A New Protection Scheme for Biometric Templates based on Random Projection and CDMA Principle

Ayoub Lahmidi[1], Khalid Minaoui[2], Mohammed Rziza[4]
LRIT Laboratory, Associated unit to CNRST (URAC29),
IT Rabat Center Faculty of Sciences in Rabat,
Mohammed V University, Rabat, Morocco

Chouaib Moujahdi[3]
Scientific Institute
Mohammed V University
Rabat, Morocco

Abstract—**Although biometric technologies have revolutionized the world of communication and dematerialized exchanges, authentication by biometrics still has many limitations, particularly in terms of privacy concerns, due to the various potential threats to which biometric templates are subject. The existence of these vulnerabilities has created an enormous need for biometric data protection. Indeed, several protection schemes have been proposed, which are normally supposed to offer certain guarantees, including the confidentiality of the collected personal data and the reliability of the recognition system. The challenge for all these techniques is to achieve a trade-off between performance accuracy and robustness against vulnerabilities, which is not always obvious. In this paper, we propose a theoretical protection model dedicated to biometric authentication systems. The objective is to ensure a high level of security for the stored reference data in such a way that it complies with the non-invertibility and revocability properties. The main idea is to incorporate a discretization tool, namely the spread spectrum technology and in particular the Code Division Multiple Access (CDMA), into a biometric system based on Random Projection. We introduce and demonstrate the proposed scheme as a non-invertible transform, while proving its effectiveness and ability to meet the requirements of revocability and unlinkability.**

Keywords—Biometric template; security; authentication; CDMA; random projection

I. Introduction

In a society where the risk of fraud continues to increase, the security of individuals within authentication systems has become a major concern. Despite the development in this sector, which has experienced a qualitative leap in terms of surveillance and access control, the traditional authentication systems, namely those based on knowledge (use of passwords) or possession (use of badges and keys) are ineffective against attacks of fraud and identity theft. Over the years, this kind of system has shown great weaknesses because of its inability to differentiate between an authorized person and an impostor who fraudulently acquires knowledge of the authorized person. Thus, the use of an authentication system that was both efficient and secure was essential, hence the emergence of biometric authentication.

In just a few years, biometrics has become the only way for authentication to guarantee rigorous access control since it is based primarily on the morphological and behavioral aspects specific to each person. Indeed, biometric systems exploit the physical characteristics (such as fingerprints, face, iris, etc.) or the behavioral aspects (such as voice, writing, the rhythm of typing on a keyboard, etc.) to construct an identity representing an individual. Commonly called modalities, these biometric identifiers are often universal, unique to each person, and permanent in time [1]. Moreover, they ensure great robustness since it is very difficult for them to be lost, forgotten, stolen, copied, or falsified. The main objective of biometrics is to provide a more secure alternative to traditional access control systems, in the sense that it avoids the use of a large number of complex passwords, concerns about loss, theft and other falsifications of keys [2].

Although biometric authentication systems provide a much higher level of security compared to traditional systems, they are not safe from tampering. The use of this kind of system has given rise to new challenges related to the protection of biometric data [3]. Biometric information is generally considered sensitive since it is specific to each individual, and through which it can identify the owner. The inappropriate use of biometrics may involve risks to respect for fundamental rights and freedoms. Some risks of privacy violation are presented as follows:

- Absence of secrecy: Biometric data can expose very sensitive information, simply because the data are publicly available, so they can serve as a basis for unjustified discrimination.
- Traceability: the tracking and monitoring of an individual identified by the same biometric data across different databases, to perform profiling of the user.
- Irrevocability: In case of a compromise of the reference biometric template, it is impossible to revoke it because of its uniqueness.
- Function creep / Misuse: extending a specific use of the biometric identifier for another unintended or unauthorized use.

The issue of preserving biometric data deserves special attention to ensure respect for privacy when using biometric data. It should be noted that despite the advantage of biometric features being virtually impossible to steal, and difficult to guess by a tier, biometric systems are still vulnerable to attacks that target this kind of system [4]. Indeed, any component of the biometric system may be susceptible to a specific attack: the sensor, the feature extractor, the biometric reference templates stored and the final decision [5, 6]. The storage and security of reference data remain among the most crucial issues for a biometric system, as it can lead to serious security and invasion problems compared to other modules such as:

- The handling sensitive information.
- The regeneration of the original biometrics from the stored template.
- The construction of a falsified biometric sample.
- The secondary use of biometric information (surveillance, discrimination, etc.).
- The inability to revoke the biometric identifier when identity theft occurred.

These tasks require imperative attention, especially in the absence and necessity of an effective protection mechanism based on biometric templates. This has undoubtedly motivated us to multiply our thoughts on this point. The challenge is to design, implement and use a cancellable biometric system that improves authentication services without unduly compromising privacy.

Each protection approach for biometric templates must be designed with strong security analysis while taking into account the scenarios where the risk of fraud threatens the stored templates, and must also offer the possibility of revoking a biometric data set in the case of interception [7]. As specified by Jain et al. [3], template protection techniques are generally divided into two families: (i) Feature Transformation and (ii) Biometric Cryptosystem. The common feature of these methods is that they do not directly store the raw biometric data in databases, but rather they are either stored on an external medium or stored after an alteration due to a transformation function.

The principle of feature transformation approach [3, 8] consists in transforming the original biometric template X by using a function $\mathfrak{F}$ which depends on a random data K. This specific information that should normally be secret is assigned to each legitimate user of the system. Thereafter, only the transformed template $\mathfrak{F}(X,K)$ will be stored. At authentication, the query features X' will be transformed in the same way using the same transformation function $\mathfrak{F}$, then is directly matched with the reference template. Authentication will succeed if $\mathfrak{F}(X',K)$ is sufficiently close to $\mathfrak{F}(X,K)$ using some measures of similarity. To guarantee the notion of revocability in case of compromise of the transformed data, it is sufficient to change the parameters of the transformation function, and this is done by directly replacing the user key K, the reason for which biometric transformations generally use secret data in addition to the original biometric data [9, 10]. The choice of the transformation function remains the paramount element in the design of a protection approach belonging to this category. The function used can be either invertible in case of *Salting*, where security is relative to the knowledge of the transformation parameters [11], or is non-invertible when a one-way function is applied to the template [12, 13], in this case, it is computationally infeasible to reconstruct the original template, even if the transformation parameters are known.

Biometric cryptosystems [14, 15] provide the means to adapt cryptographic protocols to biometric data which are very sensitive and intrinsically noisy. The use of this kind of system consists either in securing the cryptographic keys using the biometric features or else indirectly generating cryptographic keys from biometric features. They are also based on user-linked help data extracted from the biometric feature vector, which is needed during matching to extract the cryptographic key from the query biometric features. The helper data is public information that should not, in any case, reveal any significant information about the original biometric template. Biometric cryptosystems in their turns can be classified into key generation schemes, where binary keys are directly created from the acquired biometrics, and key binding schemes, which store information obtained by combining biometric data with randomly generated keys.

All evoked protection schemes have their advantages and limitations in terms of performance, accuracy, and robustness, but generally do not yet respond effectively to all desired requirements. The difficulty is that the transformation is in most cases entirely or partially invertible. Moreover, the desired criterion of revocability is not obvious to achieve without creating other risks. This is why we are motivated to design a generic transformation, in which the protected reference templates will be easy to revoke, difficult to reverse, and will not degrade performance. In this paper, we present a demonstration of a new protection model for reference templates by adapting the security aspect of a multiplexing technique defined as spread spectrum called *Code Division Multiple Access (CDMA)* within a system based on random projection. The proposal aims to verify and prove the identity of an individual only through its provided identifier while ensuring agreement with the properties of revocability, unlinkability, and non-invertibility. This paper is organized as follows. Section 2 presents related works. Section 3 is devoted to preliminary knowledge. Section 4 describes in detail the steps required to build the templates. Analysis and discussion of the revocability, diversity, and non-invertibility requirements produced by our proposal are given in Section 5. Finally, Section 6 is dedicated to the conclusion and future work.

II. Related Work

In biometric protection schemes, privacy preservation is related to the protection of the biometric templates. Ideally, as defined in several references [16], these schemes are designed to meet the requirements of non-invertibility, unlinkability, and revocability. Among the solutions that have been proposed by the research community to further protect the biometric templates, we can quote:

Ratha et al. [17] have proposed an interesting solution. The main idea is to apply geometric transformations on the fingerprint minutiae representation. Three types of transformations have been tested: Cartesian, polar and functional. This solution offers great security, as it is difficult to recover the original minutiae representation from the transformed template. However, these transformations increase the rate of intra-class variations in the protected representation, which considerably degrades the performance.

Tulyakov et al. [18] made use of symmetric hash functions as means of protecting fingerprint templates. The hash functions were constructed from the minutiae locations, considering the random shifting of the minutiae during the acquisition phase. The security of the generated templates is improved in [19] using a combination of various hash functions. However, it seems that the enhanced approach also suffered from computational complexity.

Wang and Hu [20], proposed a non-invertible transformation that can be applied to vectors derived from pair-minutiae. The proposal is an infinite-to-one mapping approach which is able to generate revocable templates. The performance of the system is very promising except that the consistency of the user key matrix leads to certain storage problems.

Moujahdi et al. [21] have developed a protected fingerprint representation that relies on the distances between fingerprint global features (Singular points) and all other fingerprint minutiae. The principal is to build special spiral curves, which will represent the final protected template rather than the features of minutiae. The accuracy performance is supposed to be maintained, however, The risk is that when a fingerprint template is compromised, it may reveal the distances used to generate the protected template.

There are a variety of other methods in this context, many of which are recent [22, 23].

III. Preliminary Knowledge

In this section, we focus on the main pillars on which our approach is based. For this, we will detail both *Random projection* and *CDMA*.

A. Random Projection

Random Projection is a technique that allows in a way to hide data in a certain space, it is considered in several works [24, 25, 26] as one of the most secure transformations concerning biometric template protection [27], as it ensures unlinkability and revocability. The principle of *Random projection* is to project a data vector $X \in \Re^n$ onto a random matrix R, to generate a vector $M \in \Re^m$ of reduced dimension $m < n$ (from the product $M = RX$). In biometry, the utility of such a projection depends on whether the distances between the different feature vectors of the same user will be preserved or not. For that purpose, S. Kaski [28] has proved that if the matrix R is orthonormal then the similarity between vectors is preserved, and therefore the matrix R becomes a basis of projection. To get an orthonormal matrix, we have to go through the Gram-Schmidt process [29], which requires that the set of randomly generated vectors must be linearly independent.

According to the literature, the *Random projection* was always a basis for many approaches that deal with biometric template protection, specifically *BioHashing* [11] and *BioPhasor* [12] approaches. The use of such a technique was to produce transformed biometric data that may be used for authentication purposes, given that it provides an impressive diversification effect for biometric templates protection. Moreover, through the *Random projection*, we can also reinforce the property of non-invertibility using quantization. This step consists in transforming the result of the projection $W = (w_1, ..., w_m)$ to a vector with binary values, by using a one-way transformation such that the resulting transformed biometric data cannot be used to reveal the original biometric data. However, the quantization requires the definition of a threshold τ_b for the computation of the resulting vector $B = (b_1, ..., b_m)$, from the following formula:

$$b_i = \begin{cases} 0 & \text{if} \quad w_i \leq \tau_b \\ 1 & \text{if} \quad w_i > \tau_b \end{cases} \tag{1}$$

Generally, the threshold τ_b is chosen equal to zero as the results of the projection have the same probability of being negative or positive.

B. Code Division Multiple Access (CDMA)

CDMA is a multiplexing technique that is widely used in the radiofrequency domain, where it provides multiple access and resource sharing that is both flexible and secure [30]. This method of access is derived from the spread transmissions used in the context of military transmissions for many years, where their objective was to resist at best narrow-band interferers and to carry out discrete transmissions. Subsequently, this technique has seen a surprising emergence and a great evolution over the following years [31].

The principle of *CDMA* consists in transmitting a set of messages coming from several transmitters simultaneously on the same physical medium. On receiving, each recipient collects the received data and then tries to retrieve only the message originating from his corresponding transmitter, notably through a code that was allocated to him at the beginning of the communication. The use of spreading sequences as codes provides a way of distinguishing between the different given users. This makes the transmission less vulnerable to selective fluctuations in frequencies, and as well as a secure transmission [32]. This results in better management of available resources. It was thus stressed that the CDMA technique based on the use of orthogonal spreading sequences, was theoretically very satisfactory so that the different trains emitted by the users do not interfere with one another [30]. The generation of orthogonal codes is such a crucial step for resistance against interferences with multiple users. According to [33], there are two important properties of spreading sequences that must be respected: autocorrelation and cross-correlation. The autocorrelation property refers to the correlation between time-shifted versions of the same code while cross-correlation concerns if the codes which are used are completely orthogonal or not, if it was not the case, the different users are interferers to each other, hence the near-far problem appears. There are several code expansion techniques to generate orthogonal codes. Probably Hadamard transform [34] is the best-known technique. According to our reflection, we will adopt the same strategy as the *CDMA* by multiplexing all the reference templates in the same instance. During the authentication, the code corresponding to the user is calculated and then used to extract the specific reference template to perform the matching. We discuss the approach in detail in the following section.

IV. The Proposed Approach

In this section, we introduce a new protection scheme for the biometric template, which consists of applying a non-invertible transformation on the biometric features in order to generate a unique compact binary code. The secure transformation is based essentially on the principle of multiplexing provided by *CDMA* and the principle of *Random projection*.

Furthermore, we made sure during the design phase, that our approach meets the requirements of revocability, unlinkability, and non-invertibility. Generally, cancellable biometrics [35] is mainly based on two factors that must be presented at each authentication [36], namely the biometric trait and the seed (which can be seen as a secret key). The seed is a user-specific component through which the transformation of the original template is carried out, this element must indeed be secret and out of the way of impostors. For this reason, we have made sure that the transformation only relies on the biometric modality as [13] to avoid any vulnerabilities that may arise in case of seed theft [37]. So, to keep the seed secure and unknown to adversaries, we integrated its generation intuitively during template generation as shown in Fig. 1. In general, biometric systems consist of two main phases: 1) enrollment and 2) authentication (which can take the form of either identity verification or identification [20]). During Enrollment, the user biometric trait is captured (acquisition) and the features are extracted and stored in a database as a reference template. At authentication, the same biometric trait is captured again, the features are extracted and compared with those previously stored in the database for an eventual matching and then produce a decision (match/no match). In the following, we outline the stages that make up our processes.

A. Enrollment Stage

Our proposed protection scheme consists of two main steps:

1) Associate for each enrolled user a unique seed, through which we can always access the same projection space.
2) Projection of the extracted original biometric features onto a secure domain generated from the seed used in the previous step.

During processing, we used *CDMA* to discretize the seed associated with each user. As mentioned above, *CDMA* is a mechanism that requires the use of spreading sequences to avoid interferences. For this reason, our thinking has led us to apply the QR *decomposition*, which decomposes a matrix into two components Q and R, where R is an upper triangular matrix and Q is orthogonal with orthonormal columns $Q^T.Q = I$ (where I is the identity matrix). When the decomposed matrix is square, then firstly it will always have a decomposition and secondly Q will be orthogonal $Q^T.Q = Q.Q^T = I$. In our approach, this decomposition assumes an important part, not only in the generation of orthogonal sequences but also in linking each identity to a unique orthogonal code. All steps of the proposed revocable approach are described in the Algorithm 1.

The enrollment phase involves the storage of three elements, namely the matrix R from which the orthogonal code is recovered, the sum S relative to the *CDMA* technique, and finally the protected templates.

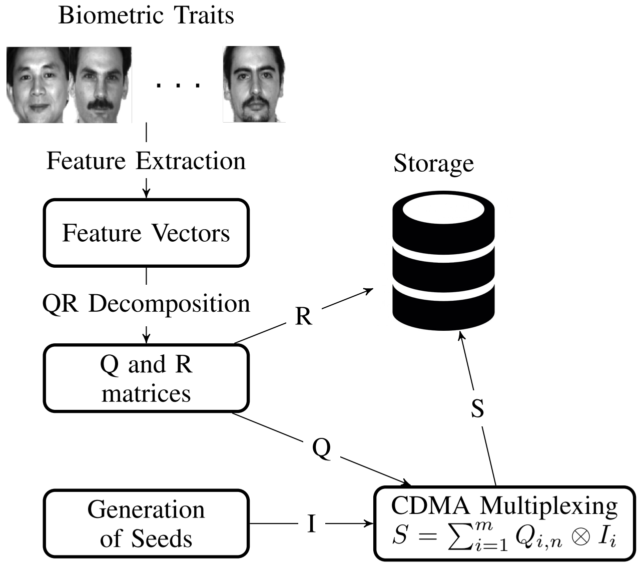

Fig. 1. Binding and Discretization of Seeds.

B. Authentication Stage

During the authentication phase, the system scans the biometric trait of the enrolled user k, hence the extraction of the feature vector V_k. Thereafter, the orthogonal code Q_k is recovered using the stored triangular matrix R according to the following formula:

$$Q_k = R^{-1}.V_k \tag{4}$$

(It should be noted that making the matrix M squared during the enrollment phase, was very useful when selecting orthogonal sequences residing at the rows of the orthogonal matrix Q). Then, the sum S is multiplied by the recovered orthogonal code Q_k to separate the seed I_k corresponding to the user k. Applying the same process of random projection during the enrollment phase, the protected template will thus be obtained. The system computes then the Hamming distance between the resulting template and the reference one stored in the database to either accept or reject the claimer. Concerning the determination of the threshold, it depends on the system design, and it is chosen such that the desired false rejection rate (FRR) and false acceptance rate (FAR) are satisfied.

V. Analysis and Discussion

Our scheme is considered as a one-way function since it is computationally infeasible to reconstruct the original template starting from the stored elements. It is true that the sum S contains all the orthogonal codes and their associated seeds, but it is almost impossible to extract them in case of compromise. Even the knowledge of the triangular matrix R can not reveal the orthogonal codes Q_i, especially with the absence of the feature vectors, knowing that $M = QR$. So the security of our scheme is ensured as long as it is difficult to reverse the transformation to obtain the original biometric template. Furthermore, the scheme meets also the requirements of revocability and unlinkability, properties for which an ideal biometric template protection technique is founded. Thus, if a

Algorithm 1 Stages of the enrollment phase

Step 1. Extraction of the biometric features vector $x \in \Re^n$ from a raw biometric image where n is the feature vector dimension.

Step 2. Assemble the set of feature vectors on a matrix $M_{m\times n}$, where m represents the user index during enrollment phase and $n > m$.

$$M_{m\times n} = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & \ddots & & \vdots \\ \vdots & & \ddots & x_{m-1,n} \\ x_{m,1} & \cdots & x_{m,n-1} & x_{m,n} \end{pmatrix}$$

Step 3. Make M a square matrix by complementing it with random numbers in a way to avoid the case where $\det(M) = 0$ (the order of the new matrix becomes $n \times n$).

Step 4. Apply the $QR\ Decomposition$ on the matrix M, which it can be expressed as $M_{n\times n} = Q_{n\times n}.R_{n\times n}$

Step 5. Generate for each identity a random vector representing the seed, $\{I_k \mid k = 1, ..., m\}$.

Step 6. Application of *CDMA* combining all the generated seeds $\{I_k \mid k = 1, ..., m\}$ with the first m orthogonal sequences residing at the first m rows of the orthogonal matrix Q into a single data as :

$$S = \sum_{i=1}^{m} Q_{i,n} \otimes I_i \qquad (2)$$

Step 7. Generate a set of pseudo-random vector, $\{\ r_i \in \Re^n \mid i = 1, ..., m\ \}$ from each seed I_k, through a random number generator (RNG), in our case we used Blum-Blum-Shub [38].

Step 8. Apply the Gram-Schmidt process on the previous set of random vectors to get an orthonormal set of r, $\{\ or_i \in \Re^n \mid i = 1, ..., m\ \}$ thereby forming a projection base.

Step 9. Project each acquired biometric vector on its associated projection base, by computing the inner product of feature vecteur $x \in \Re^n$ and each orthnonormal vector or_i , such that $\langle x, or_i \rangle$.

Step 10. Quantify the transformed template as follow:

$$b_i = \begin{cases} 0 & \text{if} \quad \langle x, or_i \rangle \le \tau \\ 1 & \text{if} \quad \langle x, or_i \rangle > \tau \end{cases} \qquad (3)$$

where τ is a predefined threshold, and m is the dimension of the protected template.

stored template is compromised, it can be protected by using a new seed instead of the one corresponding to the identity of the compromised template. The revocation requires both the storage of a new protected template resulting from the use of the new seed and also the update of the stored sum S as:

$$S_{new} = S_{stored} - (Q_{identity} \otimes I_{old}) + (Q_{identity} \otimes I_{new}) \quad (5)$$

That is how we will be able to generate multiple protected templates for the same biometric identity by using different seeds, which ensures the unlinkability or diversity property. The advantage of the proposed technique lies not only in the fact that it is perfectly secure but also in that the scheme does not require the repetition of the enrollment phase in case of a compromise of a protected biometric template.

On another hand, it should be noted that biometric identifiers are very sensitive and are affected by the variations that can occur during acquisition thus leading to a considerable degradation in accuracy performance [39]. This lack of accuracy is due to several factors: variability during capture (i.e. acquisition noise, use of multiple acquisition sensors, etc.), intra-class variability (variability of biometric data for an individual), and inter-class similarity (i.e., the similarity of biometric data for multiple individuals). The work we have proposed at this stage is dedicated to biometrics that represents high stability during the acquisition phase or non-biometric digital data to demonstrate the effectiveness of the provided discretization mechanism.

VI. Conclusion and Future Work

In this paper, we have proposed a new scheme for biometric template protection. We have indeed exploited the multiplexing property provided by the Code Division Multiple Access (CDMA) to generate a certain discritization for biometric templates as a non-invertible transformation in a system based on random projection. Our proposal is a kind of biometric protection approach, which only requires the user biometric identifier to perform the authentication of individuals. We have demonstrated that it meets the requirements of a revocable biometric system, namely, the properties of revocability, unlinkability, and non-invertibility. It must be mentioned that the nature and sensitivity of the biometrics have a crucial impact on performance preservation after the application of the non-invertible transformation. Through this work, our proposal has been proven to be effective for stable digital data. In this perspective, future work will focus on adapting sensitive biometrics and then evaluating them through experiments using public biometric databases, as well as a comparative study with some classical protection schemes in terms of revocability, unlinkability, non-invertibility, and accuracy performance.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.

[2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, November 2006.

[3] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 8, no. 2, pp. 1–17, 2008.

[4] N. Bartlow and B. Cukic, "Biometric system threats and countermeasures: A risk-based approach," in *Proceedings of the Biometric Consortium Conference (BCC 05)*, Crystal City, VA, USA, September 2005.

[5] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication(AVBPA'01)*, Halmstad, Sweden, June 2001, pp. 223–228.

[6] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[8] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, June 2008.

[9] J. B. Kho, J. Kim, I.-J. Kim, and A. B. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognition*, vol. 91, pp. 245–260, 2019.

[10] S. S. Ali, I. I. Ganapathi, S. Prakash, P. Consul, and S. Mahyo, "Securing biometric user template using modified minutiae attributes," *Pattern Recognition Letters*, vol. 129, pp. 263–270, 2020.

[11] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, "Two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, November 2004.

[12] A. Teoh and D. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *9th International Conference on Control, Automation, Robotics and Vision(ICARCV '06)*, Singapore, December 2006, pp. 1–5.

[13] C. Moujahdi, G. Bebis, S. Ghouzali, M. Mikram, and M. Rziza, "Biometric template protection using spiral cube: performance and security analysis," *International Journal on Artificial Intelligence Tools*, vol. 25, no. 01, p. 1550027, 2016.

[14] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.

[15] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template protection," *IEEE Signal Processing Letters*, vol. 17, no. 3, pp. 249–252, March 2010.

[16] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[17] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[18] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427–2436, 2007.

[19] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of symmetric hash functions for secure fingerprint matching," in *2010 20th International Conference on Pattern Recognition*. IEEE, 2010, pp. 890–893.

[20] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach," *Pattern Recognition*, vol. 45, no. 12, pp. 4129–4137, 2012.

[21] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, "Fingerprint shell: Secure representation of fingerprint template," *Pattern Recognition Letters*, vol. 45, pp. 189–196, 2014.

[22] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Computers & Security*, vol. 90, p. 101690, 2020.

[23] A. Lahmidi, K. Minaoui, C. Moujahdi, and M. Rziza, "Fingerprint template protection using irreversible minutiae tetrahedrons," *The Computer Journal*, 2021.

[24] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectored random projections for cancelable iris biometrics," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, Dallas, TX, USA, March 2010, pp. 1838–1841.

[25] ——, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, September 2011.

[26] A. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 37, no. 5, pp. 1096–1106, October 2007.

[27] S. Jassim, H. Al-Assam, and H. Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," in *Proceedings of 6th International Symposium on Image and Signal Processing and Analysis (ISPA 2009)*, Salzburg, Austria, Septembre 2009.

[28] S. Kaski, "Dimensionality reduction by random mapping," in *Int. Joint Conf. on Neural Networks Proceedings*, vol. 1, Anchorage, AK, USA, May 1998, pp. 413–418.

[29] W. Hoffmann, "Iterative algorithms for gram-schmidt orthogonalization," *Computing*, vol. 41, no. 4, pp. 335–348, December 1989.

[30] M. Z. Mushtaq, M. Ahsan, and M. S. Jamil, "Improving quality of security for cdma using orthogonal coding method," in *International Conference on Computer Science and Network Technology (ICCSNT)*, Harbin, China, December 2011, pp. 2649–2653.

[31] R. Prasad and T. Ojanpera, "An overview of cdma evolution toward wideband cdma," *IEEE Communications Surveys*, vol. 1, no. 1, pp. 2–29, First Quarter 1998.

[32] O. B. Wojuola, S. H. Mneney, and V. M. Srivastava, "Cdma in signal encryption and information security," in *Information Security for South Africa (ISSA)*, Johannesburg, South Africa, August 2016, pp. 56–61.

[33] V. P. Ipatov, *Spread Spectrum and CDMA : Principles and Applications*. Jhon wiley and Sons, 2005.

[34] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*. Prentice Hall International Editions, 1995.

[35] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.

[36] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for mcc fingerprint templates," in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 2014, pp. 1–8.

[37] A. Lahmidi, K. Minaoui, and M. Rziza, "A variant of biohashing based on the chaotic behavior of the logistic map," in *2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS)*. IEEE, 2019, pp. 1–7.

[38] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, May 1986.

[39] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of biometrics*. Springer Science & Business Media, 2007.