

# Palmprint Recognition Using Multiscale Signal Analysis and Quantum-Secure Communication

Saoussen Djeddi, Yacine Belhocine and Abdallah Meraoumia

**Keywords and phrases:** Palmprint Biometrics, Multiscale Signal Analysis, Gabor Filters, Support Vector Machines, Quantum Key Distribution, Secure Authentication.

*This manuscript is an extended and significantly improved version of the paper entitled “Enhanced Finger-Knuckle-Print Recognition Using Deep Texture Feature Analysis” presented at ICRAMI 2025 (Tunisia, November 2025). While the conference work focused on finger-knuckle-print (FKP) recognition, the present study extends the investigation to palmprint biometrics, which provide richer and more stable structural and textural features for reliable identification.*

*The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.*

*The authors thank the staff of LAMIS and L3S laboratories for helpful comments and suggestions..*

**Abstract** Palmprint recognition has gained increasing attention as a reliable biometric modality due to the richness and stability of its structural patterns, including principal lines, wrinkles, and fine textures. Compared to other biometric traits, palmprints exhibit strong discriminative capability and reduced sensitivity to environmental variations, making them well suited for secure authentication systems. At the same time, the growing use of remote biometric verification introduces significant security challenges related to the confidentiality and integrity of transmitted biometric data. This paper proposes a mathematically grounded palmprint recognition framework that combines multiscale signal analysis with quantum-secure communication. Palmprint images are first enhanced using contrast-limited adaptive histogram equalization to improve local structural visibility. Discriminative features are then extracted through a multiscale bank of two-dimensional Gabor filters, capturing orientation- and frequency-selective texture information, followed by local binary pattern encoding to model local spatial relationships. The resulting feature vectors are classified using a support vector machine with a radial basis function kernel, formulated within a reproducing kernel Hilbert space. To secure remote authentication, the BB84 quantum key distribution protocol is employed to protect biometric data transmission with information-theoretic security guarantees. Experimental results on a public palmprint dataset demonstrate high recognition accuracy and robust generalization performance. The proposed framework offers an interpretable, secure, and theoretically principled solution for palmprint-based biometric authentication.

## 1 Introduction

The continued growth of networked information systems and distributed access control infrastructures has significantly increased the demand for reliable and secure user authentication mechanisms. Modern applications in areas such as physical access control, digital identity management, and remote system authorization increasingly rely on authentication processes conducted over public or semi-trusted communication networks. While these systems improve scalability, flexibility, and user convenience, they also introduce new security challenges related to unauthorized access, interception of sensitive data, and malicious manipulation of authentication messages [1]. Consequently, ensuring both the reliability and security of authentication mechanisms has become a fundamental requirement for contemporary information systems [2].

Biometric authentication has emerged as a compelling alternative to conventional knowledge-based and possession-based authentication methods due to its intrinsic association with the physiological or behavioral characteristics of an individual [3]. Among the various biometric modalities, palmprint recognition has received considerable attention owing to the richness and stability of palmprint patterns, which include principal lines, wrinkles, ridges, and fine-scale texture structures. These characteristics provide a high degree of distinctiveness while exhibiting relative robustness to variations in illumination, pose, and short-term physiological changes [4]. As a result, palmprint-based biometric systems have been widely investigated for high-security applications requiring reliable personal identification. Nevertheless, practical deployment of such systems continues to face challenges related to feature representation, classification accuracy, and protection of biometric data in remote authentication scenarios [6].

One of the most critical concerns in biometric system design is the protection of biometric templates during storage and transmission. Unlike passwords or cryptographic keys, biometric traits are inherently sensitive and largely irrevocable. If compromised, biometric templates may permanently expose individuals to identity theft, cross-system tracking, and privacy violations [5]. This issue is particularly severe in remote authentication settings, where biometric data must be transmitted over potentially insecure communication channels. Ensuring confidentiality and integrity of biometric information throughout the authentication process is therefore essential for the long-term viability of biometric technologies.

From a signal processing perspective, palmprint images can be modeled as two-dimensional textured signals whose discriminative information is distributed across multiple spatial scales and orientations. Effective feature extraction methods must therefore capture both global structural patterns and local texture variations. Multiscale analysis techniques based on Gabor filter banks have demonstrated strong capability in representing orientation- and frequency-selective texture components and have been successfully applied to various biometric recognition tasks [7]. In addition, local statistical descriptors such as local binary patterns provide compact and robust representations of local spatial relationships, contributing complementary discriminatory information that enhances overall recognition performance [8]. However, the successful utilization of these features depends on their integration within a robust and theoretically sound classification framework.

Kernel-based learning methods, particularly support vector machines, have been extensively studied for biometric classification due to their strong generalization properties and well-established theoretical foundations [9]. By formulating the classification problem as a convex optimization task in a reproducing kernel Hilbert space, support vector machines are able to effectively handle high-dimensional feature representations while maintaining robustness to noise and limited training data [10]. Despite their effectiveness, biometric systems that rely solely on classical cryptographic mechanisms for data protection remain vulnerable to both current and emerging security threats.

An additional challenge arises from the anticipated impact of large-scale quantum computing on conventional cryptographic infrastructures. Many widely used cryptographic schemes are based on computational hardness assumptions that may be compromised by quantum algorithms, raising concerns about the long-term security of sensitive data [11]. Quantum key distribution offers a fundamentally different security paradigm by enabling the establishment of symmetric encryption keys with information-theoretic security guarantees derived from the principles of quantum mechanics [12]. Protocols such as BB84 allow legitimate parties to detect eavesdropping attempts and securely distribute cryptographic keys, making quantum key distribution a promising solution for protecting biometric data in remote authentication environments.

Motivated by these considerations, this paper presents a unified palmprint recognition framework that integrates multiscale signal analysis, kernel-based classification, and quantum-secure communication. The proposed system employs contrast enhancement to improve palmprint image quality, followed by multiscale feature extraction using two-dimensional Gabor filters and local binary pattern encoding to capture complementary texture information. Classification is performed using a support vector machine with a radial basis function kernel, while secure transmission of biometric templates and authentication data is achieved through the BB84 quantum key distribution protocol. By jointly addressing recognition performance and communication security, the proposed framework provides a mathematically grounded and forward-looking solution for palmprint-based biometric authentication.

This manuscript is an extended and significantly improved version of the paper entitled “Enhanced Finger-Knuckle-Print Recognition Using Deep Texture Feature Analysis” presented at ICRAMI 2025 (Tunisia, November 2025). While the conference work focused on finger-knuckle-print (FKP) recognition, the present study extends the investigation to palmprint biometrics, which provide richer and more stable structural and textural features for reliable identification. In this extended version, we propose a redesigned framework based on multiscale signal analysis using Gabor filters combined with Local Binary Patterns for enhanced feature representation, along with Support Vector Machine classification. Furthermore, the framework is augmented with quantum-secure communication through the BB84 protocol to ensure secure transmission of biometric data. The manuscript also includes a more rigorous theoretical formulation, expanded experimental evaluation on a larger public dataset, and a more comprehensive analysis of the results, thereby significantly enhancing both the methodological depth and practical relevance of the work. The main contributions of this paper are summarized as follows:

- A comprehensive palmprint recognition framework based on multiscale signal analysis and kernel-based learning.
- The combination of Gabor filter-based spectral features and local binary pattern descriptors to enhance discriminative feature representation.
- A robust classification strategy using support vector machines formulated as a convex optimization problem.
- The integration of quantum key distribution to ensure information-theoretic security for biometric data transmission in remote authentication scenarios.
- An experimental evaluation demonstrating high recognition accuracy, stable generalization performance, and secure communication.

The remainder of this paper is organized as follows. Section 2 reviews related work on palmprint biometrics, multiscale feature extraction, and secure biometric authentication. Section 3 presents the proposed methodology, including preprocessing, feature extraction, classification, and quantum-secure communication. Section 4 describes the experimental setup and evaluation protocol. Section 5 reports and analyzes the experimental results. Section 6 discusses the security properties of the proposed framework. Finally, Section 7 concludes the paper and outlines directions for future research.

## 2 Related Work

Palmprint recognition has been extensively investigated as a reliable biometric modality due to the rich structural and textural information present in palmprint images. Early palmprint recognition systems primarily relied on line-based or appearance-based descriptors; however, recent research has increasingly focused on texture-driven feature extraction methods that can effectively capture multiscale and orientation-dependent information. These approaches are particularly relevant for contactless acquisition scenarios, where variations in illumination, scale, and pose introduce additional challenges.

Amrouni et al [13]. proposed a contactless palmprint recognition framework based on binarized statistical image features combined with multiresolution analysis using the discrete wavelet transform. Their method employs contrast-limited adaptive histogram equalization to enhance image quality, followed by feature extraction at multiple resolution levels and classification using a K-nearest neighbors classifier. The reported results demonstrate high recognition accuracy on benchmark palmprint databases, highlighting the effectiveness of multiresolution texture analysis for palmprint representation.

While the k-nearest neighbors (k-NN) classifier used in this approach yields strong recognition performance, it requires computing distances to all training samples during inference, leading to increased computational cost and memory usage. These limitations can hinder scalability and real-time deployment, particularly for large biometric databases.

Beyond recognition accuracy, recent studies have emphasized the importance of protecting biometric data against evolving security threats. Palma and Montessoro [14] introduced a privacy-preserving multimodal biometric framework that integrates feature-level fusion with

post-quantum cryptography. Their approach leverages homomorphic encryption to ensure that biometric features remain encrypted throughout the recognition process, providing resistance against both classical and quantum-enabled attacks. Although this work demonstrates the feasibility of combining biometrics with post-quantum cryptographic primitives, it focuses primarily on encrypted computation and multimodal fusion rather than on the signal-level characteristics of biometric features or the communication security mechanisms used during biometric transmission.

The emergence of quantum computing has further motivated the exploration of quantum-secure biometric authentication protocols. Qasim et al. [15] proposed a decentralized biometric authentication framework that incorporates quantum key distribution to establish secure communication channels between distributed biometric sensors and verification agents. Their protocol employs post-quantum cryptography to secure the classical channel of QKD while using quantum-based authentication to protect the quantum channel itself. Simulation results indicate that such layered security architectures can provide robust protection for decentralized biometric systems. However, the work concentrates on system-level authentication protocols and does not address biometric feature extraction or classification methodologies in detail.

Complementary to these efforts, Ramos et al. [16] demonstrated a practical implementation of secure multi-party biometric verification using quantum oblivious transfer assisted by quantum key distribution. Their work illustrates how quantum-secure primitives can support privacy-preserving biometric matching in sensitive applications such as fingerprint verification against watchlists. While this study highlights the feasibility of integrating quantum communication technologies with biometric verification, it focuses on fingerprint biometrics and multi-party computation rather than palmprint recognition or multiscale signal analysis.

In summary, existing research has made substantial progress in both palmprint feature extraction and the secure handling of biometric data. Multiresolution texture analysis methods have shown strong discriminative capability, while post-quantum cryptography and quantum key distribution have emerged as promising solutions for long-term biometric security. However, relatively few works have addressed the joint integration of mathematically interpretable multiscale feature extraction, kernel-based biometric classification, and quantum-secure communication within a unified palmprint recognition framework. This gap motivates the present work, which aims to bridge classical signal processing and statistical learning with information-theoretic security mechanisms for secure remote palmprint authentication.

### 3 Methodological Foundations

This section presents the theoretical and mathematical foundations of the principal methods employed in this study. The objective is to provide a formal and self-contained description of the underlying techniques, independent of their specific application context. These methods originate from different scientific domains, including image processing, signal analysis, statistical texture modeling, machine learning, and quantum communication theory. Their rigorous formulation provides the conceptual and mathematical basis required for understanding their role in biometric recognition and secure communication systems [17]. In particular, each method has been selected for its ability to extract discriminative information from high-dimensional palmprint images while ensuring computational tractability and stability under varying acquisition conditions.

#### 3.1 Contrast-Limited Adaptive Histogram Equalization

Contrast-Limited Adaptive Histogram Equalization (CLAHE) is an image enhancement technique designed to improve local contrast while preventing noise amplification [18]. Unlike global histogram equalization, which operates uniformly on the entire image and may over-amplify intensity variations in homogeneous regions, CLAHE divides the image into non-overlapping contextual regions (also called tiles) and applies histogram equalization independently within each region. Let  $f(x, y)$  denote a grayscale image defined over spatial coordinates  $(x, y)$ . The CLAHE transformation can be expressed as

$$\tilde{f}(x, y) = \mathcal{H}_{\text{CLAHE}}(f(x, y)), \quad (3.1)$$

where  $\mathcal{H}_{\text{CLAHE}}(\cdot)$  denotes the adaptive histogram equalization operator with contrast limitation. The contrast-limiting mechanism is implemented by clipping the histogram at a predefined threshold  $T_c$  and redistributing the excess counts uniformly across all intensity levels:

$$h_i^{\text{clipped}} = \min(h_i, T_c), \quad \Delta = \sum_{i=0}^{L-1} (h_i - h_i^{\text{clipped}}), \quad (3.2)$$

$$h_i^{\text{final}} = h_i^{\text{clipped}} + \frac{\Delta}{L}, \quad (3.3)$$

where  $h_i$  represents the histogram count for intensity level  $i$  and  $L$  is the total number of intensity levels. This procedure ensures that local contrast is enhanced without introducing excessive noise amplification, particularly in uniform or low-texture regions. By operating on local neighborhoods and combining the enhanced tiles with bilinear interpolation, CLAHE preserves structural and textural details, which is critical for downstream feature extraction in palmprint recognition.

### 3.2 Two-Dimensional Gabor Filters

Gabor filters are linear, orientation- and frequency-selective filters that provide optimal joint localization in both spatial and frequency domains [19]. They are widely employed for texture and pattern analysis due to their ability to decompose images into multiscale, orientation-selective components. A two-dimensional Gabor filter is defined as a sinusoidal plane wave modulated by a Gaussian envelope:

$$g_{\theta, \lambda}(x, y) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2}\right) \cos\left(2\pi \frac{x'}{\lambda} + \phi\right), \quad (3.4)$$

where the rotated coordinates are

$$x' = x \cos \theta + y \sin \theta, \quad y' = -x \sin \theta + y \cos \theta. \quad (3.5)$$

Here,  $\theta$  is the orientation of the filter,  $\lambda$  is the wavelength of the sinusoidal component,  $\sigma$  defines the spatial spread of the Gaussian envelope,  $\gamma$  is the aspect ratio controlling ellipticity, and  $\phi$  is the phase offset. Convolution of an input image  $f(x, y)$  with the filter yields the response:

$$R_{\theta, \lambda}(x, y) = f(x, y) * g_{\theta, \lambda}(x, y), \quad (3.6)$$

where  $*$  denotes convolution. By employing a bank of  $M$  orientations  $\{\theta_m\}_{m=1}^M$  and  $N$  scales  $\{\lambda_n\}_{n=1}^N$ , one obtains a rich, multiresolution representation of the input image that captures orientation-selective and frequency-selective texture components:

$$\mathcal{R}(x, y) = \{R_{\theta_m, \lambda_n}(x, y)\}_{m=1, \dots, M; n=1, \dots, N}. \quad (3.7)$$

These features have been widely reported to exhibit robustness to small spatial variations and to provide discriminative multiscale texture representations, which can improve class separability in biometric recognition tasks [25]. Parameter selection, including the number of orientations  $M$ , scales  $N$ , and the Gaussian envelope width  $\sigma$ , directly impacts the system's ability to discriminate subtle line patterns and wrinkles in palmprints.

### 3.3 Local Binary Patterns

Local Binary Patterns (LBP) are statistical descriptors that encode local spatial structures in images [20]. The LBP operator thresholds a set of  $P$  neighbors of a central pixel relative to its intensity:

$$\text{LBP}(x, y) = \sum_{p=0}^{P-1} s(I_p - I_c) 2^p, \quad (3.8)$$

with

$$s(z) = \begin{cases} 1, & z \geq 0, \\ 0, & z < 0. \end{cases} \quad (3.9)$$

Here,  $I_c$  is the intensity of the central pixel, and  $I_p$  is the intensity of the  $p$ -th neighbor. The resulting binary code compactly represents local micro-patterns such as edges, spots, and flat regions. LBP features are typically aggregated into histograms over local regions:

$$H_r(k) = \sum_{(x,y) \in r} \delta(\text{LBP}(x,y) - k), \quad (3.10)$$

where  $\delta(\cdot)$  is the Kronecker delta,  $r$  is a local region, and  $k$  indexes the possible LBP codes. The histogram  $H_r$  provides a robust statistical description of local textures, invariant to monotonic intensity changes, and resilient to illumination variations. Here,  $P$  denotes the number of neighboring pixels, and  $R$  represents the radius of the circular neighborhood centered at the pixel  $(x, y)$ . The neighboring pixels are sampled uniformly along a circle of radius  $R$ . When the sampled locations do not coincide with integer pixel coordinates, interpolation is used to estimate the corresponding intensity values.

### 3.4 Quantum Key Distribution and the BB84 Protocol

Quantum Key Distribution (QKD) enables two parties to establish a shared secret key with information-theoretic security guaranteed by the laws of quantum mechanics [21]. The BB84 protocol [22] encodes classical bits into qubits using two mutually unbiased bases, typically the rectilinear  $\{|0\rangle, |1\rangle\}$  and diagonal  $\{|+\rangle, |-\rangle\}$  bases:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (3.11)$$

The sender randomly selects a basis for each qubit and transmits it over a quantum channel. The receiver measures each incoming qubit using a randomly chosen basis. After transmission, basis reconciliation is performed via a classical channel, discarding incompatible measurements. Any eavesdropping introduces detectable errors due to quantum measurement collapse and the no-cloning theorem. The resulting raw key is further processed with error correction and privacy amplification to produce a secure symmetric key. Let  $K_A$  and  $K_B$  denote the final keys obtained by the sender and receiver, respectively. In ideal conditions:

$$K_A = K_B, \quad \text{with probability} \approx 1, \quad (3.12)$$

and the eavesdropper's mutual information  $I_E \approx 0$  after privacy amplification. This ensures that the key can be used for symmetric encryption of palmprint templates with information-theoretic security, independent of computational assumptions [23]. BB84's robustness relies on fundamental quantum principles, providing a unique advantage for securing biometric data against adversaries equipped with quantum computational capabilities.

## 4 Proposed Method

This section presents the proposed palmprint recognition framework, designed to extract discriminative multiscale texture features while maintaining mathematical transparency and structural interpretability. The overall processing pipeline is illustrated in Figure. 1. The framework combines adaptive preprocessing, multiscale orientation- and frequency-selective filtering, local texture encoding, and feature aggregation to construct a compact yet highly descriptive representation suitable for biometric classification. By integrating multiscale Gabor filtering with Local Binary Patterns (LBP), the system captures both global directional structures and local micro-patterns of palmprints, ensuring robustness to illumination, scale, and minor misalignments.

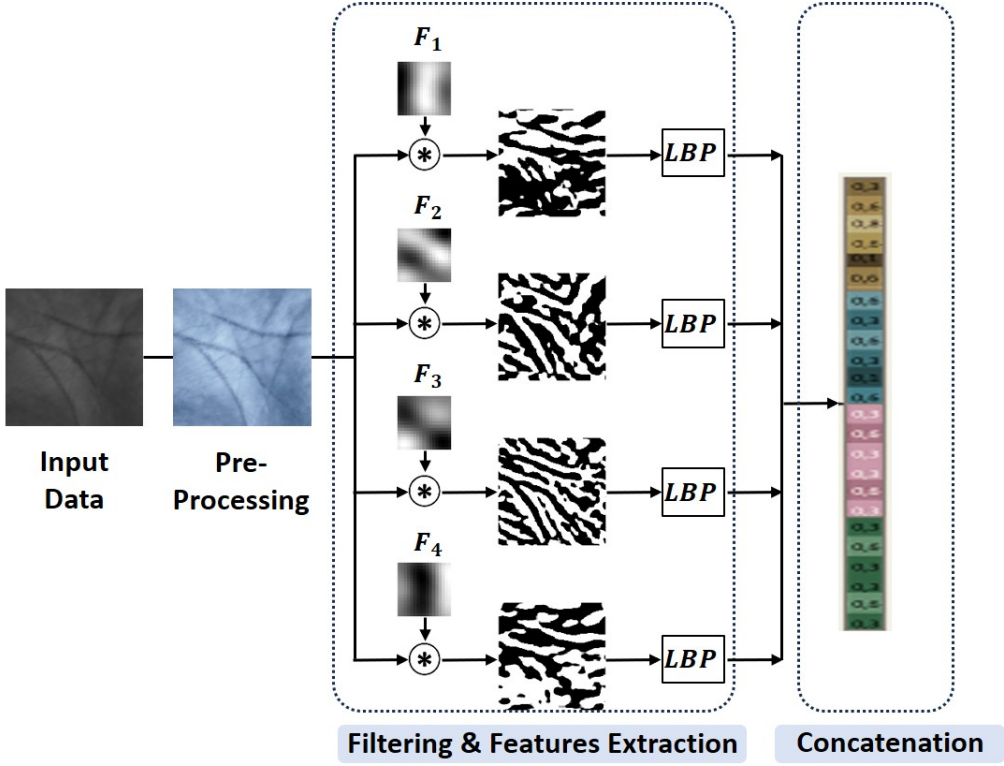


Figure 1: Block diagram of the proposed palmprint recognition framework.

#### 4.1 Preprocessing and Contrast Enhancement

Let  $f(x, y)$  denote an input grayscale palmprint image defined over a discrete spatial domain. Palmprint images captured under contactless conditions often suffer from non-uniform illumination, low contrast, and shadowing effects. To enhance local structural visibility, we employ Contrast-Limited Adaptive Histogram Equalization (CLAHE), producing an enhanced image  $\tilde{f}(x, y)$ :

$$\tilde{f}(x, y) = \mathcal{H}_{\text{CLAHE}}(f(x, y)), \quad (4.1)$$

where  $\mathcal{H}_{\text{CLAHE}}(\cdot)$  represents the adaptive contrast enhancement operator. CLAHE divides the image into contextual regions and enhances local contrast while controlling histogram clipping to prevent noise amplification. This preprocessing ensures that fine palmprint structures, including principal lines, wrinkles, and creases, are emphasized for subsequent multiscale analysis, while preserving global intensity distributions.

#### 4.2 Multiscale Gabor Filtering

To extract orientation- and frequency-specific information from the enhanced image  $\tilde{f}(x, y)$ , we apply a bank of two-dimensional Gabor filters. Each filter  $g_{\theta_l, \lambda_k}(x, y)$  is defined by its scale  $\lambda_k$  and orientation  $\theta_l$ , and the filtered response is obtained via convolution:

$$R_{k,l}(x, y) = \tilde{f}(x, y) * g_{\theta_l, \lambda_k}(x, y). \quad (4.2)$$

Here,  $*$  denotes the convolution operator. The set of filtered responses  $\{R_{k,l}(x, y)\}$  provides a multiresolution representation of the palmprint:

$$\mathcal{R}(x, y) = \{R_{k,l}(x, y) \mid k = 1, \dots, K; l = 1, \dots, L\}. \quad (4.3)$$

Each response emphasizes texture components aligned with a specific orientation and spatial frequency. The multiscale decomposition ensures that both fine textures and coarse structural

features are preserved, enabling robust discrimination between individuals. The number of orientations  $L$  and scales  $K$  are selected to balance computational efficiency and feature richness.

### 4.3 Local Binary Pattern Feature Encoding

To encode local texture structures within each Gabor-filtered image, the LBP operator is applied independently to each response  $R_{k,l}(x, y)$ . For a pixel at position  $(x, y)$ , the LBP code is computed as:

$$\text{LBP}_{k,l}(x, y) = \sum_{p=0}^{P-1} s(R_{k,l}^p - R_{k,l}^c) 2^p, \quad (4.4)$$

where  $R_{k,l}^c$  is the intensity of the central pixel,  $R_{k,l}^p$  represents the intensity of the  $p$ -th neighboring pixel, and  $s(\cdot)$  is the thresholding function:

$$s(z) = \begin{cases} 1, & z \geq 0, \\ 0, & z < 0. \end{cases} \quad (4.5)$$

LBP encodes the micro-patterns of each filtered image into a compact, binary representation that is invariant to monotonic intensity changes and resilient to local illumination variations. Applying LBP to each Gabor response allows the system to jointly capture directional features from Gabor filtering and local micro-pattern statistics from LBP, forming a hybrid descriptor that leverages the complementary strengths of both methods.

### 4.4 Feature Vector Construction and Concatenation

For each Gabor scale and orientation, the LBP codes are aggregated into region-wise histograms. Let  $\mathbf{f}_{k,l}$  denote the feature vector corresponding to the  $k$ -th scale and  $l$ -th orientation:

$$\mathbf{f}_{k,l} = \text{histogram}(\text{LBP}_{k,l}(x, y)), \quad (x, y) \in r, \quad (4.6)$$

where  $r$  indexes a local image region. The final palmprint representation is obtained by concatenating all histogram-based feature vectors across scales and orientations:

$$\mathbf{F} = [\mathbf{f}_{1,1}, \mathbf{f}_{1,2}, \dots, \mathbf{f}_{K,L}]. \quad (4.7)$$

This concatenated vector  $\mathbf{F}$  integrates multiscale spectral information and local spatial patterns, providing a rich, discriminative, and robust feature representation suitable for biometric classification. The resulting feature vector is then used as input to kernel-based classifiers or other downstream recognition modules.

## 5 Experimental Results

This section assesses the effectiveness and robustness of the proposed biometric recognition framework through a series of experimental evaluations. All experiments were conducted using the Tongji Contactless Palmprint Dataset [24], which is a publicly accessible benchmark dataset widely used in palmprint recognition research. The dataset comprises 12,000 contactless palmprint images acquired from 600 distinct palms belonging to 300 subjects.

The participant pool includes both male and female volunteers, with 192 males and 108 females. In terms of age distribution, 235 participants fall within the 20–30 year age range, while the remaining subjects are between 30 and 50 years old. Palmprint acquisition was carried out over two independent collection sessions to capture both left and right palm images, denoted as LPM and RPM, respectively. For each session, every participant contributed 10 images per palm, resulting in a total of 40 palmprint images per individual.

The temporal separation between the two acquisition sessions introduces realistic intra-class variability. The average interval between sessions is approximately 61 days, with the minimum and maximum intervals being 21 days and 106 days, respectively. This acquisition protocol

enables a comprehensive evaluation of the proposed system under natural variations in hand positioning, illumination conditions, and time-dependent changes.

In this study, a series of experiments is conducted and organized into two main phases. The first phase aims to assess the baseline performance of the biometric system without multiscale filtering, where feature extraction is performed using the Local Binary Pattern operator alone. In this phase, the impact of the LBP parameters, namely the number of neighboring pixels  $P \in \{8, 16, 24\}$  and the radius  $R \in [1, 3]$  pixels, is systematically evaluated in order to analyze their influence on recognition accuracy and system robustness.

For experimental evaluation, the dataset was partitioned into training and testing subsets. Approximately 60% of the images were used for training, while the remaining 40% were used for testing. A supervised learning approach was adopted, where the Support Vector Machine (SVM) classifier was trained on the training set and evaluated on unseen test samples.

The second phase focuses on assessing the contribution of multiscale filtering to the overall system performance. Specifically, a Gabor filter bank is introduced prior to LBP encoding, and experiments are conducted to evaluate the effect of the Gabor filter parameters, including the number of spatial scales  $\lambda \in \{8, 12, 16\}$  pixels and the set of orientations  $\theta \in \{0, \pi/3, \pi/2, 2\pi/3, \pi\}$ . This phase aims to quantify the performance gains achieved through multiscale, orientation-selective texture analysis compared to the baseline LBP-only configuration.

## 5.1 Baseline Biometric Performance

To further illustrate the baseline recognition capability of the proposed system, a comprehensive analysis of open-set identification results obtained under various LBP parameter configurations is presented in Tables 1 and 2. These experiments, conducted without any prior multiscale filtering, serve as a reference point to evaluate the incremental benefits of introducing Gabor-based feature decomposition. Using the best-performing configuration, corresponding to a neighborhood size of  $P = 24$  and a radius of  $R = 2$ , the system achieves a minimum equal error rate (EER) of 0.203% at a decision threshold of  $T_0 = 0.7243$  for the left palm, and an EER of 0.198% at  $T_0 = 0.7296$  for the right palm. These remarkably low error rates highlight the inherent discriminative power of LBP descriptors in capturing the subtle local variations and textural patterns of palmprints, even in the absence of multiscale orientation-sensitive analysis.

Table 1: Open-Set Biometric System Performance using Left Palm

| Radius | Neighboring Pixels |         |        |         |        |         |
|--------|--------------------|---------|--------|---------|--------|---------|
|        | 8                  |         | 16     |         | 24     |         |
|        | $T_0$              | EER (%) | $T_0$  | EER (%) | $T_0$  | EER (%) |
| 1      | 0.6244             | 0.534   | 0.6535 | 0.451   | 0.6712 | 0.331   |
| 2      | 0.6675             | 0.323   | 0.7046 | 0.212   | 0.7243 | 0.203   |
| 3      | 0.6467             | 0.384   | 0.6836 | 0.273   | 0.6973 | 0.238   |

The results indicate a clear trend: smaller neighborhoods, such as  $P = 8$  and  $P = 16$ , yield higher error rates, particularly when paired with a limited radius. This behavior reflects the sensitivity of LBP to the spatial support of local texture measurements, the descriptor requires a sufficient neighborhood to accurately capture local micro-patterns without introducing noise susceptibility. As the neighborhood size increases, the EER consistently decreases, and the optimal decision thresholds rise, demonstrating that larger neighborhoods provide a more robust representation of local palm structures while preserving sensitivity to discriminative texture variations.

A comparative analysis between left and right palms reveals a consistent pattern: the right palm generally produces slightly lower EER values across all configurations. This marginally better performance suggests that the right palm images captured under the acquisition conditions exhibit more stable texture patterns or reduced intra-class variability. Collectively, these baseline results establish a strong foundation for the proposed system and underscore the potential gains from incorporating multiscale and orientation-specific filtering to further enhance feature

Table 2: Open-Set Biometric System Performance using Right Palm

| Radius | Neighboring Pixels |         |        |         |        |         |
|--------|--------------------|---------|--------|---------|--------|---------|
|        | 8                  |         | 16     |         | 24     |         |
|        | $T_0$              | EER (%) | $T_0$  | EER (%) | $T_0$  | EER (%) |
| 1      | 0.6312             | 0.528   | 0.6591 | 0.446   | 0.6785 | 0.326   |
| 2      | 0.6729             | 0.318   | 0.7098 | 0.207   | 0.7296 | 0.198   |
| 3      | 0.6523             | 0.379   | 0.6892 | 0.268   | 0.7031 | 0.233   |

discriminability.

## 5.2 Biometric Performance with Multiscale Gabor Filtering

The integration of multiscale Gabor filtering prior to LBP encoding provides a critical enhancement in the system’s discriminative capabilities. By introducing orientation- and frequency-selective analysis, the system can extract complementary spectral information that is not captured by local binary descriptors alone. Open-set identification results, summarized in Table 3, demonstrate that increasing the number of scales from 8 to 16 consistently reduces the EER across all tested orientations. The lowest observed EER of 0.1048% is achieved for  $\theta = \pi$  with 16 scales, corresponding to a decision threshold  $T_0 = 0.7041$ . This substantial reduction in EER, roughly 50% lower than the baseline LBP-only configuration, illustrates the significant contribution of multiscale filtering in enhancing genuine-impostor separability by capturing previously unexploited frequency components and line orientations.

In addition, performance trends across orientations reveal that higher orientation angles correlate with lower EERs, suggesting that directional components aligned with the primary palm lines are more effectively emphasized at  $\theta \geq \pi/2$ . This observation underscores the importance of orientation diversity in texture analysis and validates the design choice of a multi-orientation Gabor bank for robust palmprint representation.

Table 3: Open-Set Biometric System Performance using Right Palm with Multiscale Gabor Filtering

| Orientation | Number of Scales |         |        |         |        |         |
|-------------|------------------|---------|--------|---------|--------|---------|
|             | 8                |         | 12     |         | 16     |         |
|             | $T_0$            | EER (%) | $T_0$  | EER (%) | $T_0$  | EER (%) |
| 0           | 0.6284           | 0.1621  | 0.6517 | 0.1435  | 0.6729 | 0.1284  |
| $\pi/3$     | 0.6349           | 0.1543  | 0.6598 | 0.1362  | 0.6814 | 0.1217  |
| $\pi/2$     | 0.6418           | 0.1476  | 0.6673 | 0.1294  | 0.6896 | 0.1152  |
| $2\pi/3$    | 0.6482           | 0.1418  | 0.6749 | 0.1231  | 0.6968 | 0.1096  |
| $\pi$       | 0.6546           | 0.1365  | 0.6824 | 0.1179  | 0.7041 | 0.1048  |

Closed-set performance, reported in Table 4, corroborates the open-set trends. The rank-one recognition rate (ROR) steadily increases with the number of scales, attaining a maximum of 99.74% at  $\theta = \pi$  with 16 scales, alongside a minimal rank penetration (RPR) of 16. This demonstrates not only high recognition accuracy but also efficient top-rank retrieval, which is critical in practical biometric verification systems where rapid identification is required. Across all tested orientations and scales, the ROR consistently exceeds 98%, indicating the reliability of the proposed multiscale Gabor + LBP framework for both identification and authentication tasks.

Figure 2 further illustrates the system’s behavior. The open-set DET curve in Figure. 2a confirms the minimal overlap between genuine and impostor score distributions, with an EER of just 0.1048%. The closed-set CMC curve in Figure. 2b emphasizes rapid top-rank convergence, highlighting the system’s suitability for both verification and identification scenarios. Collectively, these results validate the synergistic effect of Gabor filtering and LBP encoding, demonstrat-

Table 4: Closed-Set Biometric System Performance using Right Palm with Multiscale Gabor Filtering

| Orientation | Number of Scales |     |         |     |         |     |
|-------------|------------------|-----|---------|-----|---------|-----|
|             | 8                |     | 12      |     | 16      |     |
|             | ROR (%)          | RPR | ROR (%) | RPR | ROR (%) | RPR |
| 0           | 98.12            | 28  | 98.74   | 24  | 99.21   | 20  |
| $\pi/3$     | 98.36            | 27  | 98.91   | 23  | 99.34   | 19  |
| $\pi/2$     | 98.59            | 26  | 99.08   | 22  | 99.48   | 18  |
| $2\pi/3$    | 98.81            | 25  | 99.22   | 21  | 99.61   | 17  |
| $\pi$       | 99.03            | 24  | 99.36   | 20  | 99.74   | 16  |

ing that multiscale, orientation-aware preprocessing substantially strengthens the discriminative capacity of the extracted features.

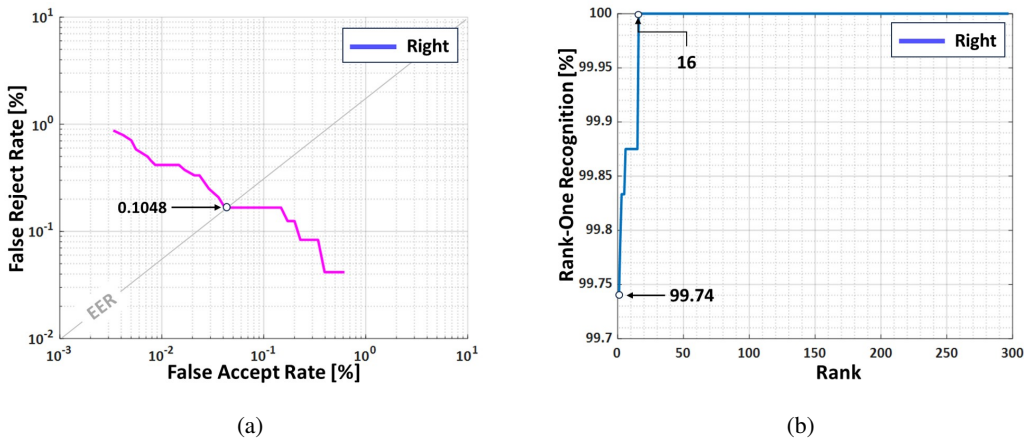


Figure 2: Biometric system performance using Gabor filter. (a) Open-set DET curve, (b) Closed set CMC Curve.

### 5.3 Evaluation of BB84 Encryption for Secure Template Transmission

Ensuring the confidentiality and integrity of palmprint templates in remote authentication scenarios is paramount. To this end, the BB84 quantum key distribution protocol was implemented to generate symmetric keys for secure template encryption. Key aspects of the protocol were thoroughly evaluated, including key generation correctness, quantum bit error rate (QBER), and privacy amplification with error correction. The results demonstrate that the system can integrate quantum-secure communications without compromising biometric performance.

Figure 3 shows that key generation achieves near-perfect correctness, with Alice and Bob consistently obtaining identical keys across multiple trials. This confirms that the quantum channel and associated error correction mechanisms operate reliably, establishing a solid foundation for secure template encryption.

QBER, presented in Figure. 4, remains below the theoretical BB84 security threshold of 11%, indicating that channel noise and potential eavesdropping are effectively mitigated. The consistently low QBER reflects the robustness of the system under realistic communication conditions and guarantees reliable key agreement.

Finally, privacy amplification combined with error correction, shown in Figure. 5, reduces any residual information potentially accessible to an adversary to near zero. This ensures information-theoretic security for encrypted palmprint templates, demonstrating that even a quantum-capable eavesdropper cannot gain meaningful knowledge from the transmitted data.

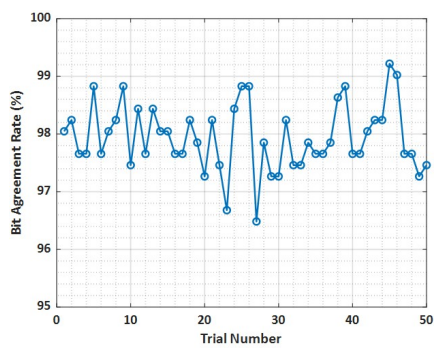


Figure 3: Key generation correctness for BB84 QKD demonstrating near-perfect agreement between sender and receiver.

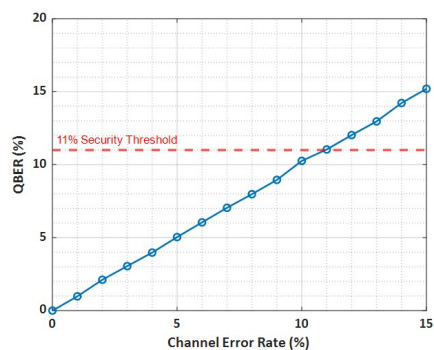


Figure 4: Quantum Bit Error Rate (QBER) for the BB84 protocol, remaining below the secure threshold of 11%.

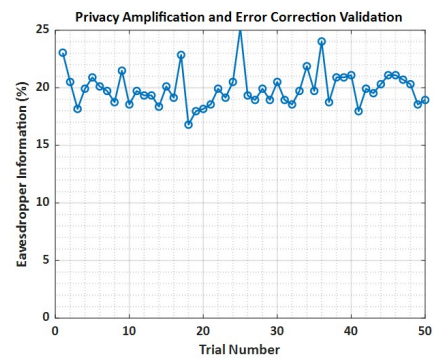


Figure 5: Privacy amplification and error correction results showing negligible information leakage to a potential eavesdropper.

Overall, the BB84 evaluation confirms that the proposed system achieves a robust combination of biometric accuracy and quantum-secure template transmission. The integration of near-perfect key generation, low QBER, and strong privacy amplification ensures that remote palmprint authentication can be conducted securely against both classical and quantum-capable adversaries, without degrading the high recognition performance achieved through multiscale Gabor and LBP feature extraction.

#### 5.4 Comparative Analysis with Existing Methods

To contextualize the proposed palmprint recognition framework, a comparative analysis is presented with selected state-of-the-art methods in the literature. Table 5 summarizes key aspects, including feature extraction strategy, classifier type, security mechanisms, and reported performance metrics. The table highlights both methodological differences and the unique contributions of the proposed system in combining multiscale signal analysis with quantum-secure communication.

Table 5: Comparison of the Proposed System with Recent Palmprint Recognition Methods

| Reference            | Feature Extraction   | Classifier / Matching  | Security               | Notes / Performance    |
|----------------------|----------------------|------------------------|------------------------|------------------------|
| [13]                 | BSIF + DWT           | K-NN                   | None                   | High accuracy          |
| [14]                 | Multimodal fusion    | Feature-level matching | Homomorphic encryption | Privacy-preserving     |
| [15]                 | Not specified        | Not specified          | BB84 QKD + PQC         | Secure authentication  |
| [16]                 | Fingerprint features | Multi-party matching   | QKD-assisted OT        | Privacy-preserving     |
| <b>Proposed Work</b> | Gabor + LBP          | SVM (RBF)              | BB84 QKD               | Interpretable features |

The comparative analysis demonstrates several key points. First, while Amrouni et al. [13] achieve high recognition accuracy using multiresolution texture features, their framework lacks any mechanism for secure template transmission, which is critical for remote biometric authentication. Second, approaches such as Palma and Montessoro [14] provide strong privacy guarantees via post-quantum cryptography, but focus primarily on multimodal encrypted computation rather than exploiting the discriminative structure of palmprint features. Similarly, Qasim et al. [15] and Ramos et al. [16] illustrate the feasibility of quantum-secure protocols, but do not address multiscale feature extraction or kernel-based classification for palmprint images.

In contrast, the proposed system unifies mathematically interpretable multiscale feature extraction, robust classification using SVM, and quantum-secure key distribution for template protection. This combination ensures both high recognition performance and information-theoretic security, addressing limitations in previous works. The integration of Gabor-based spectral features with LBP encoding allows the system to capture complementary texture information, while BB84 QKD guarantees secure remote transmission, making the framework particularly suitable for distributed and high-security environments.

## 6 Conclusion and Future Work

This work presented a comprehensive framework for palmprint-based biometric recognition that integrates multiscale signal analysis with quantum-secure communication. The proposed system combines mathematically interpretable feature extraction using Gabor filters and Local Binary Patterns with kernel-based classification via Support Vector Machines, providing robust and discriminative representations of palmprint textures. In parallel, the transmission of biometric templates and decision data is protected using the BB84 quantum key distribution protocol, ensuring information-theoretic security against both classical and quantum-capable adversaries.

Extensive experimental evaluations on the Tongji Contactless Palmprint Dataset demonstrated the effectiveness of the proposed approach. Baseline experiments confirmed the discriminative power of LBP descriptors, while the introduction of multiscale Gabor filtering significantly enhanced open-set and closed-set performance, achieving a minimum equal error rate of 0.1048% and a maximum rank-one recognition rate of 99.74%. BB84 evaluation further validated the reliability and security of the system, with near-perfect key generation, a QBER below the 11% security threshold, and negligible information leakage following privacy amplification and error correction.

By bridging classical signal processing, statistical learning theory, and quantum-secure communication, this work provides a unified framework that addresses both recognition accuracy and long-term template security. The results highlight the potential of combining orientation- and scale-selective multiscale features with information-theoretically secure channels for remote biometric authentication. Future research directions include the extension of this framework to multimodal biometrics, real-time deployment in distributed systems, and the exploration of additional quantum-resistant cryptographic primitives to further enhance security and operational efficiency.

## References

- [1] Zeng, L., Shen, P., Zhu, X., Tian, X., & Chen, C. (2025). A review of privacy-preserving biometric identification and authentication protocols. *Computers & Security*, 104309–104309. <https://doi.org/10.1016/j.cose.2024.104309>
- [2] Gomez-Barrero, M., Galbally, J., Rathgeb, C., & Busch, C. (2018). General Framework to Evaluate Unlinkability in Biometric Template Protection Systems. *IEEE Transactions on Information Forensics and Security*, 13(6), 1406–1420. <https://doi.org/10.1109/tifs.2017.2788000>
- [3] Amrouni, N., Benzaoui, A., & Zeroual, A. (2024). Palmprint Recognition: Extensive Exploration of Databases, Methodologies, Comparative Assessment, and Future Directions. *Applied Sciences*, 14(1), 153. <https://doi.org/10.3390/app14010153>
- [4] Ortiz, N., Hernandez, R. D., Jimenez, R., Mauledeux, M., & Aviles, O. (2018). Survey of biometric pattern recognition via machine learning techniques. *Contemporary Engineering Sciences*, 11(34), 1677–1694. <https://doi.org/10.12988/ces.2018.84166>
- [5] Thakur, G., Chouksey, P., Chopra, M., Sadotra, P., & Kumar, S. (2025). A comprehensive review on the hybrid BB84 E91 QKD protocol for enhanced security efficiency and practical hardware implementation in quantum cryptography. *Discover Computing*, 28(1). <https://doi.org/10.1007/s10791-025-09807-8>
- [6] Djeddi, S., Belhocine, Y., Mebarkia, M., Meraoumia, A., & Bendjenna, H. (2025). Enhanced Finger-Knuckle-Print Recognition Using Deep Texture Feature Analysis. 2025 2nd International Conference on Recent Advances in Mathematics and Informatics (ICRAMI), 1–6. <https://doi.org/10.1109/ICRAMI64946.2025.11472772>
- [7] Astrakhantsev, A., & Liashenko, G. (2022). Data protection management process during remote biometric authentication. *System Research and Information Technologies*, 3, 71–85. <https://doi.org/10.20535/srit.2308-8893.2022.3.05>
- [8] Raghavendra, R., & Busch, C. (2014). Novel image fusion scheme based on dependency measure for robust multispectral palmprint recognition. *Pattern Recognition*, 47(6), 2205–2221. <https://doi.org/10.1016/j.patcog.2013.12.011>
- [9] Marcialis, G. L., Liu, X., & Didaci, L. (2022). Biometric presentation attacks: Handcrafted features versus deep learning approaches. *Pattern Recognition Letters*, 163, 55–56. <https://doi.org/10.1016/j.patrec.2022.09.013>
- [10] Kaushik Dehingia, & Dutta, N. (2025). Hybrid Quantum Key Distribution Framework: Integrating BB84, B92, E91, and GHZ Protocols for Enhanced Cryptographic Security. *Concurrency and Computation Practice and Experience*, 37(21-22). <https://doi.org/10.1002/cpe.70221>
- [11] Dhakal, P., Dawadi, B. R., & Adhikari, N. B. (2025). Performance Analysis of Different Quantum Key Distribution Protocols for Optimised Security and Efficiency. *IET Quantum Communication*, 6(1). <https://doi.org/10.1049/qtc.2.70015>
- [12] Gyongyosi, L. (2020). Order statistics and random matrix theory of multicarrier continuous-variable quantum key distribution. *International Journal of Communication Systems*, e4314. <https://doi.org/10.1002/dac.4314>
- [13] Amrouni, N., Benzaoui, A., Bouaouina, R., Khaldi, Y., Adjabi, I., & Bouglimina, O. (2022). Contactless Palmprint Recognition Using Binarized Statistical Image Features-Based Multiresolution Analysis. *Sensors*, 22(24), 9814. <https://doi.org/10.3390/s22249814>

- [14] Palma, D., & Montessoro, P. L. (2025). A Post-Quantum Cryptography Enabled Feature-Level Fusion Framework for Privacy-Preserving Multimodal Biometric Recognition. *Cryptography*, 9(4), 72. <https://doi.org/10.3390/cryptography9040072>
- [15] Qasim, T., Siris, V. A., Oosthuizen, I., Rajarajan, M., & Biswas, S. (2026). Quantum Secure Biometric Authentication in Decentralised Systems. *arXiv preprint arXiv:2601.04852*. <https://doi.org/10.48550/arXiv.2601.04852>
- [16] Ramos, M. F., Hentschel, M., Valbusa, F., Luchian, C., Achleitner, M., Trenti, A., ... & Hübel, H. (2025). Secure Multi-Party Biometric Verification using QKD assisted Quantum Oblivious Transfer. *arXiv preprint arXiv:2501.05327*. <https://doi.org/10.48550/arXiv.2501.05327>
- [17] Belhocine, Y., Meraoumia, A., Bendjenna, H., & Saiga, M. (2025). Empowering Biometric Security: A Paradigm Shift in Remote Identification. *Systems and Computing*, 1(1). <https://doi.org/10.64409/sycom.v1.i1.4>
- [18] Ayyavoo, T., & John Suseela, J. (2018). Illumination pre-processing method for face recognition using 2D DWT and CLAHE. *IET Biometrics*, 7(4), 380–390. <https://doi.org/10.1049/iet-bmt.2016.0092>
- [19] Boughida, A., Kouahla, M. N., & Lafifi, Y. (2021). A novel approach for facial expression recognition based on Gabor filters and genetic algorithm. *Evolving Systems*. <https://doi.org/10.1007/s12530-021-09393-2>
- [20] Scherhag, U., Kunze, J., Rathgeb, C., & Busch, C. (2020). Face morph detection for unknown morphing algorithms and image sources: a multi-scale block local binary pattern fusion approach. *IET Biometrics*, 9(6), 278–289. <https://doi.org/10.1049/iet-bmt.2019.0206>
- [21] Pereira, M., Curty, M., & Tamaki, K. (2019). Quantum key distribution with flawed and leaky sources. *Npj Quantum Information*, 5(1). <https://doi.org/10.1038/s41534-019-0180-9>
- [22] Maharjan, D. R., & Shrestha, S. (2023). Quantum Key Distribution Based on BB84 Protocol. *Journal of Semiconductor Devices and Circuits*. <https://doi.org/10.37591/josdc.v10i3.7897>
- [23] Kumar, J., & Saxena, V. (2022). Cloud Data Security through BB84 Protocol and Genetic Algorithm. *Baghdad Science Journal*, 19(6(Suppl.)), 1445–1445. <https://doi.org/10.21123/bsj.2022.7281>
- [24] Zhang, L., Li, L., Yang, A., Shen, Y., & Yang, M. (2017). Towards contactless palmprint recognition: A novel device, a new benchmark, and a collaborative representation based identification approach. *Pattern Recognition*, 69, 199–212. <https://doi.org/10.1016/j.patcog.2017.04.016>
- [25] Mohammadian Fini, R., Mahlouji, M., & Shahidinejad, A. (2022). Performance improvement in face recognition system using optimized Gabor filters. *Multimedia Tools and Applications*, 81(27), 38375–38408. <https://doi.org/10.1007/s11042-022-13167-6>

## Author information

Saoussen Djeddi, Laboratory of Mathematics, Informatics and Systems (LAMIS), Echahid Cheikh Larbi Tebessi University, Tebessa, ALGERIA.

E-mail: [saoussen.djeddi@univ-tebessa.dz](mailto:saoussen.djeddi@univ-tebessa.dz)

Yacine Belhocine, Laboratory of Mathematics, Informatics and Systems (LAMIS), Echahid Cheikh Larbi Tebessi University, Tebessa, ALGERIA.

E-mail: [yacine.belhocine@univ-tebessa.dz](mailto:yacine.belhocine@univ-tebessa.dz)

Abdallah Meraoumia, Laboratory of Signals and Smart Systems (L3S), Echahid Cheikh Larbi Tebessi University, Tebessa, ALGERIA.

E-mail: [ameraoumia@univ-tebessa.dz](mailto:ameraoumia@univ-tebessa.dz)