages 265–272. Springer, 2018.

[14] Sameh Ibrahim, Mohamed G Egila, H Shawkey, Mohamed KH Elsaid, Walid El-Shafai, Fathi E Abd El-Samie, et al. Hardware implementation of cancellable biometric systems. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pages 1145–1152. IEEE, 2020.

[15] Hisham Al-Assam, Ihsan Alshahib Lami, and Torben Kuseler. Integrating cancellable biometrics with geographical location for effective unattended authentication of users of mobile devices. J. Commun., 8(11):780–787, 2013.

[16] Wei Jing Wong, Andrew BJ Teoh, ML Dennis Wong, and Yau Hee Kho. Enhanced multi-line code for minutiae-based fingerprint template protection. Pattern Recognition Letters, 34(11):1221–1229, 2013.

[17] Wei-jing Wong, Mou-ling Dennis Wong, and Yau-hee Kho. Multi-line code: a low complexity revocable fingerprint template for cancelable biometrics. Journal of Central South University, 20:1292–1297, 2013.

[18] Song Wang and Jiankun Hu. Design of alignment-free cancelable fingerprint templates via curtailed circular convolution. Pattern Recognition, 47(3):1321–1329, 2014.

[19] Zhe Jin, Meng-Hui Lim, Andrew Beng Jin Teoh, and BokMin Goi. A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. Pattern Recognition Letters, 42:137–147, 2014.

[20] Matteo Ferrara, Davide Maltoni, and Raffaele Cappelli. A two-factor protection scheme for mcc fingerprint templates. In 2014 international conference of the biometrics special interest group (BIOSIG), pages 1–8. IEEE, 2014.

[21] Christian Rathgeb, Marta Gomez-Barrero, Christoph Busch, Javier Galbally, and Julian Fierrez. Towards cancelable multi-biometrics based on bloom filters: a case study on feature level fusion of face and iris. In 3rd international workshop on biometrics and forensics (IWBF 2015), pages 1–6. IEEE, 2015.

[22] Mulagala Sandhya and Munaga VNK Prasad. knearest neighborhood structure (k-nns) based alignment-free method for fingerprint template protection. In 2015 international conference on biometrics (ICB), pages 386–393. IEEE, 2015.

[23] Harkeerat Kaur and Pritee Khanna. Gaussian random projection based non-invertible cancelable biometric templates. Procedia Computer Science, 54:661–670, 2015.

[24] Marta Gomez-Barrero, Christian Rathgeb, Javier Galbally, Christoph Busch, and Julian Fierrez. Unlinkable and irreversible biometric template protection based on bloom filters. Information Sciences, 370:18–32, 2016.

[25] Song Wang and Jiankun Hu. A blind system identification approach to cancelable fingerprint templates. Pattern Recognition, 54:14–22, 2016.

DOI: 10.17148/IJARCCE.2024.13907

[26] Song Wang, Guang Deng, and Jiankun Hu. A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. Pattern Recognition, 61:447–458, 2017.
[27] Song Wang, Wencheng Yang, and Jiankun Hu. Design of alignment-free cancelable fingerprint templates with zoned minutia pairs. Pattern Recognition, 66:295–301, 2017.
[28] Harkeerat Kaur and Pritee Khanna. Cancelable features using log-gabor filters for biometric authentication. Multimedia Tools and Applications, 76:4673–4694, 2017.
[29] Zhe Jin, Jung Yeon Hwang, Yen-Lung Lai, Soohyung Kim, and Andrew Beng Jin Teoh. Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. IEEE Transactions on Information Forensics and Security, 13(2):393–407, 2017.
[30] Riki Mukhaiyar. Generating a cancellable fingerprint using matrices operations and its fingerprint processing requirements. Asian Social Science, 14(6):1–20, 2018.
[31] Badiul Alam, Zhe Jin, Wun-She Yap, and Bok-Min Goi. An alignment-free cancelable fingerprint template for biocryptosystems. Journal of Network and Computer Applications, 115:20–32, 2018.
[32] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. A fingerprint and finger-vein based cancelable multi-biometric system. Pattern Recognition, 78:242– 251, 2018.
[33] Harkeerat Kaur and Pritee Khanna. Random distance method for generating unimodal and multimodal cancelable biometric features. IEEE Transactions on Information Forensics and Security, 14(3):709–719, 2018.
[34] Harkeerat Kaur and Pritee Khanna. Random slope method for generation of cancelable biometric features. Pattern Recognition Letters, 126:31–40, 2019.
[35] Xingbo Dong, Zhe Jin, and Andrew Teoh Beng Jin. A genetic algorithm enabled similarity-based attack on cancellable biometrics. In 2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS), pages 1–8. IEEE, 2019.
[36] Young Kyun Jang and Nam Ik Cho. Deep face image retrieval for cancelable biometric authentication. In 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pages 1–8. IEEE, 2019.
[37] Hanvit Kim and Se Young Chun. Cancelable ecg biometrics using compressive sensing-generalized likelihood ratio test. IEEE Access, 7:9232–9242, 2019.
[38] Jun Beom Kho, Jaihie Kim, Ig-Jae Kim, and Andrew BJ Teoh. Cancelable fingerprint template design with randomized non-negative least squares. Pattern Recognition, 91:245–260, 2019.
[39] Randa F Soliman, Mohamed Amin, and Fathi E Abd ElSamie. A modified cancelable biometrics scheme using random projection. Annals of Data Science, 6:223–236, 2019.
[40] Gurjit Singh Walia, Kartik Aggarwal, Kuldeep Singh, and Kunwar Singh. Design and analysis of adaptive graph-based cancelable multi-biometrics approach. IEEE Transactions on Dependable and Secure Computing, 19(1):54–66, 2020.
[41] Abeer D Algarni, Ghada El Banby, Sahar Ismail, Walid ElShafai, Fathi E Abd El-Samie, and Naglaa F. Soliman. Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. Entropy, 22(12):1361, 2020.
[42] Zhaozheng Li, Ying Bao, and Weimin Lei. Generating cancellable fingerprint template using local-similar image. In 2020 IEEE 3rd international conference on electronics and communication engineering (ICECE), pages 157–161. IEEE, 2020.
[43] Wencheng Yang, Song Wang, Muhammad Shahzad, and Wei Zhou. A cancelable biometric authentication system based on feature-adaptive random projection. Journal of Information Security and Applications, 58:102704, 2021.
[44] Muhammad Shahzad, Song Wang, Guang Deng, and Wencheng Yang. Alignment-free cancelable fingerprint templates with dual protection. Pattern Recognition, 111:107735, 2021.
[45] Likhit J Jain, Abhiram Sridhar Puranam, Ken Jonathan Pais, and Mamatha KR. A non-invertible cancellable fingerprint template for low-quality fingerprints. 2021.
[46] Ming Jie Lee, Andrew Beng Jin Teoh, Andreas Uhl, ShiuanNi Liang, and Zhe Jin. A tokenless cancellable scheme for multimodal biometric systems. Computers & Security, 108:102350, 2021.
[47] Ilaiah Kavati, A Mallikarjuna Reddy, E Suresh Babu, K Sudheer Reddy, and Ramalinga Swamy Cheruku. Design of a fingerprint template protection scheme using elliptical structures. ICT Express, 7(4):497–500, 2021.
[48] Lei Wu, Lingzhen Meng, Shengnan Zhao, Xia Wei, and Hao Wang. Privacy-preserving cancelable biometric authentication based on rdm and ecc. IEEE Access, 9:90989–91000, 2021.
[49] Luke Sperling, Nalini Ratha, Arun Ross, and Vishnu Naresh Boddeti. Heft: Homomorphically encrypted fusion of biometric templates. In 2022 IEEE International Joint Conference on Biometrics (IJCB), pages 1–10. IEEE, 2022.
[50] Xuefei Yin, Song Wang, Yanming Zhu, and Jiankun Hu. A novel length-flexible lightweight cancelable fingerprint template for privacy-preserving authentication systems in resource-constrained iot applications. IEEE Internet of Things Journal, 10(1):877–892, 2022.
[51] Jihyeon Kim, Yoon Gyo Jung, and Andrew Beng Jin Teoh. Multimodal biometric template protection based on a cancelable softmaxout fusion network. Applied Sciences, 12(4):2023, 2022.

DOI: 10.17148/IJARCCE.2024.13907

[52] Ali Elsadai, Saˇsa Adamovi´c, Marko Sarac, ˇ Muzafer Saraˇcevi´c, and Sudhir Kumar Sharma. New approach for fingerprint recognition based on stylometric features with blockchain and cancellable biometric aspects. Multimedia Tools and Applications, 81(25):36715–36733, 2022.

[53] Ahmed M Ayoup, Ashraf AM Khalaf, Walid El-Shafai, Fathi E Abd El-Samie, Fahad Alraddady, and Salwa M Serag Eldin. Cancellable multi-biometric template generation based on arnold cat map and aliasing. Computers, Materials & Continua, 72(2), 2022.

[54] Ahmed M Ayoup, A Khalaf, Fahad Alraddady, F Abd El-Samie, Walid El-Safai, and S Eldin. Selective cancellable multi-biometric template generation scheme based on multi-exposure feature fusion. Intell. Autom. Soft Comput., 33(1):549–565, 2022.

BIOGRAPHY

Diptadip Maiti, is currently a research scholar in the department of Computer Science & Engineering at Techno India University, West Bengal. He did his B. Tech. in Computer Science & Engineering and M. Tech in Information Technology in 2005 and 2009 respectively. His research interests are in Image Processing, Biometric Authentication, Machine Learning and Deep Learning.
Email: diptadipmaiti@gmail.com

Madhuchhanda Basak, is currently a research scholar in the department of Computer Science & Engineering at Techno India University, West Bengal. She did his B. Tech. & M. Tech. in Information Technology in 2006 and 2010 respectively. Her research interests are in Image Processing, Biometric Authentication, Machine Learning and Deep Learning
Email: madhuchhanda.basak@gmail.com