Lahmidi *et al. EURASIP Journal on Information Security* (2022) 2022:3
https://doi.org/10.1186/s13635-022-00129-6

EURASIP Journal on Information Security

RESEARCH Open Access

On the methodology of fingerprint template protection schemes conception : meditations on the reliability

Ayoub Lahmidi[1*], Chouaib Moujahdi[2], Khalid Minaoui[1] and Mohammed Rziza[1]

Abstract

Among the most major potential attacks against fingerprint authentication systems are those that target the stored reference templates. These threats are extremely damaging as they can lead to the invasion of user privacy. The countermeasures to secure fingerprint templates are therefore an indisputable necessity. In literature, although there are so many approaches that address this kind of vulnerability, it turns out to be very difficult to generalize their uses. Given that each system has its own particularities, going from the fingerprint trait acquisition to the matching process, the majority of protection schemes, that are proposed as generic solutions, are not sufficiently mature for large-scale deployment. Consequently, we believe that the methodology of fingerprint template protection schemes conception should be oriented to build specific protection schemes for every unprotected system, which will provide the best compromise between performance and security compared to any generic protection solution. By adopting this methodology, we propose in this paper a new protection scheme for fingerprint templates that is well adapted to a well-known existing unprotected fingerprint minutia system. Our experimental results, obtained using standard benchmarks such as FVC 2002 DB1 and DB2, have proven that the proposed technique meets the requirements of revocability, unlinkability, non-invertibility, and high recognition accuracy.

Keywords: Template protection, Cancellable biometrics, Fingerprint minutiae, Performance accuracy, Revocability, Non-invertibility

1 Introduction

Biometrics is today one of the most emerging technologies; it has been successfully deployed in various government and organizational projects, being an excellent solution for personal authentication. The relevance of biometrics is mainly perceived in surveillance and access control environments since most biometric traits give high uniqueness that allows good authentication performance. These biometric identifiers have been able to simplify all the procedures of traditional authentication systems based on possession (e.g., ID cards) or knowledge (e.g., passwords). Thus, biometric authentication systems have proven a great superiority and high efficiency over traditional authentication ones. Biometric systems can be implemented under different modalities (e.g., face, voice, iris, fingerprint, etc.) that are more or less widespread according to their uniqueness, practicality, and technological maturity. The fingerprint remains among the most commonly used biometric modality due to its consistency, distinctiveness, and efficiency in terms of automatic recognition of individuals. Fingerprint-based authentication was therefore able to provide a cost-effective solution for personal recognition systems. However, although it is nowadays very emergent, it turns out that several challenges have surfaced, especially those related to attacks that threaten this kind of authentication system.

The most damaging type of vulnerability is the compromise of the reference fingerprint database. This attack

*Correspondence: ayoub_lahmidi2@um5.ac.ma
[1]LRIT Laboratory, associated unit to CNRST (URAC29), IT Rabat Center, Faculty of Sciences, Mohammed V University, Rabat, Morocco
Full list of author information is available at the end of the article

aims at recovering the stored fingerprint templates and then exploiting them to disclose the original form of fingerprints. In this context, a lot of works have proven that from the initial minutiae, the entire fingerprint image can be reconstructed [1–4]. This attack is considered to be the most critical risk that threatens biometric authentication systems in general, and particularly those that use fingerprints, especially when the stored templates are not secured or the applied protection mechanism is not robust enough (revertible). The original templates will therefore be lost forever as the users cannot change their fingers.

Protecting fingerprint templates before their storage for future verification is, therefore, an absolute requirement to face attacks on reference biometric templates. To address these security concerns, many works have been proposed in the literature and can be classified into three main categories: biometric cryptosystems, cancellable biometrics, and hybrid approaches that try to combine the principles of the two first categories.

For biometric cryptosystems [5], the principle of classical cryptosystems has been combined with the principle of biometric recognition to improve the security of personal authentication systems based on biometrics. The general principle of most biometric cryptosystems is as follows: during enrollment, an error-correcting code is applied to the biometric template and the user key to extract a data set called Helper Data. During authentication, an error correcting code is applied to the Helper Data and the test template to recover the user key. Depending on how the helper data is extracted, biometric cryptosystems can be divided into two categories [6]: *key-binding cryptosystems* and *key-generation cryptosystems*. When helper data is obtained using a key that is independent of biometric characteristics, it is a *key-binding cryptosystem*. If the helper data is derived only from the biometric template and the key is generated directly from the biometric characteristics, it is a *key-generation cryptosystem*. The most popular approaches in the *key-generation cryptosystem* category are systems known as: *Secure Sketch* [7] and *Fuzzy Extractor* [8].

For cancellable biometric approaches [9–11], they try to transform the original biometric templates in an irreversible way using a user-specific key, the resulting version is then stored in the database as a protected reference template. The same transformation process is performed during the verification phase with the presence of the same user key, then a matching process is conducted between the enrolled and the query template to generate a final decision (match/no match). Following this way, even if the reference template is compromised by a third party who intends to retrieve the original template, it will not be able to reverse it (only if the attacker has access to the user-specific key and the transformation function is invertible). Moreover, the compromised template can be replaced by another one generated with another user key. In this paper, we give more attention to cancellable biometric methods since they are the main focus of our contribution.

In practice, there are several other challenges in protecting fingerprint templates, namely the problems of handling intra-class variations and minutiae acquisition errors due to the elastic distortion of the fingerprint. These issues are commonly manifested in low-quality fingerprints through the presence of spurious minutiae or the loss of genuine ones. It should be noted here that two impressions of the same fingerprint do not necessarily contain the same features due to the circumstances of the acquisition. The accuracy performance, in this case, depends on the quality and quantity of the extracted minutiae and the way in which they are processed for the generation of the protected templates. In response to this variability, most of the solutions proposed in the literature trade security for performance or vice versa.

In general, a best practice fingerprint template protection scheme must meet these four requirements [12]:

- Revocability: It should be possible to revoke a compromised template and replace it with a new one generated using the same original unprotected biometric data.
- Unlinkability: Several protected templates can be generated from the same biometric data such that they do not match with each other.
- Non-invertibility: The inability, computationally, to reconstruct the original template from the compromised one.
- Performance: The preservation of accuracy performance after applying the protection on biometric templates.

In literature, the most of fingerprint template protection schemes have been proposed as generic solutions, and their conception have taken place without any consideration of the specifications of original systems to be protected. Indeed, each system has its own particularities and details, going from the feature extraction method to the matching process. However, we believe that the design methodology for fingerprint template protection schemes should be geared towards developing dedicated protection schemes for each unprotected system, making the best trade-off between performance and security over any generic protection solution. In this paper, we adopt this vision to design a new protection technique that is consistent with the specifications of an existing unprotected fingerprint minutia system [13] without any changes of the original modules of this last (i.e., feature extraction and matching).

The rest of this paper is structured as follows. A literature review of cancellable fingerprint approaches is presented in the next section. The proposed methodology/technique is described in Section 3. In Section 4, an evaluation of the proposed technique is conducted. Finally, we conclude the paper in Section 5.

2 Literature review of cancellable fingerprint approaches

In the context of cancellable biometrics, the majority of the proposed approaches for fingerprint template protection have been developed based on the minutiae properties (i.e., location and orientation information) to build their protection mechanisms. However, minutiae are well known for their variability reflected either by rotation, translation, non-linear distortion, or feature extraction errors. Therefore, maintaining a balance between the performance and security of the stored templates while addressing all these issues turns out to be a challenging task. Indeed, performance often deteriorates after applying a non-invertible transformation on original templates. Thus, we believe that, technically, the reliability of the protection system depends mainly on the choice of the transformation mechanism and the nature of the stored templates. In this context, we can classify minutiae-based approaches into three different categories. For the first category, simply minutiae sets are transformed into vectors, these last are used for the matching process (i.e., Classification step). For the second category, extracted minutiae sets are used to build new presentations that will used directly in the matching process. For the third category, minutiae sets are disordered to generate new sets that keep uniqueness and entropy.

Under the first category, Farooq et al. [14] proposed a scheme in which a fingerprint is converted into a binary string representation based on the invariant features extracted from a set of selected minutiae triplets, such as the three sides of the triangle, the three angles of the minutiae orientation, and the height of the largest side from the opposite minutia. Note that the geometry of the triangle formed by the minutiae triplets does not change under a rigid transformation. The resulting binary string representation is then randomized using a user key and stored in a database for later verification. In terms of robustness, this method has proven to be strong against brute force attacks but remains cost-intensive as it deals with the invariant features of each possible minutiae triplet.

Ahn et al. [15] presented an alignment-free technique based on a non-invertible transformation. The principle consists of hiding the original minutiae properties (positions and orientations) by deriving the relevant geometrical characteristics from minutiae triplets. This technique turned out to be a bit less promising in terms of accuracy performance. Jin et al. [16] have developed an alignment-free approach for fingerprint template protection. Based on a set of minutiae points, a binary representation is generated by a polar grid-based 3-tuple quantization. The bit-string is then permuted with a user key before being stored in the database. This proposal guarantees revocability and diversity, but it is not promising enough in terms of performance in the case of low-quality fingerprint images. In their turn, Kho et al. [17] were able to generate a finite binary vector representing the protected fingerprint template. The proposed approach is based on the use of a free-alignment partial local structure (PLS) descriptor, the transformation is then formulated as a permutated randomized non-negative least square (PR-NNLS) optimization problem, to make the template more discriminative. Subsequently, a random projection and permutation are applied to the resulting representation of the PR-NNLS to ensure the revocability and unlinkability properties. However, the application of this scheme results in changing the feature extraction module on the unprotected system.

For the second category, Ferrara et al. [18] were inspired by the work of Cappelli et al. [19] to propose another version of Minutia Cylinder-Code (MCC) that improves the original MCC and generates more secure fingerprint templates. Briefly, the scheme seeks to encode the extracted information between the reference minutia and its surroundings through cylinders (local descriptor). The technique seems to trade performance for robustness. Moujahdi et al. [20] introduced a new concept of protection which consists in transforming the minutiae-based representation into a spiral curve form. The construction of the curves is based on the order of distances between singular points and all extracted fingerprint minutiae. The problem with this scheme is that once the fingerprint curve is compromised, the distances used to generate the protected template can be disclosed. In addition, it cannot be applied if singular points are absent or cannot be extracted successfully. Several works were conducted thereafter to improve the robustness of the scheme [21–24].

For the last category, among the most popular realizations, we refer to the work of Ratha et al. [25] where three types of non-invertible transformations have been proposed, namely, Cartesian, Polar, and Functional. The technique consists of geometrically transforming the minutiae with respect to the core point. The resulting templates provide great non-invertibility but are not discriminating enough to achieve a good accuracy performance. Recently, Ali et al. [26] have put forward a secure transformation that takes the positional information of minutiae points to create a protected fingerprint template. For each minutiae point, a modified location is produced based on its neighboring minutiae information and the user key parameters. The final two-dimensional representation is secured and

ensures the requirement of revocability. This technique has been later improved in [27], starting from the fact that neighboring minutiae points are sensitive and therefore reduce the system accuracy. They made use of the singular point information instead of the nearby minutiae to generate the protected template. According to the results obtained, the latter improves performance particularly in the FVC 2002 DB1 database. Our proposed protection scheme in this paper is in fact in line with these types of approaches which consist in displacing the minutiae of the original template to new locations using specific key-sets, except that our approach as mentioned above is founded on the matching process specifications using by an unprotected system.

As we have said in the previous section, the majority of techniques do not consider the specifications of the unprotected system, and also no comparison has been given between protected and unprotected systems in their experimentation. In the next section, we will present our proposed methodology to build a new fingerprint template protection scheme that is consistent with the specifications of an existing unprotected fingerprint system.

3 Proposed methodology

The design methodology we conduct in this paper is not the one usually found in standard fingerprint template protection works. Indeed, we have adopted a reflection starting from a well-known process of fingerprint minutiae matching, namely the one proposed in [13], whose purpose is to find the correspondence of two minutiae sets without the involvement of global features. The concept we have put forward entails converting the original fingerprint template using a non-invertible transformation such that the fingerprint matching process remains functional even in the transformed domain. It is for this reason that we have made sure to preserve the same quality of minutiae. We, therefore, suggest a technique that leads to some disruption in terms of the locations and orientations of the original minutiae, resulting in a new fingerprint template. To be consistent with the applied matching process, the compared fingerprint template must not contain singular points. Hence, we have taken care to respect this requirement by exploiting the singular points just to carry out the transformation and exclude them from the transformed minutiae set. In the next two subsections, we introduce first the used unprotected system, and then we describe the proposed protection scheme.

3.1 Unprotected system

Over the last decades, the matching process has always been considered a challenging task in fingerprint authentication systems, especially when facing the critical problem of intra-class variations (acquisitions from the same finger undergo a high degree of variability). According to [28], fingerprint matching can be generally classified into three main families:

- Correlation-based matching: It is a process that consists of computing the correlation between the pixel values of the query fingerprint image and those of reference for different alignments.
- Minutiae-based matching: The most used technique in fingerprint pattern recognition. It is mainly based on the minutiae points features (i.e., locations and orientations). The aim is to reach the alignment between two fingerprint templates that gives rise to the maximum number of minutiae pairs.
- Non-minutiae feature-based matching: This technique relies on the comparison of other features of the fingerprint ridge pattern that can be better extracted than the minutiae features, such as local orientation, frequency, ridge shape, and texture information.

In the present work, we have dealt with the minutiae-based matching category, which in turn can be divided into local and global minutiae matching. The local minutiae matching performs the comparison between two fingerprints based on their local minutiae structures. These are defined with respect to the minutiae neighborhoods (often in terms of Euclidean distances). The purpose is to make use of properties that can be extracted in this area and that are invariant to global transformations (e.g., translation, rotation). While the global minutiae matching, which reflects the uniqueness of the compared fingerprints. The idea is to achieve alignment of minutiae through global features such as singular points or orientation fields.

A particular fingerprint minutia matching approach has been introduced by Jiang and Yau [13], where both types of minutiae matching are involved (local and global structures). The idea behind this is to first search for the best similar minutia pair between two fingerprints using a local minutiae descriptor, which is based on invariant features (distances and angles) extracted from the minutiae neighborhoods. The task is to identify the most similar local structures. Then, a global consolidation is elaborated which consists of making an alignment according to the selected minutia in each fingerprint.

Given that each acquired minutia $\{M_i \mid i = 1, ..., n\}$ is presented as the feature vector $F_i = (x_i, y_j, \theta_i, t_i)$, where (x, y) are the coordinates in the Cartesian plane, θ is the minutia orientation angle and t refers to the minutia type (ridge ending or ridge bifurcation). The first step of this fingerprint minutiae matching consists of defining the local structure of each minutia involving its two nearest neighbors, then extracting the rotation and translation invariant features that can be formed within the neighborhood. Considering M_j and M_k the two nearest neighbors

of M_i (where M_j is the first closest to M_i and M_k is the second closest). The resulting local feature vector FV_i related to M_i can be written as follows:

$$FV_i = (d_{ij}, d_{ik}, \alpha_{ij}, \alpha_{ik}, \phi_{ij}, \phi_{ik}, n_{ij}, n_{ik}, t_i, t_j, t_k) \quad (1)$$

where d_{ij} is the Euclidean distance between M_i and M_j, α_{ij} represents the orientation difference between θ_i and θ_j, ϕ_{ij} corresponds to the orientation difference between θ_i and the orientation of the edge linking M_i and M_j. n_{ij} refers to the ridge count between M_i and M_j, and t_i is the minutia type of M_i (Fig. 1 illustrates some of these features).

The next step of the process aims at finding the most similar minutia pair between the reference and query fingerprint templates. This is done through an exhaustive search strategy where all local feature vectors extracted from the reference template are compared with those of query one. The obtained best matching structure pairs are then used to perform an alignment between the two fingerprints. All remaining minutiae will be aligned based on the minutiae pair by converting them into the polar coordinate system. Finally, a score is calculated considering the contributions of the two matching steps. In this paper, we will study the case of an unprotected system using our configuration of this minutia matching algorithm (described in Section 4.1).

3.2 Proposed protection scheme

The protective nature of the fingerprint templates proposed in this work is a kind of disorder provoke at the minutiae locations and orientations, achieved mainly through a specific key that the user is expected to provide during authentication. The generated template is a set of minutiae with different characteristics which is actually designed to be revocable and non-invertible, i.e., the system is able to generate multiple protected templates from the same fingerprint impression using different keys such that there is no correlation between the templates. Furthermore, when the generated template is intercepted, it is almost impossible to reveal any meaningful data. The main idea behind the proposed protection technique is to build four different groups of minutiae where each group will undergo a particular transformation according to the user key parameters. In the following, we describe the process of generating a secure template using our proposal which contains three main steps:

(i) Invariant features extraction.
(ii) Home group designation.
(iii) Minutiae transformation.

All the steps required to build the protected template are presented in Algorithm 1.

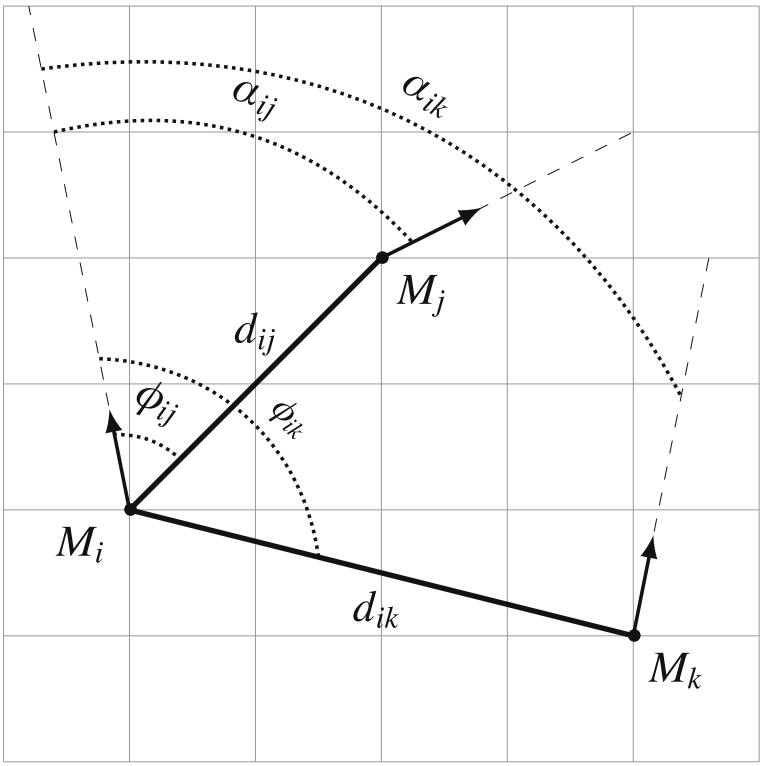

Fig. 1 Properties of the local structure involved in [13]

Algorithm 1 Generation of a protected template

Input: *Minutiae locations and orientations from a fingerprint image* $M_i = \{(x_i, y_i, \theta_i) \mid i = 1, ..., n\}$; *User key* $\{(\delta_1, \lambda_1), (\delta_2, \lambda_2), (\delta_3, \lambda_3), (\delta_4, \lambda_4)\}$; Singular Point $SP = \{(x_{SP}, y_{SP})\}$;

Output: *Modified minutiae locations and orientations* $M'_i = \{(x'_i, y'_i, \theta'_i) \mid i = 1, ..., n\}$;

// *initialize the minutia counter*
$i \leftarrow 1$;
// *Declare four empty structures*
$Grp_1 \leftarrow [\,]$; $Grp_2 \leftarrow [\,]$; $Grp_3 \leftarrow [\,]$; $Grp_4 \leftarrow [\,]$;
while $i \leq n$ **do**
  // *Invariant features extraction*(3.2.1)
  // *The label corresponding to the zone where* M_i *resides with respect to SP*
  $P_i \leftarrow Label(Position(M_i, SP))$;
  // *The label corresponding to the angle between the orientation of* M_i *and the orientation of the edge linking* M_i *and SP in counter-clockwise rotation*
  $A_i \leftarrow Label(Angle(M_i, SP))$; (Eq. 2)
  $B_i \leftarrow A_i \oplus P_i$;
  // *Home group designation* (3.2.2)
  if $B_i == 00$ **then**
    $Affect(M_i, Grp_1)$; // *Assign* M_i *to* Grp_1
  else if $B_i == 01$ **then**
    $Affect(M_i, Grp_2)$;
  else if $B_i == 10$ **then**
    $Affect(M_i, Grp_3)$;
  else
    $Affect(M_i, Grp_4)$;
  end if
  $i \leftarrow i + 1$;
end while
// *Minutiae transformation* (3.2.3)
// *initialize a counter k to browse groups and pairs of parameters*
$k \leftarrow 1$;
while $k \leq 4$ **do**
  if $IsEmpty(Grp_k) == False$ **then**
    // *For each minutia* M_j *of* Grp_k
    for $j = 1$ to $size(Grp_k)$ **do**
      $\begin{bmatrix} x_j^{Rot} \\ y_j^{Rot} \end{bmatrix} \leftarrow \begin{bmatrix} \cos(\delta_k) & -\sin(\delta_k) \\ \sin(\delta_k) & \cos(\delta_k) \end{bmatrix} \begin{bmatrix} x_j - x_{SP} \\ y_j - y_{SP} \end{bmatrix} + \begin{bmatrix} x_{SP} \\ y_{SP} \end{bmatrix}$;
      $\begin{bmatrix} x'_j \\ y'_j \end{bmatrix} \leftarrow \lambda_k \cdot \begin{bmatrix} x_j^{Rot} - x_{SP} \\ y_j^{Rot} - y_{SP} \end{bmatrix} + \begin{bmatrix} x_{SP} \\ y_{SP} \end{bmatrix}$;
      $\theta'_j \leftarrow \theta_j + \delta_k$;
      // *Replace* M_j *with* $M'_j(x'_j, y'_j, \theta'_j)$ *in* Grp_k
      $Replace(M_j, M'_j)$;
    end for
  end if
  $k \leftarrow k + 1$;
end while
// *Concatenate all groups to make a single set of transformed minutiae*
$Concatenate(Grp_1, Grp_2, Grp_3, Grp_4)$;
return $M'_i = \{(x'_i, y'_i, \theta'_i) \mid i = 1, ..., n\}$;

3.2.1 Invariant features extraction

The first step concerns the derivation of two invariant features for each acquired minutia, formed between the concerned minutia and the main singular point (referred to as *SP*). The first property to be determined is the position of the minutiae with respect to *SP*. For this purpose, the two-dimensional space is partitioned into four zones according to three radiuses r_1, r_2, r_3(empirically set) defined around *SP*. The areas formed are labeled respectively as 00, 01, 10 and 11 as shown in Fig. 2. For each minutia M_i, the two bits that refer to the area to which the minutia in question belongs are assigned to P_i. The second property concerns the angle β_i between the orientation of the minutia M_i and the orientation of the edge linking the position of M_i and *SP* in counter-clockwise rotation as shown in Fig. 3. Depending on the angle value of β_i, two bits are assigned to A_i as described below.

$$A_i = \begin{cases} 00 & \text{if } \beta_i < \dfrac{\pi}{2}, \\ 01 & \text{if } \dfrac{\pi}{2} \leqslant \beta_i < \pi, \\ 10 & \text{if } \pi \leqslant \beta_i < \dfrac{3\pi}{2}, \\ 11 & \text{if } \dfrac{3\pi}{2} \leqslant \beta_i \end{cases} \tag{2}$$

3.2.2 Home group designation

During this phase, each minutia M_i is attributed to one of the four previously defined groups depending on the values of P_i and A_i. To establish the allocation, the system carries out an exclusive OR (XOR) operation between P_i and A_i leading to two new bits. The resulting bits are responsible for deciding which group it will belong to and therefore which parameters of the transformation will be applied, considering that the four predefined groups are beforehand referenced respectively as 00, 01, 10 and 11. Each minutia is assigned to the home group whose reference coincides with the result of the the exclusive OR (XOR). As a result, there will be four groups of different

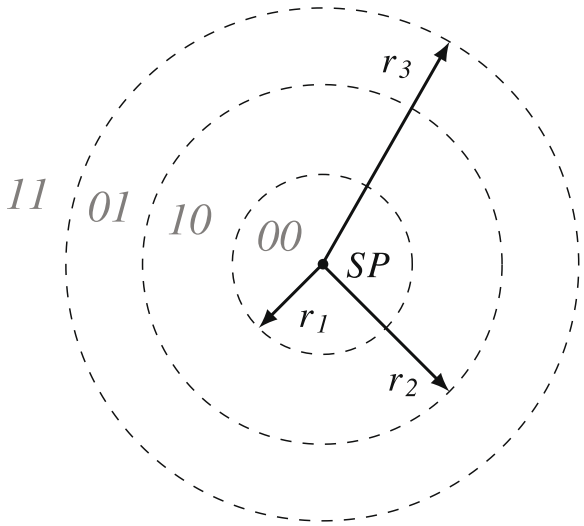

Fig. 2 Split of the two-dimensional space into four zones according to r_1, r_2, r_3 and *SP*

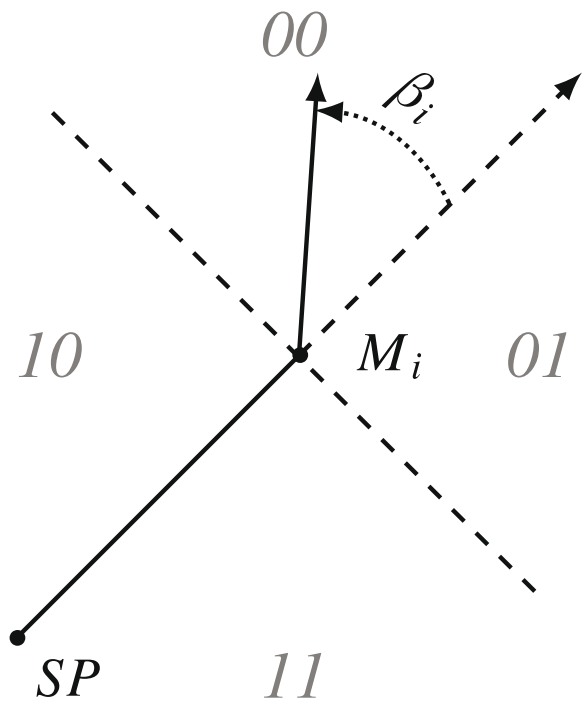

Fig. 3 Representation of the angle β_i between the orientation of a minutia M_i and the orientation of the edge linking M_i and SP in counterclockwise rotation

minutiae. This way of distribution actually prevents from applying the same transformation on minutiae that have close features, thus causing a disorder which is hard to reverse.

3.2.3 Minutiae transformation

After assigning each minutia to its home group, each group is exposed to a specific transformation, i.e., all minutia from the group will be subjected to the same transformation, which is carried out essentially with the help of a set of parameters that is supposed to be represented by a user key. The user key is made up of four pairs of parameters (Eq. 3) referenced also respectively as 00, 01, 10, and 11. Each group is concerned by the transformation whose group label is the same as the user key parameter pair label.

$$Key^{user} = \{(\delta_k, \lambda_k)^{user}\}_{k=1}^{4} \tag{3}$$

Suppose that the pair (δ_k, λ_k) corresponds to the transformation parameters of the group to which M_i belongs. The transformation of $M_i(x_i, y_i)$ consists in performing a rotation around the main singular point $SP(x_{SP}, y_{SP})$ with an angle δ_k in the counter clockwise direction (Eq. 4). The resulting point (x_i^{Rot}, y_i^{Rot}) will then be used to construct an image by homothety taking as center $SP(x_{SP}, y_{SP})$ and λ_k as ratio of the homothety (Eq. 5). The position of the new minutia M_i' is represented by the Cartesian coordinates (x_i', y_i').

As a result, all fingerprint minutiae acquire new positions in the two-dimensional space after the transformation, while in terms of orientation, their initial ones are added to the corresponding angle δ. In the end, the four groups are concatenated to give rise to a new set of minutiae representing the protected template.

$$\begin{bmatrix} x_i^{Rot} \\ y_i^{Rot} \end{bmatrix} = \begin{bmatrix} \cos(\delta_k) & -\sin(\delta_k) \\ \sin(\delta_k) & \cos(\delta_k) \end{bmatrix} \begin{bmatrix} x_{M_i} - x_{SP} \\ y_{M_i} - y_{SP} \end{bmatrix} + \begin{bmatrix} x_{SP} \\ y_{SP} \end{bmatrix} \tag{4}$$

$$\begin{bmatrix} x_i' \\ y_i' \end{bmatrix} = \lambda_k \cdot \begin{bmatrix} x_i^{Rot} - x_{SP} \\ y_i^{Rot} - y_{SP} \end{bmatrix} + \begin{bmatrix} x_{SP} \\ y_{SP} \end{bmatrix} \tag{5}$$

4 Experimental results and discussions

In this section, we present an evaluation of the proposed fingerprint protection technique over the two fingerprint databases FVC2002 DB1 and DB2. Each of these databases includes 100 fingers, where each one is presented by 8 impressions of different qualities, resulting in a total of 800 fingerprint impressions per database. To retrieve the minutiae and singular point features, the trial version of the commercial software VeriFinger SDK 6.02 was used.

In this evaluation, we have used many performance factors, namely, the FAR (false acceptance rate), the FRR (false rejection rate), the EER (equal error rate), and the ROC (the receiver operating characteristic) curve which expresses the accuracy performance of the systems. We also made use of the genuine-imposter distribution to otherwise express the system verification performance. For this purpose, the genuine and impostor scores are involved. The genuine scores are calculated by comparing each fingerprint impression with the remaining from the same finger, while the imposter scores are obtained by comparing each fingerprint impression with all the other ones from different fingers. To further explain the separations between the genuine-impostor distributions, we used the Kolmogorov-Smirnov test [29] which provides a value between 1 and 0, a value close to 1 means a better separation.

4.1 Evaluation configurations

The evaluation strategy followed in the present study was similar to that used in [30–32], which consists of comparing the template generated from the first impression with the one constructed from the second impression of the same finger to obtain the FRR, while the template of the first impression is compared with the one built from the first impression of the rest of the fingers when it comes to the FAR. According to the used strategy on FVC 2002 DB1 and DB2, a total of 100 genuine and 9900 (99×100) impostor scores are provided per each database.

Table 1 The EER values obtained from unprotected system, different-key, and stolen-key scenarios on FVC 2002 DB1 and DB2

	FVC 2002 DB1	FVC 2002 DB2
Unprotected system	1.02%	0.13%
Different-key scenario	0%	0%
Stolen-key scenario	3.09%	1.83%

As previously described, The minutiae transformation performed by the proposed system is mainly based on singular points. We have therefore extracted for each fingerprint impression only the nearest singular point to the image center, considering that only fingerprint impressions where singular points are detected are put into use.

Our own implementation of the used matching process has imposed a slightly modified configuration compared to the one defined in [13]. In fact, we only used the first six elements in Eq. 1 with an adjustment appropriate to the number of properties used. On another hand, it should be noted that the fingerprint minutia matching was evaluated in the reference paper on a fingerprint database captured via the Veridicom CMOS sensor of size 300 × 300 pixels, while the present study concerned as previously indicated the two public fingerprint databases FVC 2002 DB1 and DB2. The empirical values of the radiuses (r_1, r_2, r_3) involved in this work and for which the experiments have been performed were respectively: 100, 200, and 300.

The requirements considered in this evaluation are the performance accuracy under two different scenarios (different-key and stolen-key), revocability, unlikability, and non-invertibility.

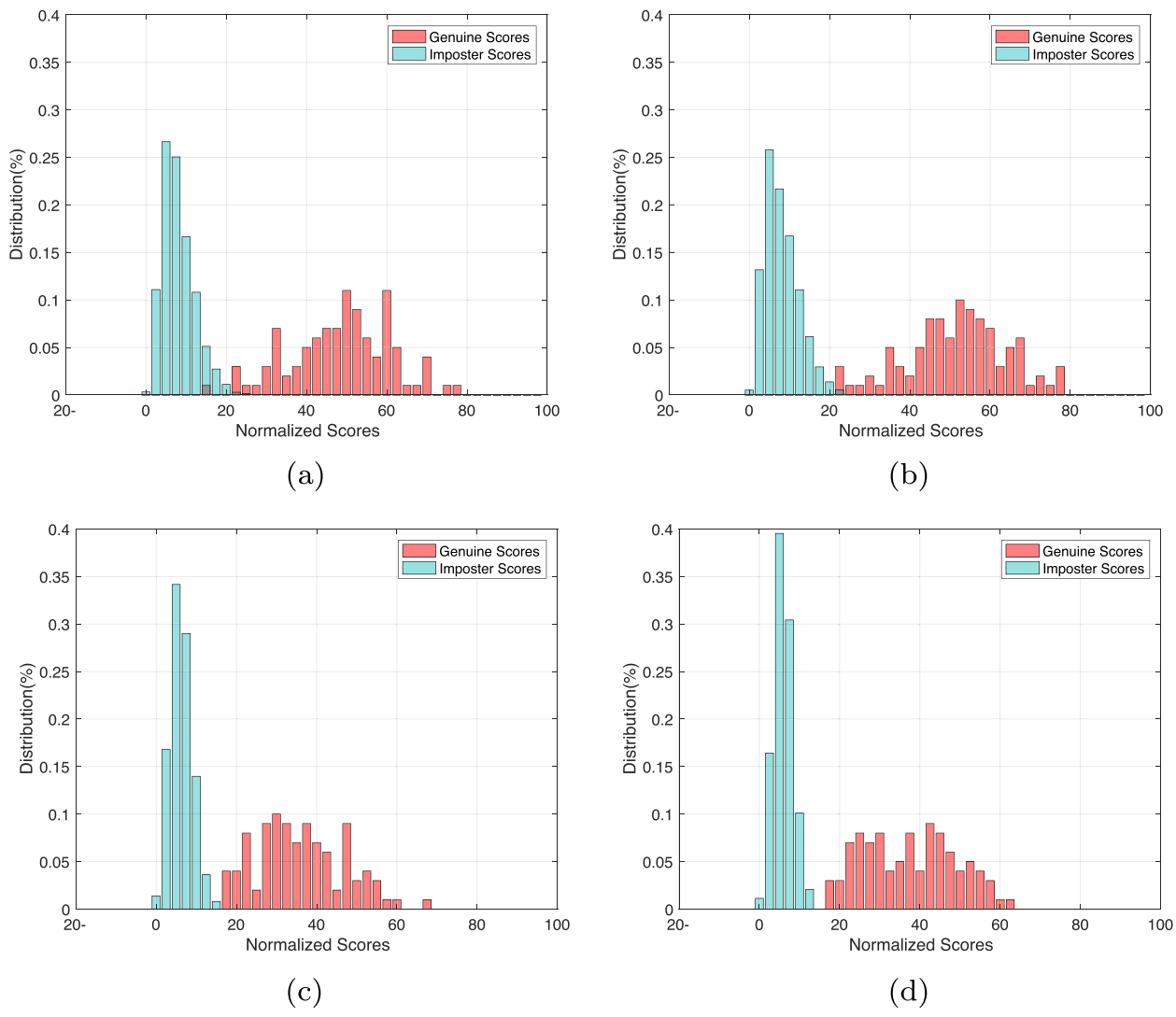

Fig. 4 The genuine-imposter scores distribution for the unprotected system on FVC 2002 DB1 (**a**) and DB2 (**b**), and for the proposed system under Different-key scenario on FVC 2002 DB1 (**c**) and DB2 (**d**)

Table 2 The Kolmogorov–Smirnov tests for unprotected system, different-key, and stolen-key scenarios on FVC 2002 DB1 and DB2

	FVC 2002 DB1	FVC 2002 DB2
Unprotected system	0.9856	0.9972
Different-key scenario	1	1
Stolen-key scenario	0.9582	0.9632

4.2 Performance accuracy

To study the proposed fingerprint system behavior in terms of recognition performance, we are going to compare the accuracy of the unprotected system (use of initial fingerprint templates) with the accuracy of the protected system where each user holds a specific user key (different-key scenario). The objective is to investigate the impact of user keys on the protected templates discriminability. According to the experimental results, it turns out that the EER obtained from the unprotected system on both FVC 2002 DB1 and DB2, respectively, yielded 1.02% and 0.13% (Table 1), while the protected system under Different-key scenario achieved perfect results with 0% EER for both databases. This means that the use of keys makes the fingerprint templates more meaningful and discriminant in terms of accuracy verification. It can be confirmed in Fig. 4 which represents the genuine-impostor scores distribution of both the unprotected and protected system. We can clearly observe that the protected system distributions are quite separate compared to the unprotected system ones. According to the Kolmogorov-Smirnov test results shown in Table 2, the distributions separation from the protected system achieved a value of 1 for both databases (a total separation), whereas those of the unprotected system, respectively, reflect 0.9856 and 0.9972 for FVC 2002 DB1 and DB2, which means that there are overlaps between the distributions.

For the stolen-key scenario, which describes the event where an impostor intercepts the key of a legitimate user, and then attempts to gain access to the system, a simulation has been carried out in this context, it consists in using the same key for all the database users. From the plot in Fig. 5 which depict the genuine-imposter scores distribution under stolen-key scenario as well as Table 1, the resulting EER values were, respectively, 3, 09% and 1.83% for FVC 2002 DB1 and DB2, with a separability of 0.9582 and 0.9632 (Table 2). It is important to note that this is quite normal for the system to react in this way under such a scenario. the performance was not significantly degraded, which proves that the system can reach a certain level of robustness under the stolen-key attack scenario. In the same context, we can notice from Table 3 that the proposed system shows its superiority compared to several state-of-the-art methods that have used the same evaluation protocol. This is obviously due to the fact that the conception of the proposed technique was carried out on the basis of the unprotected system and therefore the methodology followed was fruitful in terms of performance. On another hand, It appears that the performance accuracy on DB2 is superior than DB1 as illustrated by the receiver operating characteristic curve in Fig. 6; this is due to the quality of fingerprint impressions acquired from DB2 which is much better than DB1.

4.3 Revocability

Revocability is a primary requirement in fingerprint template protection schemes. This property manifests by replacing a compromised fingerprint template (due to an attack on the template database) with another one gener-

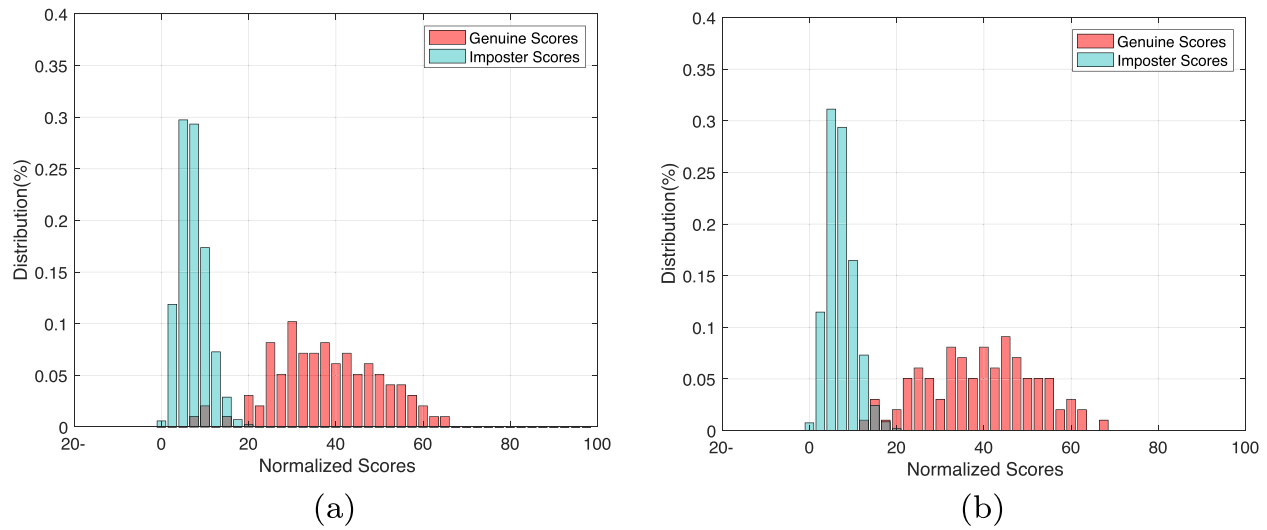

Fig. 5 The genuine-imposter scores distribution for the proposed system under stolen-key scenario on FVC 2002 DB1 (**a**) and DB2 (**b**)

Table 3 The EER(%) comparison with some state-of-the-art methods under *stolen-token* scenario on FVC2002 DB1 and DB2

Method/dataset	FVC 2002 DB1	FVC 2002 DB2
Ahmad et al. [30]	9	6
Ali et al. [26]	2	1
Ali et al. [27]	1.63	1
Jin et al. [16]	5.19	5.65
Jin et al. [33]	4.36	1.77
Sandhya and Prasad [34]	4.71	3.44
Sandhya et al. [35]	3.96	2.98
Wang and Hu [36]	3.5	4
Wang and Hu [37]	3	2
Yang et al. [38]	5.93	4
Yang et al. [39]	3.38	0.59
Proposed scheme	3.09	1.83

ated from the same fingerprint trait in such a way that the compromised and revoked templates are highly dissimilar. The process of revocation consists simply of using a new user key to generate a new protected template as shown in Fig. 7. To evaluate our proposal in terms of revocability, the revoked template attack [26] will be considered, where an opponent attempts to target the system with a compromised fingerprint template. In such a scenario, there are two types of attacks: Type-1, the compromised template is substituted by another one generated from the same fingerprint image using a different user key, and type-2, the compromised template is substituted by another one generated from a different fingerprint image of the same finger using a different user key. After experimenting on both FVC 2002 DB1 and DB2, the percentage of successful verification was 0%, which means that there is a total dissociation between the compromised and revoked templates. This proves for sure that the system is sufficiently robust against the revoked template attack and therefore revocable.

4.4 Unlinkability

Unlinkability or diversity refers to the potential of generating several distinct templates from the same biometric trait such that all of them do not have any kind of linkability not only with the original template but also with each other. To evaluate the system in terms of unlinkability, we consider two systems carrying out different transformations on the same fingerprint impressions. The first system randomly takes user key parameters from the following ranges: $\{\delta_i\}_{i=1}^{4} \in [0, 90]$, $\{\lambda_i\}_{i=1}^{4} \in [-1, 0]$. While the second system involves the following ones: $\{\delta_i\}_{i=1}^{4} \in [180, 270]$, $\{\lambda_i\}_{i=1}^{4} \in [2, 3]$. The aim of the test is to construct the pseudo-genuine scores distribution by matching the transformed fingerprint templates of the same finger generated from system 1 with those produced from system 2. From the plot in Fig. 8, we can notice that there is no overlap between the pseudo-genuine and genuine distributions. The separability according to Kolmogorov-Smirnov test achieve a value of 1 (total separation) for the two databases. the pseudo-genuine scores distribution is therefore almost identical to that of the impostors (Fig. 4c and d), which explains that although the templates are generated from the same fingerprint impression they are unmatched each other. Hence, we can

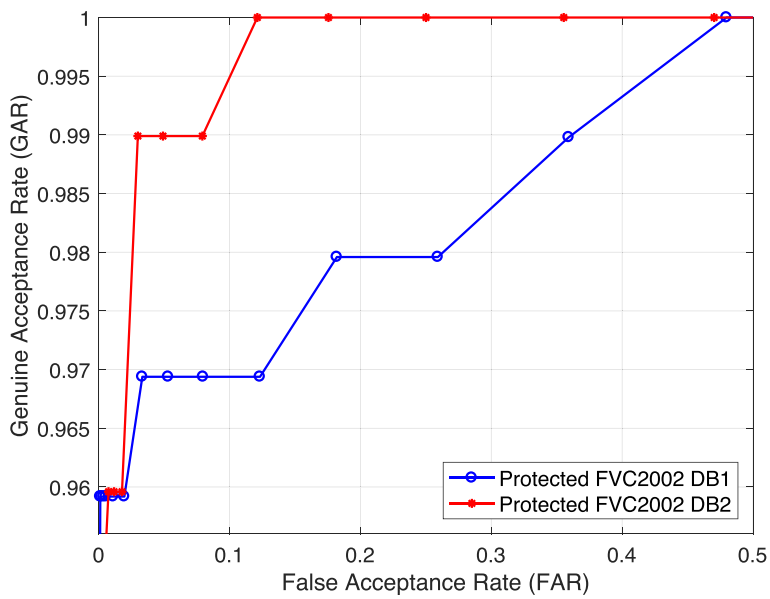

Fig. 6 The ROC curve under stolen-token scenario for FVC 2002 DB1 and DB2

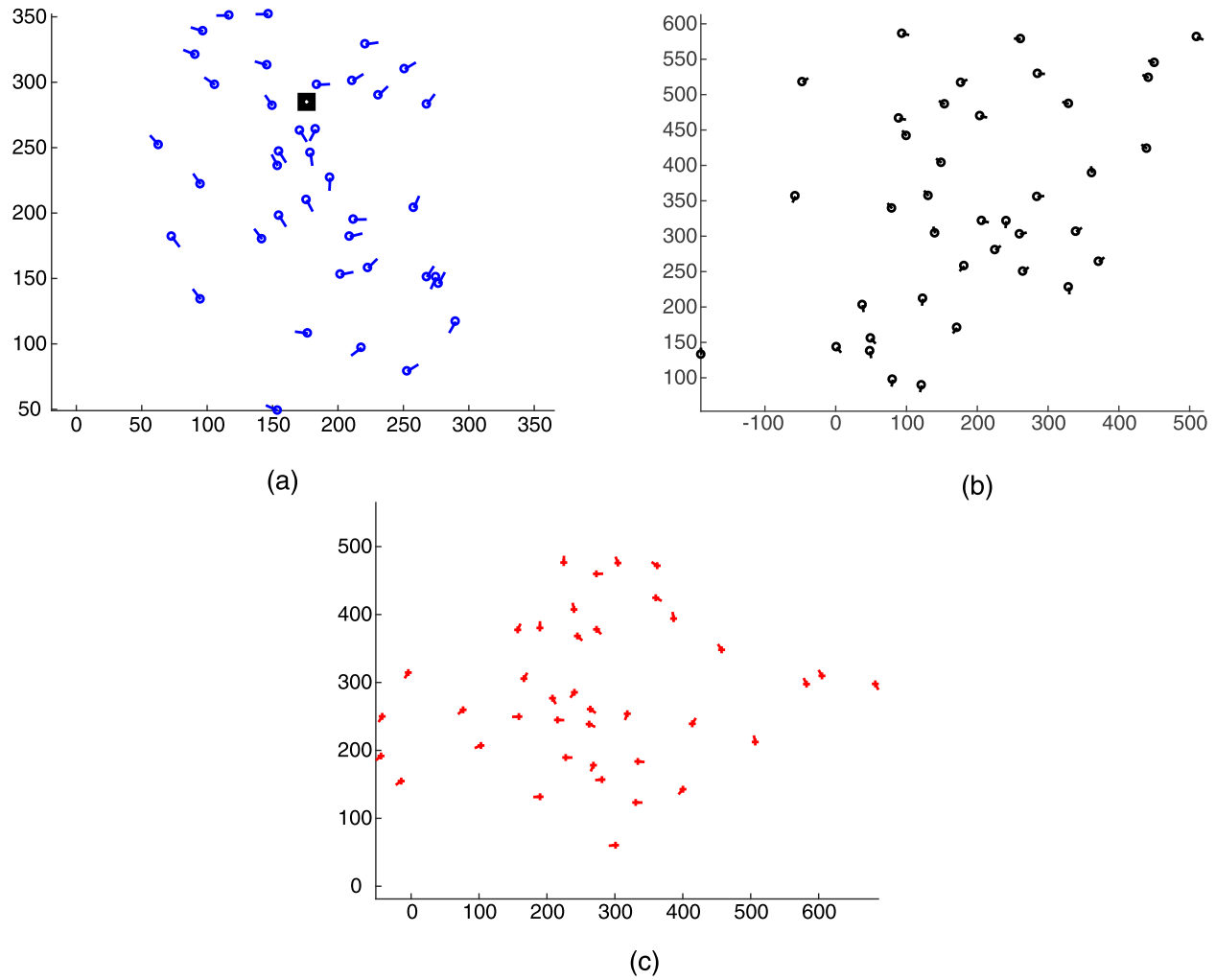

Fig. 7 Transformation of an original fingerprint template using two different sets of user key parameters. **a** Original template, **b** transformed template using the first set, and **c** transformed template using the second set

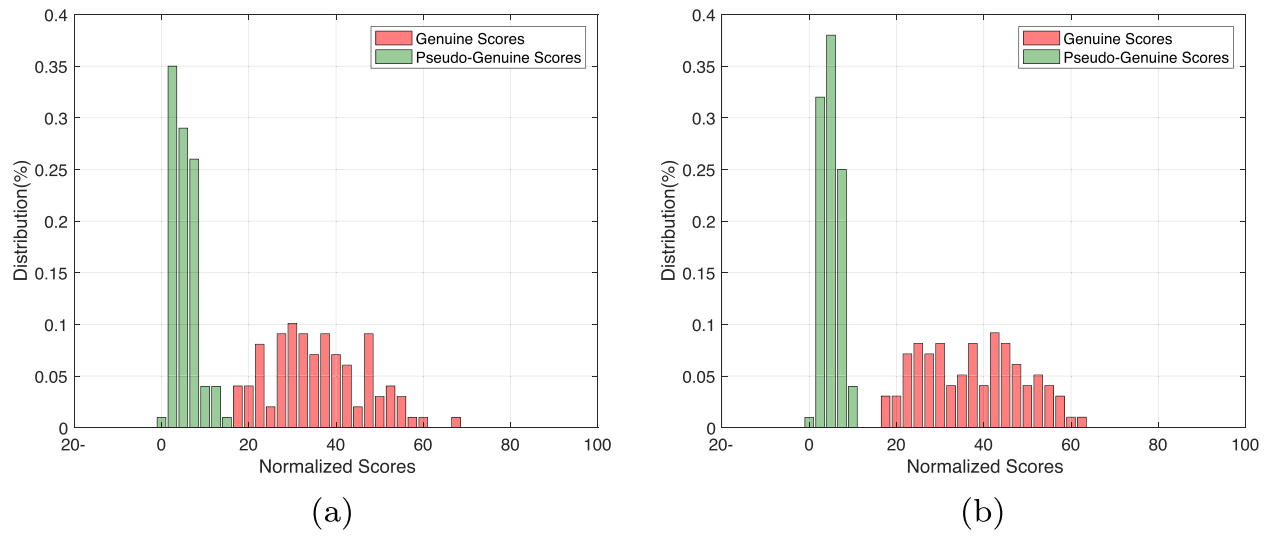

Fig. 8 The genuine-pseudo-genuine scores distribution for FVC 2002 DB1 (**a**) and DB2 (**b**)

claim that the proposed system complies with the diversity requirement.

4.5 Non-invertibility

The non-invertibility means the possibility of disclosing a partial or whole of the original template (template without transformation). A robust protection scheme must be able to make the original biometric templates hard to reconstruct in order to guarantee the user privacy. For the purpose of studying the possibilities of revelation in case of template inversion attack on our system, we assume that a protected template is intercepted by an adversary. In this situation, the opponent can get all modified minutiae positions and orientations from the compromised template (after the transformation). However, these information can not lead to those of the original domain since the transformation conducted in the proposed scheme is based mainly on the position of the used singular point and the set of user key values. In fact, with the lack of these information, the adversary cannot in any case calculate the original minutiae positions and orientations. The led transformation is actually a kind of rotation and homothety operations which take as center the singular point. The implication of this point is crucial to perform the linear changes as well as the values of δ and λ provided by the user key, where δ refers to the angle of rotation and λ represents the homothety ratio. Therefore, even if the adversary is under possession of both the compromised template and the user key parameters with which it was generated, and attempts to reach the initial minutiae information, he will be unable to reverse the homothety or the rotation as he is ignoring the singular point position as well as the distances between the minutiae and the singular point. Even if the opponent performs a brute force attack on the singular point, it leads nowhere.

5 Conclusion and perspective

The challenge of biometric protection schemes is to maintain both a high level of security and high verification accuracy. In this paper, we have adopted a new methodology for the conception of fingerprint template protection schemes. Indeed, we have taken in consideration the specification of an unprotected fingerprint verification system to build a specific protection scheme that provides the best compromise between performance and security. The proposal is a minutiae-based technique that causes disorders in terms of minutiae features and produces a new different template that perfectly satisfies revocability, diversity, security, and performance. Using the public fingerprint datasets, FVC 2002 DB1 and DB2, the experimental results show that the proposed system under the different-key scenario improves the diversity of the fingerprint templates and makes them more discriminative compared to the unprotected system. While in the stolen-key scenario, the performance has slightly degraded but remains generally acceptable over several state-of-the-art methods. As future work, we plan to extend our evaluation on other databases with lower fingerprint qualities (e.g., FVC 2002 DB3, FVC 2002 DB4, FVC 2004 DB1, and FVC 2004 DB2). We also intend to improve the used minutiae matching process to achieve perfect results in the unprotected system, using for example other properties in the local structure of minutiae.

Authors' contributions
All authors contributed to the design of this research. The authors read and approved the final manuscript.

Funding
Not applicable.

Availability of data and materials
Not applicable.

Declarations

Competing interests
The authors declare that they have no competing interests.

Author details
[1]LRIT Laboratory, associated unit to CNRST (URAC29), IT Rabat Center, Faculty of Sciences, Mohammed V University, Rabat, Morocco. [2]Scientific Institute, Mohammed V University, Rabat, Morocco.

Received: 12 July 2021 Accepted: 23 February 2022
Published online: 25 March 2022

References

1. A. Ross, J. Shah, A. K. Jain, From template to image: reconstructing fingerprints from minutiae points. IEEE Trans. Patt. Anal. Mach. Intell. **29**(4), 544–560 (2007). https://doi.org/10.1109/tpami.2007.1018
2. R. Cappelli, D. Maio, A. Lumini, D. Maltoni, Fingerprint image reconstruction from standard templates. IEEE Trans. Patt. Anal. Mach. Intell. **29**(9), 1489–1503 (2007). https://doi.org/10.1109/tpami.2007.1087
3. J. Feng, A. K. Jain, Fingerprint reconstruction: from minutiae to phase. IEEE Trans. Patt. Anal. Mach. Intell. **33**(2), 209–223 (2011). https://doi.org/10.1109/tpami.2010.77
4. K. Cao, A. K. Jain, Learning fingerprint reconstruction: from minutiae to image. IEEE Trans. Inf. Forensics Secur. **10**(1), 104–117 (2015). https://doi.org/10.1109/tifs.2014.2363951
5. U. Uludag, S. Pankanti, S. Prabhakar, A. K. Jain, Biometric cryptosystems: issues and challenges. Proc. IEEE. **92**(6), 948–960 (2004)
6. C. Rathgeb, A. Uhl, A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. **2011**(1), 1–25 (2011)
7. J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, G. Zemor, Theoretical and practical boundaries of binary secure sketches. IEEE Trans. Inf. Forensic Secur. **3**(4), 673–683 (2008)
8. Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. SIAM J. Comput. **38**(1), 97–139 (2008)
9. V. M. Patel, N. K. Ratha, R. Chellappa, Cancelable biometrics: a review. IEEE Signal Process. Mag. **32**(5), 54–65 (2015). https://doi.org/10.1109/msp.2015.2434151
10. W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, Security and accuracy of fingerprint-based biometrics: a review. Symmetry. **11**(2), 141 (2019). https://doi.org/10.3390/sym11020141
11. A. K. Trivedi, D. M. Thounaojam, S. Pal, Non-invertible cancellable fingerprint template for fingerprint biometric. Comput. Secur. **90**, 101690 (2020). https://doi.org/10.1016/j.cose.2019.101690
12. A. K. Jain, K. Nandakumar, A. Nagar, Biometric template security. EURASIP J. Adv. Signal Process. **2008**, 1–17 (2008). https://doi.org/10.1155/2008/579416

13. X. Jiang, W.-Y. Yau, in *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*. Fingerprint minutiae matching based on the local and global structures (IEEE Comput. Soc, Barcelona, 2000). https://doi.org/10.1109/icpr.2000.906252
14. F. Farooq, R. M. Bolle, T.-Y. Jea, N. Ratha, in *2007 IEEE Conference on Computer Vision and Pattern Recognition*. Anonymous and revocable fingerprint recognition (IEEE, Minneapolis, 2007). https://doi.org/10.1109/cvpr.2007.383382
15. D. Ahn, S. G. Kong, Y.-S. Chung, K. Y. Moon, in *2008 Congress on Image and Signal Processing*. Matching with secure fingerprint templates using non-invertible transform (IEEE, Sanya, 2008). https://doi.org/10.1109/cisp.2008.742
16. Z. Jin, A. B. J. Teoh, T. S. Ong, C. Tee, Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. Expert Syst. Appl. **39**(6), 6157–6167 (2012). https://doi.org/10.1016/j.eswa.2011.11.091
17. J. B. Kho, J. Kim, I.-J. Kim, A. B. J. Teoh, Cancelable fingerprint template design with randomized non-negative least squares. Pattern Recog. **91**, 245–260 (2019). https://doi.org/10.1016/j.patcog.2019.01.039
18. M. Ferrara, D. Maltoni, R. Cappelli, Noninvertible minutia cylinder-code representation. IEEE Trans. Inf. Forensic Secur. **7**(6), 1727–1737 (2012). https://doi.org/10.1109/tifs.2012.2215326
19. R. Cappelli, M. Ferrara, D. Maltoni, Minutia cylinder-code: a new representation and matching technique for fingerprint recognition. IEEE Trans. Patt. Anal. Mach. Intell. **32**(12), 2128–2141 (2010). https://doi.org/10.1109/tpami.2010.52
20. C. Moujahdi, G. Bebis, S. Ghouzali, M. Rziza, Fingerprint shell: secure representation of fingerprint template. Pattern Recogn. Lett. **45**, 189–196 (2014). https://doi.org/10.1016/j.patrec.2014.04.001
21. S. S. Ali, S. Prakash, in *2015 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*. Enhanced fingerprint shell (IEEE, Noida, 2015). https://doi.org/10.1109/spin.2015.7095438
22. S. S. Ali, S. Prakash, in *Proceedings of the 10th Annual ACM India Compute Conference (Compute 2017)*. Fingerprint shell construction with prominent minutiae points (ACM Press, Noida, 2017). https://doi.org/10.1145/3140107.3140113
23. S. S. Ali, S. Prakash, 3-dimensional secured fingerprint shell. Pattern Recogn. Lett. **126**, 68–77 (2019). https://doi.org/10.1016/j.patrec.2018.04.017
24. S. S. Ali, I. I. Ganapathi, S. Prakash, Fingerprint shell with impregnable features. J. Intell. Fuzzy Syst. **36**(5), 4091–4104 (2019). https://doi.org/10.3233/jifs-169969
25. N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle, Generating cancelable fingerprint templates. IEEE Trans. Patt. Anal. Mach. Intell. **29**(4), 561–572 (2007). https://doi.org/10.1109/tpami.2007.1004
26. S. S. Ali, I. I. Ganapathi, S. Prakash, Robust technique for fingerprint template protection. IET Biom. **7**(6), 536–549 (2018). https://doi.org/10.1049/iet-bmt.2018.5070
27. S. S. Ali, I. I. Ganapathi, S. Prakash, P. Consul, S. Mahyo, Securing biometric user template using modified minutiae attributes. Pattern Recogn. Lett. **129**, 263–270 (2020). https://doi.org/10.1016/j.patrec.2019.11.037
28. D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, *Handbook of fingerprint recognition*. (Springer, London, 2009). https://doi.org/10.1007/978-1-84882-254-2
29. R. Wilcox, Kolmogorov–Smirnov test. Encycl. Biostat. **4** (2005)
30. T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates. Pattern Recognit. **44**(10-11), 2555–2564 (2011). https://doi.org/10.1016/j.patcog.2011.03.015
31. K. Nandakumar, A. K. Jain, S. Pankanti, Fingerprint-based fuzzy vault: implementation and performance. IEEE Trans. Inf. Forensic Secur. **2**(4), 744–757 (2007). https://doi.org/10.1109/tifs.2007.908165
32. K. Xi, J. Hu, in *2009 IEEE International Conference on Communications*. Biometric mobile template protection: a composite feature based fingerprint fuzzy vault (IEEE, Dresden, 2009). https://doi.org/10.1109/icc.2009.5198785
33. Z. Jin, M.-H. Lim, A. B. J. Teoh, B.-M. Goi, A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. Pattern Recognit. Lett. **42**, 137–147 (2014). https://doi.org/10.1016/j.patrec.2014.02.011
34. M. Sandhya, M. V. N. K. Prasad, in *2015 International Conference on Biometrics (ICB)*. k-nearest neighborhood structure (k-NNS) based alignment-free method for fingerprint template protection (IEEE, Phuket, 2015). https://doi.org/10.1109/icb.2015.7139100
35. M. Sandhya, M. V. N. K. Prasad, R. R. Chillarige, Generating cancellable fingerprint templates based on delaunay triangle feature set construction. IET Biometrics. **5**(2), 131–139 (2016). https://doi.org/10.1049/iet-bmt.2015.0034
36. S. Wang, J. Hu, Alignment-free cancelable fingerprint template design: a densely infinite-to-one mapping (DITOM) approach. Pattern Recognit. **45**(12), 4129–4137 (2012). https://doi.org/10.1016/j.patcog.2012.05.004
37. S. Wang, J. Hu, A blind system identification approach to cancelable fingerprint templates. Pattern Recognit. **54**, 14–22 (2016). https://doi.org/10.1016/j.patcog.2016.01.001
38. W. Yang, J. Hu, S. Wang, J. Yang, in *Cyberspace Safety and Security*. Cancelable fingerprint templates with delaunay triangle-based local structures (Springer, Zhangjiajie, 2013), pp. 81–91. https://doi.org/10.1007/978-3-319-03584-0_7
39. W. Yang, J. Hu, S. Wang, M. Stojmenovic, An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures. Pattern Recognit. **47**(3), 1309–1320 (2014). https://doi.org/10.1016/j.patcog.2013.10.001

Publisher's Note