Securing fingerprint templates by enhanced minutiae-based encoding scheme in Fuzzy Commitment

Shivangi Shukla | Sankita J. Patel

Department of Computer Engineering, Sardar Vallabhbhai National Institute of Technology, Surat, Gujarat, India

Correspondence
Shivangi Shukla, Sardar Vallabhbhai National Institute of Technology, Surat 395007, Gujarat, India.
Email: shivangishukla968@gmail.com

[Correction added on 11 April 2021, after online publication. The duplicate values in table 1 were removed.]

Abstract
Fingerprint authentication has gained attention in recent years due to its distinctiveness, low-cost sensors, and user willingness to submit them. Its extensive deployment in our automated world raises major concerns regarding the secrecy of biometric templates and the privacy of rightful owners in biometric systems. Fuzzy Commitment (FC) focuses on securing the biometric templates by performing authentication based on the validity of secret keys from biometric features. However, the major challenge in designing Fingerprint-based FC is the requirement of efficient binary representation for unordered and variable minutiae points in fingerprint images. Additionally, its leakage can compromise an intrinsic characteristic of the individual. The paper proposes Fingerprint-based FC incorporating an encoding scheme dependent on the number and type of minutiae points present near the fingerprint's core point. The biometric templates are never identical thereby, this approach allows fuzziness in minutiae points by incorporating Bose–Chaudhuri–Hocquenghem (BCH) codes for error-correction and secures random codeword of the error-correcting scheme as secret key by SHA-256 hash mapping. The proposed approach is evaluated on FVC2000-DB2, FVC2002-DB1, FVC2002-DB2, and FVC2004-DB1, and the results illustrate the efficiency of the proposed scheme. Furthermore, the security analysis of stored helper data and hash mapping demonstrates that the proposed approach is secure.

1 | INTRODUCTION

The advancements in technology from traditional authentication systems relying on passwords and tokens, to biometric authentication raises several security and privacy concerns hindering its public acceptance. One of the potential privacy concerns of rightful owners is the usage of their stored biometric templates other than intended purposes. Additionally, biometric traits represent the intrinsic characteristics of an individual hence, they cannot be reissued or revoked if compromised.

Biometric Cryptosystem (BCS), one of the emerging biometric template protection schemes, focuses on securing biometric templates while sustaining the rightful owners' privacy. The BCS technique performs biometric matching based on the secret key extracted from helper data and query biometric template [1]. This helper data either stores information about biometric template only (Key-generation BCS) or information about both biometric template and secret key (Key-binding BCS). In both cases, helper data should store only significant information about biometric templates to sustain the rightful owners' privacy. The BCS techniques are quite useful in cryptographic applications, for instance, they are often combined with smart cards and passwords to provide multi-factor user authentication mechanism over insecure channels [2–4]. The helper data of BCS technique is stored in a smart card in the user's registration phase. This registered user presents password, smart card, and biometric in the authentication phase of biometric systems. The smart card uses stored helper data and query biometric template to generate the secret key. The user is authenticated if the password, smart card, and secret key belong to the legitimated user [5]. Recently, several researchers have proposed remote user authentication and key agreement schemes using BCS techniques for Internet of Things (IoT) [6–8], wireless sensor networks (WSNs) [9–11], cloud [5, 12] environment, and so on.

This is an open access article under the terms of the Creative Commons Attribution License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2021 The Authors. IET Information Security published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.
**Fuzzy Commitment** (FC), one of the emerging approaches in Key-binding BCS, binds codeword of error-correcting code (ECC) \( c \) with biometric feature \( x \) as helper data in the enrolment phase. The same codeword \( c \) is extracted from query biometric template \( x' \) and helper data in the authentication phase [13]. This scheme is further elaborated in Section 2. Research efforts have been put in designing FC for iris recognition in studies [14–18] as iris offers a high accuracy rate, high reliable bits and is resistant to external noise such as sweat, cuts, and bruises, unlike fingerprints. The major challenges in designing FC for fingerprint are:

- The generation of fixed-size binary representation for Fingerprint-based FC is challenging as it incorporates the presence of unordered and variable minutiae points (ridge terminations and ridge bifurcations).
- Matching of fingerprints in FC is performed by error-correction schemes, thereby eliminating several efficient matching algorithms and reducing the accuracy of authentication systems. Moreover, associating binary representation of fingerprint with the error-correction scheme is another major difficulty in designing Fingerprint-based FC.
- Achieving the same binary representation for intra-user variations is quite challenging due to the rotation, translation, and non-linear deformation in fingerprint images of the same user.

Shi et al. [19] proposed a fingerprint sector minutiae coding for FC; however, their approach considers different binary representations for maximum of two minutiae points in a sector. In other words, the sectors having three or more minutiae points in any sector are encoded by the same binary representation. To illustrate this drawback, Figure 1 provides a closer view of sectors in two sample fingerprints (from FVC2004) highlighted with red boundaries. These red highlighted sectors incorporate three or more minutiae points in them, that is, have different distinctive features but are encoded by the same binary representation as per [19]. The recognition of biometric systems can be improved by enhancing the distinctive features representation in fingerprint templates [20] thus, in case of the existing approach [19], the inclusion of more number and type of minutiae points in a sector. The paper focuses on enhancing the encoding scheme for the better performance of Fingerprint-based FC. The paper proposes an enhanced minutiae-based encoding scheme incorporating different binary representations for maximum of five minutiae points to provide a better distinctive feature representation of the sectors in fingerprint templates. The proposed approach includes BCH codes for error correction and the random codeword, also termed as secret key, is secured by SHA-256 hash mapping. The proposed approach’s performance is measured in terms of false reject rate (FRR) and false accept rate (FAR). The FRR denotes the percentage measure of incorrectly rejected genuine users and FAR denotes the percentage measure of falsely accepted impostors in the biometric system.

The major contributions of this paper are:

- The paper proposes an enhanced minutiae-based encoding scheme for different combinations of minutiae points (ridge endings and ridge bifurcations) by considering the presence of maximum of five minutiae points in a sector of the fingerprint.
- The experiment is conducted on four public-domain fingerprint databases: FVC2000-DB1, FVC2002-DB1, FVC2002-DB2, and FVC2004-DB1 incorporating BCH(31, 21, 2) for correcting corrupted minutiae points in the sector thereby, increasing helper data size while sustaining the performance of the proposed scheme.
- The paper discusses the security analysis of helper data and hash of codewords stored in the database. The proposed scheme maintains the privacy of rightful owners by ensuring that stored data in itself reveals no significant information related to biometric templates. Additionally, the security analysis discusses that it is difficult for an adversary to perform a brute-force attack on information stored in the database.

The paper is organised as follows: Section 2 discusses previous work related to FC in biometric systems and Section 3 discusses proposed Fingerprint-based FC incorporating the enrolment phase and authentication phase of biometric systems. Sections 4 and 5 covers experimental results and security analysis of the proposed scheme, respectively. Finally, the paper is concluded in Section 6.

### 2 RELATED WORK

The FC was first introduced by Juels et al. [13] to combine the concept of ECC and cryptography. The FC methodology stores commitment of biometric templates in the enrolment phase. This commitment is opened or de-committed, provided if the authentication phase’s biometric query template is sufficiently close to one in the enrolment phase. Figure 2 depicts traditional FC where the user presents biometric template \( b \) in the enrolment phase, represented by fixed-size binary string \( x \). The ECC generates a random codeword \( c \) and computes helper data \( \delta \) as \( \delta = x \oplus c \). This helper data \( \delta \) and the hash of codeword \( h(c) \) are stored in the database. In the authentication phase, the user presents a biometric template \( b' \) represented as fixed-size binary string \( x' \). Using stored helper data \( \delta \), the system computes \( c' = \delta \oplus x' \). This calculated codeword \( c' \) is decoded as \( c'' \) using the same ECC (as in the enrolment phase), and its hash \( h(c'') \) is calculated. If the biometric templates \( b \) and \( b' \) are sufficiently close, then \( h(c) = h(c'') \) else not. Thereby, the error-correcting capacity of ECC eliminates the difference in bits of fixed-size representation \( x \) and \( x' \).

Hao et al. [14] proposed FC for iris-recognition by classifying iris-code errors into two categories, random errors occurring because of CCD camera pixel, iris distortion, and so on, and burst errors occurring because of specular reflections.
and undetected or out-of-focus eyelashes. To deal with such errors, the authors [14] proposed a concatenated-coding scheme where Hadamard code deals with background errors and Reed-Solomon code deals with burst errors. Hao et al. [14] extracted iris-code of 256-byte by utilising the algorithm in [25]. This iris-code is XORed with an encoded key via Hadamard and Reed-Solomon code to generate helper data in the biometric system. This approach computes FRR = 0.47% and FAR = 0% for key size of 140 bits. The authors [14] implemented this approach using their own database, however, Bringer et al. [15] reported an increment in FRR and FAR on public ICE iris database.

Bringer et al. [15] proposed a 2D iterative min-sum decoding algorithm based on the concept that probabilities of error and erasure for each bit in iris-code are independent. The erasures are an unknown bit at known location. The authors [15] computes iris-code using algorithm [25] and calculates the maximum number of errors and erasures by the capacity in Shannon sense [26]. For fingerprint, the authors [15] used binarisation and reliable component selection on fingerprint templates. Adamovic et al. [16] proposed FC for iris-recognition by incorporating the concept of interleaving. It reduces burst errors in iris-code and mutual information between two different iris-codes. The authors [16] generated iris-code for FC by utilising 1D Gabor wavelet on iris templates followed by interleaving. Rathgeb et al. [17] proposed iris-code error analysis and bit rearrangements for iris-based FC. The methodology [17] performs an error-analysis by computing intra-class comparison on training sets to detect the number of errors occurring in each bit position. The iris-code bits are rearranged to obtain a uniform distribution of errors. Thus, error at bit positions of high probability is rearranged with bit positions of low probability and vice-versa. Rathgeb et al. [18] incorporated the usage of maximal intra-class distance (ICD) on existing iris recognition algorithms in [21, 22] to propose FC for iris-recognition. The authors [18] concatenated Reed-Solomon and Hadamard codes for iris-code generated by [21] for error correction as maximal ICD is between 48% and 85%. For iris-code generated by [22], the authors [18] used only Reed Solomon for error-correction as maximal ICD is less than 44%.

For Fingerprint-based FC, Teoh et al. [23] proposed Randomized Dynamic Quantization Transformation (RDQT)

![Figure 1](image1.png) **Figure 1** Presence of three or more minutiae points in red highlighted sectors of fingerprint samples from FVC2004

![Figure 2](image2.png) **Figure 2** Traditional Fuzzy Commitment proposed by Juels et al. [13]
wherein multichannel Gabor filter [27] extracts feature vector from fingerprints. This feature vector of length 1226 bits is reduced to 750 bits by random projection methodology. Furthermore, this feature vector is further reduced to 375 bits by dynamic quantization. The authors [23] perform core detection manually to crop the fingerprint image for feature extraction. However, the performance of this approach [23] can vary if the existing algorithms are utilised for core detection as it is difficult to extract the core point exactly on noisy fingerprints. Nandakumar [24] proposed Binarised Phase Spectrum (BiPS) for Fingerprint-based FC, wherein the Fourier phase spectrum of minutiae points is sampled on a log-polar grid to obtain fixed-size minutiae representation. The authors [24] extracted reliable bits of size 2048 bits present in this fixed-size minutiae representation. One of the major advantages of this approach [24] is the privacy enhancement of fingerprint by discarding the magnitude spectrum of minutiae points thereby, it is challenging to compute the location and orientation of minutiae points from helper data.

Shi et al. [19] proposed a Fingerprint-based FC that incorporates sector minutiae coding with short and long strategies. The region near fingerprint’s core point is divided into several sectors. These sectors are further encoded as fixed-size binary string depending on the number of minutiae points present in them. The only difference between long strategy and short strategy is the inclusion of directional information of minutiae points in long strategy. However, different encoding representations are used for a maximum of two minutiae points in the short strategy. Thus, any sector having three or more minutiae points is encoded by the same representation. Table 1 summarises the comparison of various FC schemes incorporating their biometric traits, key size, performance, database, and approach. The remarks of Table 1 points out the limitation in some of the existing methodologies. The paper aims to enhance the encoding scheme in [19] by incorporating a different representation for maximum of five minutiae points. This enhanced minutiae-based encoding scheme provides a better representation of distinctive features present in the sector of fingerprint templates. The proposed methodology constructs 72 sectors near the fingerprint’s core point and includes BCH(31, 21, 2) for error correction in each of these sectors. Thus, the proposed methodology has key-size of 1512 bits, and the performance is evaluated on databases: FVC2000-DB2, FVC2002-DB1, FVC2002-DB2, and FVC2004-DB1. The proposed methodology and experimental results are elaborated in Sections 3 and 4, respectively.

3 | PROPOSED FINGERPRINT-BASED FUZZY COMMITMENT

The FC technique demands representation of unique features of biometric templates in the form of a fixed-size binary string. The error-correcting scheme of FC allows fuzziness in this fixed-size binary string as biometric templates are never accurate. Representation of unique features in the form of fixed-size binary string for fingerprints is challenging due to varying minutiae points in terms of number, location, and orientation because of translation, rotation, and non-linear deformation of fingerprint images. This section presents the detailed design of proposed Fingerprint-based FC. Section 3.1 discusses the generation of FingerCode, that is, fixed-size binary string for fingerprint templates. Section 3.2 elaborates deployment of this FingerCode in FC wherein random codewords are binded with FingerCode as helper data in enrolment phase. Section 3.3 discusses the authentication phase wherein codewords are retrieved from query biometric template and stored helper data.

3.1 | FingerCode generation

The fingerprint template incorporates ridge endings and ridge bifurcations, collectively termed as minutiae points. The point where ridge ends abruptly is termed as ridge ending, whereas the point where ridge diverges into branch ridges is termed as ridge bifurcation [28]. These minutiae points and their relationships define the uniqueness of fingerprint templates. The proposed methodology enhances the fingerprint provided and extracts minutiae points represented as $$(x_i, y_i, \theta_i, T_i)$$ where $$(x_i, y_i)$$ represents position, $$\theta_i$$ represents direction and $$T_i$$ indicates type of minutiae $$i$$ in the fingerprint template. The core point can be defined as the point of maximum curvature of concave ridges in the fingerprint template [27]. The proposed framework uses an algorithm [29] to calculate the core point represented as $$(x_c, y_c, \theta_c)$$ where $$(x_c, y_c)$$ represents position and $$\theta_c$$ represents direction of core point. The coordinate transformation of minutiae points is performed using Equation (1) considering the fingerprint’s core point as origin of the coordinate.

$$
\begin{align*}
x_i’ &= x_i + (x_i - x_c) \times \cos \theta_i - (y_i - y_c) \times \sin \theta_i \\
y_i’ &= y_i + (x_i - x_c) \times \sin \theta_i - (y_i - y_c) \times \cos \theta_i \\
\theta_i’ &= (\theta_i + \theta_c) \mod 2\pi \\
T_i’ &= T_i
\end{align*}
$$

where $$(x_c, y_c, \theta_c)$$ denotes core point of the fingerprint, $$(x_i, y_i, \theta_i, T_i)$$ denotes original minutiae points in the fingerprint and $$(x_i’, y_i’, \theta_i’, T_i’)$$ denotes transformed minutiae points of the fingerprint.

After the coordinate conversion of minutiae points, sector construction is performed on the fingerprint template. Several concentric circles having the same width between them are constructed by using core point as centre. These circles are further partitioned by their radii having constant angle $$\theta$$ between them, thereby forming sectors. Figure 3 depicts five concentric circles having radii $$R = \{50, 80, 110, 140, 170\}$$ and each circle is partitioned by their radii having constant angle $$\theta = 30^\circ$$ between them. These sectors are numbered in an anti-clockwise direction, as depicted in Figure 3. Based on the sector construction, the fingerprint image can be parted into $$n \times (360/\theta)$$ sectors where $$n$$ denotes the number of concentric circles, and $$\theta$$ denotes the angle between radii of circles. This sector construction is helpful in analysing minutiae distribution.
in fingerprint templates, for instance, this minutiae distribution should be almost similar if the two fingerprint images belong to the same user.

We propose an enhanced minutiae-based encoding scheme to analyse the minutiae distribution in the sectors of fingerprint templates. Based on this scheme, each sector is represented by FingerCode depending on the number and type of minutiae points present in it. This encoding scheme has different FingerCode representations for different combinations for maximum of five minutiae points present in these sectors. This

| Authors                  | Biometric traits | Key size | Performance       | Database        | Approach                                                                 | Remarks                                                                 |
|--------------------------|------------------|----------|-------------------|-----------------|-------------------------------------------------------------------------|-------------------------------------------------------------------------|
| Hao et al. [14]          | Iris             | 140 bits | FRR = 0.47%, FAR = 0% | Own database    | The methodology incorporates concatenated encoding and decoding scheme to provide two-layer ECC for the iris codes | Bringer et al. [15] reported increment in FRR and FAR for ICE database (FRR = 10% and FAR = 0.80%) |
| Bringer et al. [15]      | Fingerprint      | 42 bits  | FRR = 2.73%, FAR = 5.53%, FRR = 5.62%, FAR < 10⁻⁷% | FVC2000-DB2     | The methodology incorporates 2D iterative min-sum decoding scheme for error and erasures | The size of the key incorporated in this approach is too small |
| Adamovic et al. [16]     | Iris             | 400 bits | FRR = 3.75%, FAR = 0% | CASIAv4         | The methodology introduced usage of interleaving technique for the reduction of mutual information between different iris codes |                                                                      |
| Rathgeb et al. [17]      | Iris             | 128 bits | FRR = 4.92%, FAR = 0% | CASIAv3         | The methodology incorporates bit rearrangements based on the intra-class error distribution in iris codes |                                                                      |
| Rathgeb et al. [18]      | Iris             | 128 bits | For features as per algorithm [21], FRR = 4.46%, FAR = 0% | CASIAv3         | The methodology incorporates maximal ICD for block-level ECC and bit-level ECC |                                                                      |
| Teoh et al. [23]         | Fingerprint      | 140 bits | FRR = 0.9%, FAR = 0% | FVC2002-DB1     | The methodology incorporates random projection and dynamic quantization technique to generate feature vector | The results incorporate detection of the core point in fingerprint templates manually |
| Nandakumar [24]          | Fingerprint      | 240 bits | FRR = 16.2%, FAR = 0% | FVC2002-DB1     | The methodology introduced BiPS to generate fixed-size binary strings |                                                                      |
| Shi et al. [19]          | Fingerprint      | 420 bits | FRR = 6.2%, FAR = 0.75% | FVC2004-DB1     | The methodology introduced sector coding strategy based on the number and type of minutiae points present near the core point of fingerprints | The sector coding strategy incorporates the same binary representation for different sectors having more than two minutiae points |
| Proposed FC              | Fingerprint      | 1512 bits (72 keys of 21 bits each) | FRR = 2.5%, FAR = 0.29%, FRR = 3.5%, FAR = 0.89%, FRR = 4.5%, FAR = 0.98%, FRR = 5.5%, FAR = 0.84% | FVC2000-DB2     | The methodology introduces enhanced minutiae-based encoding scheme incorporating different fixed-size representation for maximum of five minutiae points in a sector of the fingerprint |                                                                      |

TABLE 1 Comparison of Fuzzy Commitment schemes
encoding scheme incorporates corruption of one or two minutiae points using $BCH(31, 21, 2)$ for error correction. These sectors in the fingerprint template are small regions hence, the maximum count of minutiae points is limited to five minutiae points. Likewise, it is unlikely that the fingerprint templates belonging to the same user are corrupted by more than two minutiae points in a sector. This increment in number and type of minutiae points via enhanced minutiae-based encoding scheme increases the representation of distinctive features in the sectors. Figure 4 depicts the structure of FingerCode incorporating 2 bits as flag indicating absence or presence of minutiae points in the sector. The next 5 bits indicate minutiae count, that is, the number of minutiae points present in sector, and the next 20 bits represent the type of minutiae point present in the sector. We need to append extra 6 bits in FingerCode to XOR with ECC’s random codeword (size 31 bits) to generate helper data. It should be noted that flag bits are not XORed with ECC’s codeword; however, they are useful in calculating sectors with the absence of minutiae points in the authentication phase.

Table 2 discusses the enhanced minutiae-based encoding scheme for generating FingerCode based on type and number of minutiae points present in a sector. For instance, if the sector of fingerprint image has two ridge ending and one ridge bifurcation, then its FingerCode is represented as $1101110000000000000000011000000$. Similarly, if the sector has four ridge ending and zero ridge bifurcation points present, the FingerCode is represented as $110111100000000000000000111000000$.

This enhanced minutiae-based encoding scheme is designed to incorporate corruption of one or two minutiae points in a sector, that is, sectors varying by one or two minutiae points can generate the same codeword by utilising $BCH(31, 21, 2)$ for error correction. The sectors are small regions, and it is unlikely that the fingerprint templates belonging to the same user are corrupted by more than two minutiae points. For instance, consider in enrolment phase, the first sector of fingerprint image has three ridge termination and zero ridge bifurcation, thereby its FingerCode $FC_{E}^{E} = 110011100000000000000000111000000$. As fingerprint images are never accurate, the same sector in query template during authentication incorporates two ridge termination and zero ridge bifurcation that is, FingerCode $FC_{Q}^{Q} = 11000111000000000000000011000000$. The hamming distance between $FC_{E}^{E}$ and $FC_{Q}^{Q}$ is 2, that is, within the error correction capacity of BCH code, authentication phase can decode the same codeword as in enrolment phase using stored helper data. Similarly, in case the same sector in query template incorporates four ridge termination and zero ridge bifurcation (FingerCode $FC_{Q}^{Q} = 110111100000000000000000111000000$), BCH code can decode the same codeword as the hamming distance between $FC_{E}^{E}$ and $FC_{Q}^{Q}$ is within its error correction capacity. However, in case the sector has corruption of more than two minutiae points, for instance having one termination and two bifurcations (FingerCode $FC_{Q}^{Q} = 110011101000000000000000001000000$), the hamming distance exceeds the error correction capacity, resulting in decoding of different codeword at the time of authentication.

### 3.2 | Enrolment phase

In the enrolment phase, a new user presents his/her biometric template converted to FingerCode using sector construction and encoding scheme. For each user, helper data are generated by binding the ECC’s random codeword with FingerCode of the biometric template. Furthermore, random codewords of ECC are securely stored in the database by hash mapping. It should be noted that only helper data and the hash of codewords are stored in the database. The other information is discarded to sustain the user’s privacy in biometric systems. Figure 5 depicts the block diagram of the enrolment and authentication phases in the proposed Fingerprint-based FC.

In this phase, minutiae points and core points are extracted from the enhanced fingerprint template. Further, minutiae transformation is performed, and sectors are constructed as discussed in Section 3.1. Depending on the number and type of minutiae present in sectors, the fingerprint template is transformed to FingerCode $FC = \{FC_{1}, FC_{2}, FC_{3}, \ldots, FC_{N}\}$ where $N$ denotes the number of sectors constructed in fingerprint template. Considering $BCH(31, 21, 2)$ for error correction, the system generates random codeword $C = \{C_{1}, C_{2}, C_{3}, \ldots, C_{N}\}$, each of size 31 bits and $N$ represents the number of sectors in fingerprint template.

For FingerCode $FC = \{FC_{1}, FC_{2}, FC_{3}, \ldots, FC_{N}\}$ and codeword $C = \{C_{1}, C_{2}, C_{3}, \ldots, C_{N}\}$, FingerCode $FC_{i}$ and $C_{i}$ ($1 \leq i \leq N$) represents FingerCode and codeword for $i^{th}$ sector in fingerprint template, respectively. It’s helper data $\delta_{i}$ is calculated by binding $FC_{i}$ with random codeword $C_{i}$ of ECC. However, the flag bits of each FingerCode are excluded in this process of binding. The combination of Minutiae Count ($MC$) bits, Minutiae Type ($MT$) bits, and Extra ($E$) bits of FingerCode $FC_{i}$, that is, $\{MC_{i} + MT_{i} + E_{i}\}$ are XORed with codeword $C_{i}$ of ECC and flag bits $F_{i}$ are appended to this resultant. The generation of helper data is depicted in Figure 6 where helper data $\delta = \{\delta_{1}, \delta_{2}, \delta_{3}, \ldots, \delta_{N}\}$ are obtained from FingerCode $FC = \{FC_{1}, FC_{2}, FC_{3}, \ldots, FC_{N}\}$ and codeword $C = \{C_{1}, C_{2}, C_{3}, \ldots, C_{N}\}$ in the enrolment phase of biometric system.
After generating helper data of the fingerprint, hash of each random codeword $C_i$ is calculated as $H(C) = \{H(C_0), H(C_1), H(C_2), ..., H(C_N)\}$ using SHA-256 as one-way hash function. This hash $H(C)$ and helper data $\delta$ are stored in the biometric database, later used for authenticating users in the proposed Fingerprint-based FC system.

### 3.3 Authentication phase

In the authentication phase of proposed Fingerprint-based FC, minutiae points and core points are extracted, and coordinate transformation is performed on the query template. Similar to the enrolment phase, several sectors are constructed using core point as the centre, and FingerCode $FC'$ are generated depending on number and type of minutiae points present in the sector of query template. This FingerCode in the authentication phase is represented as $FC' = \{FC'_1, FC'_2, FC'_3, ..., FC'_{N'}\}$ where $N'$ denotes the number of sectors constructed in fingerprint template.

The codeword $C' = \{C'_1, C'_2, C'_3, ..., C'_{N'}\}$ is calculated from stored helper data $\delta = \{\delta_1, \delta_2, \delta_3, ..., \delta_{N'}\}$ and authentication FingerCode $FC = \{FC'_1, FC'_2, FC'_3, ..., FC'_{N'}\}$. Considering FingerCode $FC'_i$ and helper data $\delta_i$ for $i^{th}$ sector in the fingerprint template, codeword $C'_i$ is

| Flag | Minutiae count | Minutiae type |
|------|----------------|---------------|
| No. of minutiae | Representation | Type of minutiae | Representation | Extra |
| 00 | 0 | 00000 | Zero ending and zero bifurcation | 000000000000000001111111 | 000000 |
| 11 | 1 | 0001 | one ending and zero bifurcation | 000000000000000011111111 | 000001 |
| 2 | 00011 | Zero ending and one bifurcation | 100000000000000000000001 |
| 3 | 0011 | Two ending and zero bifurcation | 000000000000000000000001 |
| 4 | 0111 | Three ending and zero bifurcation | 110000000000000000000001 |
| 5 | 1111 | Four ending and zero bifurcation | 111100000000000000000001 |
| 6 | 1111 | Five ending and zero bifurcation | 111110000000000000000001 |

**FIGURE 4** The structure of FingerCode

**TABLE 2** The enhanced minutiae-based encoding scheme based on number and type of minutiae present in a sector
calculated by performing XOR operation between helper data $\delta_i$ and FingerCode $FC'_i$. The flag bits of helper data and FingerCode are excluded in this process. This calculation of codeword is depicted in the authentication phase of Figure 6. This codeword $C' = \{C'_1, C'_2, C'_3, \ldots, C'_N\}$ is provided as input to BCH for error correction that generates...
decoded codeword as  \( C'' = \{ C''_1, C''_2, \ldots C''_N \} \). Thus, hash of each decoded codeword is calculated as \( H(C'') = \{ H(C''_1), H(C''_2), \ldots H(C''_N) \} \) using the same hash function as in the enrolment phase of biometric system.

The comparison between biometric templates is performed using two parameters, that is, \( \text{CompScore} \) and \( \sigma \) defined in Equations (2) and (3).

\[
\text{CompScore} = \frac{N_m}{N - \alpha - \beta + \gamma} \times 100 \tag{2}
\]

\[
\sigma = \alpha + \beta + \gamma + N_m \tag{3}
\]

where \( N_m \) denotes the total number of matched hash of codewords in enrolment and authentication phase, \( N \) denotes the total number of sectors constructed in the fingerprint template, \( \alpha \) and \( \beta \) denotes the number of sectors with absence of minutiae points in enrolment phase and authentication phase respectively and \( \gamma \) denotes common sectors with absence of minutiae points both in enrolment and authentication phase. It should be noted that the flag bits \( F_i \) of helper data \( \delta_i \) indicates absence of minutiae points in the \( i^{th} \) sector of enrolment template. The threshold is defined as combination of \( \text{CompScore} \) and \( \sigma \), where the user is accepted if threshold is satisfied else rejected.

### 4 | EXPERIMENTAL RESULTS

The performance evaluation of proposed Fingerprint-based FC is conducted on four public-domain fingerprint databases: FVC2000-DDB2, FVC2002-DDB1, FVC2002-DDB2, and FVC2004-DDB1. Each of these databases incorporates fingerprint images of 100 users and eight impressions per user, that is, a total of 800 fingerprint images. Table 3 presents detailed information on these fingerprint databases.

For evaluation of the proposed Fingerprint-based FC, FRR and FAR are computed. For experimentation, four images per user are utilised in the enrolment phase, and two images per user are utilised in the authentication phase. However, two images per user from each database are not utilised in experiments as they are of low quality. It is reasonable to assume that users in the BCS are cooperative and provide good quality fingerprint images for binding secret keys with biometric templates [30, 31]. Thus, the experiment incorporates a total count of 200 genuine attempts and 19,800 impostor attempts in the authentication phase of biometric system.

The algorithm proposed in [29] is utilised for detection of the core point in fingerprint images. For experimentation, six concentric circles are constructed having radii \( R = \{8, 31, 54, 77, 100, 123\} \) and further partitioned into sectors by radii having constant angle \( \theta = 30^\circ \) between them thereby, constructing 72 sectors on the fingerprint image. The enrolment and authentication of users are performed, as mentioned in Sections 3.2 and 3.3, respectively. The \( \text{BCH}(31, 21, 2) \) are utilised for error correction, and their codewords in the enrolment and authentication phase are secured by SHA-256 hashing. The comparison between biometric templates are performed using two parameters, that is, \( \text{CompScore} \) and \( \sigma \) defined by Equations (2) and (3), respectively, in Section 3.3.

Table 4 summarises FRR and FAR for different values of \( \text{CompScore} \) and \( \sigma \) as the performance of proposed Fingerprint-based FC for FVC2000-DDB2, FVC2002-DDB1, FVC2002-DDB2, and FVC2004-DDB1. The threshold condition varies with varying sizes and quality of different images.

Table 5 compares the performance of proposed approach with other existing Fingerprint-based FC [15, 19, 24]. We have not considered Teoh et al. [23] approach for comparison as the results in [23] incorporate manual detection of fingerprint’s core point. This result can degrade if the existing algorithms are utilised for core detection as it is difficult to extract the core point exactly on noisy fingerprints. The proposed Fingerprint-based FC performs better than Bringer et al. [15]. In comparison with Pandakumar [24] and Shi et al. [19], the FRR of proposed Fingerprint-based FC is reduced, due to better representation of distinctive features by the enhanced minutiae-based encoding scheme of the proposed approach. However, the FAR of proposed Fingerprint-based FC is more than [19, 24] due to strong ECC in the enhanced encoding scheme of the biometric system. This enhanced minutiae-based encoding scheme incorporates different FingerCode representation for different combinations for maximum of five minutiae points. The proposed approach deploys strong ECC by allowing minutiae corruption of one or two points out of five minutiae points in each sector of the fingerprint template. Thus, the proposed Fingerprint-based FC provides acceptable performance in comparison to the other existing schemes.

**Table 3** Detailed information of the database incorporated in our experiment

| Parameter         | FVC2000-DDB2 | FVC2002-DDB1 | FVC2002-DDB2 | FVC2004-DDB1 |
|-------------------|--------------|--------------|--------------|--------------|
| Resolution        | 500 dpi      | 500 dpi      | 569 dpi      | 500 dpi      |
| Sensor type       | Low-cost capacitive sensor | Optical sensor | Optical sensor | Optical sensor |
| Number of fingers | 100          | 100          | 100          | 100          |
| Number of images per finger | 8            | 8            | 8            | 8            |
| Image size        | 256 × 364    | 388 × 374    | 296 × 560    | 640 × 480    |
| Image quality     | Medium       | Medium       | Medium       | Extremely low |
5 | SECURITY ANALYSIS

The proposed FingerCode-based FC stores only helper data \( \delta = \{ \delta_1, \delta_2, \delta_3, \ldots, \delta_N \} \) and hash of codeword \( H(C) = \{ H(C_1), H(C_2), H(C_3), \ldots, H(C_N) \} \) where \( N \) denotes the number of sectors constructed on fingerprint image, in the database and discards rest of the information. The security of FC has been studied theoretically in [13]. This section provides the security analysis of stored information, that is, helper data and codewords in the proposed Fingerprint-based FC.

- **Codeword**: For the security of codeword stored in database, the proposed Fingerprint-based FC deploys SHA-256 hash mappings. The security of codeword can be analysed in two cases: in case 1, the adversary gains knowledge about hash mappings deployed in the biometric system, and in case 2, the adversary gains knowledge about error correction scheme utilised in the biometric system.

Case 1: The hash mappings are one-way functions that are computationally difficult to invert thereby, secures codewords in the database. However, the birthday attack is the most effective method to find a collision in \( q \)-bit hash function which requires \( 2^{q/2} \) operations [32]. The proposed methodology incorporates SHA-256 therefore, the security parameter is \( q = 256 \) corresponds to the minimum of \( 2^{128} \) operations to find a colliding pair of codewords. The proposed scheme constructs 72 sectors in the fingerprint image therefore, the adversary requires \( 2^{128} \times 72 \) colliding pairs of codewords for the proposed Fingerprint-based FC.

Case 2: If the adversary gains knowledge about error-correcting scheme utilised in biometric system then, the security depends on the codeword space size of ECC. The proposed scheme utilises \( BCH(31, 21, 2) \) for correcting corrupted minutiae points in sector of fingerprint template. This corresponds to the codeword space size of \( 2^{21} \) hence, the adversary needs \( 2^{33} \times 72 \) attempts to break the security of codewords stored in the database.

- **Helper data**: The helper data \( \delta = \{ \delta_1, \delta_2, \delta_3, \ldots, \delta_N \} \) stored in the database are of size 33 bits each. This helper data is the combination of codeword and FingerCode thereby, helper data in itself is not sufficient to provide any information regarding codeword or FingerCode of the user. For the successful verification of user, authentication FingerCode \( FC = \{ FC_1', FC_2', FC_3', \ldots FC_N' \} \) should be sufficiently close to enrolment FingerCode \( FC = \{ FC_1, FC_2, FC_3, \ldots FC_N \} \) where both \( FC_i \) and \( FC_i' \) for \( 1 \leq i \leq N \) are of size 33 bits each. As the proposed scheme constructs 72 sectors on a fingerprint template, the adversary requires \( 2^{33} \times 72 \) attempts to generate codewords from helper data via brute force. Hence, it is difficult for an adversary to gain knowledge about codewords from helper data stored in the database.

6 | CONCLUSION

For authenticating individuals in real-world applications, biometric recognition systems offer authentication of the individual based on their distinctive traits of biometric. As these traits are intrinsic in nature, these recognition system calls for secure storage of biometric templates. The BCS techniques address rightful owners' security and privacy concerns by utilising significant information about biometric templates to retrieve or generate secret keys. FC is one of the techniques in Key-binding BCS. The paper proposes Fingerprint-based FC wherein helper data are generated by utilising the number and type of minutiae points present near the fingerprint's core point. This approach deploys BCH codes for error correction, and their codewords are secured by SHA-256 hash function. This approach's performance is evaluated on four public-domain fingerprint databases: FVC2000-DB2, FVC2002-DB1, FVC2002-DB2, and FVC2004-DB1. The proposed Fingerprint-based FC provides acceptable performance in terms of FRR and FAR. Furthermore, we have analysed the security of helper data and codewords stored in the database.

| Database          | Threshold | FRR (%) | FAR (%) |
|-------------------|-----------|---------|---------|
| FVC2000-DB2       | CompScore < 1150 and \( \sigma > 170 \) | 2.5%    | 0.29%   |
| FVC2002-DB1       | CompScore < 1250 and \( \sigma > 175 \) | 3.5%    | 0.89%   |
| FVC2002-DB2       | CompScore < 1450 and \( \sigma > 175 \) | 4.5%    | 0.98%   |
| FVC2004-DB1       | CompScore < 1150 and \( \sigma > 170 \) | 5.5%    | 0.84%   |

**Table 4** Performance of proposed Fingerprint-based Fuzzy Commitment

| Technique           | FVC2000-DB2 | FVC2002-DB1 | FVC2002-DB2 | FVC2004-DB1 |
|---------------------|-------------|-------------|-------------|-------------|
|                     | FRR | FAR | FRR | FAR | FRR | FAR | FRR | FAR |
| Bringer et al. [15] | 2.73% | 5.53% | – | – | – | – | – | – |
| Nandakumar [24]     | – | – | 16.2% | 0% | 12.6% | 0% | – | – |
| Shi et al. [19]     | – | – | – | – | 6.2% | 0.75% | – | – |
| Proposed fingerprint-based FC | 2.5% | 0.29% | 3.5% | 0.89% | 4.5% | 0.98% | 5.5% | 0.84% |

**Table 5** Performance comparison of the proposed Fingerprint-based Fuzzy Commitment with other existing techniques

**Note**: The symbol ‘–’ denotes the non-availability of that particular value for the database.

**Abbreviations**: FAR, false accept rate; FRR, false reject rate.
The proposed Fingerprint-based FC can be utilised for remote user authentication and key agreement schemes in the cloud environment. The user provides a fingerprint template for which helper data and secret keys are generated using the proposed Fingerprint-based FC in the registration phase. This helper data is stored in the smart card along with the hash of identity, password, and secret key of the proposed Fingerprint-based FC. Later in the authentication phase, the registered user can log in by providing identity, password and query fingerprint template. The secret key is re-generated by the authentication phase of proposed Fingerprint-based FC, using query fingerprint template and helper data stored in the smart card. Thus, the registered user is authenticated by comparing the hash of identity, password, and secret key in the registration and authentication phase of the biometric system.

The performance of proposed methodology can be further enhanced by utilising multiple fingerprints for authenticating users in the biometric system. Apart from increasing the number and type of minutiae present near the fingerprint's core point, additional attributes, such as minutiae orientation, it is distance with the core point, and so on, can also be incorporated for better performance of Fingerprint-based FC. The major limitation in designing FC is the usage of error-correcting codes for matching biometric templates. Thereby, depending on the types of features incorporated in the encoding scheme of FC accordingly, error-correcting codes should be deployed in the biometric system.

**ORCID**

Shivangi Shukla  
https://orcid.org/0000-0001-8945-2721

**REFERENCES**

1. Natgunanathan, I., et al.: Protection of privacy in biometric data. IEEE Access. 4, 880–892 (2016)
2. Jain, A.K., et al.: Biometric template security. EURASIP J. Adv. Signal Process., 2008, 1–17 (2008)
3. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur., 2011(1), 3 (2011)
4. Ferrag, M.A., et al.: Authentication and authorization for mobile iot devices using biofeatures: recent advances and future trends. Secur. Commun. Netw. 2019 (2019)
5. Jiang, Q., et al.: A privacy preserving three-factor authentication protocol for e-health clouds. J. Supercomput. 72(10), 3826–3849 (2016)
6. Sahoo, S.S., et al.: A secure three factor based authentication scheme for health care systems using IoT enabled devices. J. Ambient Intell. Humaniz. Comput., 1–16 (2020)
7. Li, X., et al.: A robust and energy efficient authentication protocol for industrial internet of things. IEEE Inter. Things J. 5(3), 1606–1615 (2017)
8. Mahmood, K., et al.: An enhanced and provably secure multi-factor authentication scheme for internet-of-multimedia-things environments. Comput. Electr. Eng. 88, 106888 (2020)
9. Alotaibi, M.: An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access. 6, 70072–70087 (2018)
10. Srinivas, J., et al.: Provably secure biometric based authentication and key agreement protocol for wireless sensor networks. J. Ambient Intell. Humaniz. Comput. 9(4), 875–895 (2018)
11. Li, X., et al.: A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. J. Netw. Comput. Appl. 103, 194–204 (2018)
12. Wu, F., et al.: A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client-server networks. Comput. Electr. Eng. 45, 274–285 (2015)
13. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: Proceedings of the 6th ACM conference on computer and communications security, 26–36 Association for Computing Machinery, New York (1999)
14. Hao, F., et al.: Combining crypto with biometrics effectively. IEEE Trans. Comput. 55(9), 1081–1088 (2006)
15. Bringer, J., et al.: Theoretical and practical boundaries of binary secure sketches. IEEE Trans. Inform. Forensic Secur. 3(4), 673–683 (2008)
16. Adamovic, S., et al.: Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. IET Biom. 6(2), 89–96 (2016)
17. Rathgeb, C., Uhl, A.: Adaptive fuzzy commitment scheme based on iris-code error analysis. In: Proceedings of the 2010 2nd European workshop on visual information processing, pp. 41–44. IEEE, Paris (2010)
18. Rathgeb, C., Uhl, A.: Systematic construction of iris-based fuzzy commitment schemes. In: Proceedings of the international conference on biometrics, 940–949 Springer, Berlin (2009)
19. Shi, S., et al.: Fingerprint recognition strategies based on a fuzzy commitment for cloud-assisted iot: a minutiae-based sector coding approach. IEEE Access. 7, 44803–44812 (2019)
20. Yang, W., et al.: Security and accuracy of fingerprint-based biometrics: a review. Symmetry. 11(2), 141 (2019)
21. Ma, L., et al.: Efficient iris recognition by characterizing key local variations. IEEE Trans. Image Process. 13(6), 739–750 (2004)
22. Ko, J-G., et al.: A novel and efficient feature extraction method for iris recognition. ETRI J. 29(3), 399–401 (2007)
23. Teh, A.B.J., Kim, J.: Secure biometric template protection in fuzzy commitment scheme. IEEE Electron. Express. 4(23), 724–730 (2007)
24. Nandakumar, K.: A fingerprint cryptosystem based on minutiae phase spectrum. In: Proceedings of the 2010 IEEE international workshop on information forensics and security, pp. 1–6. IEEE, Seattle (2010)
25. Daugman, J.: The importance of being random: statistical principles of iris recognition. Pattern Recogn. 36(2), 279–291 (2003)
26. Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. 27(3), 379–423 (1948)
27. Jain, A.K., et al.: Filterbank-based fingerprint matching. IEEE Trans. Image Process. 9(5), 846–859 (2000)
28. Zaeri, N.: Minutiae-based fingerprint extraction and recognition. Biometrics. IntechOpen, Rijeka (2011)
29. Bahgat, G.A., et al.: Fast and accurate algorithm for core point detection in fingerprint images. Egypt Inform. J. 14(1), 15–25 (2013)
30. Cai, D., et al.: Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. Pattern Recogn. 56, 50–62 (2016)
31. Menezes, A.J., et al.: Handbook of Applied Cryptography. CRC Press USA (1996)

**How to cite this article:** Shukla S, Patel SJ. Securing fingerprint templates by enhanced minutiae-based encoding scheme in Fuzzy Commitment. IET Inf. Secur. 2021;15:256–266. https://doi.org/10.1049/ise2.12024