Journal of Information Systems Engineering and Management
2025, 10(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

An Efficient Automatic Fingerprint Authentication System Using a Template Protection Technique

Dr.D.Deepakraj[1], Dr.T.Padmapriya[2], Dr.S.V.Manikanthan[3], G.Kannan[4], Dr.S.Selvakumar[5]

[1]*Assistant Professor/ Programmer, Department of Computer and Information Science, Annamalai University, Tamilnadu. deepakraj0708@gmail.com*

[2]*Melange Publications, Puducherry, India. padmapriyaa85@ptuniv.edu.in*

[3]*Melange Academic Research Associates, Puducherry, India. prof.manikanthan@gmail.com*

[4]*Assistant Professor/CSE, Sriram Engineering College, Tamilnadu. gopkan1972@gmail.com*

[5]*Professor, Department of Computer Science and Business Systems, Panimalar Engineering College (Autonomous), Chennai – 600 123, Tamilnadu. selvathendral1981@gmail.com*

ARTICLE INFO

Received: 02 Oct 2024
Revised: 30 Nov 2024
Accepted: 10 Dec 2024

ABSTRACT

The disclosure of biometric template data is one of the possible weaknesses in a biometric system, posing major security and privacy risks. The majority of template protection methods on the market fall short of meeting all the necessary specifications for a workable biometric system, including high matching accuracy, security, privacy, and revocability. Research on automated fingerprint-based identification began in the early 1960s since fingerprints have been a vital tool for forensics and law enforcement for more than a century. Our proposal includes a system that uses extraction of minutiae approach to verify fingerprints and an automated system that takes attendance. Unimodal fingerprint biometric systems, which analyze distinctive sequences to protect authentication information, deal with issues including noisy data, non-universality, intra-class deviation, and susceptibility to spoof attacks. Multimodal fingerprint biometric systems overcome these issues by compensating for the shortcomings of different biometric sources. Our test findings demonstrate that, while maintaining template security, the suggested multi-biometric template protection strategy outperforms its unibiometric equivalents regarding verification outcomes.

Keywords: Matching Algorithms; Template Protection Schemes; Automatic Identification; Minutiae Extraction; Segmentation.

INTRODUCTION

A person can be validated or authenticated with a high degree of assurance using biometric attributes or biometric modalities, such as fingerprint, iris biometrics, face (2D, 3D), the retina, handprint biometrics, the moment veins, ear, knuckles, DNA, voice, signature, gait biometrics, typing pattern, etc. Hackers can reveal, steal, and reuse PINs, passwords, tokens, and other information used on traditional authentication systems. However, biometric-based authentication is gradually overtaking traditional authentication methods in usage [1]. Biometrics offers all the security advantages offered by traditional authentication or verification systems while measuring each person's distinct physical and behavioral characteristics. Based on a person's physical and behavioral characteristics, the biometric-based verification system can reliably identify them. A person can also be recognized by his or her actions, such as the way he walks or moves his hands, the way he types letters from the keyboard, or the way he punches the keys.

Five different components make up a unique biometric identification structure: a sensor module, a feature extraction module, a template library module, a matcher module, and a decision-making module. A traditional biometric authentication system is shown in Figure 1. The sensor creates a barrier between the user and the biometric authentication system. A specialized module then processes the scanned biometric data to extract features. This particular module, which extracts the key characteristics from the scanned data, is known as a biometric template and aids in user differentiation. This feature extraction process is occasionally used in conjunction with the quality evaluation module to improve the quality of collected biometric data.

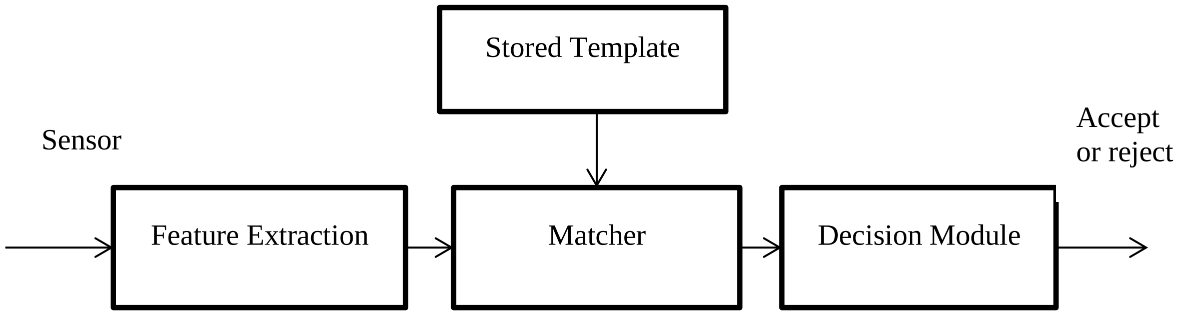

Figure 1: A distinct biometric authentication system component

The distinctive pattern displayed by the positions of a fingerprint's minute points, flaws, ridge termination, and bifurcations is what gives each fingerprint its individuality. A brand-new minutiae-based method [3] has been put forth to use comparable structures to compare fingerprint photos. Finding the ideal match becomes extremely challenging due to distortion, which promotes false minutiae and poses major risks through changed geometry. Depending on the level of distortion, this technique separates fingerprint images into two concentric circular regions: the inner and outer. Based on the region in which the pair resides, the algorithm determines weight ages for a minutiae–pair match. There are two steps in the algorithm. The first step involves extracting the minutiae points, while the second step involves aligning and matching the fingerprint images.

The algorithm's goal is to shorten the alignment time as soon as the digital picture is calculated. Fingerprints are being used more often in government and private applications like border control, employment background checks, and secure facility access as a result of recent developments in automated fingerprint identification technology and the rising demand for accurate person identification. The skin on the fingertip starts to differentiate, revealing the fingerprint's general characteristics. The benefits of fingerprint recognition systems are affordability and ease of use. Fingerprints are the most often used biometric modality because they have one of the highest levels of performance and distinctiveness among the other biometric identifiers, including voice, signature, and face. These features make it possible to combine template protection schemes that need a fixed-length feature vector with fingerprint recognition systems. The location-based spectral minutiae representation and the orientation-based spectral minutiae representation are the two representation techniques for which this method presents the idea of algorithms. Two correlation-based spectral minutiae matching methods are used to assess both approaches. Singular points and a fusion strategy can be used to boost performance.

This article is structured as follows. The related works of this system are discussed in Section 2. The use of the suggested methodology is explained in Section 3. Experimental results and discussions are presented in Section 4. The system's conclusion and future scope are presented in Section 5.

RELATED WORKS

Every person on the planet has a permanently distinct fingerprint. The ridges and furrows that make up a fingerprint exhibit good commonalities, such as average width and parallelism [4]. Nonetheless, studies on fingerprint recognition and verification demonstrate that minutiae—a few aberrant spots on the ridges—can be used to differentiate fingerprints. There are two types of minutiae termination: bifurcation, which is the point on the hillside from which further branches drive, and instantaneous termination, which is the place where ridges stop suddenly or end immediately. An optical, solid state, or ultrasonic sensor—likely the user interface—records a fingerprint. For fingerprint verification systems, two methods are typically employed. The first is a minutiae-based methodology, where minutiae are expressed by bifurcations and endings or terminations.

Since our goal is to leak privacy analysis, it makes sense that we concentrate on internal adversaries because they are more formidable than outside attackers when it comes to compromising a system's privacy features. Additionally, our design divides the internal parts of a biometric system into four physical entities: the database, the matcher, the authentication server, and the sensor [5]. This is a crucial component since a system cannot guarantee the maximum privacy qualities against internal adversaries like malevolent controllers if these entities are not separated. The divide into four entities, however, cannot be seen as the only guarantee. For this reason, we examine situations in which multiple entities conspire or are malevolent, emphasizing that in these circumstances, certain entities are more powerful than others.

Optical matching verification systems frequently use representations based on the full grayscale profile of a fingerprint image. However, because these systems are basically using template-matching strategies for verification [6], their usefulness may be limited by things like brightness variations, image-quality variations, scars, and large global distortions present in the fingerprint image. Furthermore, representations that use the full grayscale profile fingerprint photos are not desired in many verification applications, which choose terser representations. By limiting the representation to a little (yet reliable) portion of the finger, some system designers try to get around this issue. However, because there are only a finite number of recognizable templates, the resulting systems may run the danger of limiting the variety of unique identities that can be handled if this same formulation is also utilized for identification purposes.

Attacks and eavesdropping are possible with embedded devices. Therefore, it is necessary to look at alternate protection strategies. The fuzzy commitment strategy is a brand-new cryptographic method that has recently been put out for fingerprint authentication [7]. The plan creates a new kind of cryptographic system by combining popular error-control coding strategies with cryptographic approaches. The commitment can be decrypted using an acceptable close witness in lieu of a precise, one-of-a-kind decryption key.

First off, many low-security applications, such computers, home security systems, restricted entrance control, corporate networks, etc., cannot afford the sensor cost of eye-based features. Furthermore, for privacy reasons, the majority of users are reluctant to provide their fingerprint data to a business or system because fingerprint features are employed specifically in criminal investigations and business transactions [8]. "The requirements of the particular app, the features of the applications, and the properties of the biometrics determine whether a biometric and an application are a good fit." In this work, we suggest a technique that uses palm prints to identify users of entry control systems.

METHODS AND MATERIALS

3.1 Biometric System Types

There are two varieties of biometric systems:

❖ **UBI (UNIODAL BIOMETRIC SYSTEM)**

A single biometric characteristic is used by a unimodal biometric authentication system to identify and authenticate users. This system records and examines information from a certain biological or behavioral trait that is particular to each person. Unimodal systems have constraints that could jeopardize their dependability, safety, capacity, efficacy, precision, and privacy, even though they provide a high level of security for identity detection. The details are as follows:

- A person should be able to be reliably identified by any traditional biometric technique. The accuracy of biometric systems that rely on a single trait is influenced by a number of factors: Uncertainty in the collected data: The process of gathering biometric data may be impacted by a number of variables, such as physical injury and environmental conditions. Contamination on the fingerprint scanner's surface may reduce the precision of the fingerprint features. The whole precision of the system decreases due to inadequate biometric input.

- Non-universality: A higher failure to enroll rate (FER) may arise from a portion of the population's inability or unwillingness to provide the necessary biometric feature accurately. Put on gloves if someone has cuts or wounds, or if their fingerprints are smudged by debris or oil. They cannot be identified by fingerprint sensors, which could limit and interfere with a biometric system's functionality. Thus, fingerprints in attendance systems are not preferred by those employed in the mining, construction, and manufacturing sectors. The ability of a group or individual to sign up for an authentication system may be limited by cultural or religious factors in addition to technical, physical, and physiological difficulties.

- Differences in samples taken from people during the enrollment and recognition phases are referred to as intra-class variations. These variations may result from scarring or bruising of the fingerprint, or from reader malfunctions (such as translation, pressure changes, or rotation on the fingerprint sensor). The result is a rise in the FAR.

- Scalability: Longer identification times were caused by the increasing computing difficulty of matching queries against the growing database as the number of enrolled users grew. The query must correspond with the database's N enrolled user templates. A larger frequency of false matches or mismatches could result from this database increase; these could be caused by variations in image quality or fingerprint resemblances.

❖ MULTIMODAL BIOMETRIC SYSTEM (MBS)

In practical applications, multimodal biometric systems are becoming more and more common. To improve accuracy and security, a multimodal biometric system makes use of several biometric characteristics. Even though multimodal biometric systems use numerous modalities to improve accuracy and reliability, scalability issues may still affect them. Scalability issues can arise from managing data from several modalities, guaranteeing component interoperability, and maintaining performance under growing strain. For large-scale deployment scenarios to function well, scalability must be addressed. However, multimodal systems may also display comparable traits, suggesting that scalability problems are not limited to unimodal systems. Some advantages of multibiometric systems over unimodal biometric systems are listed below.

- By drastically lowering the impact of noise and poor quality in the collected biometric features, recognition systems' precision and accuracy are increased. A multibiometric system becomes more resilient and effective when it incorporates several biometric sources. This method recognizes the possible restrictions or unpredictabilities connected to unique biometric characteristics. Another trait, like a fingerprint, can be used as a backup if one, like a user's speech attribute, is difficult to identify due to things like background noise or medical issues.

- Adequate population coverage is made possible by the resolution of enrollment phase issues such non-universality with the use of multibiometric systems. Therefore, a user can still enroll and be identified by supplying a different biometric trait even if they are unable to furnish one. For example, a manual laborer can still be hired and identified by their face, voice, iris, and other characteristics even if their fingerprints are not very good. As a result, FER falls as population coverage rises.

- A multibiometric system can considerably lessen the overlap between the picture features of several individuals (inter-class similarities) by fusing biometric attributes and employing a fusion technique. Gathering information from multiple sources will make the feature vector more dimensional, but the biometric system's overall accuracy will rise. For example, two family members may have the same voice, but their fingerprints and iris characteristics are different.

3.2 The biometric authentication system for fingerprints

A biometric identification system, which is a classification and recognition tool, is used to record an individual's fingerprint trait. It accomplishes this by contrasting a template of fingerprint data kept in the system's database with a number of distinct aspects from the trait evidence. When deciding whether or not to proceed, the comparison's outcomes are taken into account. The four fundamental modules that make up a conventional fingerprint biometric system's general design are shown in Figure 2, along with the sequence in which they occur.

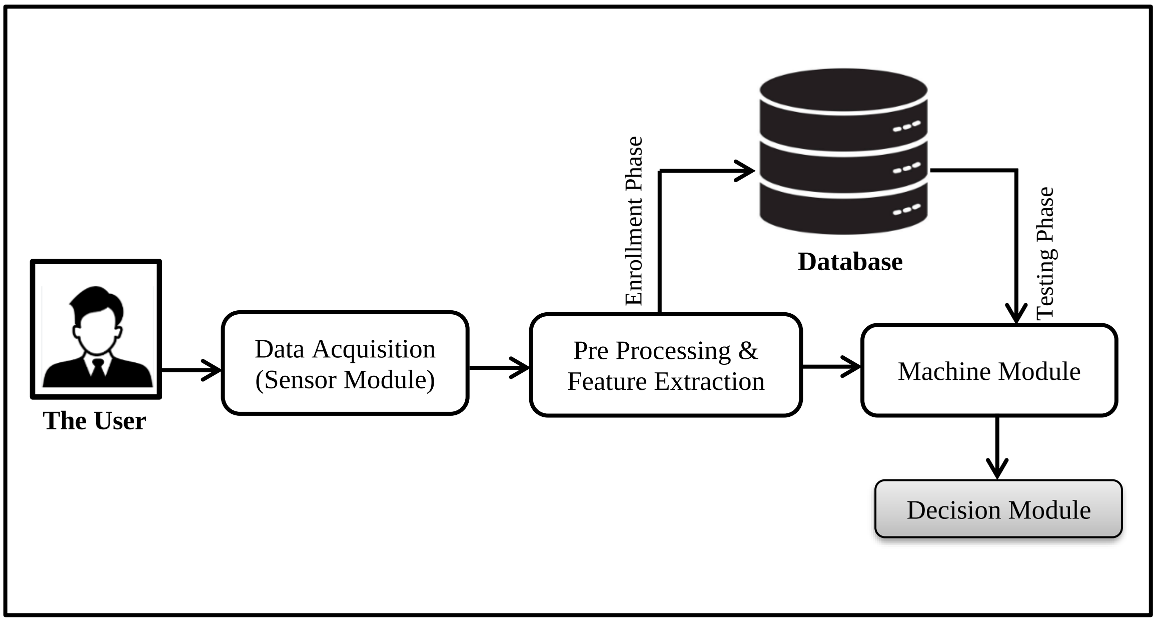

Figure 2: An Identification System Using Fingerprint Biometrics

Depending on the application scenario, a fingerprint biometric system can be used for identification, verification, and enrollment. "Recognition" refers to the latter two features.

- Enrolment: A fingerprint is taken from a person using a sensor, which then digitizes and stores the information in a database using templates. Figure 3 illustrates this procedure, also known as enrollment or training, and includes biographical data (such as their residence, PIN, and profile) to aid in their identification. To guarantee its protection, the design is encrypted.

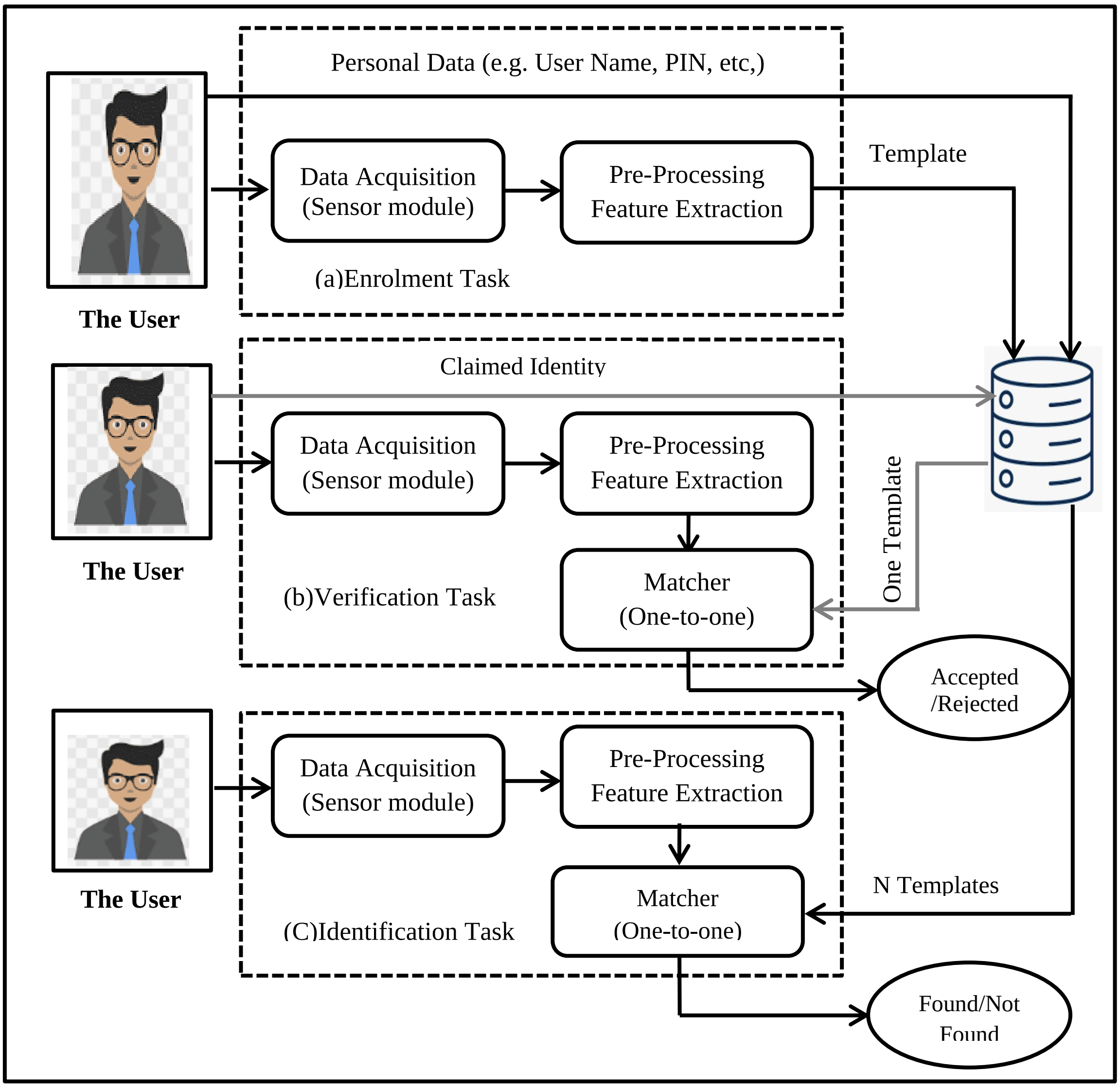
Personal Data (e.g. User Name, PIN, etc,)
Data Acquisition (Sensor module)
Pre-Processing Feature Extraction
Template
(a)Enrolment Task
The User
Claimed Identity
Data Acquisition (Sensor module)
Pre-Processing Feature Extraction
One Template
Matcher (One-to-one)
(b)Verification Task
The User
Accepted /Rejected
Data Acquisition (Sensor module)
Pre-Processing Feature Extraction
Matcher (One-to-one)
N Templates
(C)Identification Task
The User
Found/Not Found

Figure 3: Features of a Biometric Fingerprint System

• Confirmation: Creating a unique template based on a person's fingerprint characteristics is the process of fingerprint verification via pattern matching. A user's fingerprint is taken throughout the verification process, pertinent features are retrieved, and these features are compared to the stored template to generate a similarity score. If the score is higher than a predetermined threshold, access is allowed. If not, it is turned down. The intrinsic uniqueness of the fingerprint patterns determines how effective this technology is, guaranteeing safe and trustworthy authentication.

• Compared to verification, identification is more time-consuming and labor-intensive. By matching a person's registered fingerprint template with a database of known fingerprint templates, identification is the process of proving their identity. A similarity score is produced by this comparison, which measures how similar the fingerprints that were taken and those that were saved in the database are.

3.3 The Template protection

Generally speaking, the biometric template protection technique must meet the following specifications.

- Diversification: Each template created using a user's fingerprints should be tailored to its particular use. Stated differently, no identically altered biometric template may be utilized in several applications.

- Revocability: The suggested approach enables straightforward revocation by simply substituting new templates with the user's original biometric input.

- Non-inevitability: To protect the privacy of biometric information, it is computationally challenging to return a template to its initial state.

- Efficiency: The accuracy of the algorithm would not be impacted by the design of the biometric template protection technique; that is, matching using the modified biometric template would not result in a decline in recognition efficiency.

3.4 Conditions for protecting biometric templates

Conversely, entities that are needed for both enrollment and authentication but are not kept in the database are referred to as additional information. A password or secret key that the user provides in addition to his biometric characteristic is an example of supplemental data. Although it is not required, using supplemental data adds another layer of authentication.

Another optional phase in a template protection plan is feature adaption. It is commonly known that a number of factors, including sensor noise, variations in user engagement, environmental changes, and trait aging, can cause intrasubject variability in biometric samples. Minimizing intrasubject fluctuations in the observed biometric signal and/or representing the original features in a simplified format (such as a binary string) without sacrificing their individuality are the goals of feature adaptation. It is important to note that both intrasubject and intersubject variables affect how distinctive a biometric representation is.

○ Non-invertibility or irreversibility: Retrieving the original biometric template from a person's protected biometric reference should be computationally challenging. If an issue cannot be resolved with a polynomial-time methodology, it might be deemed computationally complex or difficult. The non-invertibility enhances the security of the biometric system by preventing the misuse of recorded biometric data to initiate replay or spoof attacks.

○ Revocability or sustainability: It should be highly computational to extract the original biometric template from several protected biometric reference instances that are based on an individual's same biometric characteristic. In the event that a biometric database is compromised, this enables the revocation and issuance of fresh instances of protected biometric reference. Additionally, this stops a hacker from compromising other biometric databases where the same person can be registered in order to retrieve the initial design.

○ It should be computationally challenging to determine if two or more instances of a protected biometric reference were generated from the same user biometric feature. This is known as nonlinkability or unlinkability. The nonlinkability attribute protects individual privacy by preventing cross-matching between several apps.

3.5 Risks Associated with Biometric Templates

After researching biometric system assaults, we looked into the vulnerabilities that biometric templates were subjected to a result of these hacks. According to a more recent training, assaults against biometric templates may result in the following weaknesses:

○ To obtain unauthorized access, an impostor's biometric template can be used in place of a legitimate one.

○ It is possible to obtain unauthorized access to the system, including other systems that have the same biometric fingerprint trait, by creating a physical spoof of a biometric template.

○ Unauthorized access beyond authentication vaults can be obtained by replaying stolen biometric templates to the matcher.

○ When biometric templates are not adequately protected, attackers may use them to match information from other databases and secretly follow an individual without that person's knowledge or agreement.

IMPLEMENTATION AND EXPERIMENTAL RESULTS

There are two palmprint databases and three fingerprint databases in total. Eight photos and 100 individuals were randomly selected for the studies from each database. Each fingerprint and palmprint pair's ROI was first and foremost retrieved and standardized to 150 pixels by 150 pixels.

The following are the specifics and symbols of the three fingerprint databases:

Table 1: Comparing the Performance of RT Versus the Unibiometric Approach in the Case of Stolen Tokens

Database	Fused with	EER (%)
F1	-	16.23
	P1	7.43
	P2	4.41
F2	-	11.27
	P1	5.44
	P2	2.65
F3	-	27.24
	P1	9.98
	P2	5.94
P1	-	4.65
	F1	7.43
	F2	5.44
	F3	9.98
P2	-	5.72
	F1	4.41
	F2	2.65
	F3	5.94

- F1: Database. DB1 Set for FVC2004. A database. The photos were taken using CrossMatch's visual sensor, the "V300." Each of the 100 subjects in this collection has eight greyscale photos, for a total of 800 photos.
- F2. Using a digital camera called the Canon PowerShot Pro1, 103 people supplied a total of 1030 color photos, each of which had 10 fingerprint photographs.
- F3: FVC2002 DB1 Assign and database. Identix's "TouchView II" optical sensor was used to take the fingerprint pictures. Each of the 100 subjects has eight greyscale photos, for a total of 800 photographs.

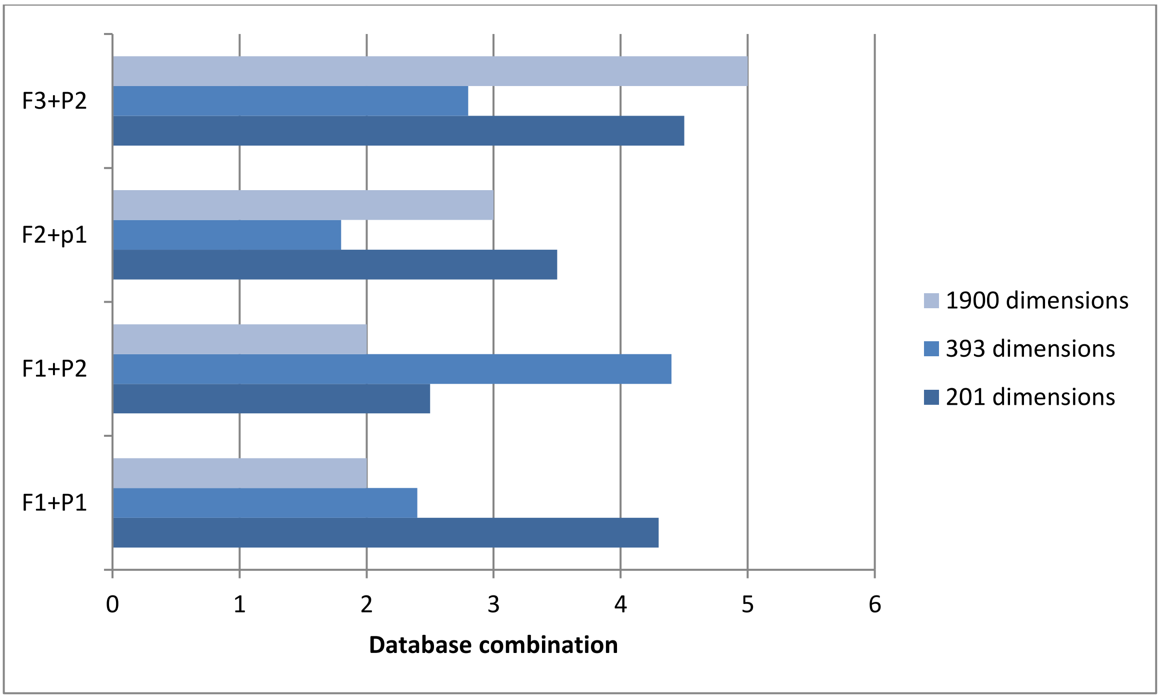

Figure 4: RT's Performance Report for Various Feature Durations

4.1 Feature level fusion validation in comparison to unibiometrics

However, by using a stolen token and setting the feature length to 200 dimensions, Table 1 provides an outline of RT's recognition performance. With the exception of the P1 database, the reported EERs are at least equal to their unibiometric counterparts, even if 0% EER is no longer achievable in the stolen token scenario. For instance, database F1 originally records an EER of 15.22%; but, upon its fusion with database P1, the EER decreases to 6.42%.

We then looked at the results of using various feature lengths in RT. The reported EERs for each database combination vary very little, as Figure 4 illustrates.

Table 2: Comparison of pseudo-impostor verification vs plain verification performance

Databases	**EER(%)**	
	Plain Verification	**Pseudo-imposter Verification**
F1+F2	0.0001	0.0001
F1+F2	0.0001	0.0001
F2+P1	0.0001	0.0001
F2+P2	0.0001	0.0001
F3+P1	0.4284	0.2399
F3+P2	0.1153	0.0003

For random tiling, each user has a total of 200 distinct user-specific tokens. This result in 45,000 pseudo-impostor scores overall, with 200 pseudo-impostor scores each sample. The EERs derived via pseudo-impostor verification are remarkably comparable to, if not identical to, those derived from simple verification, as indicated in Table 2.

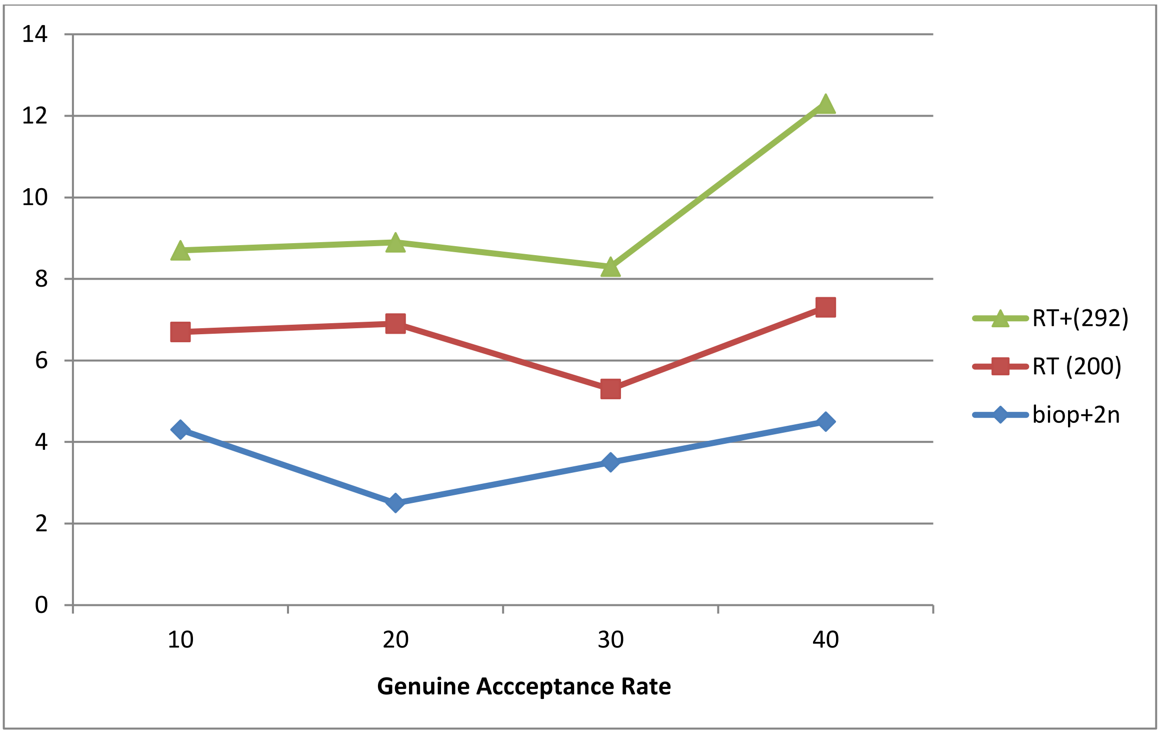

Figure 5: ROC curves for the F2 and P2 Database Combinations in the Case of Stolen Tickets

The ROC curves of F2 and P2 fusion using various hybrid template protection techniques in the stolen token scenario are shown in Figure 5. The not-discretized feature lengths are 200 and 392, whereas the biop, random tiling, equal-width 2N discretization, and equal-probable 2N discretization are represented as biop, RT, 2N, and eq2N, respectively. The suggested RT and equal-probability 2N discretization combination can achieve very low EER in comparison to RT, solitary feature level fusion, or 2N discretized BioPhasor. With zero EER, there is a significant overlap between the curves of RT-incorporated 2N discretization and equal-probable 2N separation.

CONCLUSION

We conducted a performance analysis of each type of fingerprint recognition system to evaluate its advantages and disadvantages. The significant developments in fingerprint biometrics, both unimodal and multimodal, are the subject of this article. While discussing the advantages of fingerprint biometric systems, emphasis is placed on several application situations that highlight the algorithms utilized to build these systems. We discovered that while some dynamic biometric devices require increased verification accuracy, the majority of the available solutions have security and privacy issues. Combining data from many sources can greatly increase the precision of biometric authentication systems. Because it is easy to find and combine the matching scores, score level fusion remains the most advantageous of all the data fusion levels. Furthermore, it was discovered that limitations are removed when multimodal biometric frameworks are used instead of unimodal biometrics. It is necessary to enhance multimodal biometric systems by adding more sensors, refining matching algorithms, managing noise issues, and doing data analysis.

According to empirical assessments, this approach may reduce the impostor distribution's width, improving the ability to identify imposters. We have also shown that the suggested approach can produce a variety of revocable templates.

REFERENCES

[1] Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37), 27721-27776.

[2] Chin, Y. J., Ong, T. S., Teoh, A. B. J., & Goh, K. O. M. (2014). Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Information Fusion, 18, 161-174.

[3] Ramakrishnan, J., & Ramakrishnan, M. (2012). An efficient automatic attendance system using fingerprint reconstruction technique. arXiv preprint arXiv:1208.1672.

[4] Saraswat, C., & Kumar, A. (2010). An efficient automatic attendance system using fingerprint verification technique. International Journal on Computer Science and Engineering, 2(02), 264-269.

[5] Simoens, K., Bringer, J., Chabanne, H., & Seys, S. (2012). A framework for analyzing template security and privacy in biometric authentication systems. IEEE Transactions on Information forensics and security, 7(2), 833-841.

[6] Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. Proceedings of the IEEE, 85(9), 1365-1388.

[7] Yang, S., & Verbauwhede, I. (2005, March). Automatic secure fingerprint verification system based on fuzzy vault scheme. In Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. (Vol. 5, pp. v-609). IEEE.

[8] Han, C. C., Cheng, H. L., Lin, C. L., & Fan, K. C. (2003). Personal authentication using palm-print features. Pattern recognition, 36(2), 371-381.

[9] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. *IEEE Access*.

[10] Chin, Y. J., Ong, T. S., Teoh, A. B. J., & Goh, K. O. M. (2014). Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. Information Fusion, 18, 161-174.

[11] Ramakrishnan, J., & Ramakrishnan, M. (2012). An efficient automatic attendance system using fingerprint reconstruction technique. arXiv preprint arXiv:1208.1672.

[12] Mwema, J., Kimwele, M., & Kimani, S. (2015). A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates. International Journal of Computer Trends and Technology, 20(1), 12-18.

[13] Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. IEEE Access.

[14] Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. Pattern Recognition, 48(2), 458-472.

[15] Yang, W. (2015). Local structure based fingerprint authentication systems with template protection (Doctoral dissertation, UNSW Sydney).