Systems and Computing
Volume 1, Issue 1, 44-67, 2025.
https://doi.org/10.64409/sycom.v1.i1.4

Research Article Open Access

Empowering Biometric Security: A Paradigm Shift in Remote Identification

Yacine Belhocine[1*], Abdallah Meraoumia[2], Hakim Bendjenna[1] and Mohammed Saigaa[2]

1. *LAboratory of Mathematics, Informatics and Systems (LAMIS), Echahid Cheikh Larbi Tebessi University, Tebessa, Algeria*
2. *Laboratory of Signals and Smart Systems (L3S), Echahid Cheikh Larbi Tebessi University, Tebessa, Algeria*

Corresponding author: Yacine Belhocine (yacine.belhocine@univ-tebessa.dz)

Manuscript Review Record:

Submitted:
May 13, 2025

Accepted:
June 24, 2025

Published:
July 19, 2025

Cite This:
Y. Belhocine, A. Meraoumia, H. Bendjenna, M. Saigaa, "Empowering Biometric Security: A Paradigm Shift in Remote Identification". *Systems and Computing*, Volume 1, Issue 1, 44-67, 2025.
https://doi.org/10.64409/sycom.v1.i1.4

Abstract- **Context**: In an increasingly digital world, the need for secure and reliable identity verification is more critical than ever. Biometric authentication stands out due to its inherent uniqueness and resistance to forgery, yet its performance is still affected by real-world challenges such as image noise and lighting inconsistencies. **Objective**: This paper aims to enhance the robustness and accuracy of biometric systems, specifically for remote authentication scenarios, by addressing the limitations posed by environmental variations. **Method**: The proposed solution is a novel FKP-based biometric authentication system that employs a Triple Texture Feature Extraction (TTFE) technique to capture detailed information from both spatial and frequency domains. To further improve recognition performance, Projective Dictionary Learning is used to refine the feature representation. For secure data handling, a fuzzy vault scheme is integrated to encrypt biometric templates using secret keys, allowing secure authentication over potentially untrusted networks. **Results**: Experiments conducted on standard benchmark datasets demonstrate significant improvements in both accuracy and resilience to challenging conditions such as noise and lighting variations. **Conclusions**: This integrated approach successfully enhances the reliability and security of biometric authentication systems, paving the way for more practical and scalable real-world deployments.

Keywords- Biometric authentication, Dictionary learning, FKP, Fuzzy vault, Identity protection, Secure remote identification.

Acknowledgement

This research was conducted as part of the PRFU project (Grant: A01L08UN120120220001) under the Department of Electronics and Communicaions at the University of Echahid Cheikh Larbi Tebessi, Tebessa. The authors extend they're thanks to the staff of the LAMIS and L3S laboratories for their insightful comments and suggestions.

1. Introduction

In today's rapidly evolving digital landscape, ensuring secure and reliable identity verification has become a fundamental requirement in cyber-security [1]. With the proliferation of online services, mobile applications, and cloud-based platforms, the volume of sensitive data exchanged over digital networks is growing exponentially. This expansion has been paralleled by a corresponding rise in cyber threats, including identity theft, unauthorized access, and fraudulent transactions. Traditional authentication methods, such as passwords and PINs, have increasingly shown their limitations in addressing modern security challenges. These conventional approaches are susceptible to various attack vectors, including credential leaks, brute-force attempts, social engineering, and phishing campaigns [2]. As a result, there is a growing consensus in both industry and academia that more advanced, user-centric, and secure authentication systems are urgently needed.

Biometric authentication has emerged as a powerful and promising solution to meet these demands. By leveraging the unique physiological and behavioral characteristics of individuals, biometric systems provide a natural and intuitive means of verifying identity [3]. Unlike knowledge-based or token-based methods, biometric traits are inherently bound to an individual and are difficult to forge, steal, or replicate [4]. These advantages make biometrics particularly well-suited for high-security applications, including access control, border surveillance, financial services, and personal device security.

Among the various biometric modalities explored in recent years, Finger-Knuckle Print (FKP) recognition has attracted increasing attention due to its rich texture patterns, high distinctiveness, and long-term stability. Compared to fingerprints, which may be affected by wear or external conditions, and facial recognition, which can suffer from changes in lighting, occlusion, or expression, FKP offers a more robust and reliable alternative [5]. The intricate ridge structures, wrinkles, and creases present in the finger-knuckle region provide a set of discriminative features that can be effectively used for individual identification. Furthermore, FKP-based systems have demonstrated promising results in terms of usability and acquisition convenience, requiring minimal user cooperation while capturing robust biometric data.

Despite these advantages, the performance of FKP-based biometric systems is still constrained by several challenges. Variations in image acquisition conditions, changes in finger orientation or positioning, background noise, and inconsistent illumination can all adversely affect feature extraction and classification accuracy [6]. To overcome these limitations, researchers have increasingly focused on developing more robust and discriminative feature extraction techniques, as well as advanced classification models capable of handling high-dimensional and complex data representations.

In this context, this paper proposes an innovative biometric identification system that integrates Triple-Type Feature Extraction (TTFE) and Projective Dictionary Pair Learning (DPL) to address these challenges. The TTFE framework is designed to extract three complementary types of features, texture-based, gradient-based, and direction-based, from FKP images. By capturing information from different domains, TTFE provides a more holistic and comprehensive representation of biometric patterns, enhancing both discriminability and robustness [7]. Unlike traditional feature extraction methods that typically rely on a single descriptor, this multi-modal approach significantly improves system resilience to environmental variations and acquisition inconsistencies [9].

On the classification side, the proposed system adopts Projective Dictionary Pair Learning (DPL), an advanced learning-based classification strategy that optimizes both feature representation and decision-making simultaneously. Rather than depending on sparse coding alone or predefined classifiers, DPL learns a pair of dictionaries: a synthesis dictionary that reconstructs class-specific representations, and an analysis dictionary that projects features into a discriminative subspace. This dual structure enables more accurate and computationally efficient classification, particularly in

scenarios involving high-dimensional feature vectors [8]. Compared to traditional classifiers such as Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), or deep learning models, DPL offers a more interpretable, scalable, and tunable solution for biometric tasks [10].

To complement this feature-classification synergy, and to meet the increasing demand for privacy-preserving and secure remote authentication, the proposed framework incorporates a fuzzy vault scheme. The fuzzy vault mechanism is a cryptographic technique designed to bind biometric features with secret keys in such a way that the actual biometric template is never exposed directly. In this system, the extracted TTFE features are used to lock and unlock secure keys within the fuzzy vault structure, enabling authentication without the need to transmit or store raw biometric data [11]. This integration enhances security, ensures template protection, and supports secure matching over potentially untrusted communication channels, a critical feature for distance-based and decentralized authentication scenarios [12].

The synergy of these three components, multi-modal feature extraction, structured dictionary-based classification, and cryptographic protection through fuzzy vault, forms a robust, secure, and efficient biometric identification system. The framework not only improves recognition accuracy but also addresses real-world concerns such as data security, remote accessibility, and resistance to spoofing or adversarial attacks.

To evaluate the performance of the proposed system, extensive experiments were conducted using a publicly available FKP dataset. The analysis involved incremental integration of feature types, evaluating single-type, dual-type, and full triple-type combinations, to assess their individual and combined impact on classification accuracy. The results demonstrate a clear correlation between feature diversity and recognition performance, with the full TTFE integration yielding the highest accuracy and robustness. Additionally, the fuzzy vault component was tested for its ability to securely encode and decode biometric data, confirming its practical viability in real-world deployment scenarios [13].

This study contributes to the advancement of biometric security in several key ways:

- A robust and comprehensive feature extraction method that leverages three distinct and complementary feature types, ensuring superior biometric representation.
- A projective dictionary-based classification model that enhances both discriminability and computational efficiency.
- A cryptographic layer through fuzzy vault encoding, providing strong protection for biometric templates and enabling secure, remote authentication.
- A modular, scalable system architecture suitable for integration into a wide range of identity verification platforms, including mobile, cloud-based, and border security systems.

As cyber threats become increasingly sophisticated and pervasive, the importance of designing secure, reliable, and privacy-aware authentication systems cannot be overstated [14]. Biometric solutions, particularly those that combine strong feature extraction, intelligent classification, and secure encryption, are poised to become a cornerstone of future identity verification infrastructures.

The structure of this paper is organized as follows: Section 2 presents a comprehensive overview of related work in biometric authentication and cryptographic security. Section 3 discusses the primary motivations and problem formulation. Section 4 outlines the proposed biometric authentication framework, detailing the TTFE method, DPL model, and fuzzy vault integration. Section 5 presents the experimental evaluation, analyzing the contribution of each component and their combined effectiveness. Section 6 provides a security analysis of the overall system. Finally, Section 7 concludes the paper with a summary of findings and future research directions, including real-time implementation, adversarial robustness, and multi-modal biometric fusion.

2. Related works

In [15], Gu et al. introduced a novel framework for discriminative dictionary learning called Projective Dictionary Pair Learning (DPL). In their work, they address the computational burden of traditional dictionary learning methods, which rely on costly \ell_0 or \ell_1-norm sparsity constraints during the sparse coding process. Instead, DPL jointly learns both a synthesis dictionary and an analysis dictionary. The analysis dictionary enables a direct linear projection of the input signal, effectively bypassing the need for iterative sparse coding while still capturing the discriminative features necessary for accurate classification. This dual-dictionary approach not only greatly reduces training and testing time but also achieves highly competitive accuracies across a variety of visual classification tasks by integrating signal representation and discrimination into a unified framework.

In [16], Jiang et al. introduced the LC-KSVD algorithm, a label consistent K-SVD method that integrates class labels into the dictionary learning process. By associating each dictionary atom with label information and introducing a "discriminative sparse-code error" alongside reconstruction and classification errors, LC-KSVD encourages samples from the same class to yield similar sparse codes. This unified objective enables the joint learning of an over complete dictionary and an optimal linear classifier, leading to improved recognition performance across various tasks such as face, action, scene, and object recognition.

In [17], the authors challenge the conventional emphasis on \ell_1-norm sparsity in sparse representation based classification (SRC) for face recognition. Their work reveals that the collaborative representation (CR) aspect of SRC plays a more pivotal role in achieving high recognition accuracy than the sparsity constraint itself. Based on this insight, they propose a simpler yet highly efficient classification scheme, CR based classification with regularized least squares (CRC_RLS). Experimental results demonstrate that CRC_RLS not only delivers competitive performance in face classification tasks but also significantly reduces computational complexity compared to traditional SRC approaches.

In [18], Abhijit Dasa et al. proposed a projective pair wise dictionary learning approach for multimodal eye biometrics. Their method, known as Projective Pairwise Discriminative Dictionary (PPDD), jointly learns a synthesis dictionary and an analysis dictionary, thereby bypassing the computational burden imposed by traditional \ell_0 or \ell_1-norm sparsity constraints. By leveraging this dual-dictionary framework, PPDD efficiently captures complex eye pattern features and enhances discriminability. In their work, the authors demonstrate that integrating both sclera and iris traits yields a robust multimodal biometric system. Extensive experiments conducted on a portion of the UBIRIS version 1 dataset validate that their approach not only speeds up the dictionary learning process but also achieves competitive recognition performance.

While previous works in discriminative dictionary learning and multimodal biometrics have shown promising results, many of these methods are limited by their reliance on computationally intensive sparse coding and are predominantly tailored for modalities such as palmprints or eye biometrics. Such approaches often fail to capture the intricate texture and structural details present in finger-knuckle prints, which are crucial for high-accuracy recognition in contactless systems. To overcome these challenges, we propose the TTFE-DPL system, specifically designed for the Finger-Knuckle Print modality. By integrating Triple-Type Feature Extraction with Projective Dictionary Pair Learning, our method effectively fuses texture, gradient, and directional information while eliminating the heavy computational burden associated with traditional sparse coding. In addition to enhancing feature discriminability and enabling efficient classification, our framework addresses a critical shortcoming in existing literature: the lack of integrated security mechanisms for protecting biometric templates. Most prior approaches prioritize recognition accuracy while neglecting the protection of sensitive biometric data, leaving systems vulnerable to reconstruction and misuse. To mitigate this risk, we incorporate a fuzzy vault scheme into our system, enabling secure binding of biometric features through cryptographic obfuscation with chaff points. This ensures that the original biometric data remains protected even in the

event of exposure, without degrading system performance. As a result, the proposed TTFE-DPL framework offers a balanced solution that advances both recognition capability and security, making it well-suited for practical deployment in modern biometric authentication environments.

3. Key motivation

The widespread shift toward digital platforms in sectors such as finance, healthcare, and government services has underscored the urgent need for secure, accurate, and user-friendly authentication mechanisms. Traditional credentials like passwords and PINs continue to pose significant security risks, being highly vulnerable to phishing, brute-force, shoulder surfing, and other cyber attacks [19]. Biometric authentication has emerged as a promising solution, offering inherent uniqueness and convenience by leveraging physiological traits. Among these, Finger-Knuckle Print (FKP) recognition stands out for its stable ridge structures, contactless acquisition, and strong resistance to forgery and duplication. However, the effectiveness of FKP-based systems is often hindered by reliance on single-type feature extraction methods, which fail to capture the complex, multi-dimensional patterns present in FKP images. Additionally, traditional classification techniques struggle with high-dimensional features, leading to computational inefficiencies and degraded performance under real-world constraints. To address these limitations, this study introduces a robust biometric authentication framework that integrates Triple-Type Feature Extraction (TTFE) with Projective Dictionary Pair Learning (DPL). This combination enables the extraction of rich texture, gradient, and directional features, while DPL facilitates efficient and accurate classification by jointly learning synthesis and analysis dictionaries. Beyond recognition accuracy, this work also addresses a critical gap in biometric system design: the lack of integrated security for protecting stored biometric templates. Unlike many previous methods that overlook this aspect, the proposed framework incorporates a fuzzy vault scheme to ensure privacy-preserving storage of biometric data. By encoding genuine features into a secure polynomial and camouflaging them among chaff points, the fuzzy vault offers strong resistance against reconstruction attacks and unauthorized access. This holistic approach not only improves recognition performance and computational efficiency but also ensures robust protection of sensitive biometric information, making it highly suitable for deployment in high-security applications such as access control systems, digital identity verification platforms, and secure financial services.

4. Proposed biometric system

Designing a secure and high-performing biometric authentication system requires not only accurate feature extraction and efficient classification but also robust mechanisms for protecting biometric templates. This section presents the proposed Finger-Knuckle Print (FKP) authentication system, illustrated in Fig. 1, which integrates Triple-Type Feature Extraction (TTFE), Projective Dictionary Pair Learning (DPL), and a fuzzy vault scheme to achieve a comprehensive solution for recognition and security. The TTFE module extracts texture, gradient, and directional information to generate a rich and discriminative feature representation, while the DPL framework jointly learns synthesis and analysis dictionaries to enable accurate and computationally efficient classification. To ensure privacy and resilience against template leakage or misuse, the extracted features are further secured using a fuzzy vault encoding process, which binds the genuine feature points to a secret polynomial while concealing them among randomly generated chaff points. This combination not only improves recognition accuracy and runtime performance but also introduces a strong layer of cryptographic protection, for a practical and scalable solution by addressing both biometric performance and security within a unified architecture.

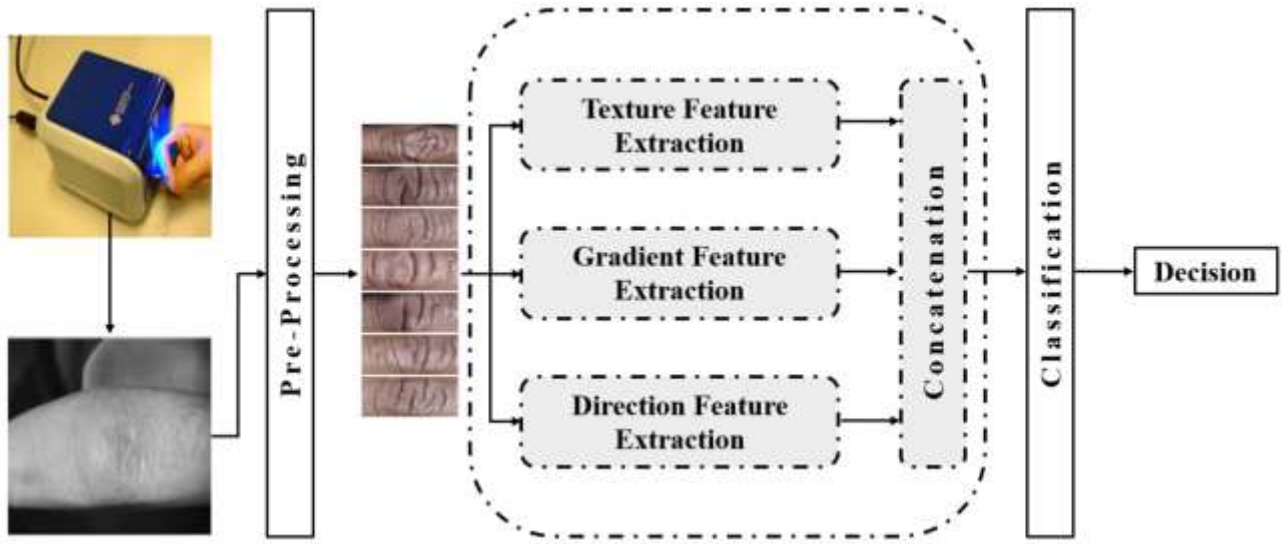


Figure 1. Framework of the proposed biometric recognition system.

4.1.Pre-processing

The extraction of the region of interest (ROI) for FKP involves several steps [20]. First, Gaussian smoothing is applied to the original image [21], which is then down sampled to 150 dpi. Next, the x-axis of the coordinate system is determined by fitting it to the bottom boundary of the finger, easily extracted using a Canny edge detector [22]. The y-axis is selected by applying a Canny edge detector to a cropped sub-image, previously extracted based on the x-axis, followed by identifying the convex direction coding scheme. Finally, the ROI is extracted, with the rectangle indicating the ROI area to be used for further user recognition, as illustrated in Figure 2.

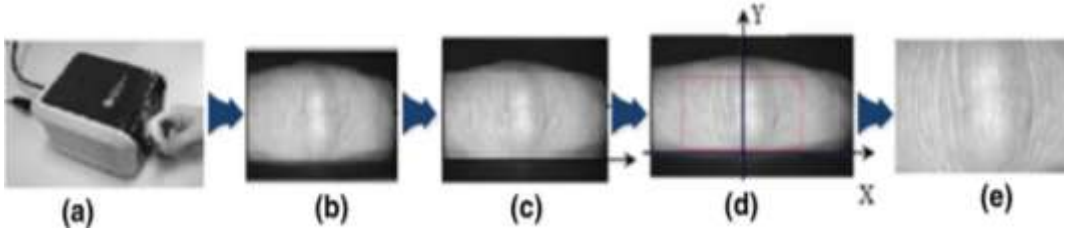


Figure 2. The steps for extracting the ROI from an FKP image**.**

4.2.Triple type feature extraction

Triple-Type Feature Extraction is designed to capture the inherent characteristics of a biometric image by extracting three distinct types of features: texture, gradient, and direction. These three feature types provide complementary information that, when fused, yield a robust descriptor for biometric recognition [23]. In our work, we follow the same rationale as in the original method.

4.2.1.Texture feature extraction

Texture information is critical in representing the fine details of an image. For a given pixel in an image, we consider its 3×3 neighborhood. First, we compute the absolute gray value differences between the center pixel and each of its eight neighbors. Let these differences be denoted as: $di(i = 1,2, \ldots,8)$. Next, these differences are sorted in descending order. We then select the two neighbors that yield the highest gray value differences. Denote the direction (or position index) corresponding to the maximum difference as m_1 and that of the second maximum (excluding the first) as m_2.

The texture feature code, T_{code}, is then computed by encoding these two directional indices as:

$$T_{code} = (m_1 - 1) \times 8 + (m_2 - 1) \quad (1)$$

Here, m_1 is defined by:

$$m_1 = \arg\max_j \{d_j\} \quad (2)$$

And m_2 is defined as:

$$m_2 = \arg\max_j \{d_j : j \neq m_1\} \quad (3)$$

This encoding yields a value ranging from 1 to 62, ensuring that the most significant texture information is captured robustly against small noise variations. Figure 3 illustrates the basic idea of the robust texture feature extraction scheme.

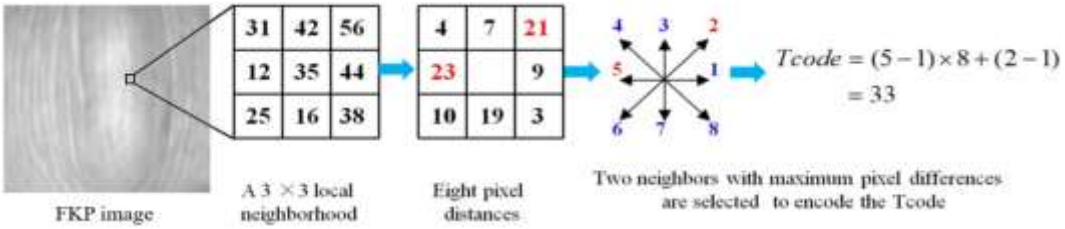


Figure. 3 The basic procedure of texture feature code calculation [23].

4.2.2. Gradient feature extraction

Edge information in an image often highlights the presence of lines and wrinkles, which are also key to biometric discrimination. To extract these gradient features, we employ eight directional edge operators (e.g., Kirsch operators). Each operator is applied to the image, resulting in eight convolution responses, one per direction. Let these responses be denoted as: $Rj(j = 1,2, \ldots,8)$. We then sort the absolute values of these responses and select the two directions corresponding to the highest responses. Denote these indices as p_1 and p_2. The gradient feature code, G_{code}, is encoded similarly as:

$$G_{code} = (p_1 - 1) \times 8 + (p_2 - 1) \quad (4)$$

with p_1 and p_2 determined in the same manner as m_1 and m_2 for texture. Figure 4 illustrates the basic idea of the robust gradient feature extraction scheme.

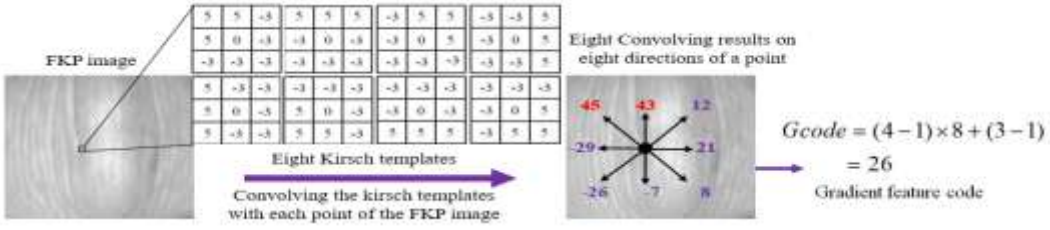


Figure 4. The basic procedure of gradient feature code calculation [23].

4.2.3. Direction feature extraction

As illustrates in Figure 5 the basic idea of the direction features extraction aims to capture the dominant orientation information of the image. In this step, a set of N_θ(typically 12) directional templates based on Gabor filters is used. For each direction θ_j, where:

$$\theta_j = \frac{(j-1)\pi}{N_\theta}, \quad j = 1,2,\dots,N_\theta \tag{5}$$

We compute the convolution response of the image $I(x,y)$ with the template $G(\theta_j)$:

$$c_j(x,y) = G(\theta_j) * I(x,y), \quad j = 1,2,\dots,N_\theta \tag{6}$$

Where " $*$ " denotes the convolution operation.

We first identify the dominant direction q_1 as the index corresponding to the maximum response:

$$q_1 = \arg\max_j\{c_j(x,y)\} \tag{7}$$

To further capture discriminative orientation details, we compute the Direction Response Interval (DRI) for each direction. For a given direction j, its DRI is defined as:

$$DRI_j(x,y) = \left|c_j(x,y) - c_{\varphi(j)}(x,y)\right| + \left|c_j(x,y) - c_{\phi(j)}(x,y)\right| \tag{8}$$

Where $\varphi(j)$ and $\phi(j)$ denote the indices of the nearest neighboring directions. Specifically, we define:

$$\varphi(j) = \begin{cases} N_\theta & if\ j = 1 \\ j-1, & otherwise \end{cases} \tag{9}$$

$$\phi(j) = \begin{cases} 1 & if\ j = N_\theta \\ j+1, & otherwise \end{cases} \tag{10}$$

Then, the second discriminative direction q_2 is determined as:

$$q_2 = \arg\max_j\{DRI_j(x,y)\} \tag{11}$$

Finally, the direction feature code $D_{code}(x,y)$ is obtained by encoding these two indices:

$$D_{code}(x,y) = (q_1 - 1) \times N_\theta + q_2 \tag{12}$$

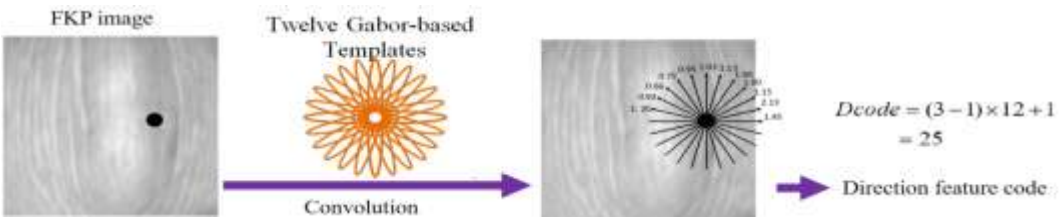


Figure 5. The basic procedure of direction feature code calculation [23].

4.2.4. Feature fusion

After generating the three feature code maps (texture, gradient, and direction), the next step is to form robust feature descriptors. This is achieved by dividing each feature code map into non-overlapping blocks (for instance, 16×16 pixels per block) and computing the histogram of codes within each block. These block-wise histograms are then concatenated to form the final feature descriptor for each feature type.

$$S_i(u,v) = \sum_{k=1}^{N_i} \frac{(u_{i,k}-v_{i,k})^2}{u_{i,k}+v_{i,k}}, \quad i = 1,2,3 \tag{13}$$

Where N_i is the number of bins in the histogram and $u_{i,k}$ and $v_{i,k}$ denote the k^{th} bin values.

4.3. Projective dictionary pair learning

Dictionary learning is a widely used technique for feature representation and classification, where the goal is to learn a structured representation of data that enhances classification performance. Traditional dictionary learning methods focus on optimizing a synthesis dictionary *D* and finding sparse codes *A*, often using l_0 or l_1 norm regularization, which can be computationally expensive .

To address these limitations, Projective Dictionary Pair Learning introduces an analysis dictionary *P* in addition to the synthesis dictionary *D*. The analysis dictionary allows direct linear projection of input samples into a discriminative feature space, eliminating the need for expensive sparse coding [16].

The following sections present the full theoretical formulation of DPL, including its discriminative dictionary learning framework, optimization process, classification scheme, and computational complexity analysis.

4.3.1. Discriminative dictionary learning

Let $X = [X_1, X_2, \dots, X_K]$ be a dataset containing training samples from *K* different classes, where each class *k* contains a subset $X_k \in R^{p\times n}$ consisting of *n* samples. The objective of dictionary learning is to represent *X* using a learned dictionary *D* and coefficient matrix *A* such that:

$$\min_{D,A} ||X - DA||_F^2 + \lambda||A||_p + \Psi(D,A,Y) \tag{14}$$

Where:

- $D \in R^{p\times m}$ is the synthesis dictionary
- $A \in R^{m\times n}$ is the sparse coefficient matrix
- λ is a regularization parameter enforcing sparsity
- $\Psi(D,A,Y)$ is a discrimination constraint ensuring class separation
- *Y* is the class label matrix

Traditional discriminative dictionary learning methods fall into two categories. A Shared Dictionary Learning which is a single dictionary *D* learned for all classes, and classification is performed based on the sparse codes *A*. Structured

Dictionary Learning which is Class-specific sub-dictionaries enforced to enhance class separability. However, these methods rely on expensive sparse coding, which significantly increases computational complexity.

4.3.2. The dictionary pair learning model

To overcome the limitations of traditional dictionary learning, DPL jointly learns an analysis dictionary P and a synthesis dictionary D to enable direct feature extraction without sparse coding. The DPL model is formulated as:

$$\{P^*, D^*\} = \arg\min_{P,D} ||X - DPX||_F^2 + \Psi(D, P, X, Y) \quad (15)$$

Where:

- $P \in R^{mK \times p}$ is the analysis dictionary
- $D \in R^{p \times mK}$ is the synthesis dictionary
- PX directly produces feature representations
- DPX reconstructs the original data while ensuring class separation

Instead of solving for sparse codes A, DPL computes representations using a simple linear projection:

$$A = PX \quad (16)$$

The dictionary pair is structured as:

$$D = [D_1, D_2, \dots, D_K], \quad P = [P_1; P_2; \dots; P_K] \quad (17)$$

Where D_k and P_k form a class-specific dictionary pair, ensuring a class-discriminative projections: $P_k X_i \approx 0$ for $i \neq k$. Thus, each class is mapped into a separate subspace, improving classification.

4.3.3. Optimization

The DPL optimization problem is non-convex, so it is solved iteratively using an alternative minimization approach. The full objective function is:

$$\{P^*, A^*, D^*\} = \arg\min_{P,A,D} \sum_{k=1}^{K} (|X_k - D_k A_k|_F^2 + \tau |P_k X_k - A_k|_F^2 + \lambda |P_k \overline{X_k}|_F^2) \quad (18)$$

Where:

- $\overline{X_k}$ is the set of all samples excluding class k
- $\tau, \lambda > 0$ are regularization parameters

The optimization is performed in three steps:

❖ **Step 1:** Update A (Projected Representation)

Fixing P and D, the optimal representation is given by:

$$A_k^* = \left(D_k^T D_k + \tau I\right)^{-1}\left(\tau P_k X_k + D_k^T X_k\right) \tag{19}$$

❖ **Step 2:** Update *P* (Analysis Dictionary)

Fixing *A* and *D*, the analysis dictionary is updated as:

$$P_k^* = \tau A_k X_k^T \left(\tau X_k X_k^T + \lambda \overline{X_k \overline{X_k^T}} + \gamma I\right)^{-1} \tag{20}$$

where $\gamma = 10^{-4}$ is a small numerical stability factor.

❖ **Step 3:** Update *D* (Synthesis Dictionary)

Fixing *P* and *A*, *D* is updated using:

$$D^{(r+1)} = \arg\min_D \sum_{k=1}^{K} |X_k - D_k A_k|_F^2 + \rho |D_k - S_k^{(r)} + T_k^{(r)}|_F^2 \tag{21}$$

4.3.4. Classification scheme

During testing, a new sample *y* is classified using the reconstruction residual:

$$\text{identity}(y) = \arg\min_k |y - D_k P_k y|_F^2 \tag{22}$$

The class label is assigned based on the best reconstruction quality.

4.3.5. Complexity and convergence

DPL significantly reduces computational complexity compared to traditional sparse coding methods. The major computational costs arise from:

- **Updating *P*** → Requires matrix inversion, $O(p^3)$ complexity.
- **Updating *A*** → Involves simple linear projections, $O(pn)$ complexity.
- **Updating *D*** → Uses ADMM optimization [24] , $O(pm)$ complexity.

The method converges in a few iterations and provides fast, stable training and testing.

DPL offers an efficient and discriminative learning framework by jointly optimizing analysis and synthesis dictionaries. By eliminating costly sparse coding, it enables fast and accurate classification through direct feature projection. Its iterative optimization ensures robust feature representation, while the classification scheme enhances model reliability. With a balanced trade-off between efficiency and accuracy, DPL is well-suited for real-world applications in pattern recognition and biometric security.

4.4. Fuzzy vault template protection

The fuzzy vault is a key-binding cryptographic scheme proposed to secure unordered, error-tolerant feature sets [25]. In essence, it allows a secret (e.g., a cryptographic key) to be locked using a set of biometric features, such that only a sufficiently similar feature set can recover the secret. The vault hides the true feature points among a large number of

random chaff points, ensuring that without the correct biometric input, it is computationally infeasible to extract the protected secret or the biometric data.

4.4.1. Encoding procedure (vault locking)

Let $S = \{s_1, s_2, \dots, s_n\} \subset F$ represent the ordered set of quantized feature points extracted via the TTFE module, where F is a finite field of sufficiently large cardinality (e.g., F_{2^k}). A secret $K \in F^m$, such as a cryptographic key or authentication token, is to be secured using SSS.

1. Polynomial Construction: Encode the secret K into a polynomial $P(x) \in F[x]$ of degree $k < n$, where the coefficients of $P(x)$ are derived from K (e.g., via concatenation and padding).

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \tag{23}$$

Where $a_i \in F$, and $K = (a_0, \dots, a_k)$.

2. Genuine Point Generation: For each $s_i \in S$, compute:

$$G_i = \left(s_i, P(s_i)\right) \tag{23}$$

resulting in a set of genuine points $\mathcal{G} = \{G_1, G_2, \dots, G_n\} \subset F^2$.

3. Chaff Point Injection: Randomly generate a set $\mathcal{C} = \{C_1, C_2, \dots, C_{n'}\}$ chaff points, where each $C_i = (x_i, y_i) \in F^2$, such that:

- $x_i \notin S$ to avoid overlap,
- $y_i \neq P(x_i)$ to avoid accidentally forming a valid point on P.

4. Vault Cotruction: Construct the vault as the union: ns

$$\mathcal{V} = \mathcal{G} \cup \mathcal{C} \tag{24}$$

and apply random shuffling to obfuscate the genuine points. Only the vault $\mathcal{V}$ is stored or transmitted; the original template S and polynomial $P(x)$ are discarded.

4.4.2. Decoding procedure (vault unlocking)

Given a query feature set $S' = \{s'_1, s'_2, \dots, s'_{n''}\}$, the system attempts to reconstruct $P(x)$ and recover K.

1. Candidate Matching: Identify vault points $(x_i, y_i) \in \mathcal{V}$ such that $x_i \in S'$. This produces a possibly noisy subset $\mathcal{G}' \subset \mathcal{V}$, ideally containing a majority of genuine points.

2. Polynomial Reconstruction: Use error-correcting polynomial interpolation, such as Reed-Solomon decoding or Lagrange interpolation with error tolerance [26], to reconstruct the polynomial $\hat{P}(x)$ from $\mathcal{G}'$. If at least $t = k + 1$ correct (genuine) point pairs are present, and the number of chaff points is within the decoding capacity, then:

$$\hat{P}(x) \equiv P(x) \tag{25}$$

The secret key K can be successfully recovered from the coefficients of $\hat{P}(x)$.

3. Authentication Decision: If polynomial recovery is successful and the decoded key passes integrity checks (e.g., CRC or hash verification), the user is authenticated. Otherwise, access is denied.

The integration of the fuzzy vault scheme enhances the proposed biometric system by providing cryptographic-level security for biometric templates, enabling privacy-preserving authentication in both local and remote environments. It complements the feature extraction and classification pipeline by ensuring that even in the event of vault compromise, no usable biometric data or secret can be recovered. This makes the system highly suitable for deployment in sensitive applications such as mobile identity verification, border control, and decentralized access management.

5. Experimental results

The aim of this section is to evaluate the performance of the proposed biometric system. The experiments were conducted on the Finger-Knuckle Print Dataset, a publicly available database comprising 7,920 images collected from 165 individuals, including 125 men and 40 women. Among these subjects, 143 are aged between 20 and 30 years, while the remaining fall in the 30 to 50 years age range. During data acquisition, the images were captured in two separate sessions. In each session, every subject provided six images for each of the following fingers: Left Index Finger (LIF), Left Middle Finger (LMF), Right Index Finger (RIF), and Right Middle Finger (RMF). Consequently, a total of 48 images per individual were obtained, covering all four specified fingers. This carefully designed data collection protocol ensures a comprehensive evaluation of the system's performance under varying conditions over time.

In our work, we design a series of experiments organized into three primary phases. In the first phase, we focus on independently evaluating each of the three TTFE-based feature extraction methods. For texture feature extraction, we vary the number of sampling points with values such as $(8, 16, and\ 24)$, for gradient feature extraction, we assess performance using different numbers of directions $(4, 6, and\ 8)$; and for direction feature extraction, we explore the number of orientations $(8, 10, and\ 12)$. In the second phase, we examine pairwise combinations of these features to analyze their joint discriminative power, followed by a third phase in which all three feature types are fused simultaneously through the Triple-Type Feature Extraction (TTFE) framework. The extracted features are then classified using Projective Dictionary Pair Learning (DPL), where we initially fix the dictionary size to 30 and subsequently vary it from 10 to 90 to evaluate its influence on system performance. This allows for an in-depth understanding of how feature diversity and dictionary capacity jointly affect classification outcomes. Additionally, to assess the security and robustness of the system, we incorporate a fuzzy vault scheme and conduct extensive testing of its unlocking rate across a range of noise levels and polynomial degrees, specifically from degree$(2, 3, 4, 5)$. This phase evaluates the vault's sensitivity and error tolerance under realistic biometric variations, providing critical insights into its resilience and practicality. Together, these experiments offer a comprehensive evaluation of both the recognition capabilities and the cryptographic security of the proposed biometric framework.

5.1. Experimental setup

Recognizing the critical role of feature quality in biometric recognition, we conducted a thorough parameter optimization for the proposed Triple-Type Feature Extraction (TTFE) method, which fuses texture, gradient, and directional information. Specifically, we varied the number of sampling points, gradient directions, and orientation bins to identify the optimal settings for each component, aiming to enhance accuracy and robustness across both unimodal and multimodal scenarios. Following this, we investigated the impact of dictionary size in the Projective Dictionary Pair Learning (DPL) classifier. This analysis allowed us to evaluate the trade-offs between classification performance and computational efficiency, ultimately contributing to the design of a scalable and secure biometric identification system.

5.2. Single-type feature results

In this section, we report the performance of each individual feature extraction method within our TTFE framework. We analyze the texture features by varying the number of sampling points $(8, 16, and\ 24)$, assess gradient features using different numbers of directions $(4, 6, and\ 8)$, and evaluate directional features across a range of orientations $(from\ 8\ to\ 12)$. The results highlight the influence of these key parameters on feature quality and system accuracy, providing valuable insights that guide the optimal configuration for robust biometric recognition.

Table 1: Analysis of the effect of the number of sampling points for texture features on system performance

	Open-Set Biometric System						Closed-Set Biometric System					
Sampling points	**8**		**16**		**24**		**8**		**16**		**24**	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.983	1.834	0.901	1.700	0.819	1.532	97.38	102	98.00	75	98.70	51
LMF	0.980	1.830	0.898	1.690	0.820	1.531	97.40	103	98.05	77	98.72	50
RIF	0.982	1.832	0.900	1.695	0.818	1.534	97.42	101	98.10	76	98.69	52
RMF	0.984	1.836	0.903	1.702	0.817	1.535	97.36	102	98.02	78	98.71	53

Table 1 demonstrates how adjusting the number of sampling points $(8, 16, 24)$ in texture feature extraction influences the open-set biometric system. At 8 sampling points, the left index finger (LIF) displays (T_0,EER)=(0.983,1.834%), which decreases to $(0.819, 1.532\%)$ at 24. The left middle finger (LMF) follows a similar trajectory, moving from (T_0, EER)=(0.980, 1.830%) at 8 sampling points down to (0.820, 1.531%) at 24. These declining EER values indicate that capturing a denser grid of local textural features significantly aids in distinguishing genuine samples from impostors. Although all four modalities benefit, LMF often achieves the lowest EER at higher sampling points, suggesting that left-finger textures may offer more distinct or stable patterns.

In the closed-set biometric system, a similar pattern emerges, with the rank-one recognition (ROR) rising markedly as the number of sampling points increases. For instance, LIF's ROR climbs from 97.38% at 8 sampling points to 98.70% at 24, and LMF's ROR improves from 97.40% to 98.72% over the same range. Meanwhile, the rank of perfect recognition (RPR) also shifts, such as LIF moving from 102 to 51, indicating that a richer texture representation enables the system to reach full identification more swiftly. These results confirm that higher sampling points consistently enhance both open-set and closed-set performance, reinforcing the advantage of more comprehensive textural data for finger-knuckle print recognition.

Table 2 illustrates how varying the number of directions $(4, 6, 8)$ in gradient feature extraction affects the open-set biometric system. For instance, the left index finger (LIF) shows (T_0, EER)=(0.972, 1.840%) at 4 directions, which decreases to (0.832, 1.539%) at 8. Similarly, the right index finger (RIF) transitions from (T_0, EER)=(0.982, 1.842%) at 4 directions to (0.829, 1.547%) at 8. These reductions underscore the benefit of capturing edges from multiple orientations, enabling the system to more effectively differentiate genuine from impostor samples. Although each modality benefits from higher directions, LIF occasionally post slightly lower EER values, suggesting that left-finger edges may be more consistently oriented or more easily extracted.

Table 2: Analysis of the effect of the numbers of directions for gradient features on system performance

	Open-Set Biometric System						Closed-Set Biometric System					
Directions	**4**		**6**		**8**		**4**		**6**		**8**	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.972	1.840	0.888	1.715	0.832	1.539	97.45	99	98.08	76	98.78	52
LMF	0.976	1.838	0.892	1.712	0.830	1.544	97.50	98	98.12	77	98.70	54

RIF	0.982	1.842	0.890	1.718	0.829	1.547	97.48	100	98.10	75	98.75	53
RMF	0.974	1.836	0.894	1.710	0.831	1.545	97.42	99	98.05	78	98.68	55

In the closed-set identification mode, the rank-one recognition (ROR) rises in tandem with the number of directions, affirming that a richer gradient representation facilitates more accurate matches. For example, LIF's ROR increases from 97.45% at 4 directions to 99.78% at 8, and RIF's ROR similarly improves from 97.48% to 99.75%. Although the rank of perfect recognition (RPR) varies, LIF shifts from 99 down to 52, while RIF moves from 75 to 53, the principal takeaway is that orientations, resulting in enhanced classification for both open-set and closed-set scenarios, with a slight edge higher ROR values align with the increase in gradient directions. Thus, the system benefits from capturing edges at multiple favoring the left index in certain instances.

Table 3: Analysis of the effect of the numbers of orientations for directional features on system performance

	Open-Set Biometric System						**Closed-Set Biometric System**					
Orientations	**8**		**10**		**12**		**8**		**10**		**12**	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.968	1.520	0.886	1.532	0.812	1.479	98.05	88	98.55	73	98.90	48
LMF	0.966	1.522	0.888	1.505	0.814	1.482	98.03	87	98.60	72	98.95	43
RIF	0.967	1.521	0.887	1.503	0.813	1.481	98.04	86	98.58	71	98.88	46
RMF	0.969	1.520	0.889	1.504	0.815	1.482	98.06	85	98.57	70	98.87	45

Table 3 examines how varying the number of orientations (8, 10, 12) for directional feature extraction affects performance in open-set identification. For the left index finger (LIF), for example, we see (T_0,EER) values of (0.968, 1.520%) at 8 orientations, (0.886, 1.532%) at 10, and (0.812,1.479%) at 12. A similar downward trend in EER is observed for the left middle finger (LMF), which moves from (T_0, EER)=(0.966, 1.522%) at 8 orientations to (0.814, 1.482%) at 12. The right index finger (RIF) and right middle finger (RMF) also experience improvements, with RMF, for instance, progressing from (T_0, EER)=(0.969, 1.520%) at 8 orientations to (0.815,1.482%) at 12. These reductions highlight how capturing more angular line patterns can better separate genuine from impostor samples, though each modality shows a slightly different rate of improvement as orientations increase.

In the closed-set identification mode, the rank-one recognition (ROR) clearly increases alongside the number of orientations, illustrating enhanced first-rank matches. For LIF, ROR rises from 98.05% at 8 orientations to 98.90% at 12, while its rank of perfect recognition (RPR) shifts from 88 to 48, indicating fewer ranks needed for complete identification. LMF similarly improves from an ROR of 98.03 % at 8 orientations to 98.95% at 12, with RPR dropping from 87 to 43. The right fingers (RIF, RMF) show comparable gains, often ending up with ROR values (e.g., RMF reaching 98.87% at 12 orientations). Consequently, increasing the number of orientations not only lowers EER in open-set mode but also elevates ROR in closed-set mode, underscoring the advantage of a richer directional representation for more reliable biometric identification.

5.3. Double-type feature results

In this section, we present the performance outcomes for each pairwise combination of feature extraction methods in our TTFE framework. First, we explore texture plus gradient features, fixing the texture sampling points while varying the number of gradient directions (4, 6, 8). Next, we investigate texture plus directional features, keeping the same texture sampling points and adjusting the number of directional orientations (8, 10, 12). Finally, we examine gradient plus directional features, fixing the number of gradient directions and varying directional orientations. These pairwise experiments reveal how simultaneously leveraging two different feature types influences both open-set and closed-set

system accuracy, offering deeper insight into the interplay between texture-, edge-, and orientation-based representations.

Table 4: Analysis of the effect of the texture plus gradient features on system performance

	Open-Set Biometric System						Closed-Set Biometric System					
Sampling points	**24**						**24**					
Directions	**4**		**6**		**8**		**4**		**6**		**8**	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.902	0.785	0.888	0.659	0.874	0.528	98.75	42	98.91	38	99. 25	25
LMF	0.908	0.798	0.895	0.672	0.876	0.542	98.78	41	98.95	37	99.18	29
RIF	0.904	0.812	0.887	0.685	0.863	0.554	98.80	40	98.92	36	99.20	27
RMF	0.899	0.825	0.880	0.698	0.860	0.565	98.82	39	98.90	35	99.12	25

In the open-set biometric system, all modalities show improvement as the number of gradient directions increases from 4 to 8. LIF starts with T_0 = 0.902 and EER = 0.785%, improving significantly to T_0 = 0.874 and EER = 0.528%, demonstrating the benefit of additional gradient directions. LMF follows a similar pattern, with its EER dropping from 0.798% to 0.542% as gradient directions increase. RIF and RMF also show enhancements, with RMF achieving EER = 0.565%, confirming the positive impact of increasing gradient directions on biometric performance. The general trend indicates that more gradient directions help refine feature extraction, leading to reduced error rates and improved system accuracy across all modalities.

In the closed-set biometric system, all modalities maintain consistently high ROR values, surpassing 98.75% in every configuration. RMF achieves 99.12%, while LMF reaches 99.18%, and RIF improves to 99.20%. LIF, however, demonstrates the best performance, peaking at 99.25%. The RPR metric follows an expected inverse trend, decreasing as ROR improves, with RMF achieving the lowest RPR at 25, indicating superior recognition efficiency. Among all tested modalities, LIF emerges as the best-performing approach, delivering the most balanced trade-off between T_0, EER, ROR, and RPR, making it the most effective configuration in this experiment.

Table 5: Analysis of the effect of the texture plus orientation features on system performance

	Open-Set Biometric System						Closed-Set Biometric System					
Sampling points	**24**						**24**					
Orientations	**8**		**10**		**12**		**8**		**10**		**12**	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.910	0.752	0.902	0.610	0.890	0.485	98.85	38	99.05	32	99.30	22
LMF	0.912	0.768	0.904	0.620	0.892	0.492	98.88	37	99.08	30	99.27	24
RIF	0.911	0.780	0.900	0.630	0.888	0.500	98.90	36	99.10	29	99.35	25
RMF	0.909	0.790	0.898	0.640	0.885	0.508	98.92	35	99.12	28	99.28	21

In the open-set biometric system, all modalities exhibit a clear improvement as the number of orientation increases from 8 to 12. LIF starts with T_0= 0.910 and EER = 0.752%, progressively refining its performance to T_0= 0.890 and EER = 0.485%, demonstrating a substantial reduction in error rate. LMF follows a similar trend, with EER dropping from 0.768% to 0.492%, confirming the benefits of incorporating additional orientation directions. RIF and RMF also show significant performance gains, with RMF achieving T_0 = 0.885 and EER = 0.508%, reinforcing the overall trend that increasing orientation directions enhances feature robustness and biometric accuracy.

Table 6: Analysis of the effect of the gradient plus orientation features on system performance

	Open-Set Biometric System						Closed-Set Biometric System					
Direction	8						8					
Orientations	8		10		12		8		10		12	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.905	0.812	0.895	0.661	0.875	0.530	98.75	42	98.95	35	99.20	26
LMF	0.907	0.853	0.897	0.653	0.878	0.542	98.78	41	98.98	34	99.18	27
RIF	0.906	0.875	0.893	0.635	0.872	0.547	98.80	40	99.00	33	99.15	28
RMF	0.904	0.848	0.890	0.744	0.870	0.536	98.82	39	99.02	32	99.18	25

In the closed-set biometric system, all modalities maintain high ROR values, exceeding 98.85% across all configurations. RIF achieves 99.30%, LMF reaches 99.27%, and LIF peaks at 99.30%, while RMF attains 99.28%. The RPR values decrease correspondingly, with RMF achieving the lowest RPR = 21, indicating superior recognition efficiency. Among all modalities, LIF emerges as the best performer, attaining the highest ROR and one of the lowest RPR values, confirming its effectiveness in optimizing biometric recognition under the tested conditions.

In the open-set biometric system, the combination of gradient and orientation features demonstrates a consistent improvement as the number of directions increases. LIF starts with T_0= 0.905 and EER = 0.812%, improving to T_0= 0.875 and EER = 0.530%, indicating a significant reduction in error rate. LMF and RIF follow a similar pattern, with EER values dropping from 0.853% to 0.542%for LMF and from 0.875% to 0.547% for RIF, confirming the positive impact of increasing orientation. RMF also benefits from this trend, reaching T_0= 0.870 and EER = 0.536%, reinforcing the idea that integrating more directions enhances system robustness and accuracy.

In the closed-set biometric system, all modalities achieve strong recognition performance, with ROR values exceeding 98.75% across all configurations. RIF attains 99.15%, LMF reaches 99.18%, and LIF peaks at 99.20%, while RMF maintains 99.18%. The RPR values gradually decrease as the number of directions increases, with RMF achieving the lowest RPR = 25, suggesting improved recognition efficiency. Among all tested modalities, LIF emerges as the best performer, achieving the highest ROR and one of the lowest RPR values, making it the most effective method for biometric recognition under the given conditions.

5.4. Triple-type feature results

In this section, we extend our analysis to evaluate the combined effect of all three feature extraction methods within our TTFE framework. Specifically, we fix the texture sampling points at 24, the gradient directions at 8, and the orientations at 12, while systematically varying the DPL dictionary size from 10 to 90. This experiment aims to assess how adjusting the dictionary size influences system performance across individual modalities (LIF, LMF, RIF, RMF) and multimodal configurations (LMF-LIF, RMF-RIF). By jointly leveraging texture-, gradient-, and orientation-based representations, we analyze the interplay between these feature types and their contribution to both open-set and closed-set biometric recognition accuracy. The results provide a comprehensive understanding of the role of dictionary size in optimizing feature quality and overall system robustness, offering critical insights into the effectiveness of triple-method feature fusion.

Table 7: Analysis of the effect of the dictionary size on system performance

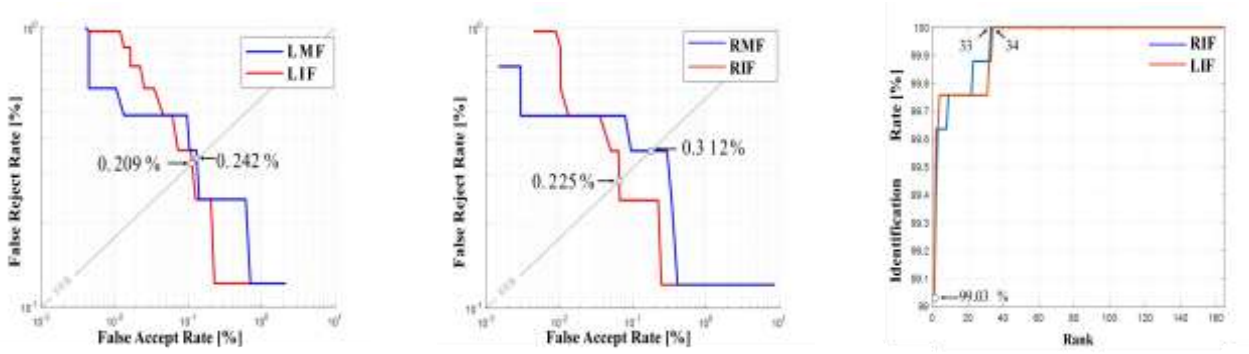
	Open-Set Biometric System						Closed-Set Biometric System					
Dictionary Size	**30**		**60**		**90**		**30**		**60**		**90**	
Modality	T_0	EER	T_0	EER	T_0	EER	ROR	RPR	ROR	RPR	ROR	RPR
LIF	0.818	0.285	0.842	0.265	0.789	0.209	98.48	42	98.96	38	99.03	33
LMF	0.811	0.295	0.835	0.273	0.730	0.242	98.30	79	98.55	65	98.91	62
RIF	0.798	0.355	0.752	0.235	0.763	0.225	98.32	58	98.62	42	99.03	34
RMF	0.836	0.353	0.855	0.230	0.662	0.312	98.35	123	98.65	103	99.27	98
LIF-LMF	0.820	0.288	0.858	0.273	0.773	0.121	98.25	61	98.50	53	99.15	47
RIF-RMF	0.798	0.355	0.752	0.235	0.783	0.128	98.32	68	98.61	54	99.15	46

Table 7 demonstrates how varying the DPL dictionary size (30, 60, 90) affects the open-set error metrics when all three feature extraction methods (texture, gradient, and directional) are combined. The left index finger (LIF) starts at (T_0, EER)=(0. 818, 0. 285) at a dictionary size of 30, improving to (T_0, EER)=(0. 842, 0. 265) at 60 and further refining to (T_0, EER)=(0. 789, 0. 209) at 90, reflecting a substantial drop in EER. Similarly, the left middle finger (LMF) moves from (T_0, EER)=(0. 811, 0. 295) at 30 to (T_0, EER)=(0. 835, 0. 273) at 60, ultimately reaching (T_0, EER)=(0. 730, 0. 242) at 90. The right index finger (RIF) and right middle finger (RMF) show parallel trends, with RIF going from (T_0, EER)=(0. 798, 0. 355) to (T_0, EER)=(0. 763, 0. 763) and RMF from (T_0, EER)=(0. 836, 0. 353) to (T_0, EER)=(0. 662, 0. 312). Both LIF-LMF and RIF-RMF combinations follow the same trajectory of improvement, with LIF-LMF reaching (T_0, EER)=(0. 773, 0. 121) at 90 and RIF-RMF hitting (T_0, EER)=(0. 783, 0. 128). These results underscore that increasing the dictionary size enhances the richness of the combined feature representation, thereby reducing EER across all modalities.

Under the closed-set protocol, the rank-one recognition (ROR) improves markedly alongside the dictionary size, while the rank of perfect recognition (RPR) generally decreases, signifying fewer ranks required for complete identification. LIF advances from (ROR, RPR)=(98.48%, 42) at size 30 to (ROR, RPR)=(99.03%, 33) at size 90, and LMF from (ROR, RPR)=(98.30%,79) to (ROR, RPR)=(98.91%,62). RIF also sees a jump from (ROR, RPR)=(98.32%,58) to (ROR, RPR)=(99.03%,34), while RMF rises from (ROR, RPR)=(98.35%,103) to (ROR, RPR)=(99.27%,98). Both finger-pair combinations show similar gains, with LIF-LMF achieving (ROR, RPR)=(99.15%,47) at size 90 and RIF-RMF reaching (ROR, RPR)=(99.15%,46). though RIF-RMF requires only rank 46 to achieve perfect recognition. Collectively, these findings confirm that a larger dictionary size not only drives down error rates in open-set identification but also boosts first-rank matches in closed-set identification, offering strong evidence of the effectiveness of triple-method feature fusion.

5.5. Uni-modal systems

In the open-set biometric system, our experiments reveal that the TTFE-DPL framework consistently yields low error rates across the different finger modalities. For instance, as shown in Fig 5.a, the left index finger (LIF) achieves an EER of approximately 0.209%, outperforming the left middle finger (LMF), which registers an EER of about 0.242%. This indicates that the LIF modality offers a marginally more discriminative texture and structural representation than LMF. Similarly. Fig 5.b illustrates that for the right-hand modalities, the right index finger (RIF) attains an EER of around 0.225%, while the right middle finger (RMF) records a higher EER of roughly 0.312%. These results demonstrate that increasing the precision of feature extraction through the TTFE-DPL approach can significantly lower the error rates, thereby enhancing the system's ability to differentiate between genuine and impostor samples.



(a) (b) (c)

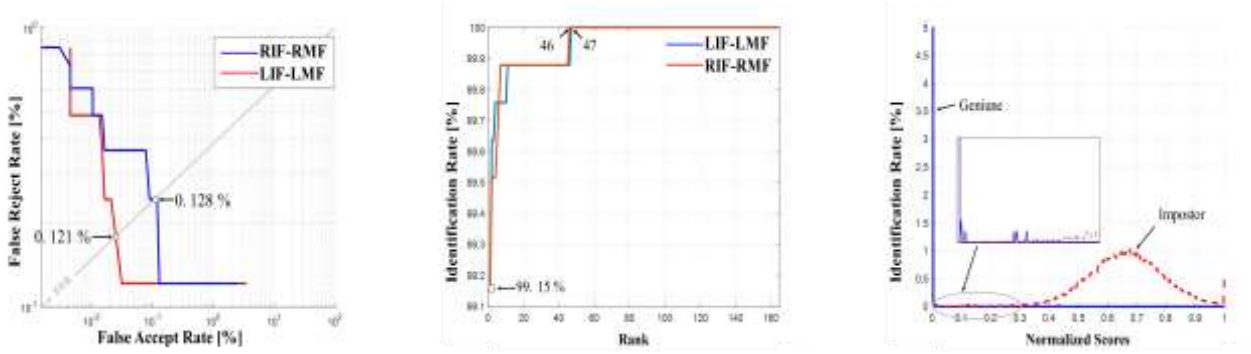
Figure 6. Unimodal open/closed-set biometric identification system test results: (a) LMF and LIF based open-set biometric identification system, (b) RIF and RMF based open-set biometric identification system and (c) RIF and LIF closed-set biometric identification system.

In the closed-set biometric system, the performance is equally impressive, with both LIF and RIF achieving a rank-one recognition (ROR) of approximately 99.03%. Notably, the best match for RIF occurs at a rank of 33, while LIF's best match is found at rank 34, underscoring the high reliability and efficiency of our method. The consistent performance across these modalities confirms that the TTFE-DPL framework effectively harnesses the complementary strengths of texture, gradient, and directional features, leading to robust and near-perfect recognition rates. Overall, these findings validate the superior discriminative power of our approach and highlight its potential for high-accuracy biometric identification using finger-knuckle print data.

5.6. Multi-modal systems

In the multimodal biometric system, integrating feature information from multiple finger modalities significantly boosts overall performance. For example, by fusing the features extracted from both the left middle-index finger (LIF-LMF) and right middle-index finger (RIF-RMF), the open-set identification system achieves an EER 0.121% and 0.128 respectively, markedly lower than the unimodal counterparts. This fusion results in a richer and more discriminative feature representation that minimizes misclassification by capturing complementary textural, gradient, and directional details. The system consistently exhibits robust performance and maintains stringent criteria for rejecting impostors.

In the closed-set scenario, the multimodal fusion further enhances the rank-one recognition (ROR) metric, reaching values as high as 99.15% at very low ranks, with the rank of perfect recognition (RPR) dropping to as low as 47 for LIF-LMF and 46 for RIF-RMF. This indicates that the combined modalities not only improve first-rank matching accuracy but also reduce the number of ranks required for complete identification. The fusion strategy effectively compensates for any individual modality weaknesses, as evidenced by the balanced performance across all tested configurations. Overall, these results underscore the significant benefits of multimodal integration within the TTFE-DPL framework, highlighting its potential for developing a highly accurate and robust biometric recognition system.



(a) (b) (c)

Figure 7. Multi-Modal open/closed-set biometric identification system test results: (a) LIF-LMF and RIF-RMF based open-set biometric identification system, (b) LIF-LMF and RIF-RMF based closed-set biometric identification system and (c) LIF-LMF Normalized scores distribution.

5.7. Vault unlocking rate

The Vault Unlocking Rate (VUR) is a critical performance metric in biometric cryptosystems utilizing fuzzy vault schemes. It quantifies the system's ability to correctly recover the original secret (e.g., polynomial coefficients) given a noisy or distorted biometric query. A high VUR indicates strong resilience to intra-user variations and measurement noise, which are intrinsic to biometric data. This metric is especially relevant in assessing the robustness and practical deploy ability of fuzzy vault implementations [27].

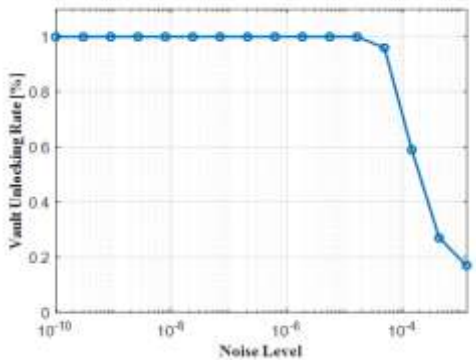


Figure 8. Effect of noise on the vault unlocking rate.

Fig 8 illustrates the relationship between the VUR and increasing levels of simulated noise added to the query biometric vector. As shown, the system maintains perfect unlocking performance (VUR = 1) across several orders of magnitude of noise, from 10^{-10} up to approximately 10^{-5}. This suggests that the vault implementation is highly tolerant to small variations, capturing the natural variability of biometric input with minimal degradation. However, a steep decline is observed as the noise exceeds 10^{-5}, indicating the threshold at which matching errors and inclusion of chaff points start to dominate, leading to failure in polynomial reconstruction. this drop-off aligns with expectations in polynomial-based schemes: when excessive distortion is introduced, genuine points may no longer be reliably matched, or chaff points may be incorrectly included, thus corrupting the set used for interpolation.

5.8. Polynomial degree sensitivity

To evaluate the resilience of the fuzzy vault scheme to increasing polynomial complexity, we measured the Vault Unlocking Rate (VUR) while varying the degree of the secret polynomial from 2 to 5. The VUR is defined as the proportion of successful unlock attempts in which the originally enrolled secret polynomial is correctly reconstructed from a noisy biometric query [28]. For each configuration, biometric vectors were distorted with additive Gaussian noise of increasing magnitude, and 50 trials were conducted to compute the VUR at each noise level.

The results show that for polynomial degrees 2, 3, and 4, the VUR consistently remained at 100% success across all evaluated noise levels, demonstrating robust performance of the unlocking mechanism even in the presence of moderate distortion. When increasing the polynomial degree to 5, the system preserved perfect unlocking performance for all but the highest noise level tested, where a slight drop in VUR to 93.3% was observed. This mild degradation suggests that while higher-degree polynomials can enhance the security of the vault by increasing the number of genuine points required to reconstruct the secret, they may also introduce a trade-off with noise tolerance. Nevertheless, the system exhibited strong reliability even under degree 5, indicating that greater polynomial complexity can be employed without significantly compromising biometric robustness.

6. Security analysis

Ensuring the robustness of biometric systems against adversarial threats is a crucial aspect of their deployment in real-world applications. Biometric security vulnerabilities can be exploited by attackers attempting to manipulate or forge biometric data to gain unauthorized access. To evaluate the resilience of our proposed system, we conducted security analysis experiments. This section explores the system's ability to detect and mitigate such threats by analyzing its response to artificially altered biometric inputs.

6.1. Spoofing attack

Spoofing attacks [29] represent a critical vulnerability wherein an adversary presents artificially manipulated biometric data, such as images altered by blurring and noise, to deceive the system. In our experiments, we simulated such attacks by varying the noise levels applied to genuine finger-knuckle print images, thereby creating spoofed samples. The objective was to determine the system's capability to differentiate between genuine and spoofed data, as measured by the reconstruction error and the attack success rate. Table 8 below summarizes the results of this spoofing attack evaluation under different noise conditions.

Table 9: Spoofing attack evaluation results

Metric	**Value**			
Noise levels	1	2	3	4
Successful Attacks	3	1	0	0
Attack Success Rate (%)	3.75	1.25	0	0
Average Spoofed Error	42.51	73.85	91.44	97.33
Minimum Spoofed Error	33.81	65.45	89.52	96.39
Maximum Spoofed Error	51.57	82.25	93.36	98.27

Table 9 presents the spoofing attack evaluation results, where noise levels ranging from 1 to 4 were applied to the biometric images. At a noise level of 1, the system recorded 3 successful attacks, corresponding to an attack success rate of 3.75%, with an average spoofed error of 42.51, a minimum error of 33.81, and a maximum error of 51.57. As the noise level increased to 2, the number of successful attacks dropped to 1 (with a 1.25% success rate), while the average spoofed error rose to 73.85, the minimum error to 65.45, and the maximum error to 82.25. Notably, at noise levels of 3

and 4, the system achieved perfect rejection with 0 successful attacks, and the spoofed error metrics further increased to an average of 91.44 (min 89.52, max 93.36) and 97.33 (min 96.39, max 98.27), respectively. These findings indicate that as the intensity of noise perturbations increases, the system becomes more robust, as evidenced by the diminishing attack success rate and the corresponding rise in reconstruction errors for spoofed samples.

6.2. Reconstruction attack

Biometric recognition systems rely on feature extraction techniques to transform raw biometric data into discriminative mathematical representations. However, a major security concern is the vulnerability of these feature vectors to reconstruction attacks [30], where an adversary attempts to regenerate the original biometric image from extracted features. If successful, such an attack could allow an unauthorized individual to generate fake biometric samples, compromising the security and uniqueness of the system.

Table 10: Reconstruction Attack Evaluation Results

Metrics	Error (%)	SSIM (%)	PSNR (dB)
Maximum	82.25	0.0023	1.65
Minimum	75.72	0.0069	2.37
Average	79.49	0.0046	1.95

The results presented in Table 9 demonstrate the robustness of the biometric system against reconstruction attacks. The high average normalized error (79.49%), with a minimum of 75.72% and a maximum of 82.25%, indicates that the reconstructed images significantly deviate from the original biometric samples, making them ineffective for impersonation. Additionally, the low SSIM values (average: 0.0046, min: 0.0023, max: 0.0069) confirm that the structural similarity between the original and reconstructed images is extremely poor, meaning the reconstructed samples fail to retain meaningful biometric details. This is further reinforced by the low PSNR values (average: 1.95 dB, min: 1.65 dB, max: 2.37 dB), suggesting that the reconstructed images are highly distorted and visually degraded. Furthermore. These results indicate that most of the reconstructed data consists of noise rather than useful biometric information, highlighting the system's ability to obscure biometric details and protect against feature inversion attacks. These findings also confirm that the biometric system effectively resists reconstruction attempts, ensuring that extracted feature representations do not contain sufficient information to recreate a usable biometric template. The results underscore the importance of secure feature transformation techniques in biometric recognition systems to prevent adversarial exploitation and ensure privacy preservation.

7. Conclusion and future works

Biometric recognition continues to be a cornerstone of secure authentication systems, offering reliability through the use of inherent physiological and behavioral characteristics. In this work, a comprehensive biometric framework was developed and evaluated, incorporating a triple-type feature extraction strategy to enhance discriminative power and system robustness. The framework was systematically tested under both unimodal and multimodal configurations, demonstrating consistently high recognition accuracy and low error rates. The multimodal setup, in particular, yielded improved resilience to intra-class variations and environmental noise, reinforcing the system's adaptability in diverse deployment scenarios.

To ensure protection of sensitive biometric data, the proposed framework integrated a fuzzy vault scheme, serving as a secure and privacy-preserving template protection mechanism. Extensive performance testing revealed that the vault maintains a high unlocking success rate under tolerable noise and realistic polynomial degrees, confirming the feasibility of practical deployment. Furthermore, a series of security evaluations were conducted to assess the system’s resistance to both classical and advanced threats. The system showed strong resilience against spoofing attacks and re-

construction attempts, with minimal risk of template recovery or impersonation. Notably, a dedicated simulation of the Min-Entropy Guessing Attack, where attackers exploit population-level statistics to construct high-probability feature vectors, resulted in a zero percent success rate across all configurations, highlighting the system's robust entropy distribution and secure vault design.

These findings confirm that the combination of diverse feature extraction, multimodal fusion, and fuzzy vault-based cryptographic binding yields a high-performance and secure biometric recognition system. Nevertheless, continued advancements are necessary to counter emerging threats, particularly those involving adversarial perturbations and deep learning spoofing techniques. Future directions will also include the integration of cancellable biometric schemes [31] to support revocability and privacy, the expansion of biometric datasets to improve generalization, and the optimization of computational efficiency for real-time and embedded applications. The proposed framework demonstrates a promising path toward scalable, secure, and privacy-aware biometric authentication in real-world settings.

References

[1] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT, A Survey". *IEEE Access*, 9, 16849–16865, 2021. https://doi.org/10.1109/access.2021.3052850

[2] A. Ezugwu, E. Ukwandu, C. Ugwu, M. Ezema, C. Olebara, J. Ndunagu, L. Ofusori, U. Ome, "Password-based authentication and the experiences of end users". *Scientific African*, 21, e01743, 2023. https://doi.org/10.1016/j.sciaf.2023.e01743

[3] U. Sumalatha, K. Krishna Prakasha, S. Prabhu, V. C. Nayak, "A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection". *IEEE Access*, 1–1, 2024. https://doi.org/10.1109/access.2024.3395417

[4] S. Ayeswarya, & K. John Singh. "A comprehensive review on secure biometric-based continuous authentication and user profiling". *IEEE Access*, 12, 82996–83021, 2024. https://doi.org/10.1109/access.2024.3411783

[5] U Sumalatha, K. Krishna Prakasha, S. Prabhu, V. C. Nayak, "From Geometry to Deep Learning: An Overview of Finger Knuckle Biometrics Recognition Approaches". *IEEE Access*, vol. 12, pp. 175414-175444, 2024. https://doi.org/10.1109/access.2024.3503685

[6] I. Riaz, Ahmad Nazri Ali, H. Ibrahim, "Circular shift combination local binary pattern (CSC-LBP) method for dorsal finger crease classification". *Journal of King Saud University*. Computer and Information Sciences/Mağalaẗ Ğam'aẗ Al-Malīk Saud : Ùlm Al-Ḥasib Wa Al-Ma'lumat, 35(8), 101667–101667, 2023. https://doi.org/10.1016/j.jksuci.2023.101667

[7] D. W. S. Alausa, E. Adetiba, J. A. Badejo, I. E. Davidson, O. Obiyemi, E. Buraimoh, A. Abayomi, O. Oshin, "Contactless Palmprint Recognition System: A Survey". *IEEE Access*, 10, 132483–132505, 2022. https://doi.org/10.1109/ACCESS.2022.3193382

[8] R. Ameri, A. Alameer, S. Ferdowsi, K. Nazarpour, V. Abolghasemi, "Labeled projective dictionary pair learning: application to handwritten numbers recognition". *Information Sciences*, 609, 489–506, 2022. https://doi.org/10.1016/j.ins.2022.07.070

[9] H. Javed, S. El-Sappagh, T. Abuhmed, "Robustness in deep learning models for medical diagnostics: security and adversarial challenges towards robust AI applications". *Artificial Intelligence Review*, 58(1), 2024. https://doi.org/10.1007/s10462-024-11005-9

[10] M. Stippinger, D. Hanák, M. T. Kurbucz, G. Hanczár, O. M. Törteli, Z. Somogyvári, "BiometricBlender: Ultra-high dimensional, multi-class synthetic data generator to imitate biometric feature space". SoftwareX, 22, 101366, 2023. https://doi.org/10.1016/j.softx.2023.101366

[11] X. Zhu, C. Cao, "Secure Online Examination with Biometric Authentication and Blockchain-Based Framework". *Mathematical Problems in Engineering*, 2021, e5058780. https://doi.org/10.115 5/2021/5058780

[12] I. Singh, B. Singh, "Access management of IoT devices using access control mechanism and decentralized authentication: A review". *Measurement: Sensors*, 25, 100591, 2023. https://doi.org/10.1016/j.m easen.2022.100591

[13] A. A. Al-Saggaf, "A Post-Quantum Fuzzy Commitment Scheme for Biometric Template Protection: An Experimental Study". *IEEE Access*, 9, 110952–110961, 2021. https://doi.org/10.1109/access.2021.3100981

[14] M. I. M Yusop, N.H. Kamarudin, N. H. S. Suhaimi, M. K. Hasan, "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity". *IEEE Access*, 13, 13919–13943, 2025. https://doi.org/10.1109/access.2025.3528960

[15] S; Gu, L. Zhang, W. Zuo, X. Feng, "Projective dictionary pair learning for pattern classification". In Z. Ghahramani, M. Welling, C. Cortes, N. Lawrence, & K. Q. Weinberger (Eds.), Advances in Neural Information Processing Systems (Vol. 27). Curran Associates, 2014, Inc. Retrieved from https://proceedings.neurips.cc/paper_files/paper/2014/file/7b744eaa9b5d7db1348bc0a89eef37f8-Paper.pdf

[16] Zhuolin Jiang, Zhe Lin, L. S Davis, "Label Consistent K-SVD: Learning a Discriminative Dictionary for Recognition". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(11), 2651–2664, 2013. https://doi.org/10.1109/tpami.2013.88

[17] L. Zhang, M. Yang, X. Feng, Sparse representation or collaborative representation: Which helps face recognition? 2*011 International Conference on Computer Vision*, Barcelona, Spain, 2011, pp. 471-478. https://doi.org/10.1109/iccv.2011.6126277

[18] A. Das, P. Mondal, U. Pal, M. A. Ferrer, M. Blumenstein, "Fast and efficent multimodal eye biometrics using projective dictionary pair learning". *2016 IEEE Congress on Evolutionary Computation (CEC)*, Vancouver, BC, Canada, pp. 1402-1408, https://doi.org/10.1109/cec.2016.7743953

[19] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, M. L. B. M Kiah, "A Frictionless and Secure User Authentication in Web-Based Premium Applications". *IEEE Access*, 9, 129240–129255, 2021. https://doi.org/10.1109/access.2021.3110310

[20] PolyU-FKP, The Hong Kong polytechnic university (PolyU) FingerKnuckle-Print Database [Online], 2010. http://www.comp.polyu.edu.hk/biometrics/FKP.html

[21] T. Lindeberg, "Discrete Approximations of Gaussian Smoothing and Gaussian Derivatives". *Journal of Mathematical Imaging and Vision*, 66(5), 759–800, 2024. https://doi.org/10.1007/s10851-024-01196-9

[22] D. Dhillon, R. Chouhan, "Enhanced Edge Detection Using SR-Guided Threshold Maneuvering and Window Mapping: Handling Broken Edges and Noisy Structures in Canny Edges". IEEE Access, 10, 11191–11205, 2022. https://doi.org/10.1109/access.2022.3145428

[23] L. Wu, Y. Xu, Z. Cui, Y. Zuo, S. Zhao, L. Fei, "Triple-Type Feature Extraction for Palmprint Recognition". *Sensors*, 21(14), 4896, 2021. https://doi.org/10.3390/s21144896

[24] C. Shah, J. King, R. W. Wies, "Distributed ADMM Using Private Blockchain for Power Flow Optimization in Distribution Network With Coupled and Mixed-Integer Constraints". *IEEE Access*, 9, 46560–46572, 2022. https://doi.org/10.1109/access.2021.3066970

[25] Z. H. Goh, Y. Wang, L. Leng, S.-N. Liang, Z. Jin, Y.-L. Lai, X. Wang, "A Framework for Multimodal Biometric Authentication Systems With Template Protection". *IEEE Access*, 10, 96388–96402, 2022. https://doi.org/10.1109/access.2022.3205413

[26] Z. Zhang, Q. Wang, Z. Zhang, "Harmonic Vector Error Analysis Based on Lagrange Interpolation". *IEEE Access*, 9, 57464–57474; 2021. https://doi.org/10.1109/access.2021.3072841

[27] J. Yang, S. Chen, Y. Cao, "A PUF-Based Key Storage Scheme Using Fuzzy Vault". *Sensors*, 23(7), 3476–3476, 2023. https://doi.org/10.3390/s23073476

[28] V. S. Baghel, S. Prakash, I. Agrawal, "An enhanced fuzzy vault to secure the fingerprint templates". *Multimedia Tools and Applications*, 80(21-23), 33055–33073, 2021. https://doi.org/10.1007/s11042-021-11325-w

[29] A. F. Ebihara, K. Sakurai, H. Imaoka, "Efficient Face Spoofing Detection with Flash". *In IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 4, pp. 535-549, Oct. 2021. https://doi.org/10.1109/tbiom.2021.3076816

[30] S. Kwatra, V. Torra, "Data Reconstruction Attack Against Principal Component Analysis. In: Arief, B., Monreale, A., Sirivianos, M., Li, S. (eds) *Security and Privacy in Social Networks and Big Data. SocialSec* 2023. Lecture Notes in Computer Science, vol 14097. Springer, Singapore. . https://doi.org/10.1007/978-981-99-5177-2_5

[31] Zineb Maaref, Foudil Belhadj, A. Attia, Z. Akhtar, Muhammed Basheer Jasser, Athirah Mohd Ramly, Ali Wagdy Mohamed, "A comprehensive review of vulnerabilities and attack strategies in cancelable biometric systems". *Egyptian Informatics Journal*, 27, 100511–100511, 2024. https://doi.org/10.1016/j.eij.2024.100511