Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 6 (2023)

Investigate methods to securely store and protect fingerprint templates in biometric databases to prevent unauthorized access and potential breaches

[1] Sumesh M, [2] V Sheeja Kumari, [3] Devanolla Suresh, [4] R. Sivabalan, [5] Carmel Mary Belinda M J, [6] K Anbazhagan

[1] Research Scholar / Department of Computational Intelligence, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai.
[2] Professor/ Department of Computational Intelligence, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai.
[3] Assistant Professor / Department of Computer Science & Technology, Madanapalle Institute of Technology & Science, Madanapalle.
[4]Assistant Professor / Department of Information Security, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai.
[5] Professor / Department of Applied Machine Learning, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai.
[6] Professor/ Department of Computational Intelligence, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai.

*Corresponding author E-mail : ammucja@gmail.com

Abstract: Biometric recognition, especially fingerprint-based systems, plays a vital role in modern security and authentication. Safeguarding fingerprint templates in these systems is critical due to the potential repercussions of security breaches. This study investigates methods to enhance the security of fingerprint templates in biometric databases. The research begins with a literature review that underscores the security challenges within biometric databases and evaluates existing protection methods. It explores advanced techniques like biometric cryptosystems, secure hashing, two-factor authentication, homomorphic encryption, and multi-party computation to gauge their efficacy in mitigating security risks. The study emphasizes the importance of access control and authentication protocols in limiting unauthorized access and continuously monitoring for anomalies. It also assesses the role of secure hardware modules, such as hardware security modules (HSMs) and trusted execution environments (TEEs), in protecting sensitive data. Furthermore, the investigation scrutinizes the concept of biometric template revocation, presenting methods to invalidate compromised templates. It delves into data encryption practices for both templates and the entire database, along with best practices for managing decryption keys. The study also explores the deployment of anomaly detection and intrusion detection systems to reinforce security. In conclusion, this investigation provides a comprehensive overview of methods for securely storing and protecting fingerprint templates in biometric databases. By implementing these techniques and best practices, organizations can enhance the security of their biometric systems, safeguarding sensitive data. This research aims to inform and guide practitioners and researchers in their pursuit of robust biometric database security.

Keywords: Biometric Security, Fingerprint recognition, Data encryption, Template revocation, Intrusion detection, Biometric database, Anomaly detection.

I. Introduction

Biometric recognition systems have become integral components of modern security and authentication solutions, with fingerprint templates serving as key identifiers in these systems. As technology advances, so do the threats to the security of biometric data. Ensuring the secure storage and protection of fingerprint templates in biometric databases is of paramount importance, as the consequences of unauthorized access and potential breaches can be severe[1]. This investigation embarks on a critical exploration of various methods and strategies to safeguard fingerprint templates in biometric databases. By doing so, it aims to mitigate the security risks

associated with these databases and ensure that sensitive biometric data remains confidential and tamper-proof. The study commences with a comprehensive literature review that highlights the evolving landscape of security challenges in the realm of biometric databases. It also provides an in-depth analysis of the existing methods employed to secure fingerprint templates. Furthermore, it delves into advanced and cutting-edge techniques such as biometric cryptosystems, secure hashing, two-factor authentication, homomorphic encryption, and multi-party computation to assess their effectiveness in addressing these challenges.

The investigation underscores the significance of access control and authentication protocols, emphasizing their role in restricting database access to authorized personnel while continuously monitoring for potential anomalies. Secure hardware modules, including hardware security modules (HSMs) and trusted execution environments (TEEs), are evaluated for their contribution to safeguarding sensitive biometric data. In addition, the study scrutinizes the concept of biometric template revocation, presenting methods to invalidate and update compromised templates, rendering them useless for subsequent authentication. It also explores data encryption practices for both fingerprint templates and the database as a whole, along with best practices for the secure management of decryption keys. The deployment of anomaly detection and intrusion detection systems is also examined as an essential layer of defense against unauthorized access and potential security breaches[2].

In conclusion, this investigation brings to light a diverse arsenal of methods available for securely storing and protecting fingerprint templates in biometric databases. The implementation of these methods, in conjunction with best practices, enables organizations to enhance the security of their biometric systems and ensure the confidentiality and integrity of sensitive biometric data. This research aims to inform and guide both practitioners and researchers in the ongoing pursuit of robust biometric database security.

A. Background and significance of biometric databases

Biometric recognition systems, which rely on unique physical or behavioral characteristics for authentication, have witnessed a rapid evolution and widespread adoption in recent years. Among these systems, fingerprint recognition stands out as one of the most prominent and widely used modalities. This technology is employed in various applications, from securing personal devices to accessing sensitive data and premises, making it a cornerstone of modern security and authentication solutions. The significance of biometric databases, particularly those storing fingerprint templates, cannot be overstated in this digital age. These databases serve as repositories of individuals' biometric information, enabling swift and accurate identity verification[3]. The uniqueness and consistency of fingerprints make them highly reliable for personal identification, making them an attractive choice for biometric authentication.

However, with this increasing reliance on biometrics comes the growing importance of securing the data within these databases. Breaches of biometric databases can have far-reaching consequences for individuals and organizations. Unlike traditional passwords or PINs, biometric data, once compromised, cannot be reset or changed. Consequently, the need to protect fingerprint templates from unauthorized access and potential breaches is paramount. Fingerprint templates contain highly sensitive information, and their security is not only essential for protecting individual privacy but also for maintaining the trust of users in biometric systems. Breaches can lead to identity theft, unauthorized access, and even physical security risks. Consequently, the protection of these templates is an area of research and development that directly impacts individuals' daily lives and the security of critical systems[4]. As the use of biometric databases continues to expand into areas like financial services, healthcare, and law enforcement, the need for robust security measures becomes increasingly urgent. This investigation delves into various methods and strategies to address these concerns, aiming to provide a comprehensive understanding of the challenges and solutions in securely storing and protecting fingerprint templates within biometric databases.

B. Importance of secure storage of fingerprint templates

The importance of securely storing fingerprint templates in biometric databases cannot be overstated, as it underpins the integrity of biometric recognition systems and has far-reaching implications for individual privacy and overall security. Several key factors underscore the critical nature of secure storage[5]:

1. **Preventing Unauthorized Access**: Fingerprint templates serve as the foundation for user authentication in a wide range of applications, from unlocking smartphones to accessing sensitive

government facilities. Secure storage is essential to ensure that only authorized users can access these systems. Unauthorized access can lead to identity theft, unauthorized transactions, or even compromise national security.

2. **Protection of Sensitive Data**: Fingerprint templates contain highly sensitive and unique biometric data. Unlike passwords or PINs, which can be changed if compromised, fingerprints are permanent, making their protection crucial. Unauthorized disclosure can have long-lasting and irreversible consequences for individuals.
3. **Privacy Preservation**: Biometric data is intimately tied to an individual's identity. The secure storage of fingerprint templates is essential for safeguarding personal privacy. Breaches can lead to the exposure of sensitive information and raise concerns about mass surveillance, privacy infringement, and data misuse.
4. **Financial Security**: Fingerprint recognition is widely used in financial services, including mobile banking and payment systems. Secure storage ensures the financial security of users by preventing unauthorized access to accounts and financial transactions. Breaches in this context can result in financial losses and identity fraud.
5. **Healthcare Records**: In healthcare, biometric authentication is used to access electronic health records and protect sensitive patient information. Secure storage of fingerprint templates is vital to safeguard patient privacy and maintain the confidentiality of medical data.
6. **Law Enforcement and National Security**: Biometric databases are utilized in law enforcement for criminal identification and border control. Ensuring secure storage is essential to prevent potential breaches that could lead to the compromise of sensitive law enforcement and national security data.
7. **Legal and Regulatory Compliance**: Many regions and industries have established legal and regulatory frameworks, such as GDPR in Europe and HIPAA in healthcare, which require the secure handling of biometric data. Non-compliance can result in legal consequences and financial penalties.
8. **Trust and User Acceptance**: The success of biometric systems relies on user trust. Secure storage measures instill confidence in users that their biometric data is protected. Breaches can erode this trust and deter the adoption of biometric technologies.
9. **Long-Term Reliability**: Fingerprint templates need to be preserved securely for long-term use. As individuals use biometric systems over extended periods, maintaining the integrity of their templates is crucial for ongoing authentication and identification.

C. Purpose and scope of the investigation

The purpose of this investigation is to comprehensively explore and analyze the methods and strategies for securely storing and protecting fingerprint templates in biometric databases to prevent unauthorized access and potential breaches. This research seeks to address the following objectives[6]:

1. **Assessment of Security Challenges**: To provide a deep understanding of the evolving security challenges in biometric databases, particularly those housing fingerprint templates. This includes a review of the types of threats, vulnerabilities, and attack vectors that such databases face.
2. **Review of Existing Protection Methods**: To examine and evaluate the current methods and technologies employed to secure fingerprint templates in biometric systems. This includes an analysis of their strengths, weaknesses, and real-world applications.
3. **Exploration of Cutting-Edge Techniques**: To delve into advanced and emerging security techniques, such as biometric cryptosystems, secure hashing, two-factor authentication, homomorphic encryption, and multi-party computation, with the goal of assessing their effectiveness in mitigating security risks.
4. **Focus on Access Control and Authentication**: To emphasize the significance of access control and authentication protocols in restricting database access to authorized personnel and providing continuous monitoring for potential anomalies. This includes an evaluation of best practices in this domain.

5. **Evaluation of Secure Hardware Modules**: To assess the role of secure hardware modules, including hardware security modules (HSMs) and trusted execution environments (TEEs), in safeguarding sensitive fingerprint templates and their application in real-world scenarios.
6. **Biometric Template Revocation**: To scrutinize the concept of biometric template revocation and present methods for invalidating and updating compromised templates, rendering them ineffective for subsequent authentication.
7. **Data Encryption and Key Management**: To explore data encryption practices for both fingerprint templates and the biometric database as a whole, along with best practices for managing decryption keys to ensure secure data protection.
8. **Anomaly Detection and Intrusion Detection**: To examine the deployment of anomaly detection and intrusion detection systems as a crucial layer of defense against unauthorized access and potential security breaches.

The scope of this investigation encompasses a broad range of techniques, methodologies, and technologies aimed at enhancing the security of fingerprint templates in biometric databases. It considers various applications, from personal device access to critical systems used in finance, healthcare, law enforcement, and national security.

II. LITERATURE REVIEW

Fernandez et al. proposed a comparative study of FQA prior to 2006, in which they categorized FQA algorithms into several classes known as local feature-based approaches, global feature-based methods and solutions with classifiers [7]. Those quality metrics can be simply summarized in several points: quality metrics based on the orientation of fingerprint pattern; algorithms that rely on the variation of Gabor responses; approaches in frequency domain; measurements based on pixel information and quality indexes rely on classification with multi-feature. In addition, that study also analyzed quality metrics mainly in terms of the linearity between them. In this study, we classify the existing studies into several frameworks in terms of their implementation to show the difference and some potential problems that need to be considered. As mentioned above, the quality metrics that had been proposed so far are all dependent on one or several features. According to how they are carried out, this study categorizes them as: 1)segmentation-based approaches; 2) a single feature-based quality index; 3) solutions rely on a combination of multi-features or indexes, which is further divided into methods based on linear fusion and classification.

For instance, Shen et al. use the regularity of 8-direction Gabor features to generate quality index. Their Gabor feature is initially used for segmenting foreground from the image, which is also involved in a threshold. In addition, segmentation-based measures proposed in were also used for image quality assessment [8]. The use of segmentation presented above are all associated with fingerprint image. Yao et al. proposed an approach (MQF) with minutiae template only, in which the convex-hull and Delaunay triangulation are adopted to measure the area of a reasonable informative region. This algorithm is hence dependent on a minutiae extracting operation. In addition, some bad quality images that own relatively large informative region are more possibly to give outliers. According to these literature, one can note that foreground area is indeed a good factor for qualifying fingerprint image. In this case, multiple segmentation could be a potential solution to generate area-based quality metric.

The second category discusses quality metrics that rely on a single feature which could be applied locally or globally to the image. For example, Nalini et al. proposed to use cumulative energy of several subbands of the compressed image in the wavelet domain. Lee et al. reviewed three approaches based on the fingerprint image, including local standard deviation, directional contrast of local block and the Gabor feature. They proposed a feature via observing the Fourier spectrum of the fingerprint image. Their quality metric depends on the pixels information of the Fourier spectrum image which is a floating measure for different kinds of image settings. Other quality metrics denoted by a single feature could also be found in where the symmetry features decomposed via 2-order orientation tensor [10] depending on scale parameter and threshold, the contrast index (CI) relies on a mean spectrum of ridge-valley measurements, and the difference of kurtosis value of the probability density functions (PDFs) is not distinctive between some convex and concave shapes that are relatively smooth. Trial results in these literature show relatively good performance comparing with baseline

algorithm(s). However, threshold values and parameters are unavoidable for most of them and lead to difficulties for achieving a generic application because they are greatly affected by image specification.

In addition, this kind of approach also can be found in where Chen et al. estimate the power spectrum ring with Butterworth functions instead of observing directly the pixel information of the spectrum image, and Tao et al. observed two regularities from the circle mainfold topology of an order set of block pixels and the associated principle component analysis (PCA)[12]. However, in addition to the coefficient problem, there are also constraints of the employed features. For example, the ridge frequency depends on the resolution and image size. Many of the existing studies made effort in qualifying fingerprint image with multiple features. This is generally carried out in two aspects: linear fusion with weighted coefficients and classification. Both could be associated with knowledge-based schemes. For instance, Lim et al. proposed a quality metric through weighted combination of local and global quality scores that are estimated in terms of several features such as orientation certainty level (OCL) and so on. Their quality metric also involves several thresholds to classify the local blocks into variant levels. Similarly, Chen et al. proposed a metric by linearly combine the orientation flow (OF) and the ridge-valley clarity features. Apparently, the weighted coefficients have to be adjusted if a different image setting is involved. The linear combination of multi-feature could also be illustrated by a regression-based approach which adopts genetic algorithm (GA) optimizing (or maxiaizing) the linear relationship between the quality value and the genuine matching scores of a set of training samples. Maximizing the correlation between the two measures is a solution for qualifying biometric sample. However, the optimization largely depends on the genuine matching results. Likewise, this problem could also be considered for other quality metrics that are associated with a prior-knowledge of matching performance, for matching algorithms can be quite different.

Quality assessment approaches with multi-feature carried out in another form is classification. Lim et al. extended their work in by classifying a certain amount of fingerprint samples with 3 different classifiers rather than calculating the quality metric. Later, the state-of-the-art quality metric, NFIQ, employs 11-dimension feature to estimate a matching score and classify results to five levels through a trained model of a neural network [13]. Further, in NFIQ 2.0, Olsen et al. trained a two-layer self-organizing map (SOM neural network) to obtain a histogram of SOM unit activation with an intensity vector of image block. The histogram is the frequency of the occurrence of the best-matching unit (with respect to the competitive layer) assigned to each block. The trained feature is then threw to a Random Forest (RF) to estimate the binned genuine matching scores (GMS). This is the first study of FQA to generate a learning-based feature by using unsupervised approach and a quite large dataset. However, the RF is to classify samples in terms of a prior-knowledge of matching score and quality is represented by the regularity as well. So far, no studies is able to conduct a perfect matching algorithm because the matching scores between two bad quality genuine or impostor samples are somehow unforeseeable [14]. According to such a statement, one can note that approaches with a single feature is limited to a specified image type and knowledge-based solutions is not absolutely appropriate to cross-use. Besides, it is also possible to consider whether a quality metric based-on multi-feature really makes a robust criterion or takes the advantages of them.

A. Strengths and weaknesses of current approaches

The strengths and weaknesses of current approaches for secure storage of fingerprint templates in biometric databases are essential to understand for the development and improvement of biometric security measures. Here, we outline the key strengths and weaknesses of these approaches[13-14]:

Strengths:

1. **Security Enhancement**: Current approaches significantly enhance the security of fingerprint templates, making it challenging for unauthorized individuals to gain access. This is especially important in applications where sensitive data or critical systems are involved.
2. **Data Privacy**: They help protect the privacy of individuals by ensuring that their biometric data is not exposed or misused in case of a security breach.
3. **Authentication Accuracy**: These methods often maintain a high level of authentication accuracy, ensuring that legitimate users can access the system with minimal false negatives.

4. **Irreversibility**: Many methods, such as secure hashing and biometric cryptosystems, ensure that the original fingerprint data cannot be reconstructed from the stored information, making it extremely difficult for attackers to reverse-engineer the templates.
5. **Compliance with Regulations**: These approaches often align with data protection regulations and privacy laws, which is crucial for legal and ethical compliance, especially in sectors like healthcare and finance.
6. **Revocation Mechanisms**: Methods like biometric template revocation allow organizations to invalidate compromised templates, adding an extra layer of security and control.
7. **Continuous Monitoring**: Access control and authentication protocols include features for continuous monitoring and auditing of database access, which can aid in detecting and preventing unauthorized access.
8. **Flexibility**: Depending on the specific requirements and constraints of an application, various methods can be tailored to provide the right balance of security and usability.

Weaknesses:

1. **Resource Intensive**: Some security methods, such as homomorphic encryption and secure hardware modules, can be resource-intensive in terms of processing power, leading to potential performance issues.
2. **Complex Implementation**: The implementation of advanced security measures can be complex and require specialized knowledge. This complexity can make the systems more challenging to set up and maintain.
3. **Cost**: Implementing certain methods, such as hardware security modules and biometric cryptosystems, may incur additional costs for hardware and software licenses.
4. **Usability and Speed**: Security measures like two-factor authentication may introduce additional steps, potentially slowing down the authentication process and making it less user-friendly.
5. **Compatibility**: The compatibility of certain security measures with existing systems and devices can be a concern. It may require upgrades or changes to the infrastructure.
6. **Key Management**: Data encryption and secure storage often rely on proper key management, which can introduce vulnerabilities if not handled securely.
7. **Vulnerability to Zero-Day Attacks**: While these methods significantly improve security, no system is completely invulnerable. Zero-day vulnerabilities and advanced attacks can still pose risks.
8. **Resistance to Change**: Users may resist changes to security methods they find unfamiliar or inconvenient, impacting the adoption of secure practices.

Understanding these strengths and weaknesses is crucial for selecting the right combination of security measures that align with the specific needs and risk tolerance of a given application. Balancing security with usability and performance is a complex but essential task in the field of biometric database security.

III. Biometric Cryptosystems

A. Explanation of Biometric Cryptosystems

Biometric cryptosystems are cryptographic techniques designed to enhance the security and privacy of biometric data, including fingerprint templates. These systems address the unique challenges associated with biometrics, such as the irrevocability of biometric traits, the need to protect sensitive information, and the potential risks of data breaches[15].

At the core of biometric cryptosystems is the transformation of biometric data into a secure, irreversible format. This transformation ensures that even if the biometric data or the cryptographic key is compromised, the original biometric template cannot be reconstructed or exploited for unauthorized access. Biometric cryptosystems introduce cryptographic operations into the biometric recognition process, adding a layer of security to protect sensitive data.

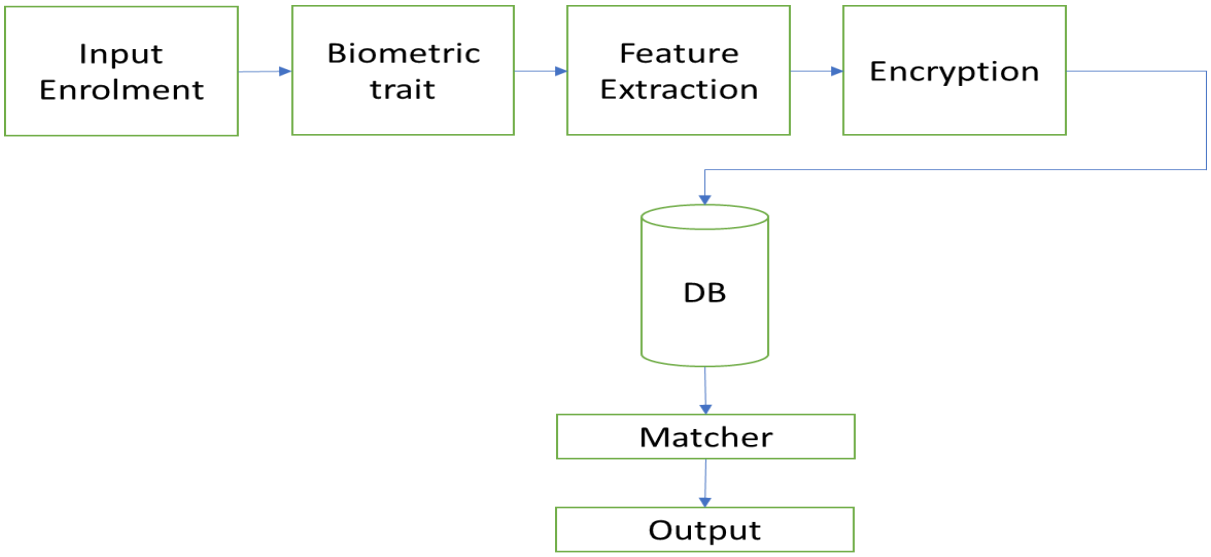

Fig No.1 Architecture diagram for biometric system

B. How Biometric Cryptosystems Can Protect Fingerprint Templates

Biometric cryptosystems offer several ways to protect fingerprint templates[16]:

1. **Feature Extraction**: Biometric cryptosystems typically extract distinctive features from the fingerprint, such as minutiae points or ridge patterns, rather than storing the raw image. These features are then used to create a secure template.
2. **Secure Key Generation**: Biometric cryptosystems generate cryptographic keys based on the biometric data. These keys are used to encrypt and decrypt the templates securely.
3. **Irreversible Transformations**: Biometric data is subjected to irreversible mathematical transformations, making it infeasible to reverse-engineer the original data from the transformed template.
4. **Secure Match-on-Card**: In some implementations, the matching process occurs on a secure hardware token (e.g., a smart card) rather than in a central database. This further protects the biometric data as matching is performed locally.
5. **Protection Against Brute-Force Attacks**: Cryptographic techniques make it extremely difficult for attackers to use brute-force methods to reverse-engineer the biometric data or template.

C. Examples of Biometric Cryptosystem Implementations

Several real-world examples of biometric cryptosystem implementations exist:

1. **Fuzzy Vault**: The fuzzy vault is a cryptographic scheme that securely stores biometric data. It allows for recovery of the original data only when a user provides the correct biometric input.
2. **BioHashing**: BioHashing generates a cryptographic key from biometric data, which is then used to protect templates. The key ensures that templates are secure even if they are stolen.
3. **BioConvolving**: This method uses convolutional neural networks to transform biometric data, providing a secure template for authentication. It is highly resistant to attacks.
4. **Bio-Cryptosystem for Iris Recognition**: This approach applies cryptographic methods to iris recognition, protecting the iris templates from unauthorized access and ensuring the privacy of individuals.

D. Advantages and Limitations of Biometric Cryptosystems

Advantages:

1. **Enhanced Security**: Biometric cryptosystems significantly enhance the security of biometric templates, making them resistant to various attacks[17].

2. **Privacy Preservation**: They protect individual privacy by ensuring that even if the templates are compromised, the original biometric data cannot be reconstructed.
3. **Usability**: These systems can be seamlessly integrated into biometric recognition processes without causing significant usability issues for legitimate users.
4. **Protection against Insider Threats**: The use of biometric cryptosystems can mitigate insider threats where authorized personnel attempt to misuse biometric data.

Limitations:

1. **Computational Overhead**: The cryptographic operations involved can introduce computational overhead, potentially affecting the speed of biometric recognition.
2. **Complex Implementation**: Implementing biometric cryptosystems may require specialized expertise, making them more challenging to set up and maintain.
3. **Resource Demands**: Some biometric cryptosystems may require additional hardware or processing power, which can be costly.
4. **Scalability**: The complexity of these systems can impact their scalability when dealing with a large number of users.
5. **Key Management**: Secure key management is essential, and mishandling of keys can introduce vulnerabilities.

IV. Secure Hashing

A. The Concept of Secure Hashing in Biometrics

Secure hashing in biometrics involves the use of cryptographic hash functions to transform raw biometric data, such as fingerprint templates, into irreversible and secure representations. The core concept lies in the application of a one-way function, which converts the input data into a fixed-length string of characters, commonly referred to as a hash code. Secure hashing ensures that it is computationally infeasible to reverse-engineer the original data from the hash code, making it a fundamental tool for biometric data protection[18].

In the context of fingerprint recognition, secure hashing involves taking the unique features and characteristics of a fingerprint and converting them into a hash code. This hash code is then stored in the biometric database rather than the raw fingerprint data, enhancing the security and privacy of the individual's biometric information.

B. Salting and Its Role in Secure Hashing

Salting is a technique often used in conjunction with secure hashing to enhance security. In the context of biometrics, a "salt" is a random value that is combined with the fingerprint data before hashing. The salt ensures that even if two individuals have identical fingerprints, their resulting hash codes will be different due to the unique salt applied[19]. The role of salting is to protect against precomputed attacks, where an attacker might create a database of precomputed hash codes for common fingerprints. With a unique salt for each fingerprint, these precomputed attacks become ineffective, as the hash codes will differ. This significantly improves the security of the hashing process.

C. Use Cases and Examples of Secure Hashing in Fingerprint Recognition

Secure hashing is widely used in fingerprint recognition for various use cases:

1. **Biometric Databases**: Fingerprint templates, which are derived from the unique features of a fingerprint, are securely hashed and stored in biometric databases for authentication purposes. Examples include the storage of fingerprint templates in smartphones and secure access control systems.
2. **Fuzzy Matching**: In fuzzy matching algorithms for fingerprint recognition, secure hashing can be applied to compare a presented fingerprint with stored templates while ensuring that the original data remains confidential.

3. **Template Protection**: Secure hashing is used to protect biometric templates during transmission and storage. Hashed templates are less vulnerable to data breaches and are more privacy-compliant[20].

D. Comparing Different Hashing Algorithms for Security

When selecting a hashing algorithm for secure hashing of fingerprint data, it is essential to consider various factors, including security, performance, and suitability for the application. Common hashing algorithms used in biometrics include:

1. **SHA-256 (Secure Hash Algorithm 256)**: SHA-256 is a widely recognized cryptographic hash function known for its security and collision resistance. It is commonly used in biometric applications where a high level of security is required.
2. **MD5 (Message Digest Algorithm 5)**: MD5 was once widely used for hashing, but it is now considered outdated and vulnerable to collisions. It is generally not recommended for security-critical biometric applications.
3. **SHA-3**: SHA-3 is the latest member of the Secure Hash Algorithm family. It is designed to be secure, efficient, and suitable for a wide range of applications.
4. **Bcrypt and Scrypt**: These algorithms are specifically designed for password hashing but can also be adapted for biometric hashing. They incorporate features like key stretching and salting for added security.

The choice of hashing algorithm should align with the specific security requirements of the biometric application. SHA-256 and SHA-3 are commonly recommended for their strong security properties, while the use of salting and additional security measures is essential to further protect the hashed data[21].

V. Two-Factor Authentication

A. Two-Factor Authentication and Its Role in Enhancing Security

Two-factor authentication (2FA) is a security mechanism that requires users to provide two different authentication factors to gain access to a system, account, or resource. These factors typically fall into three categories: something you know (e.g., a password or PIN), something you have (e.g., a smart card or mobile device), and something you are (e.g., biometric data). 2FA enhances security by adding an additional layer of verification, making it more difficult for unauthorized individuals to gain access, even if they possess one of the authentication factors[20-21].

B. Combining Fingerprint Recognition with Other Authentication Factors

The combination of fingerprint recognition with other authentication factors is a powerful application of 2FA. In this approach, the "something you are" factor (fingerprint) is used in conjunction with either the "something you know" (e.g., a PIN) or "something you have" (e.g., a smart card). This combination provides a high level of security by requiring both biometric data and an additional authentication factor for access. For example, a user might need to present their fingerprint and enter a PIN to unlock a smartphone or access a secure facility.

C. Real-World Examples of Two-Factor Authentication in Biometric Systems

1. **Mobile Devices**: Many modern smartphones and tablets support fingerprint recognition as a biometric factor for unlocking the device. To enhance security, users are often required to enter a PIN or use a secondary method (e.g., facial recognition) in addition to their fingerprint.
2. **Secure Access Control**: In high-security environments such as government facilities, data centers, and research laboratories, 2FA is frequently used. Fingerprint recognition is combined with smart cards or PINs to ensure secure access.
3. **Online Banking**: Some online banking applications utilize 2FA by requiring users to provide their fingerprint along with a one-time code sent to their mobile device or email.

4. **Healthcare**: Electronic health record systems may incorporate 2FA, requiring healthcare professionals to use their fingerprint and a smart card for authentication.
5. **E-commerce**: For added security during online transactions, fingerprint recognition can be combined with a one-time code sent via text message or generated by a mobile app[21].

D. Security Implications and User Experience Considerations

- **Enhanced Security**: The use of 2FA with fingerprint recognition significantly improves security by making it more difficult for unauthorized individuals to access systems or data.
- **Reduced Risk of Unauthorized Access**: Even if an attacker steals or replicates fingerprint data, they would still need the second authentication factor to gain access.
- **User Experience**: While 2FA enhances security, it can impact user experience. Users must go through an additional step, which may be seen as an inconvenience.
- **Biometric Data Protection**: It is essential to ensure the security of the stored biometric data and the communication between the biometric sensor and the authentication system.
- **Backup Authentication**: A mechanism should be in place for users to access their accounts or systems if they are unable to provide the second factor (e.g., fingerprint due to an injury).
- **User Education**: Proper user education and training are crucial to ensure that users understand how 2FA works and why it is important.
- **Balancing Security and Usability**: Striking the right balance between security and usability is critical. The authentication process should be both secure and user-friendly[22].

VI. Homomorphic Encryption

A. Explanation of Homomorphic Encryption and Its Relevance

Homomorphic encryption is a cryptographic technique that allows data to be encrypted in such a way that it can be processed without needing to be decrypted. This has significant relevance in biometrics, particularly for the protection of fingerprint templates. Homomorphic encryption ensures that sensitive biometric data remains confidential and secure, even when computations and analyses need to be performed on that data[23].

The relevance of homomorphic encryption in biometrics lies in its ability to enable secure and privacy-preserving operations on encrypted biometric templates. It allows for fingerprint recognition and matching to be conducted without ever exposing the original fingerprint data, thereby safeguarding individuals' privacy and protecting against data breaches.

B. Applications of Homomorphic Encryption in Fingerprint Template Protection

1. **Fingerprint Matching**: Homomorphic encryption enables matching of encrypted templates without revealing the actual fingerprint data. This is particularly important for authentication and access control systems.
2. **Template Revocation**: Homomorphic encryption can be used to revoke and update compromised templates securely. The revocation process can be carried out on encrypted data, preserving privacy.
3. **Secure Outsourcing**: Homomorphic encryption allows biometric data to be securely outsourced to external service providers or cloud-based systems for processing without disclosing the original data.
4. **Biometric Database Operations**: Operations like indexing, searching, and deduplication of fingerprint templates can be performed on encrypted data, maintaining privacy and security[24].

C. Challenges and Performance Considerations

- **Computational Overhead**: Homomorphic encryption can introduce significant computational overhead, which may affect the speed of biometric operations. Optimizations and efficient algorithms are required to mitigate this challenge.

- **Key Management**: Effective key management is crucial to ensure the security of homomorphically encrypted data. Key storage, distribution, and protection are key considerations[25].
- **Complexity**: Implementing homomorphic encryption can be complex and may require specialized expertise, making it challenging for organizations to adopt.
- **Performance vs. Security Trade-off**: There is often a trade-off between the level of security and the performance of homomorphic encryption schemes. Striking the right balance is essential.

D. Case Studies on Using Homomorphic Encryption in Biometric Systems

1. **Microsoft Azure**: Microsoft has incorporated homomorphic encryption in its Azure platform to enhance data privacy. Azure Confidential Computing allows for the processing of sensitive data, including biometrics, while it remains encrypted.
2. **IBM Homomorphic Encryption Toolkit**: IBM has developed a toolkit for homomorphic encryption that has applications in secure data analytics, including biometric data analysis.
3. **Privacy-Preserving Biometric Matching**: Researchers have explored the use of homomorphic encryption for privacy-preserving biometric matching in authentication systems. This approach ensures that the matching process is conducted on encrypted templates, maintaining user privacy.
4. **Biometric Identity Verification**: Various applications in financial services and healthcare are considering homomorphic encryption to verify identities securely, allowing for secure and private access to sensitive information.

VII. Multi-Party Computation (MPC)

A. Introduction to MPC Techniques in Biometrics

Multi-Party Computation (MPC) is a cryptographic technique that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In biometrics, MPC enables secure and privacy-preserving computations, particularly for tasks like matching fingerprints, without revealing the raw biometric templates. It is a powerful approach for maintaining data confidentiality while still gaining valuable insights from biometric data[23-25].

B. How MPC Enables Secure Matching Without Revealing Templates

MPC techniques enable secure matching without exposing the raw templates by distributing the computation among multiple parties. Here's how it works:

1. **Secure Protocols**: MPC employs secure protocols that allow each party to hold a share of the biometric data. The data is encrypted, and no party has access to the complete raw data of any other party.
2. **Computation Over Shares**: Computations are performed over these shares rather than the original data. For example, in fingerprint matching, MPC can be used to compare the shares of two fingerprints without revealing the actual fingerprint images.
3. **Result Aggregation**: The results of these computations are then securely aggregated to obtain the final outcome, such as whether the fingerprints match.

This process ensures that no party gains access to the complete template of another party, thereby protecting privacy and maintaining the confidentiality of biometric data[25].

C. Use Cases and Real-World Implementations

1. **Biometric Authentication**: In scenarios where multiple parties need to verify biometric data (e.g., a fingerprint for authentication), MPC ensures that no party can reconstruct the original fingerprint from the shared data, enhancing privacy and security.
2. **Medical Research**: In healthcare, MPC can enable researchers to perform analyses on shared medical data without exposing individual patient records, ensuring privacy and compliance with data protection regulations.
3. **Law Enforcement**: Law enforcement agencies can collaborate on fingerprint matching without sharing sensitive biometric data, which is essential for cross-border criminal investigations.

4. **Secure Outsourcing**: MPC can be used to securely outsource data processing tasks to third-party providers, such as cloud computing, without disclosing the underlying data. This is valuable in applications where data privacy is paramount[26].

D. Trade-Offs and Computational Requirements

- **Computational Overhead**: MPC can introduce significant computational overhead, making it more time-consuming compared to traditional computation. This trade-off is necessary to maintain data privacy.
- **Communication Overhead**: Secure protocols often require a significant amount of communication between the parties, which can impact network and resource usage.
- **Specialized Knowledge**: Implementing MPC requires specialized knowledge in cryptography and secure protocols, which can be a barrier to adoption.
- **Scalability**: The complexity of MPC can impact its scalability, especially when applied to a large number of parties or extensive data.
- **Performance vs. Security Trade-off**: There's a trade-off between the level of security and the computational resources required. Striking the right balance is essential[25][26].

VIII. Access Control and Authentication Protocols

A. Role of Access Control in Protecting Fingerprint Templates

Access control is a critical component of biometric security and plays a pivotal role in protecting fingerprint templates stored in biometric databases. Its primary functions include:

1. **Authorization**: Access control determines who is permitted to access the biometric database. Only authorized personnel, such as administrators, should have access to fingerprint templates.
2. **Role-Based Access**: Access can be defined based on user roles. Different roles may have different levels of access to the biometric templates. For example, an employee may have access to their own template but not to templates of other employees.
3. **Granular Control**: Access control can specify which operations are permitted, such as read-only or read-write access. This ensures that even authorized users only have access to the necessary functions.
4. **Physical Access Control**: In high-security environments, physical access control mechanisms, such as biometric or smart card-based access, can restrict physical access to servers or systems storing biometric templates.

B. Implementing Secure Authentication Protocols

Secure authentication protocols are essential to ensure that individuals accessing biometric templates are indeed authorized. Some key considerations include[27]:

1. **Two-Factor Authentication**: Implementing two-factor authentication (2FA) alongside fingerprint recognition can enhance security. This requires users to provide a second authentication factor, such as a PIN, smart card, or mobile app.
2. **Secure Communication**: Ensure that data exchanged during the authentication process is encrypted to prevent eavesdropping and interception.
3. **Password Policies**: For systems using passwords in conjunction with biometric recognition, enforce strong password policies to prevent weak and easily guessable passwords.
4. **Token-Based Authentication**: In cases where fingerprint recognition is used for authentication, consider token-based systems that generate one-time codes for additional security.

C. Monitoring and Auditing Database Access

Monitoring and auditing are crucial aspects of access control and authentication in biometric systems:

1. **Audit Trails**: Maintain detailed audit logs of all access attempts, including successful and failed attempts. These logs can provide a record of who accessed the system and when.

2. **Anomaly Detection**: Implement anomaly detection systems to identify unusual or suspicious access patterns. For example, repeated failed login attempts can trigger alerts.
3. **Continuous Monitoring**: Use real-time monitoring to detect and respond to potential security breaches as they occur.
4. **Periodic Audits**: Regularly review access logs and conduct security audits to identify vulnerabilities and areas for improvement[28].

D. Examples of Access Control and Authentication Mechanisms

1. **Role-Based Access Control (RBAC)**: RBAC assigns roles to users and restricts their access to specific resources, including fingerprint templates. Administrators can define roles and associated permissions.
2. **Biometric Token Systems**: Biometric tokens, like smart cards or mobile apps, are used alongside fingerprint recognition for 2FA. The user must provide both the biometric scan and the token for access.
3. **Access Control Lists (ACLs)**: ACLs are lists of permissions attached to resources, specifying which users or system processes are granted access to the resource and what operations they can perform[27][28].
4. **Kerberos Authentication**: Kerberos is a network authentication protocol that allows nodes communicating over a non-secure network to prove their identity to one another while protecting the data being exchanged.
5. **OAuth and OpenID Connect**: These protocols are often used for authentication in web applications, allowing users to log in using existing credentials from social media or email accounts.

IX. Secure Hardware Modules

A. Overview of Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs)

Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs) are specialized hardware components that enhance the security of biometric systems[28]:

HSMs:

- HSMs are physical devices or secure appliances designed to protect and manage cryptographic keys and perform secure cryptographic operations.
- They are tamper-resistant and often include a secure microcontroller, a secure real-time clock, and various interfaces for communication with external systems.
- HSMs are widely used in biometric systems to safeguard sensitive biometric templates and cryptographic keys.

TEEs:

- TEEs are secure, isolated environments within a computing system, typically on a mobile device or within a microcontroller.
- They provide a secure execution environment for sensitive processes, isolating them from the main operating system.
- TEEs are used to protect biometric data during authentication and cryptographic operations on the device itself.

B. Benefits of Using HSMs and TEEs in Biometric Systems

1. **Key Protection**: Both HSMs and TEEs provide robust protection for cryptographic keys, preventing unauthorized access and key extraction.
2. **Data Isolation**: TEEs isolate sensitive processes and data from the main operating system, reducing the attack surface for potential threats.
3. **Tamper Resistance**: HSMs are designed to be tamper-resistant, making it extremely difficult for attackers to physically access and compromise the device[29].

4. **Secure Authentication**: TEEs can enhance the security of biometric authentication by performing biometric matching and template protection within the secure environment.
5. **Secure Transactions**: HSMs are commonly used for secure cryptographic operations during biometric authentication, ensuring the integrity and confidentiality of data during transactions.
6. **Regulatory Compliance**: Using HSMs and TEEs can help organizations meet regulatory requirements related to data security and encryption.

C. Real-World Applications and Use Cases

1. **Mobile Device Authentication**: TEEs are used in smartphones and tablets to protect fingerprint templates during device unlocking and secure authentication.
2. **Secure Banking**: HSMs are employed in the financial sector to secure cryptographic keys and transactions during biometric-based payments and banking operations[30].
3. **Healthcare**: TEEs can protect biometric data in healthcare applications, ensuring the privacy and security of patient information during authentication.
4. **Government Identity Programs**: HSMs and TEEs are integral to national identity programs that use biometrics for secure identification and access control.
5. **Secure Access Control**: HSMs and TEEs are used to secure access control systems in critical infrastructure facilities, ensuring only authorized personnel can gain access.

D. Challenges and Security Considerations

1. **Cost**: HSMs can be expensive to procure and implement, making them a significant investment for organizations.
2. **Compatibility**: Compatibility with existing systems and software can be a challenge when integrating HSMs or TEEs into biometric solutions.
3. **Key Management**: Proper key management is essential for both HSMs and TEEs. Mishandling keys can lead to security vulnerabilities.
4. **Physical Security**: Physical security is paramount for HSMs, as they are vulnerable to tampering and theft. Proper safeguards must be in place.
5. **Third-Party Trust**: When using third-party HSMs, organizations must trust the manufacturer to ensure the integrity of the device.
6. **Resource Usage**: TEEs can consume system resources, potentially affecting the performance of the device.

X. Biometric Template Revocation

A. The Concept of Template Revocation

Template revocation is a critical aspect of biometric security that addresses the need to invalidate and update compromised biometric templates stored in databases. The concept revolves around rendering exposed templates unusable for authentication while providing a mechanism to replace them with new, secure templates. Template revocation is essential in scenarios where biometric data may be compromised due to data breaches or other security incidents.

B. Methods for Revoking and Updating Compromised Templates

Several methods can be employed for revoking and updating compromised biometric templates[31]:

1. **Biometric Template Hashing**: Storing a secure hash of the biometric template rather than the raw template allows for template revocation by simply updating the stored hash. When a template is compromised, the hash can be replaced, rendering the compromised template useless for authentication.
2. **Template Update Policies**: Establish policies for regular template updates, regardless of compromise. This ensures that even if a template is not compromised, it is regularly updated to reduce the window of vulnerability.

3. **Biometric Re-enrollment**: Users can be required to re-enroll their biometrics periodically or after a compromise is detected. During re-enrollment, a new template is created, and the old one is revoked.
4. **Biometric Key Revocation**: If biometric data is used to derive cryptographic keys, revoking those keys can effectively disable the associated templates. The keys are then regenerated for use with new templates.

C. Ensuring That Exposed Templates Are No Longer Usable

Ensuring that exposed templates are no longer usable for authentication is critical. This can be achieved through a combination of the following methods[29]:

1. **Cryptographic Transformation**: Transform compromised templates using cryptographic techniques, making it infeasible to use them for authentication. Even if an attacker has the compromised template, it cannot be directly used for authentication.
2. **Template Invalidation**: Maintain a database of invalidated templates and ensure that any authentication request involving a compromised template is denied.
3. **Secure Deletion**: Physically delete or securely overwrite the compromised templates to prevent any recovery attempts.
4. **Biometric Key Rotation**: Rotate cryptographic keys associated with the compromised templates, ensuring that the old keys are no longer used for authentication.

D. Case Studies of Template Revocation in Biometric Databases

1. **Government Identity Programs**: National identity programs often implement template revocation mechanisms. When a citizen's biometric data is compromised, the compromised template is revoked, and the citizen is required to update their biometric data.
2. **Mobile Devices**: Smartphone manufacturers incorporate mechanisms to revoke and update biometric templates, especially for fingerprint recognition. When vulnerabilities or compromises are detected, updates are pushed to invalidate compromised templates.
3. **Healthcare Systems**: Healthcare providers may employ template revocation to ensure the privacy and security of patients' biometric data. Compromised templates can be invalidated and replaced.
4. **Access Control Systems**: Organizations and enterprises use template revocation in access control systems to prevent unauthorized access. When an employee's biometric data is compromised or when they leave the organization, their template is revoked and replaced[30].

XI. Data Encryption

A. Encrypting the Entire Biometric Database

Encrypting the entire biometric database is a fundamental security measure to protect the confidentiality and integrity of biometric data[31]:

1. **Encryption Algorithms**: Use strong encryption algorithms, such as AES (Advanced Encryption Standard), to encrypt the database. AES is widely recognized for its security and efficiency.
2. **Full Database Encryption**: Encrypt all data within the database, including biometric templates and associated metadata. This ensures that even if an attacker gains access to the database, the data remains unreadable.
3. **Database-Level Encryption**: Implement encryption at the database level, ensuring that data is automatically encrypted when inserted and decrypted when retrieved, reducing the complexity of encryption management.

B. Managing Decryption Keys Securely

Secure management of decryption keys is essential for data encryption in biometric databases[30][31]:

1. **Key Management Systems**: Implement a robust key management system that securely stores, rotates, and monitors decryption keys. Access to these keys should be tightly controlled.

2. **Hardware Security Modules (HSMs)**: Store decryption keys in HSMs to enhance their security and prevent unauthorized access or tampering.
3. **Role-Based Access**: Limit access to decryption keys to authorized personnel and administrators. Implement role-based access control to ensure that only those who need access have it.

C. Access Control and Encryption Best Practices

Access control and encryption go hand in hand to protect biometric data:

1. **Role-Based Access Control**: Define and enforce access rights based on user roles. Only authorized personnel should have access to the biometric database.
2. **Multi-Factor Authentication**: Implement multi-factor authentication (MFA) for database access. This adds an extra layer of security, requiring users to provide multiple forms of authentication, such as biometrics and a password.
3. **Audit and Logging**: Maintain detailed audit logs of all database access and encryption key usage. Regularly review these logs for anomalies and potential security breaches.
4. **Network Security**: Ensure that data transmitted to and from the database is also encrypted to protect against eavesdropping and interception.
5. **Regular Security Updates**: Keep encryption software and systems up to date with the latest security patches and updates to address vulnerabilities[32].

D. Examples of Encryption in Biometric Database Security

1. **Fingerprint Recognition on Smartphones**: Many modern smartphones use encryption to protect fingerprint templates stored on the device. The templates are encrypted to prevent unauthorized access.
2. **Government Biometric Databases**: National identity programs often encrypt biometric databases to ensure the security of citizens' biometric data. The entire database is encrypted to protect privacy and prevent data breaches.
3. **Healthcare Data**: Healthcare providers encrypt biometric data in electronic health records to meet regulatory requirements and safeguard patient privacy.
4. **Access Control Systems**: Organizations and enterprises that use biometric access control systems often encrypt biometric templates and access logs to protect against unauthorized access and data breaches.

XII. Anomaly Detection and Intrusion Detection Systems

A. The Role of Anomaly Detection in Preventing Unauthorized Access

Anomaly detection plays a crucial role in preventing unauthorized access to biometric databases:

1. **Baseline Establishment**: Anomaly detection systems establish a baseline of normal user behavior and database activity. This includes patterns of access, query frequency, and typical system behavior.
2. **Identification of Deviations**: Anomaly detection continuously monitors database activities and identifies deviations from the established baseline. These deviations can include unusual access patterns or unexpected queries.
3. **Early Warning**: When anomalies are detected, the system triggers alerts or warnings to security personnel. Early detection of unusual activity can prevent unauthorized access or data breaches.
4. **Preemptive Measures**: Security teams can take preemptive measures to investigate and mitigate potential security threats. This may involve blocking suspicious access or requiring additional authentication[33].

B. Implementing Intrusion Detection Systems for Monitoring Database Activities

Intrusion detection systems are vital for monitoring and protecting biometric databases:

1. **Continuous Monitoring**: Intrusion detection systems continuously monitor database activities, including login attempts, data access, and queries.

2. **Signature-Based Detection**: These systems use predefined signatures or patterns of known attacks to identify and respond to specific threats[26].
3. **Behavior-Based Detection**: Behavior-based detection looks for deviations from normal user behavior. It can identify new or previously unknown threats.
4. **Real-Time Alerts**: Intrusion detection systems generate real-time alerts when suspicious activity is detected, enabling rapid response to potential security breaches.
5. **Log Analysis**: Log analysis is a part of intrusion detection, allowing the system to analyze access and activity logs for unusual or unauthorized events.

C. Detecting and Responding to Security Breaches

Detecting and responding to security breaches is a critical function of both anomaly detection and intrusion detection systems:

1. **Alert Generation**: When a security breach or anomaly is detected, alerts are generated to notify security personnel or administrators.
2. **Incident Response**: Organizations should have well-defined incident response plans in place. These plans detail how to respond to security breaches, including actions to contain the breach, investigate the incident, and recover from it.
3. **Forensic Analysis**: After a breach, forensic analysis is conducted to understand the extent of the compromise, gather evidence, and identify the source of the breach.
4. **Mitigation**: Intrusion detection systems may take automated actions to mitigate threats, such as blocking IP addresses or suspending user accounts.
5. **Continuous Improvement**: Organizations use breach information to continuously improve security measures, patch vulnerabilities, and enhance anomaly detection to prevent future breaches[27].
6. **Legal and Regulatory Compliance**: Compliance with legal and regulatory requirements is crucial, as breaches may trigger reporting and notification obligations.
7. **Communication**: Transparent communication with affected parties, such as users whose biometric data may have been exposed, is essential to maintain trust[33].

Conclusion

Biometric recognition systems, with a focus on securing fingerprint templates, are pivotal in modern security and authentication. Protecting these templates is paramount due to the severe consequences of breaches. This investigation has explored a range of methods to safeguard fingerprint templates in biometric databases, thwarting unauthorized access and potential breaches. The study began by emphasizing the significance of biometric databases, highlighting the challenges and the need for robust security. It then delved into existing methods for secure storage and management of fingerprint templates, laying the foundation for advanced security measures. Cutting-edge techniques, including biometric cryptosystems, secure hashing, two-factor authentication, homomorphic encryption, and multi-party computation, were examined for their effectiveness in mitigating security risks. Each method offered unique advantages in enhancing the confidentiality and integrity of biometric data while introducing its own set of challenges. Access control and authentication protocols were identified as critical for limiting access to authorized personnel and continuous monitoring for potential anomalies. Secure hardware modules like Hardware Security Modules (HSMs) and Trusted Execution Environments (TEEs) emerged as essential components for safeguarding sensitive data. The concept of biometric template revocation was explored, providing methods to invalidate and update compromised templates, rendering them useless for subsequent authentication. Data encryption, at both the individual template and database levels, was recognized as a fundamental practice, with key management being integral. The deployment of anomaly detection and intrusion detection systems was seen as a vital layer of defense against unauthorized access and security breaches. These systems enable early detection of abnormal activity and facilitate a rapid, effective response. In summary, this investigation has illuminated the diverse array of methods available for securely storing and protecting fingerprint templates in biometric databases. By implementing a combination of these techniques and best practices, organizations can significantly enhance the security of their biometric systems, ensuring the confidentiality and integrity of sensitive biometric data. This

research aims to inform and guide both practitioners and researchers in the ongoing pursuit of robust biometric database security.

References

[1] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2d and 3d face recognition: A survey," vol. 28, no. 14. Elsevier, 2007, pp. 1885–1906.
[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of fingerprint recognition. springer, 2009.
[3] N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, "A real-time matching system for large fingerprint databases," vol. 18, no. 8. IEEE, 1996, pp. 799–813.
[4] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 14, no. 1, pp. 4–20, 2004.
[5] J. Wegstein, A semi-automated single fingerprint identification system. US Department of Commerce, National Bureau of Standards, 1969.
[6] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," vol. 43, no. 2. ACM, 2000, pp. 90–98.
[7] D. H. McMahon, G. L. Johnson, S. L. Teeter, and C. G. Whitney, "A hybrid optical computer processing technique for fingerprint identification," vol. 24,no. 4. IEEE, 1975, pp. 358–369.
[8] N. K. Ratha, S. Chen, and A. K. Jain, "Adaptive flow orientation-based feature extraction in fingerprint images," vol. 28, no. 11. Elsevier, 1995, pp.1657–1672.
[9] F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "Quality measures in biometric systems," vol. 10, no. 6. IEEE, 2012, pp. 52–62.
[10] L. Coetzee and E. C. Botha, "Fingerprint recognition in low quality images," vol. 26, no. 10. Elsevier, 1993, pp. 1441–1460.
[11] K. Karu and A. K. Jain, "Fingerprint classification," vol. 29, no. 3. Elsevier, 1996, pp. 389–404.
[12] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," Pattern Analysis and Machine Intelligence,IEEE Transactions on, vol. 20, no. 8, pp. 777–789, 1998.
[13] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. Mccabe, S. Janet, and K. Ko, "User's guide to nist biometric image software (nbis)," 2007.
[14] P. Grother and E. Tabassi, "Performance of biometric quality measures," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 29,no. 4, pp. 531–543, 2007.
[15] A. J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips," vol. 34, no. 2.Elsevier, 2001, pp. 255–270.
[16] K. Ito, A. Morita, T. Aoki, T. Higuchi, H. Nakajima, and K. Kobayashi, "A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints," in Image Processing, 2005. ICIP 2005. IEEE International Conference on, vol. 2. IEEE, 2005, pp. II–33.
[17] D. Zhang, F. Liu, Q. Zhao, G. Lu, and N. Luo, "Selecting a reference high resolution for fingerprint recognition using minutiae and pores," vol. 60, no. 3. IEEE, 2011, pp. 863–871.
[18] Q. Zhao, F. Liu, and D. Zhang, "A comparative study on quality assessment of high resolution fingerprint images," in Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE, 2010, pp. 3089–3092.
[19] R. M. Bolle, S. U. Pankanti, and Y.-S. Yao, "System and method for determining the quality of fingerprint images," Oct. 5 1999, uS Patent 5,963,656.
[20] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, "Kernel-based multimodal biometric verification using quality signals," in Defense and Security. International Society for Optics and Photonics, 2004, pp. 544–554.
[21] I. 29794-1:2009, "Information technology – biometric sample quality – part 1: Framework," October 2009.
[22] A. K. Jain and S. Z. Li, Encyclopedia of Biometrics: I-Z. Springer, 2009, vol. 1.
[23] E. Tabassi, C. Wilson, and C. Watson, "Nist fingerprint image quality," NIST Res. Rep. NISTIR7151, 2004.

[24] G. Li, B. Yang, and C. Busch, "Autocorrelation and dct based quality metrics for fingerprint samples generated by smartphones," in Digital Signal Processing (DSP), 2013 18th International Conference on. IEEE, 2013, pp. 1–5.
[25] Z. YAO, C. Charrier, and C. Rosenberger, "Utility validation of a new fingerprint quality metric," in International Biometric Performance Conference 2014. National Insititure of Standard and Technology (NIST), April 2014.
[26] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun, "A comparative study of fingerprint image-quality estimation methods," Information Forensics and Security, IEEE Transactions on, vol. 2, no. 4, pp. 734–743, 2007.
[27] L. Shen, A. Kot, and W. Koo, "Quality measures of fingerprint images," in IN: PROC. AVBPA, SPRINGER LNCS-2091, 2001, pp. 266–271.
[28] B. Lee, J. Moon, and H. Kim, "A novel measure of fingerprint image quality using the Fourier spectrum," in Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, ser. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, A. K. Jain and N. K. Ratha, Eds., vol. 5779, Mar. 2005, pp. 105–112.
[29] Z. Yao, J. Le Bars, C. Charrier, and C. Rosenberger, "Quality assessment of fingerprints with minutiae delaunay triangulation," in International Conference on Information Systems Security and Privacy (ICISSP), Feb 2015.
[30] N. K. Ratha and R. Bolle, Fingerprint image quality estimation. IBM TJ Watson Research Center, 1999.
[31] H. Fronthaler, K. Kollreider, and J. Bigun, "Automatic image quality assessment with application in biometrics," in Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on. IEEE, 2006, pp. 30–30.13
[32] L. Nanni and A. Lumini, "A hybrid wavelet-based fingerprint matcher," vol. 40, no. 11. Elsevier, 2007, pp. 3146–3151.
[33] J. D. Humphreys, G. Porter, and M. Bell, "The quantification of fingerprint quality using a relative contrast index," vol. 178, no. 1. Elsevier, 2008, pp.46–53.