Journal of Network Intelligence ©2025 ISSN 2414-8105 (Online)
Taiwan Ubiquitous Information Volume **10**, Number **4**, November **2025**

Secure and Verifiable CNN-oriented Face Template Protection

Cheng-Yuan Liu*

School of Computing and Data Science
Xiamen University, Selangor 43900, Malaysia
CST2109166@xmu.edu.my

Abubaker Wahaballa

Computer Science Department
Arab East Colleges, Riyadh 53354, Saudi Arabia
wahaballah@arabeast.edu.sa

*Corresponding author: Cheng-Yuan Liu

Received September 24, 2024, revised January 15, 2025, accepted June 19, 2025.

Abstract. *The application of convolutional neural networks in facial template protection has been widely studied, but existing schemes usually have security vulnerabilities, especially face challenges in achieving non-repudiation, and cannot meet high security and compliance requirements.This study proposes a face template protection scheme that combines BLS signature with SHA3-512 hash algorithm. The aggregation function of BLS signatures has been elegantly utilized to optimize storage efficiency and verification time during the verification of multiple signatures. By comparison, the scheme has advantages in ensuring the integrity and tamper resistance of biometric templates, and is suitable for biometric systems that require high security and privacy protection.*

Keywords: deep convolutional neural network , privacy protection , BLS , SHA3-513

1. Introduction.

1.1. Background.

With the widespread application of face recognition technology in security authentication and privacy protection, it is crucial to protect the security and integrity of face template data. Currently, Convolutional Neural Networks have become a key technology in face recognition systems due to their strong capability in extracting facial features and generating stable feature vectors. By applying a series of convolutional and pooling operations, CNNs are able to capture complex patterns in facial images, making them ideal for biometric template generation and protection. And in terms of security, the SHA3-512 hash algorithm is widely used for the encryption protection of biometric data due to its strong anti-collision and data integrity protection capabilities. However, with the continuous development of information technology and the strict implementation of laws and regulations (such as the General Data Protection Regulation), the protection mechanism that relies solely on the hash algorithm can no longer meet the growing security and non-repudiation requirements [1,2]. Therefore, based on the existing SHA3-512 hash algorithm, this paper introduces the BLS signature algorithm to further enhance the non-repudiation and legal compliance of the face recognition system.

In 2017, Equifax, one of the world's largest credit reporting agencies, experienced a massive data breach, compromising the sensitive information of 143 million American citizens shown in Figure 1. Despite using encryption technology, Equifax lacked an effective non-repudiation mechanism, making it difficult to trace the specific intrusion path and access records. This deficiency hindered the company's ability to defend itself legally, leading to over $700 million in financial losses and severe reputational damage. This incident shows the critical role of non-repudiation in information security, as even encrypted data can cause significant legal and financial risks without it [3].

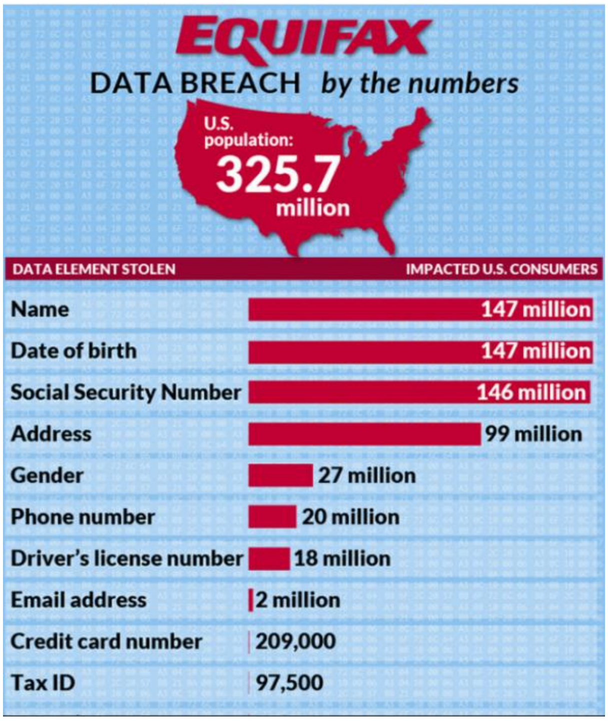
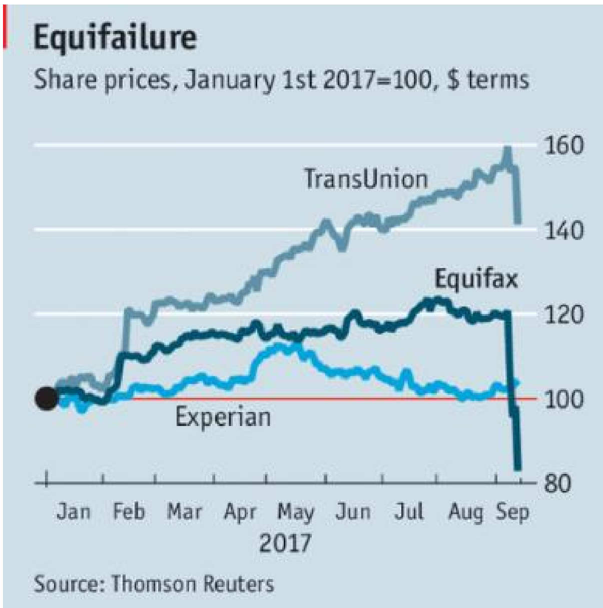


FIGURE 1. Amount of data leaked



Source: Thomson Reuters

FIGURE 2. Economic loss

Figure 2 shows another example occurred in India, where Aadhaar, a biometric system for national identity authentication, suffered from widespread identity fraud due to its lack of non-repudiation, which led to frequent identity theft, misuse of personal data, and raised alarm among the population about system security and the government [4].

These examples demonstrate the importance of non-repudiation, especially in scenarios involving sensitive data. While SHA3-512 effectively protects data integrity, it falls short in preventing repudiation issues. Therefore, this paper proposed to enhance the non-repudiation of the face recognition system by integrating the BLS signature algorithm, aiming to implement its security [5].

1.2. **Research Motivation.** In today's information security environment, it is very necessary to ensure the non-repudiation and authenticity of biometric data. Although SHA3-512 can effectively prevent data tampering, it does not guarantee non-repudiation. BLS signature can provide non-repudiation, and has the advantages of strong aggregate signature ability and efficient verification, which can provide significant help in the field of biometric data protection. This study aims to combine BLS signatures with SHA3-512 to enhance the security and non-repudiation of face templates, meet strict legal compliance requirements and protect face template data.

1.3. **Contribution of this paper.** This paper innovates on the existing face template protection technology and adds the BLS signature algorithm to the original SHA3-512 hash algorithm to enhance the security and non-repudiation of the system.

The integration of the BLS signature algorithm into face template protection, as proposed in this paper, represents a novel approach that has not been widely explored in current research. Most existing studies focus on other biometric template protection methods, such as fuzzy commitment or cancellable biometrics, which primarily ensure template security and privacy. The main innovation of this paper lies in applying the BLS signature algorithm to face template protection, where the hashed binary code is BLS-signed and sent to the server for verification. Hashing ensures data security, while the signature confirms the face image's legitimacy, protecting against tampering and providing non-repudiation.

In terms of the implementation of the specific code, I successfully reproduced the code of the original research using SHA3-512 for face template protection, and introduced the BLS signature algorithm on this basis. The Python code was implemented and successfully run, proving the feasibility of combining BLS signature with SHA3-512. Although non-repudiation was not verified through physical experiments due to technical and equipment limitations, the inherent properties of the BLS signature algorithm theoretically guarantee non-repudiation. Additionally, the aggregation feature of BLS signatures was leveraged to minimize storage requirements and accelerate verification, enhancing system security and offering new directions for future biometric data protection applications.

2. Preliminary knowledge.

2.1. **Research on the protection of original face templates.** In the referenced study, the authors used the SHA3-512 hash algorithm to protect face template data [6]. In the specific implementation, we divide the whole process into two stages. The first stage is the registration stage. First, facial features are extracted through CNN, and a random 256-bit or 1024-bit binary code is assigned to each registered user to ensure that the binary code of each user is unique. Then the extracted facial features are mapped to the binary code of the corresponding user through robust mapping. Then, these binary codes are used to train the model to obtain the trained model. Finally, these binary features are hashed using SHA3-512 to generate a hash value of fixed length. We combine the hash values obtained from multiple copies of the same person used in the registration stage into a set.

In the second stage, which is the verification stage, we use the trained model to predict the verified face and obtain its corresponding binary code. Then, we hash it before transmission to obtain its corresponding hash value. Next, the hash value is transmitted to the server and compared with the hash value of the corresponding user in the set to identify the user [6].

This SHA3-512-based protection scheme performs well in preventing data tampering, but it is insufficient in achieving non-repudiation due to the lack of support for digital signatures.

2.2. **SHA3-512 hash algorithm.** SHA3-512 is a widely used cryptographic hash algorithm ,it is widely used to protect biometric data, to prevent data from being tampered with or forged. The working principle of SHA3-512 is based on the Keccak algorithm, which generates a fixed-length hash value through multiple rounds of compression function operations. Although it performs well in providing data integrity, it has shortcomings in dealing with achieving non-repudiation [7, 8].

2.3. **BLS signature algorithm.** BLS signature algorithm is based on elliptic curve bilinear pairings, which can aggregate multiple signatures and verify them efficiently [9]. In biometric systems, integrating BLS signatures can greatly enhance data non-repudiation and ensure the authenticity of data sources [5].

2.4. **Characteristics and reasons for choosing BLS signatures.** The BLS signature algorithm's strong aggregation capability allows multiple signatures to be combined into one, simplifying data storage and verification processes. During registration, face data is augmented to produce multiple images, each generating hash-signature pairs that can be efficiently aggregated [9–11]. Hu et al. 's asynchronous aggregation algorithm has shown outstanding performance in model training and efficiency improvement. Similarly, through the aggregation function of BLS signature, this paper effectively reduces the storage requirements and computational complexity of the system in the verification process of multi-signatures [12].

BLS signature also supports batch verification, which can Ensure high system efficiency in real-time scenarios where multiple templates need to be verified at the same time [10]. In reality, the recognition of face templates will occur in many places at the same time, and a large amount of data will be transmitted to the database for recognition, at which time BLS is very advantageous.

Additionally, BLS signatures provide robust security, leveraging elliptic curve bilinear pairing to ensure data integrity and non-repudiation, compensating for the limitations of SHA3-512 in these areas [9].

3. Proposed solution.

3.1. **Brief introduction of the solution.** In this study, we offer a face template protection scheme that integrates the BLS digital signature algorithm to enhance data security and non-repudiation in face recognition systems. This approach take advantage of advanced digital signature technology on top of the existing face template data, ensuring that user face template data remains secure and non-repudiable during transmission [6].

The core of the scheme was to map the face image to a unique binary code for each user, and then use SHA3-512 to hash these codes, and apply BLS to sign them. Finally, the hash value and signature were used for face recognition verification. This ensures that each binary code is uniquely signed and verifiable, guaranteeing data integrity and non-repudiation. The process includes:

(1) Face Image Acquisition: Collect face images from users.

(2) Binary Code Assignment: Assign a random, unique 256-bit or 1024-bit binary code to each registered user.

(3) Image Processing and Robust Mapping: Extract features from the collected face image and map them to a binary code.

(4) Hash Processing: Hash the mapped binary code using SHA3-512.

(5) Data Signature: Apply the BLS signature algorithm to the hashed binary code.

(6) Storage and Verification: Store the signature and hash in a secure database. For verification, the hash and signature are checked to confirm the integrity and authenticity of the data [6].

3.2. **Specific structure.**

3.2.1. **Flow chart**. Figure 3 shows the flowchart of the whole process

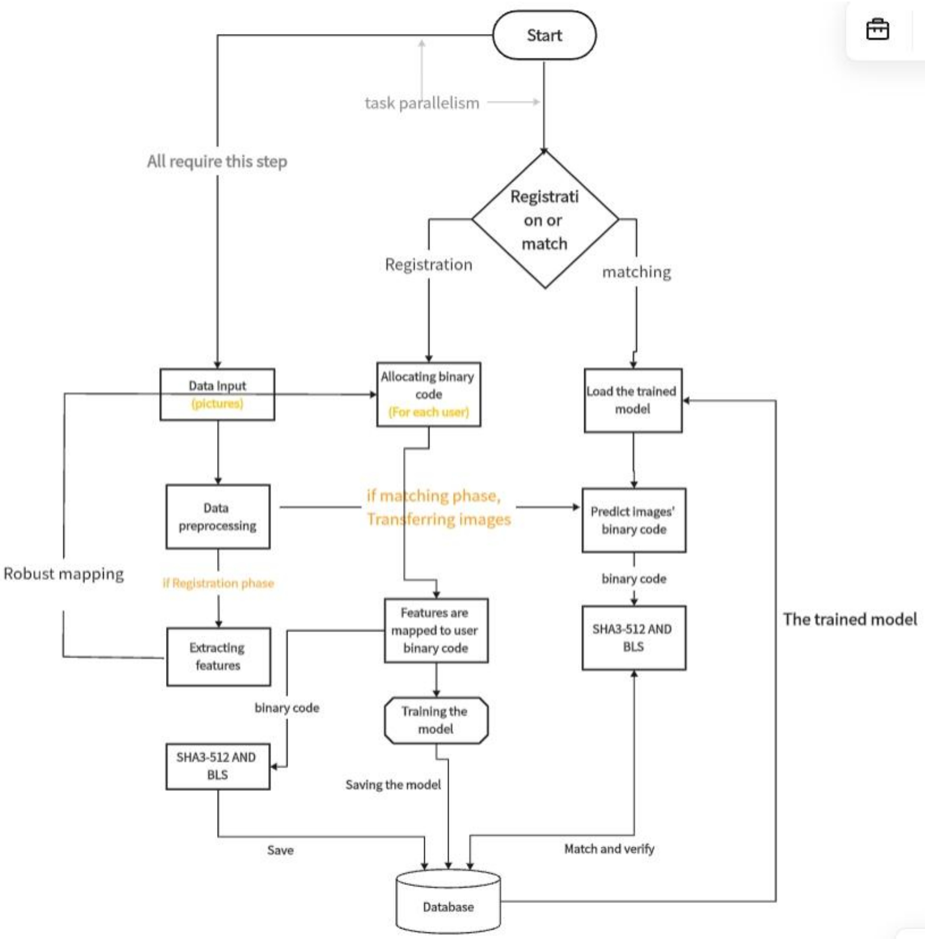


FIGURE 3. Structure construction

3.2.2. **Sensors**. The sensor captures the facial image of each user, some of which are used for registration and the rest for verification.

3.2.3. **Preprocessing**. Face Detection: The face detection algorithm is used to identify the face in the image and determine the location of the face in the image, so as to perform further analysis and feature extraction. The detected face image will be resized to 224*224 pixels and saved [13].

Data augmentation is an effective way to increase the number of image samples for each user. The specific steps include 1. Use the image data generator API provided by Keras to perform a series of image transformation operations on each face image. 2. For each transformed image, perform a systematic cropping operation to extract all possible image regions of size $n * n$, and obtain $(m - n + 1) \times (m - n + 1)$ crops. Subsequently, these crops are resized to $m * m$ size again. 3. Through the above data augmentation steps, $5 \times (m - n + 1) \times (m - n + 1)$ training samples are finally generated for each original face image [14].

3.2.4. **Binary code generation and assignment.** During user registration, we generate a unique, high-entropy binary code for each user, independent of the original biometric data (face image). This ensures the binary code's uniqueness and randomness. The code is exclusively used to train the deep convolutional neural network. Once registration is completed, these codes are not stored in unencrypted form and are not visible to the user [6].

3.2.5. **Deep Convolutional Neural Network (CNN)**. In order to learn a robust mapping from a user's facial image to a unique binary code, we use a deep CNN. This network ensure high matching performance by maximizing differences between users and minimizing differences within users.

Figure 4 and Figure 5 show the deep CNNs that map face images to 256-bit and 1024-bit binary codes, respectively

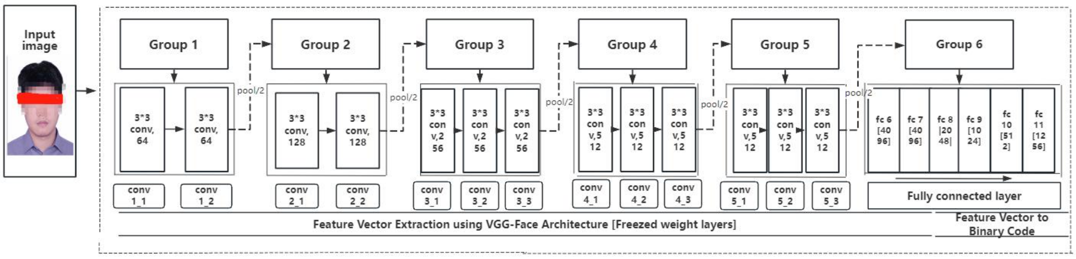


Figure 4. 256-bit binary codes

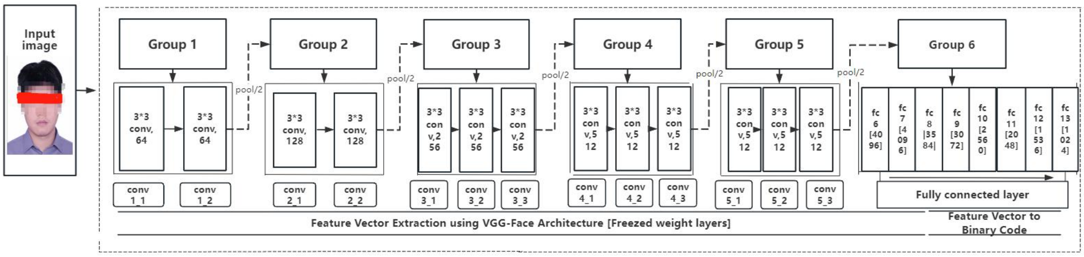


Figure 5. 1024-bit binary codes

1) Feature vector extraction network. We use the pre-trained VGG-Face CNN for feature extraction, which enhances the quality of the extracted features and improves the model's recognition capability.

2) During feature extraction, the first 15 layers of VGG-Face CNN—comprising 13 convolutional layers and 2 fully connected layers—process the input image to extract

highly discriminative facial features. These features are then compressed into a compact 4096-dimensional feature vector by the fully connected layer (fc7) [14].

3) Feature vector to binary code mapping network and its training. During the registration stage, the deep CNN learns to map the extracted feature vector (representing the user's facial image) to a designated binary code, using a sigmoid activation function at the end of the network. To prevent overfitting, dropout with a rate of 0.25 is applied during training [15].

In the user verification stage, the trained CNN predicts the binary code assigned during registration when a user's facial image is input. A threshold operation is then applied to the network output, converting each neuron's output to 0 (for values ≤ 0.5) or 1 (for values > 0.5), generating the binary code [16]. This mapping network is optimized to maximize differences between users while minimizing variations within a user, enhancing the system's matching performance and security [14].

3.2.6. **Hashing (SHA3-512).** The purpose of this step is to protect the data of the face template. We use SHA3-512 to convert the binary code of each user in the registration phase into a 512-bit encrypted hash to ensure the security of the face template. During the registration phase, the SHA3-512 hash value of each binary code is stored in the database. In the verification phase, the trained deep CNN generates binary codes, which are then hashed by SHA3-512 for matching [7].

3.2.7. **Digital Signature (BLS Signature).** We take the hash value as input, which is further used to generate BLS signatures to enhance the non-repudiation of the system.

BLS signature is based on elliptic curve bilinear pairing technology, which is an efficient digital signature algorithm. To complete the signature of this step, first, the 512-bit hash value h generated by SHA3-512 is mapped to a point H in the elliptic curve group G. We denote by *HashToPoint* a mapping function for converting the hash value to a point on the elliptic curve, and this process can be expressed as $H = \mathit{HashToPoint}(h)$ [9].

We then sign H with the user's private key sk to generate a signature σ.

Since each face template usually generates multiple hash values (each face template image will generate multiple images after data enhancement), a corresponding signature needs to be generated for each hash value. Assume that for a certain user, n different hash values $h_1, h_2, \ldots, h_n$ are generated,and n corresponding signatures $\sigma_1, \sigma_2, \ldots, \sigma_n$ are generated through the above process.

An important feature of BLS signatures is their signature aggregation capability. Through the aggregation function, n signatures can be combined into a single signature σ_{agg}, which can be expressed by the formula $\sigma_{\text{agg}} = \prod_{i=1}^{n} \sigma_i = \prod_{i=1}^{n} H_i^{\text{sk}}$ [9–11].

This aggregate signature σ_{agg} can still verify its validity through the original signature verification process, and can represent all generated hash values at the same time. This method not only saves storage space, but also improves the verification efficiency of the system. Especially when processing large-scale face templates in real time, it can implement good performance and security of the system.

Through this process, the combination of BLS signature technology and SHA3-512 provides a strong security guarantee for the protection of face templates, while also ensuring the non-repudiation of the data source [9–11].

3.2.8. **Matcher.** Visually speaking, the whole process is shown in Figure 6. In the details, during the verification phase, the matching module receives two biometric templates, T_x (protected face template) and T_y (query template), and outputs a match score S of true or false nature. In order to adjust the false acceptance rate and false rejection rate of the biometric recognition system, multiple data augmentation images are generated for each verification image. Then, the binary code corresponding to each augmented image is predicted using the CNN trained in the enrollment phase.

First, each predicted binary code is hashed with SHA3-512 to generate a set of hash values H. The preliminary matching process compares each hash value in H with the hash values stored in the database. If a matching hash value is found, it indicates that T_y may match T_x, meaning that they are from the same person.

In the verification process of the BLS signature, the aggregate signature σ and the public key set $\mathrm{pk}_1, \mathrm{pk}_2, \ldots, \mathrm{pk}_n$ are first obtained from the database. Enter a single signature σ_i and news M_i, to hash $H(M_i)$. Next, the accuracy of this single signature is verified by checking $e(\sigma_i, g) = e(H(M_i), \mathrm{pk}_i)$. This equation verifies that the signature matches the message [17].

Next it is verified that the aggregate signature contains that single signature. Compute the bilinear pairing $e(\sigma, g)$ of the aggregate signature and compare it with the bilinear pairing product of all message hashes and the corresponding public key:

$$e(\sigma, g) = \prod_{i=1}^{n} e(H(M_i), \mathrm{pk}_i)$$

. If the equation holds, it means that this single signature is involved in the generation of the aggregate signature [17].

If the preliminary hash match is successful, the system will further verify by comparing the hash value generated by the augmented image of T_y with the aggregate hash value stored in T_x. This aggregate hash value is composed of the hash values of all augmented images of the protected template and utilizes the aggregation property of BLS signatures.

The final matching score S is determined by the number of hashes in H that match the stored aggregate hash value, and is scaled according to the cardinality of H [18]. Through this two-step verification process, the system takes advantage of the SHA3-512 hash and BLS signature aggregation to ensure verification efficiency and higher security.

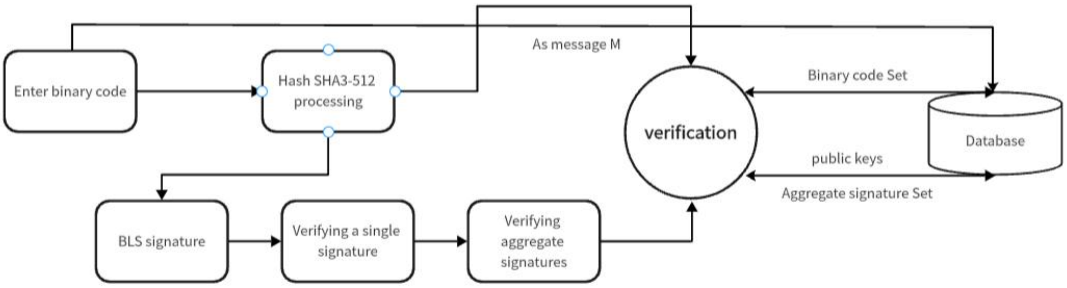


Figure 6. Verification process

4. **Analysis and comparison.** In this section, we conduct a detailed comparative analysis of the biometric template protection scheme based on BLS signature proposed in this study and the latest research results shown in Table 1. Demonstrate the advantages of this solution through multiple dimensions such as function, performance and security.

4.1. **Function comparison.** Functionally, this research significantly enhances the non-repudiation of data by introducing BLS signatures, while the above research mainly focuses on the resistance and privacy protection of templates.ignatures, digital signatures use encryption technology to generate signatures using the signer's private key, and only the corresponding public key can verify the authenti

Since non-repudiation is the basic property of digital scity of the signature. Therefore, signers cannot deny their signature behavior on the signed content. Therefore, this study did not prove and compare its non-repudiation through experiments.

Table 1. Function Comparison Table

Function	**This study**	**Deep Learning in the Field of Biometric Template Protection: An Overview [19]**	**A New Protection Scheme for Biometric Templates based on Random Projection and CDMA Principle [11]**	**Face Template Protection using Deep Convolutional Neural Network [6]**	**MLP-Hash: Protecting Face Templates via Hashing of Randomized Multi-Layer Perceptron [20]**
Non-repudiation	Strong (BLS signature guarantee)	Medium (relies on unbiometrics)	Medium (based on random projection and CDMA)	Weak (SHA3-512 hashes only)	Medium (the hash mechanism that depends on the random weight of the MLP is not completely prevented from denying)
Tamper resistance	Strong (signature bound to template)	Strong (template not reversible)	Strong (nonlinear conversion combined with CDMA)	Strong (SHA3-512 hashing)	Medium (with a random weight hash protection template, but for reverse engineering is certain vulnerability)
Privacy protection	Strong (BLS signature combined with hashing)	Strong (cancelability protects privacy)	Strong (privacy preserving random projection)	Medium (relies on hashing for privacy protection)	Strong (randomized multilayer perceptron hash implements privacy protection, but relies on the randomness of specific users)

4.2. **Performance comparison (theoretical).** In terms of performance, this study utilizes the aggregation function of BLS signatures, showing significant storage and computing efficiency advantages, especially when processing large-scale data, compared to other signature methods.

5. Conclusion.

This paper proposes a biometric template protection scheme based on BLS signature to enhance the non-repudiation and security of the face recognition system. By combining the SHA3-512 hash algorithm with BLS signatures, it not only ensures data integrity, but also solves the problem of insufficient non-repudiation in traditional methods. This paper theoretically verifies the significant advantages of this scheme in terms of security, as well as the advantages of BLS in storage efficiency and verification speed compared to other signature methods. It also conducts a detailed comparative analysis with several related studies in recent years, further proving the effectiveness and innovation of this solution.

For future work, the solution can be deployed and tested in real-world scenarios to collect performance data for further optimization and validation.Additionally, incorporating advanced encryption techniques like Revocable Attribute-Based Encryption [21] can improve fine-grained access control in biometric systems, enhancing scalability and security.

Exploring improved key agreement schemes [22] may bolster system authentication, while adopting techniques such as forward privacy [23] could enhance privacy during data storage and retrieval. These methods would enable broader adoption in biometric systems, enhancing information security and privacy protection.

REFERENCES

[1] E. Bertino, L. Khan, R. Sandhu, and B. Thuraisingham, "Secure knowledge management: confidentiality, trust, and privacy," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 36, no. 3, pp. 429–438, 2006.

[2] P. Voigt and A. Von Dem Bussche, *The EU general data protection regulation (GDPR).* Springer eBooks, 2017.

[3] B. News, "Massive equifax data breach hits 143 million," https://www.bbc.com/news/business-41192163, September 7 2017.

[4] F. Li, "Science and technology lament! the world's largest biometric system is killing poor indians," Business Week, October 18 2019. [Online]. Available: https://www.businessweekly.com.tw/international/blog/3000499

[5] I. B. S., *BS ISO/IEC 20248. Information technology: Automatic identification and data capture techniques. Digital Signature Data Structure Schema.* ISO/IEC, 2021.

[6] A. K. Jindal, S. Chalamala, and S. K. Jami, "Face template protection using deep convolutional neural network," in *IEEE CVPR Workshops*, 2018, pp. 541–548.

[7] M. J. Dworkin, "Sha-3 standard: Permutation-based hash and extendable-output functions," NIST, Tech. Rep., 2015.

[8] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "The keccak sha-3 submission to nist (version 3)," National Institute of Standards and Technology, Tech. Rep., 2011. [Online]. Available: https://keccak.team/files/Keccak-submission-3.pdf

[9] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[10] F. Baldimtsi, K. K. Chalkias, F. Garillot, J. Lindstrom, B. Riva, A. Roy, M. Sedaghat, A. Sonnino, P. Waiwitlikhit, and J. Wang, "Subset-optimized bls multi-signature with key aggregation," *IACR Cryptology ePrint Archive*, 2024. [Online]. Available: https://ia.cr/2023/498

[11] A. Lahmidi, K. Minaoui, C. Moujahdi, and M. Rziza, "A new protection scheme for biometric templates based on random projection and cdma principle," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10, 2021.

[12] H. Xiong, H. Yan, M. S. Obaidat, J. Chen, M. Cao, S. Kumar, K. Agarwal, and S. Kumari, "Efficient and Privacy-Enhanced asynchronous federated learning for multimedia data in edge-based IoT," *ACM Transactions on Multimedia Computing Communications and Applications*, 8 2024. [Online]. Available: https://doi.org/10.1145/3688002

[13] L. Liu, W. Ouyang, X. Wang, P. Fieguth, J. Chen, X. Liu, and M. Pietikäinen, "Deep learning for generic object detection: A survey," *International Journal of Computer Vision*, vol. 128, no. 2, pp. 261–318, 2019.

[14] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, no. 1, 2011.

[15] K. Bobkowska, K. Nagaty, and M. Przyborski, "Incorporating iris, fingerprint, and face biometric for fraud prevention in e-passports using fuzzy vault," *IET Image Processing*, vol. 13, no. 13, pp. 2516–2528, 2019.

[16] G. E. Hinton, N. Srivastava, A. Krizhevsky, I. Sutskever, and R. R. Salakhutdinov, "Improving neural networks by preventing co-adaptation of feature detectors," *arXiv*, 2012. [Online]. Available: https://doi.org/10.48550/arxiv.1207.0580

[17] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "A survey of two signature aggregation techniques," pp. 1–10, Summer 2003. [Online]. Available: https://crypto.stanford.edu/ dabo/pubs/papers/aggsurvey.pdf

[18] R. K. Pandey, Y. Zhou, B. U. Kota, and V. Govindaraju, "Deep secure encoding for face template protection," in *IEEE CVPR Workshops*, 2016, pp. 34–42.

[19] C. Rathgeb, J. Kolberg, A. Uhl, and C. Busch, "Deep learning in the field of biometric template protection: An overview," *arXiv*, March 5 2023. [Online]. Available: https://arxiv.org/abs/2303.02715

[20] H. O. Shahreza, V. K. Hahn, and S. Marcel, "Mlp-hash: Protecting face templates via hashing of randomized multi-layer perceptron," in *2023 31st European Signal Processing Conference (EUSIPCO)*. IEEE, 2023.

[21] H. Xiong, Z. Qu, X. Huang, and K.-H. Yeh, "Revocable and unbounded attribute-based encryption scheme with adaptive security for integrating digital twins in internet of things," *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 10, pp. 3306–3317, 2023.

[22] T.-Y. Wu, T. Wang, Y.-Q. Lee, W. Zheng, S. Kumari, and S. Kumar, "Improved authenticated key agreement scheme for fog-driven iot healthcare system," *Security and Communication Networks*, vol. 2021, p. 6658041, 2021.

[23] C.-M. Chen, Z. Tie, E. K. Wang, M. K. Khan, S. Kumar, and S. Kumari, "Verifiable dynamic ranked search with forward privacy over encrypted cloud data," *Peer-to-Peer Networking and Applications*, pp. 1–15, 2021.