



## Article

# Optimized Authentication System with High Security and Privacy

Uttam Sharma <sup>1,\*</sup>, Pradeep Tomar <sup>1</sup>, Syed Sadaf Ali <sup>2,\*</sup>, Neetesh Saxena <sup>3</sup>  and Robin Singh Bhadoria <sup>4</sup> 

<sup>1</sup> Discipline of Computer Science and Engineering, School of ICT, Gautam Buddha University, Greater Noida 201312, India; pradeep.tomar@gbu.ac.in

<sup>2</sup> ETIS, ENSEA, CY Cergy Paris Université, CNRS, 95000 Cergy, France

<sup>3</sup> School of Computer Science and Informatics, Cardiff University, Cardiff CF10 3AT, UK; nsaxena@ieee.org

<sup>4</sup> Department of Computer Science and Engineering, Birla Institute of Applied Sciences (BIAS), Bhimtal 263136, India; robin19@ieee.org

\* Correspondence: phdict1906@gbu.ac.in (U.S.); sadaf.ali@ensea.fr (S.S.A.)

**Abstract:** Authentication and privacy play an important role in the present electronic world. Biometrics and especially fingerprint-based authentication are extremely useful for unlocking doors, mobile phones, etc. Fingerprint biometrics usually store the attributes of the minutia point of a fingerprint directly in the database as a user template. Existing research works have shown that from such insecure user templates, original fingerprints can be constructed. If the database gets compromised, the attacker may construct the fingerprint of a user, which is a serious security and privacy issue. Security of original fingerprints is therefore extremely important. Ali et al. have designed a system for secure fingerprint biometrics; however, their technique has various limitations and is not optimized. In this paper, first we have proposed a secure technique which is highly robust, optimized, and fast. Secondly, unlike most of the fingerprint biometrics apart from the minutiae point location and orientation, we have used the quality of minutiae points as well to construct an optimized template. Third, the template constructed is in 3D shell shape. We have rigorously evaluated the technique on nine different fingerprint databases. The obtained results from the experiments are highly promising and show the effectiveness of the technique.

**Keywords:** authentication; privacy; security; recognition; user template; performance; fingerprint; biometrics; revocability



**Citation:** Sharma, U.; Tomar, P.; Ali, S.S.; Saxena, N.; Bhadoria, R.S. Optimized Authentication System with High Security and Privacy. *Electronics* **2021**, *10*, 458. <https://doi.org/10.3390/electronics10040458>

Academic Editor: Priyadarsi Nanda  
Received: 30 December 2020  
Accepted: 8 February 2021  
Published: 13 February 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Authentication is an extremely important mechanism to maintain in the present computerized world [1–3]. Life has become easier due to computerization; however, huge damage can be caused due to an insecure automated user authentication system [4,5]. Traditional authentication systems rely on tokens and passwords [6], though these techniques are highly popular; however, there are various limitations associated with them such as a token can be lost/stolen, the physical presence of the person getting authenticated is not compulsory, etc. In these systems, if the user credentials are compromised by an adversary then it may lead to huge damage to the user in terms of money (adversary can access the bank account of a user). Other than that, an adversary can even do something offensive (e.g., send a threatening message to anyone) by using the user's credentials and then instead of the adversary, the user will be suspected. In such scenarios tracing down the culprit is also difficult [7]. There are various security and privacy challenges [8–10] with the traditional authentication systems and a highly secure authentication system is required [11]. The limitations of the traditional frameworks can be overcome by using biometrics, which is based on biometric traits of a human [12,13]. Biometric data of a human has gained immense popularity for user authentication and sensors are also easily available for presently [14]. Non-invasive biosensors are available for forensics, biometrics,

and cybersecurity [15]. The use of biometrics for authentication provides many advantages [16] over conventional authentication methods and demands the physical presence of the person to be verified at the time of the authentication [17]. It is becoming popular for the Internet of Things [18].

In biometrics there are two main steps, enrollment and verification [19] that are as follows:

- *Enrollment:* From the data provided by the user a template is computed, which is saved in the repository/database to facilitate the user verification in future.
- *Verification:* Similar to the above step a user template is computed from the data provided by the user and then its similarity is computed with the template available in the repository. Depending on scores computed a person is verified.

Out of various biometric traits, the fingerprint is a highly popular one. It can also be used by light devices [20]. Nevertheless, there are many open issues where security is the prominent one related to fingerprint [21]. Multiple types of attacks are possible fingerprint-based biometrics, among which the compromising of the database is a disastrous one [22–24]. Various threats/attacks possible on secured fingerprint template present in the database and for which the proposed technique has been compared with the other state of the art techniques are given in [24].

Mostly, fingerprint-based biometric systems save the minutiae points (fingerprint features shown in Figure 1) as a template [25]. However, by using minutiae points, original fingerprint reconstruction is possible [26–29]. The cyberattacks are increasing day by day and an attacker can attack the biometric databases as well [7], hence it is important to secure the biometric data in biometrics as they cannot be revoked if leaked [30]. The compromised biometric data/features may have serious consequences and can lead to cross-matching attack [31,32].



**Figure 1.** A singular point (circle) and minutiae points (squares are minutiae points and arrows are their orientations) in a fingerprint.

As there are numerous issues related to fingerprint biometrics [33], there is a need for a highly secure fingerprint-based authentication method. Any secure biometric system is expected to depict the essential requirements [19,34] given below:

- *Revocability*: By the use of the same data (biometric features) provided by the user, it must be possible to construct multiple templates.
- *Diversity*: There must be no similarity among the different templates generated by using the same data of the user.
- *Security*: Original data provided by the user must never get compromised under any scenario.
- *Performance*: Due to security enhancement the recognition performance of the system should not get reduced.

To achieve the essential requirements mentioned above, the main concept used [24] is to transform the user data (biometric features)  $UD$ , provided by the user through a function  $F$  and a unique key for user  $key_1$ . Transformed template  $F(UD, key_1)$  obtained after transformation is saved in the repository/database. In case the user template has been captured by the adversary, then through modification of the key from  $key_1$  to  $key_2$ , a different template  $F(UD, key_2)$  can be constructed. In this paper, a highly secure and optimized fingerprint-based biometrics has been proposed. The major contributions of the technique proposed in this paper are as follows:

- A completely secure template is constructed by using the features of the fingerprint provided by a user that depicts exceptional revocability, diversity, security, and recognition performance.
- Generally during minutiae extraction, there exists a problem of missing minutiae points. The proposed technique has shown good resistance against the missing minutiae points problem.
- The proposed technique exhibits superior recognition performance in comparison to other existing techniques and has achieved 0% equal error rate (EER).
- Rotation/translation of fingerprint on the fingerprint scanner leads to variation in the fingerprint images captured, the proposed technique is highly robust against such variations.
- Mostly the fingerprint-based authentication techniques generate a user template which is not optimized. The proposed technique uses the quality of minutiae points and generates a highly optimized user template.

The remaining paper is organized as follows. The literature review of the approaches available for biometric template recognition and protection is presented in Section 2. Section 3 represents the proposed technique. Section 4 contains the discussion of the experimental results. The last section summarizes the conclusions.

## 2. Literature Review

With various advantages biometric authentication has many challenges [22,33] as well. Various frameworks present in the literature for biometric template recognition and protection are mentioned below.

Cappelli et al. [35] transformed fingerprint of a user into a cylinder form known as Minutia Cylinder-Code (MCC). MCC is an efficient way to represent a fingerprint; however, it is insecure as it is an invertible technique. Ferrara et al. [36] proposed a non-invertible framework of [35], in which transformations are applied that are non-invertible in nature. However, it was observed that [36] is non-revocable. Ferrara et al. [37] have proposed an enhanced version of MCC, which depicts good revocability apart from being secure. By using  $l_1$  minimization, matching in the encrypted domain for MCC has been designed by Liu et al. [38].

To classify the fingerprints Nurtantioet al. [39] proposed a decomposition based on the singular value which uses image compressing. Feng et al. [40] has introduced a hybrid framework for securing data. Trivedi et al. [41] have introduced a cancellable non-invertible

fingerprint-based biometrics. Azzakhnini et al. [42] have proposed a scheme which relies on RGB-D data, user's emotional state, ethnicity, and gender are recognized. Yang et al. [43] used the combination of scattering and convolutional networks for the estimation of age and expression. Balazia and Sojka [44] have designed a framework for recognition by using the motion of the user. Dave et al. [45] have designed an approach for human biometric data acquisition and recognition. Ilyas et al. [23] have designed an anti-spoofing framework for user age verification. Kumar et al. [46] have developed a framework for authentication by the combination of a symmetric hash function. Ganapathi et al. [47] have introduced a scheme for recognition that is based on the geometric descriptor.

By using the nearest  $k$ -neighborhood structure, Sandhya and Prasad [48] have designed a cancelable template. Sandhya et al. [49] have designed an approach that relies on the use of Delaunay triangles to obtain a cancelable template for a user. In order to secure the biometric data, Sandhya and Prasad [50] have introduced a technique that uses fused structures. Iula and Micucci [13] have validated the use of biometrics relying on ultrasound images. Nakanishi and Maruoka [14] have proposed a biometric authentication using electroencephalograms stimulated by ultrasound. To obtain cancelable templates Wang et al. [51] used transformation that is non-invertible on the binary fingerprint presentation. Derman and Keskinöz [52] have developed a method based on distortion rectification for authentication. Wang and Hu [53] secured the fingerprint features by designing a method that is based on the heavy many-to-one mapping, and Si et al. [54] have used the approach of dense registration. Many times, biometrics can be traced and due to this they are have been combined with the traditional techniques for better security in [20,55,56].

An alignment free framework has been proposed by Wang and Hu [57] through the use of the non-invertible transformation for securing the templates that are cancelable. Another alignment invariant technique based on minutiae triplet is designed by Ahn et al. [58]. Tran et al. [59] have designed a method based on hybrid matcher for user authentication. Wang et al. [60] used zoned minutia pair for local minutiae structure to design a scheme that computes cancelable user template. Boulton et al. [61] have introduced Biotop biotoken, which are generated through encryption of user data. The fingerprint image is enhanced by Khan et al. in [62] by using anisotropic Gaussian. Ali et al. in [33] designed a technique in which secured fingerprint features are used, which has been further enhanced in [63]. Ali et al. [6] have designed a secure 3-dimensional secured user template through the relocation of minutiae points. The fingerprint features used are the translation/rotation variant.

Ali et al. [24] have proposed Polynomial Vault, in which they used polynomial functions and the fingerprint to generate a polynomial function which is treated a user template. In this technique, all the minutiae points of a fingerprint are used, due to which it is not optimized. Fingerprint shell [64] has been introduced by Moujahdi et al., in this technique, the template computed has a 2D shell shape structure. Based on [64], Ali and Prakash [65] proposed a technique with better recognition performance. However, features of a fingerprint are insecure in Fingerprint Shell [66], Ali et al. [7] designed a secure version of [64] which was a 3D fingerprint shell and was much more secure than the 2D fingerprint shell [64]. It is observed that the ridge count for different minutiae points (with respect to the singular point) is found to be different. Ali et al. used it in [31] and added high randomness to the generated user template.

The present frameworks for fingerprint-based biometrics are generally insecure and unoptimized. In some techniques, it is even possible to obtain the original biometric features information from the user template [7,64]. Apart from security, the available techniques usually use all the minutiae points for the template generation, leading to an unoptimized user template that makes the authentication system slow. Hence, in the proposed technique we have generated a highly robust and irreversible template for a user. The template generated by the proposed technique is a 3D shell and hence much stronger than a 2D fingerprint shell [7,64]. With other attributes of minutiae points of a

fingerprint, we have used the quality of minutia point as well, leading to a highly secure and optimized user template. As only good-quality minutiae points (with better ridge termination or bifurcation [19]) are used, this makes the authentication system much faster. In case adversary gets the user template generated by the proposed technique, then it is not possible (computationally very hard) for the adversary to obtain the original fingerprint of a user from it; and the compromised user template can be easily replaced with a new template (very different from the compromised template) by changing the user keys.

### 3. Proposed Technique

In the proposed technique a secure and optimized user template is generated by using the secured features (explained below) of the fingerprint and a user key-set. The template generated by the proposed technique has a shell shape structure. This template is stored in the database at the time of enrollment for a user and is further used for the user verification. Figure 2 shows the overview of the proposed technique and a detailed description of it is given below.

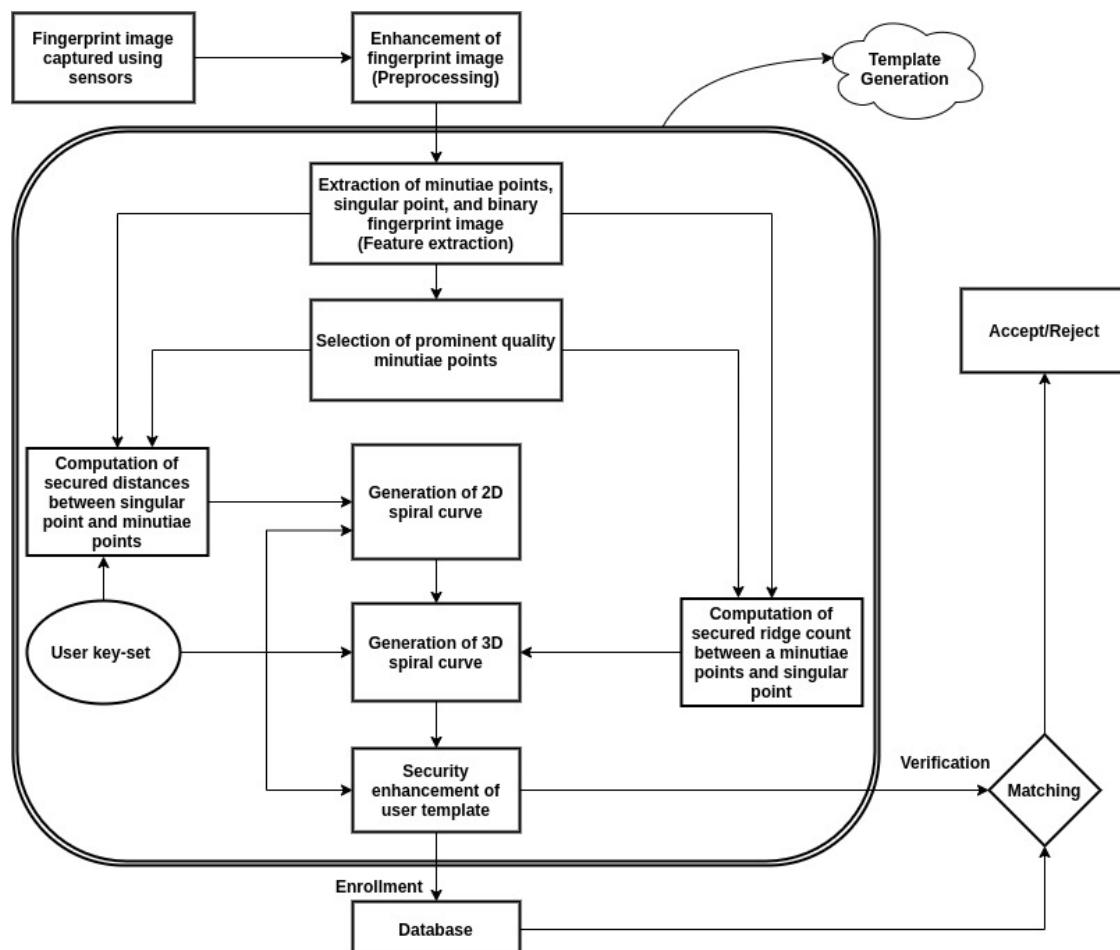


Figure 2. Overview of the proposed technique.

Fingerprints are easy to capture and provide various advantages which make them suitable for the biometrics. A fingerprint mainly consists of ridges and valleys (shown in Figure 1). The points where these ridges have very high curvature are known as singular points; delta, core and arch are the major types. Usually, there can be up to four singular points in the fingerprint. The location of the singular point is its major attribute. Let us denote a singular point as Singular  $(u_{sing}, v_{sing})$ , where  $u_{sing}$  is the value of the abscissa and  $v_{sing}$  is the ordinate value. There is another type of special points in a fingerprint which are known as minutiae points. A minutia point is a point in a fingerprint where a

ridge begins/ends or bifurcate. The major attributes of a minutia point are its location, orientation with respect to the abscissa axis (denoted  $u$ -axis in this paper), type (ridge bifurcation or starting/termination), and quality of a minutia point.

Let us denote the  $j$ th minutia point of a fingerprint as  $Minutia_j(u_j, v_j, \phi, t_j, q_j)$ , where  $u_j$  is the abscissa value,  $v_j$  is the ordinate value,  $\phi$  is the orientation of the minutia point with respect to abscissa axis,  $t_j$  is the type of minutia, and  $q_j$  is the quality of minutia point  $Minutia_j$ . We have denoted abscissa axis as  $u$ -axis, ordinate axis as  $v$ -axis, and apply axis as  $w$ -axis. Usually, only the location and orientation information of minutiae points are used as the template for a user and is directly saved into the database. As the attacker can attack the database and can generate the original fingerprint from the compromised template present in the database. Fingerprints are permanent and non-revocable, directly storing minutiae points is extremely dangerous. Most of the techniques generate a user template by using all the minutiae points. Such techniques usually use only the orientation, location, and type of minutia (ridge bifurcation or starting/ending) point information. Quality of minutia point is not used so extensively. We have taken the advantage of quality of minutia point information and used it as well for the generation of a secured template, by using key-set  $\{k_1, k_2, k_3, k_4\}$ . We have used only superior quality minutiae points for the template generation. This reduces the problem of missing minutiae points (as poor-quality minutiae points that leads to missing minutiae problem gets eliminated), which leads to a highly robust and optimized user template. In the proposed technique, in place of storing the insecure minutiae attributes, a transformed form of minutiae attributes is saved. The highly secured template generated is in the shape of a spiral shell.

### 3.1. Features Required for Template Generation

Following features of the fingerprint of a user are required for the template generation (Algorithm 1 contains the steps involved):

- *Singular Point*: Only the location of it is used.
- *Minutiae Points*: Their location, orientation, and quality are used. Instead of directly using the location of a minutia point, a secured location computed corresponding to it is used.
- *Ridge Counts*: Ridge counts, which are the number of ridges between minutiae points and a singular point are used. Instead of directly using the ridge counts, secured ridge counts are calculated, which are further used.

In fingerprint-based biometrics there are various issues related to the capturing of the fingerprint of a user that leads to intra-subject variance. During fingerprint capturing there can be rotation as well as the translation of the finger on the sensor, leading to rotational and translational variations. In order to avoid such effects, the rotation and translation invariant information present in a fingerprint are used which are given below:

- Secured distance between singular point and minutiae point. Let  $dis_j$  be the distance between singular and the  $j$ th minutia point. It can be noted that  $dis_j$  is rotation/translation invariant; however, it is not secure to directly use  $dis_j$  because it is permanent and cannot be changed if compromised. Instead of using  $dis_j$ , a secured distance  $sdis_j$  is used, corresponding to  $j$ th minutia point. The secured distance  $sdis_j$  is generated with the help of  $dis_j$ , orientation of  $j$ th minutia, and the user keys  $k_1, k_2$ . This is pictorially shown in Figure 3.
- Secured ridge count between the singular and minutia point. Similar to above, it is not safe to directly use the ridge count between the  $j$ th minutia point and the singular point. Instead, a secured ridge count  $src_j$  is calculated with the help of keys  $k_1, k_2$ . As shown in Figure 3.

The above features of a fingerprint are used for the generation of the user template along with a unique user key-set  $k_1, k_2, k_3, k_4$ . Following are the major steps required to construct a highly secure, robust, and optimized template for a user.

**Algorithm 1** Secured Features Calculation.

**Input:** Thinned binary image of fingerprint:  $fthin$ , Minutia $_j$  ( $u_j, v_j, \phi, t_j, q_j$ ) were  $j$  varies from 1 to total (total minutiae points present in the fingerprint), Singular Point ( $u_{sing}, v_{sing}$ ) and key-set  $\{k_1, k_2, k_3, k_4\}$

**Output:** Ridge count :  $sdis$  and  $src$  (Secured features)

**for**  $j = 1$  **to** total **do**

$m = 0$

**if**  $q_j \geq threshold_{value}$  **then**

$m = m + 1$

$dis_m = \sqrt{(u_j - u_{sing})^2 + (v_j - v_{sing})^2}$

$sdis_m = \sqrt{dis_j^2 + k_1^2 + 2(dis_j \times k_1 \times \cos(k_2 + \phi_j))}$

$src_m = 0$

$u_j = u_j + k_1 \times \cos(k_2 + \phi_j)$

$v_j = v_j + k_1 \times \sin(k_2 + \phi_j)$

$orientation = \frac{v_j - v_{sing}}{u_j - u_{sing}}$

$step = v_j - orientation * u_j$

**if**  $|u_j - u_{sing}| \geq |v_j - v_{sing}|$  **then**

**for**  $u = u_j$  **to**  $u_{sing}$  **do**

$v = \text{int}(orientation * u + step)$

**if**  $fthin(u - 1, v - 1)$  **or**  $fthin(u - 1, v)$  **or**  $fthin(u - 1, v + 1)$  **or**  $fthin(u, v - 1)$  **or**  $fthin(u, v)$  **or**  $fthin(u, v + 1)$

**or**  $fthin(u + 1, v - 1)$  **or**  $fthin(u + 1, v)$  **or**  $fthin(u + 1, v + 1)$  **then**

**if**  $on - Ridge == \text{false}$  **then**

$src_m = src_m + 1$

$on - Ridge = \text{true}$

**end if**

**else**

$on - Ridge = \text{false}$

**end if**

**end for**

**else**

**for**  $v = v_j$  **to**  $v_{sing}$  **do**

$u = \text{int}(\frac{v - step}{orientation})$

**if**  $fthin(u - 1, v - 1)$  **or**  $fthin(u - 1, v)$  **or**  $fthin(u - 1, v + 1)$  **or**  $fthin(u, v - 1)$  **or**  $fthin(u, v)$  **or**  $fthin(u, v + 1)$

**or**  $fthin(u + 1, v - 1)$  **or**  $fthin(u + 1, v)$  **or**  $fthin(u + 1, v + 1)$  **then**

**if**  $on - Ridge == \text{false}$  **then**

$src_m = src_m + 1$

$on - Ridge = \text{true}$

**end if**

**else**

$on - Ridge = \text{false}$

**end if**

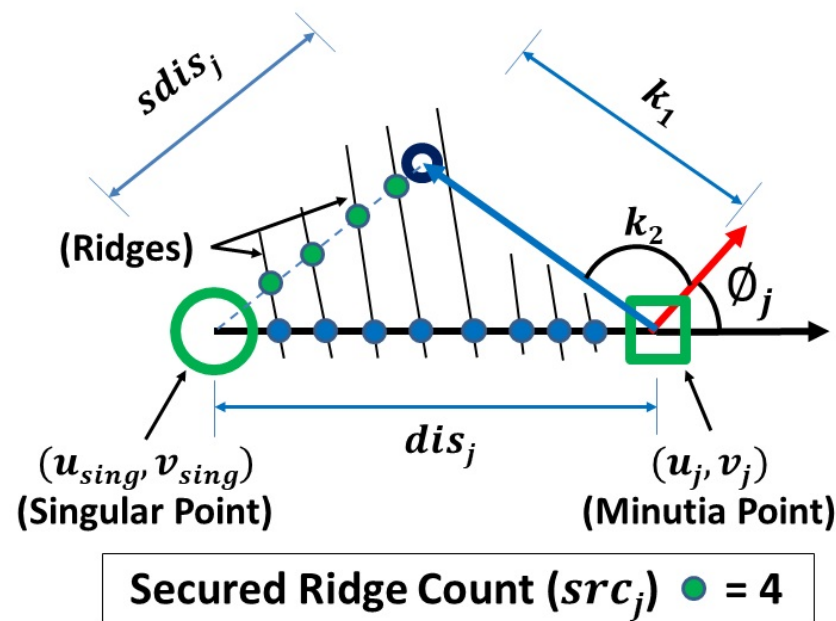
**end for**

**end if**

**end if**

**end for**

$FeatureSet = \{(sdis_j, src_j) \mid j = 1 \rightarrow m, \text{sorted with respect to } sdis_j\}$



**Figure 3.** Computation of secured features with the help of user keys.

### 3.2. Enrollment

During the enrollment process, the following steps are involved for the computation of a secure user template from the fingerprint of a user, with the help of a user key-set.

#### 3.2.1. Extraction of Features

First, the fingerprint of a user is captured. From the fingerprint singular point, minutiae points, and the ridge count between them is obtained. Now instead of using all the minutiae points, only good-quality minutiae points and their ridge count from the singular point is used. This reduces the computations required for template generation and matching. Suppose  $m$  good-quality minutiae points are obtained from a fingerprint. From these minutiae points secured distances  $sdis_j$  and secured ridge counts  $src_j$  ( $j$  varies from 1 to  $m$ ) are computed, and sorted according to  $sdis_j$ .

#### 3.2.2. Template Generation

Algorithm 2 contains the computational steps involved for template generation. By using the secured distances  $sdis_j$  ( $j$  varies from 1 to  $m$ ) and user key  $k_3$  a spiral curve is constructed. We have secured distances  $sdis_1, sdis_2, \dots, sdis_m$  in sorted order, to these distances we add  $k_3$  and get new distance set, i.e.,  $sdis_1 + k_3, sdis_2 + k_3, \dots, sdis_m + k_3$ . Now the spiral curve is formed in such a way that these distances forms contiguous right-triangles with  $sdis_j$  ( $j$  varies from 1 to  $m$ ) as hypotenuse of the triangle, as shown in Figure 4. Base of first triangle has length  $k_3$  and hypotenuse has length  $sdis_1 + k_3$ , base of second triangle has length  $sdis_1 + k_3$  and hypotenuse has length  $sdis_2 + k_3$ ; and so on it continues. As these secured distances are in sorted order, so the final curve formed is of a spiral/shell shape.



**Algorithm 2** User Template Construction.

```

1: Input: Secured Features Set (sdis1, src1), (sdis2, src2), ..., (sdism, srcm) and key-set {k1, k2, k3, k4}
2: Output: Secure 3D Template (ST)
3: for j = 1 to m do
4:   /* Hypotenuses of the triangles */
5:   sdisj = sdisj + k3
6:   if j == 1 then
7:     uj = k3
8:     vj = √(sdisj2 - k32)
9:     θj = tan-1(vj/uj)
10:  end if
11:  if j > 1 then
12:    /* Angle between axis of abscissas and hypotenuse */
13:    θj = θj-1 + sin-1(√(sdisj2 - (sdisj-1)2) / sdisj)
14:    uj = sdisj × cos(θ)
15:    vj = sdisj × sin(θ)
16:  end if
17: end for
18: for j = 1 to m do
19:   /* 2D to 3D conversion */
20:   wj = srcj × k4
21: end for
22: /* Calculation of kcombined */
23: kcombined = [k1] + [k2] × (216) + [k3] × (232) + [k4] × (248)
24: for j = 1 to m do
25:   /* Enhancement of Template */

$$\begin{bmatrix} u_j & v_j & w_j \end{bmatrix} = \begin{bmatrix} u_j & v_j & w_j \end{bmatrix} \times \begin{bmatrix} \cos(k_2) & \sin(k_2) & 0 \\ -\sin(k_2) & \cos(k_2) & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} \cos(k_4) & 0 & -\sin(k_4) \\ 0 & 1 & 0 \\ \sin(k_4) & 0 & \cos(k_4) \end{bmatrix}$$


$$\begin{bmatrix} u_j \\ v_j \\ w_j \end{bmatrix} = \begin{bmatrix} k_{combined} \times \sin(k_4) \times \sin(k_2) \\ k_{combined} \times \cos(k_4) \\ k_{combined} \times \sin(k_4) \times \cos(k_2) \end{bmatrix} + \begin{bmatrix} u_j \\ v_j \\ w_j \end{bmatrix}$$

26: end for
27: /* User Template (3-D Spiral Curve) */
28: SUT = {(uj, vj, wj) | j = 1 → m}

```

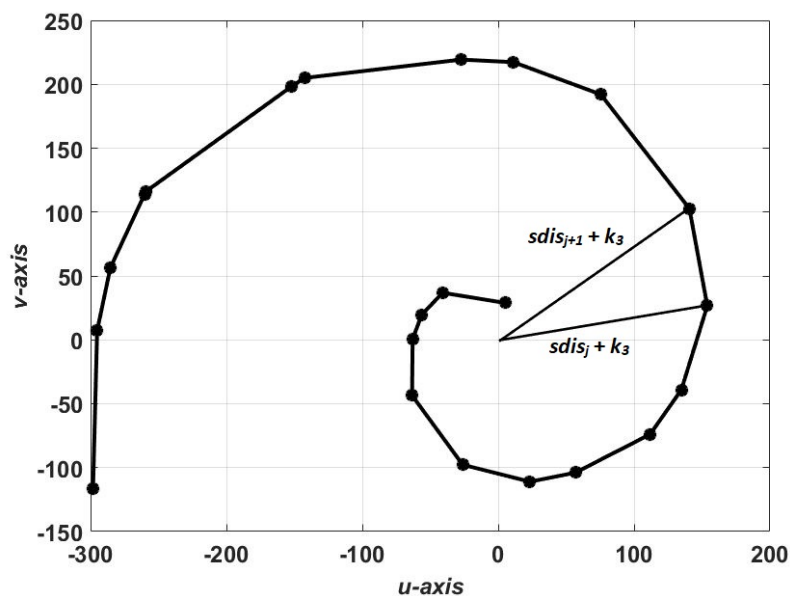
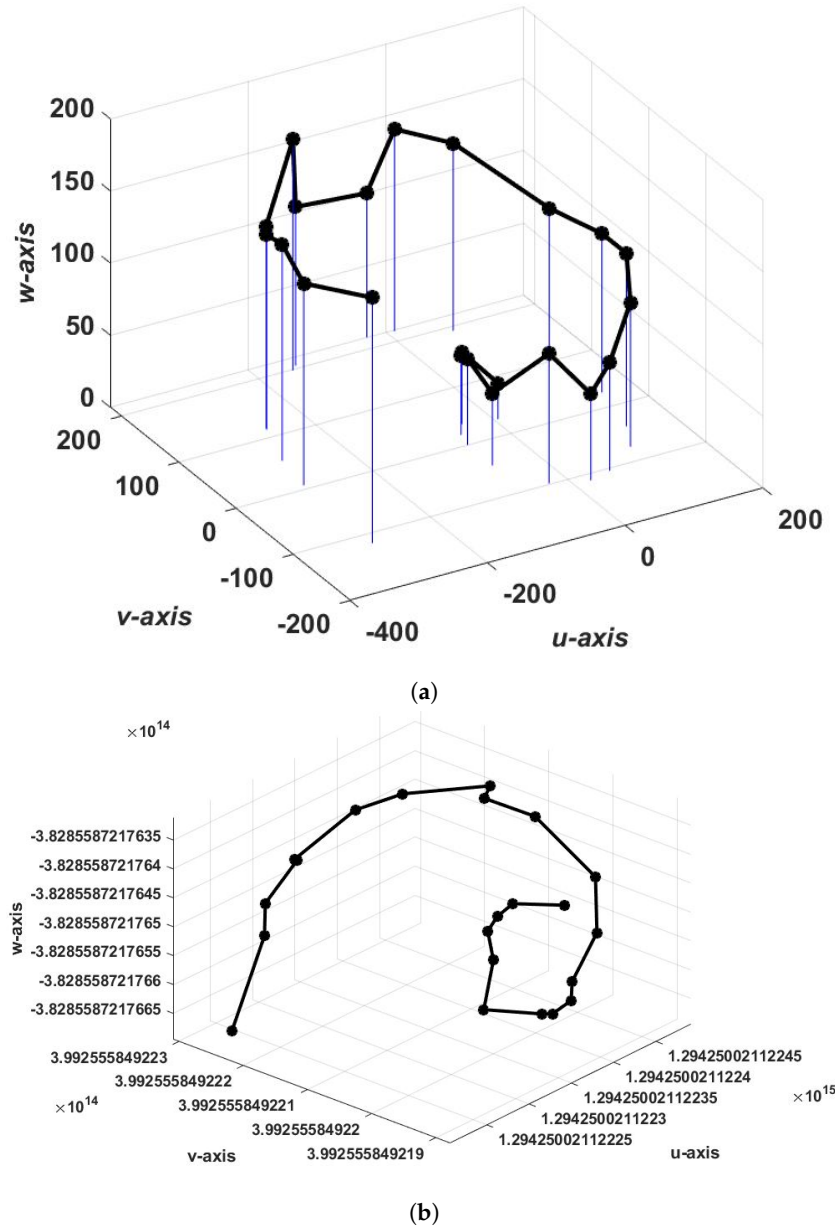


Figure 4. Construction of 2D spiral curve.

Right now, the curve is two-dimensional, now corresponding to each distance  $sdis_j + k_3$  ( $j$  varies from 1 to  $m$ ) in the user curve, the applicate value is updated to  $k_4$  times  $src_j$  ( $j$  varies from 1 to  $m$ ). This converts the two-dimensional user template into a three-dimensional secured user template, as shown in Figure 5a.



**Figure 5.** 3D user template (a) Initial 3D template, blue lines are the applicate values computed by using the secured ridge count  $src_j$  and  $k_3$ , (b) Final 3D user template after the user curve transformation.

It can be observed that the center of the curve generated for different users is the origin. This is not an optimized use of the three-dimensional space. To avoid this the curves of different users can be relocated to new different locations with the help of user key  $k_2$ ,  $k_4$  and a new key  $k_{combined}$ , which is the generated from  $k_1, k_2, k_3$ , and  $k_4$ . Key  $k_{combined}$  is a 64-bit key generated from the integral values of  $k_1, k_2, k_3$ , and  $k_4$ , as shown in Figure 6. Using  $k_2, k_4$ , and  $k_{combined}$ , the user curve is rotated and translated to a new location as shown in the Figure 7. The 3D transformed curve is in the form as shown in Figure 5b. If a user template is leaked, a very different template can be constructed by altering the key-set value as depicted in Figure 8.

$k_{combined}$  (64 bit key)

|                         |     |     |    |                         |     |     |    |                         |     |     |    |                         |     |     |    |
|-------------------------|-----|-----|----|-------------------------|-----|-----|----|-------------------------|-----|-----|----|-------------------------|-----|-----|----|
| 1                       | ... | ... | 16 | 17                      | ... | ... | 32 | 33                      | ... | ... | 48 | 49                      | ... | ... | 64 |
| 16 bits                 |     |     |    | 16 bits                 |     |     |    | 16 bits                 |     |     |    | 16 bits                 |     |     |    |
| Integral value of $k_1$ |     |     |    | Integral value of $k_2$ |     |     |    | Integral value of $k_3$ |     |     |    | Integral value of $k_4$ |     |     |    |

Figure 6. Calculation of key  $k_{combined}$  by using  $k_1, k_2, k_3,$  and  $k_4$ .

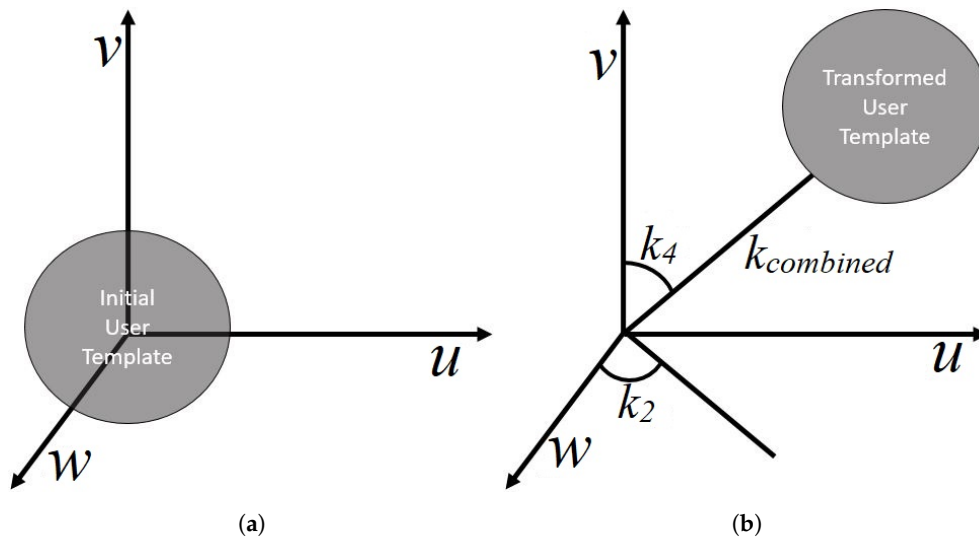


Figure 7. Security enhancement (a) Initial template, (b) Final template after transformation using the keys  $k_2, k_4,$  and  $k_{combined}$ .

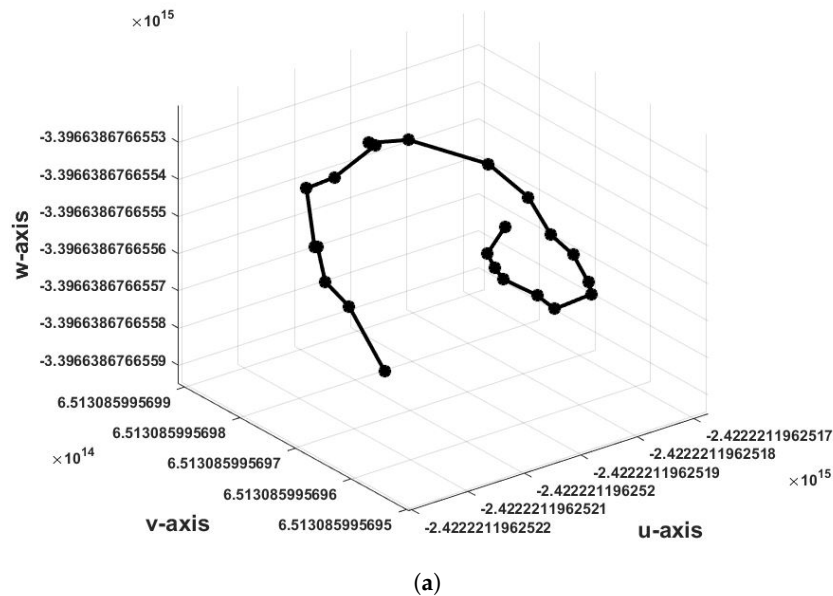
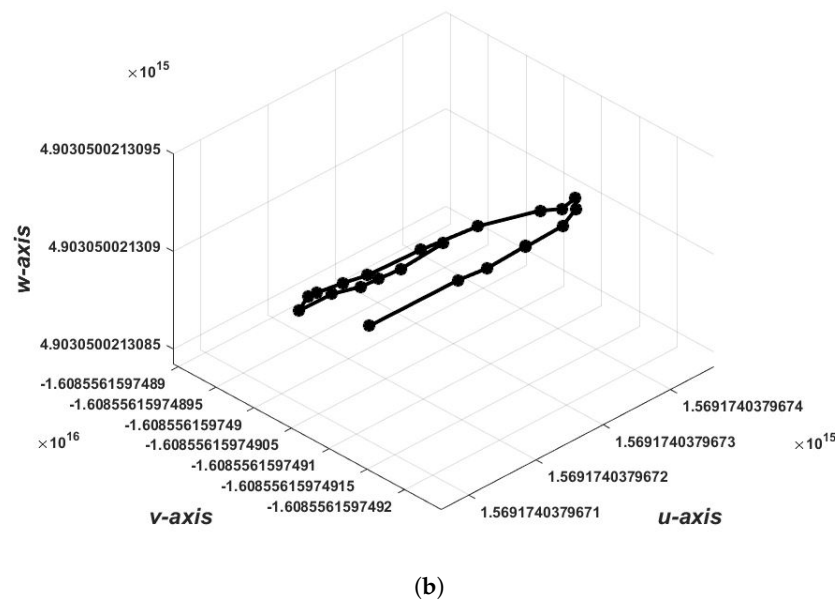


Figure 8. Cont.



**Figure 8.** Very different user templates (in the shape of spiral curves) generated from the same biometric data (fingerprint) (a) Template generated for a user, (b) Template generated for the same user by using different user-keys.

This is the final user template, if there is more than one singular point, then with respect to each singular point a template is computed and stored in the database.

### 3.3. Template Matching for Verification

To verify a user, a template is generated by following the above steps (same as during the enrollment), which is compared with the one present in the database. To compare the two templates Hausdorff distance is calculated. Hausdorff distance (HD) [67] is a popular matrix used for comparison in the field of computer vision. The Hausdorff distance between a set of points  $K$  and  $L$  is calculated as given below.

$$HD(K, L) = \max[hdis(K, L), hdis(L, K)]$$

$$hdis(K, L) = \max_{k \in K} \min_{l \in L} (DisMat(k, l))$$

Here  $DisMat(k, l)$  can be any distance matrix such as Manhattans distance, Euclidean distance etc. We have used Euclidean distance for calculation of Hausdorff distance. Lesser the Hausdorff distance means that the templates are highly similar.

## 4. Experimental Results and Discussion

To evaluate the efficiency of the proposed technique, we have used nine different databases. These are FVC2000 DB1, FVC2000 DB2, FVC2002 DB1, FVC2002 DB2, FVC2002 DB3, FVC2002 DB4, FVC2004 DB1, FVC2004 DB2, and IIT Kanpur (large database) [7,24] fingerprint databases. All contain 800 images obtained from 100 fingers (8 samples per finger), except IIT Kanpur database. IIT Kanpur database has 5512 fingerprint images taken from 1378 fingers (4 samples per finger). It must be noted that all databases are of moderate size; however, the IIT Kanpur database is a large size database. NIST Biometric Image Software (NBIS) [68] has been used for the minutiae points extraction. Arch-type singular points are captured by the method given in [69] and for other types, the method given in [70] is used. A processor (Intel(R) Core(TM) i5-2400 CPU @ 3.1 GHz (Intel, Santa Clara, CA, USA )) with 4 GB RAM has been used for experimentation. Kolmogorov–Smirnov (KS) test has been used to statically analysis imposter and genuine scores. This test gives the output value in the range of zero to one, a value near one means better separation [71]. The important quantities [16,47,72] that are calculated have been listed below:

- *False Acceptance Rate (FAR)*: Percentage of time an attacker is recognized as a genuine user.
- *False Rejection Rate (FRR)*: Percentage of time a genuine user is not recognized as a genuine user.
- *Equal Error Rate (EER)*: FRR or FAR value, when they both are equal.
- $FAR_{1000}$ : FRR value when the FAR value is 0.001%.
- $Zero_{FAR}$ : Least value of FRR, when the FAR value is zero.
- *Genuine Acceptance Rate (GAR)*: It is the percentage of time a genuine user is recognized correctly as a genuine user.

FVC protocol [73] and 1 vs. 1 [7] protocol has been used for the evaluation. In FVC and 1 vs. 1 protocol, to compute FAR, the first sample of every subject is matched with the first sample of all other subjects. To calculate FRR in FVC protocol, each sample of every subject is matched with every other sample of the same subject. However, to calculate FRR in 1vs1 protocol, two samples of every subject are compared with each other. The proposed technique has been rigorously tested for revocability, diversity, security, and performance; which is given below in detail.

#### 4.1. Revocability and Diversity

A technique is called revocable if it can generate multiple templates from the same information. This provides the liberty to change the compromised user template in case of the security breach. To check this we have generated multiple templates for the same fingerprint by altering the key-set  $\{k_1, k_2, k_3, k_4\}$  values. It was observed that these templates are quite different from each other. This can be pictorially seen from Figure 8. Though the two templates have been computed from the same fingerprint, they are totally different from one another as the key-set values  $\{k_1, k_2, k_3, k_4\}$  used to generate them are different.

A technique is diverse if the templates computed from different key-sets and the same user data are non-linkable. To check this we have evaluated the proposed technique for the revoked template attack for the two scenarios given below:

- *Attack Scenario I*: Attacker possess the user template, compromised by attacking the database. A new template for the user is constructed by using the same fingerprint sample of the user with different user key-set values.
- *Attack Scenario II*: Attacker possess the old template, compromised by attacking the database. A new user template is computed by using the different fingerprint sample of the same user with different user key-set values.

The results obtained for the above are given in Table 1. It is clear from the results that the proposed technique can handle revoked template attack efficiently and there will not be any security breach in case of revoked template attack by an adversary. This also demonstrates its resistance towards the crossmatch attack [7], and if the template of a user is compromised in any application, in that case, the other applications will not get affected due to it. Hence the proposed technique is revocable and diverse.

**Table 1.** Revoked template attack (successful attacks in percentage), proposed technique can overcome it efficiently.

| Database    | Ali and Prakash [7] |             | Ali et al. [31] |             | Proposed Technique |             |
|-------------|---------------------|-------------|-----------------|-------------|--------------------|-------------|
|             | Scenario I          | Scenario II | Scenario I      | Scenario II | Scenario I         | Scenario II |
| FVC2000 DB1 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2000 DB2 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2002 DB1 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2002 DB2 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2002 DB3 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2002 DB4 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2004 DB1 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| FVC2004 DB2 | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |
| IIT KANPUR  | 0.00                | 0.00        | 0.00            | 0.00        | 0.00               | 0.00        |

#### 4.2. Security Analysis

Attack on a database is a big threat, as user templates are present in the database. And by using the user template from the compromised database, an adversary can obtain the original biometric features of a user. Biometric features are non-revocable, hence, a technique is considered to be secured if it is very hard or computationally almost impossible to get the original fingerprint by using the compromised template.

In the case of the proposed technique, if the template as well as the key-set are compromised, then it is not possible to generate the original fingerprint of a user by using it. And as we can observe by reversing Algorithm 2 that at most an adversary can get the secured distances and ridge counts only, and no other information an adversary can get.

As we know that to construct the original fingerprint of a user the minutiae points location and orientation are essential [26–29]. In the proposed technique the orientation information is not stored anywhere, so the adversary cannot get the minutiae points orientation information. Now it is not possible for the adversary to get the location of a minutia point as well, they can only get the secured distance and ridge count. It must be noted that the secured distance and ridge count between minutia and the singular point is revocable in nature; hence even if an adversary gets this information, we can revoke it. Another thing to notice is that as the proposed technique generates an optimized user template with good-quality minutiae points (with quality value more than a particular threshold). This eliminates the poor-quality minutiae points, which further reduces the information. As no important information adversary can get from the user template by which the original fingerprint can be reconstructed, so the proposed technique is extremely secure.

#### 4.3. Performance

To evaluate of the recognition performance, we have generated the user key-set value randomly from the given key range values;  $k_1 \in [0, 40]$ ,  $k_2 \in [0, 360]$ ,  $k_3 \in [0, 50]$ , and  $k_4 \in [0, 360]$ . Similar results were obtained for other key range values also (more than 1000 different key-set ranges).

Table 2 contains the comparison of EER values for the FVC protocol, and the comparison of the EER values, following the 1vs1 protocol is given in Table 3. The proposed technique has achieved 0% EER for the different-different type of fingerprint databases. The proposed technique has shown better performance than the other existing techniques, hence, the proposed technique is highly accurate in discriminating the genuine user and an imposter, as it used the secured features, as well as the user template generated, is highly optimized.

**Table 2.** Comparison of the EER values of the proposed technique with the other techniques by following the FVC protocol (values are in percentage).

| Techniques                | FVC2000 DB1         |          |                     | FVC2000 DB2         |          |                     | FVC2002 DB1         |          |                     | FVC2002 DB2         |          |                     | FVC2002 DB3         |          |                     | FVC2002 DB4         |          |                     | FVC2004 DB1         |          |                     | FVC2004 DB2         |          |                     | IIT Kanpur<br>(Large Database) |          |                     |   |
|---------------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|---------------------|----------|---------------------|--------------------------------|----------|---------------------|---|
|                           | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1000</sub>            | EER      | Zero <sub>FMR</sub> |   |
| Cappelli et al. [35]      | -                   | -        | -                   | -                   | -        | -                   | 1.64                | 1.00     | 3.18                | 0.68                | 0.49     | 0.89                | 7.18                | 3.14     | 8.96                | 5.75                | 3.00     | 7.46                | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   | - |
| Kumar et al. [46]         | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | 4.98     | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   |   |
| Derman and Keskinöz [52]  | -                   | -        | -                   | -                   | -        | -                   | -                   | 6        | -                   | -                   | 6        | -                   | -                   | 14       | -                   | -                   | 7        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   |   |
| Ali and Prakash [19]      | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | 0.001    | -                   |   |
| Ferrara et al. [36]       | -                   | -        | -                   | -                   | -        | -                   | 3.14                | 1.88     | 5.07                | 1.43                | 0.99     | 2.54                | 10.04               | 5.24     | 12.43               | 9.75                | 4.84     | 11.89               | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   |   |
| Moujahdi et al. [64]      | -                   | -        | -                   | -                   | -        | -                   | 4.18                | 2.03     | 6.36                | 1.39                | 1.01     | 2.21                | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   |   |
| Ali and Prakash [65]      | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | 0.001    | -                   |   |
| Ferrara et al. [37]       | -                   | -        | -                   | -                   | -        | -                   | 3.1                 | 2.0      | 4.3                 | 1.3                 | 1.1      | 1.4                 | 8.4                 | 4.4      | 11.8                | 5.0                 | 3.1      | 6.6                 | 6.8                 | 3.0      | 9.1                 | -                   | -        | -                   | -                              | -        | -                   |   |
| Ahn et al. [58]           | -                   | -        | -                   | -                   | -        | -                   | -                   | 7.18     | -                   | -                   | 3.61     | -                   | -                   | 11.80    | -                   | -                   | 11.46    | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   |   |
| Khan et al. [62]          | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | 9.03     | -                   | -                   | 9.71     | -                   | -                              | -        | -                   |   |
| Si et al. [54]            | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | 1.96                | 0.89                | 3.36     | -                   | -                              | -        | -                   |   |
| Boult et al. [61]         | -                   | 2.9      | -                   | -                   | 2.5      | -                   | -                   | 2.1      | -                   | -                   | 1.2      | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | 8.6      | -                   | -                   | 7.5      | -                   | -                              | -        | -                   |   |
| Ali et al. [31]           | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                              | 0        | 0                   |   |
| Ali and Prakash [7]       | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                   | 0        | 0                   | 0                              | 0        | 0                   |   |
| Tran et al. [59]          | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | 0.67                | 0.49     | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                   | -        | -                   | -                              | -        | -                   |   |
| <b>Proposed Technique</b> | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>            | <b>0</b> | <b>0</b>            | <b>0</b>                       | <b>0</b> | <b>0</b>            |   |

Note: “-” means that the results are not reported by the authors of those technique.

**Table 3.** Comparison of the EER values of the proposed technique with the other techniques by following the 1vs1 protocol (values are in percentage).

| Techniques                | FVC2002              |          |                     |                      |          |                     |                      |          |                     |                      |          |                     | IIT Kanpur<br>(Large Database) |          |                     |
|---------------------------|----------------------|----------|---------------------|----------------------|----------|---------------------|----------------------|----------|---------------------|----------------------|----------|---------------------|--------------------------------|----------|---------------------|
|                           | DB1                  |          |                     | DB2                  |          |                     | DB3                  |          |                     | DB4                  |          |                     | FMR <sub>1,000</sub>           | EER      | Zero <sub>FMR</sub> |
|                           | FMR <sub>1,000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1,000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1,000</sub> | EER      | Zero <sub>FMR</sub> | FMR <sub>1,000</sub> | EER      | Zero <sub>FMR</sub> |                                |          |                     |
| Sandhya et al. [49]       | -                    | 0        | -                   | -                    | 0        | -                   | -                    | 1.65     | -                   | -                    | -        | -                   | -                              | -        | -                   |
| Cappelli et al. [35]      | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 3                    | 2        | 5                   | 5                    | 3.48     | 5                   | -                              | -        | -                   |
| Sandhya et al. [50]       | -                    | 0        | -                   | -                    | 0        | -                   | -                    | 1.65     | -                   | -                    | -        | -                   | -                              | -        | -                   |
| Ferrara et al. [36]       | 0                    | 0        | 0                   | 0                    | 0.02     | 1                   | 4                    | 3.43     | 5                   | 9                    | 3.37     | 11                  | -                              | -        | -                   |
| Sandhya et al. [48]       | -                    | 0        | -                   | -                    | 0        | -                   | -                    | 3.65     | -                   | -                    | -        | -                   | -                              | -        | -                   |
| Ali et al. [33]           | -                    | 0        | -                   | -                    | 0        | -                   | -                    | 0        | -                   | -                    | -        | -                   | -                              | -        | -                   |
| Liu and Zhao [38]         | 0                    | -        | 0                   | 0                    | -        | 0                   | -                    | -        | -                   | -                    | -        | -                   | -                              | -        | -                   |
| Ali et al. [31]           | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 0                              | 0        | 0                   |
| Ali and Prakash [7]       | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 0                    | 0        | 0                   | 0                              | 0        | 0                   |
| <b>Proposed Technique</b> | <b>0</b>             | <b>0</b> | <b>0</b>            | <b>0</b>             | <b>0</b> | <b>0</b>            | <b>0</b>             | <b>0</b> | <b>0</b>            | <b>0</b>             | <b>0</b> | <b>0</b>            | <b>0</b>                       | <b>0</b> | <b>0</b>            |

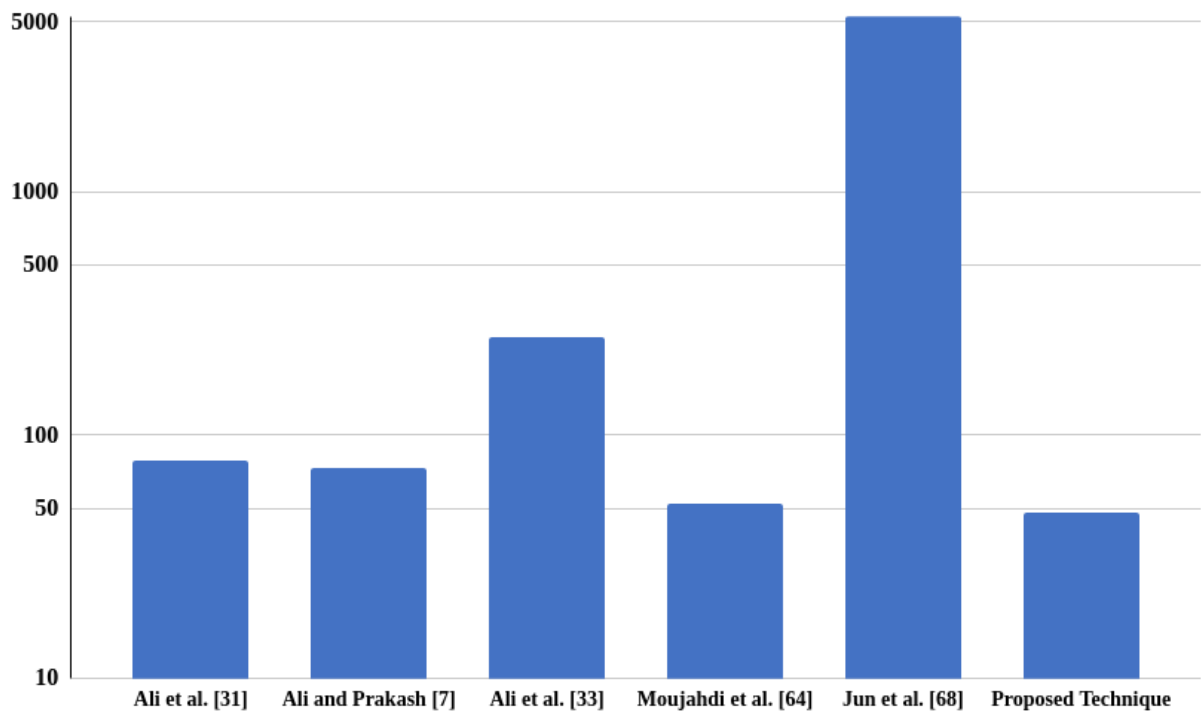
Note: “-” means that the result is not reported by the authors of the technique, for that particular database.

In [7,31] user template is generated by using all the minutiae points (good as well as bad quality minutiae point) of the fingerprint; however, the proposed technique uses only good-quality minutiae points leading to a much-optimized user template. The time taken by the proposed technique has been compared with other techniques in Table 4. The techniques present in Table 4 have been implemented either on a faster processor with more RAM or on a similar processor on which the proposed technique has been implemented. The average time taken for the template generation is 48 milliseconds and 0.8 milliseconds for template matching which is much better than the other techniques and due to this, the proposed technique can be used for light devices as well. As the proposed technique only uses good-quality minutiae points, it reduces the computations involved, which makes it a highly optimized technique, and Figure 9 pictorially depicts it is this which shows the efficiency of the proposed technique in terms of time taken.

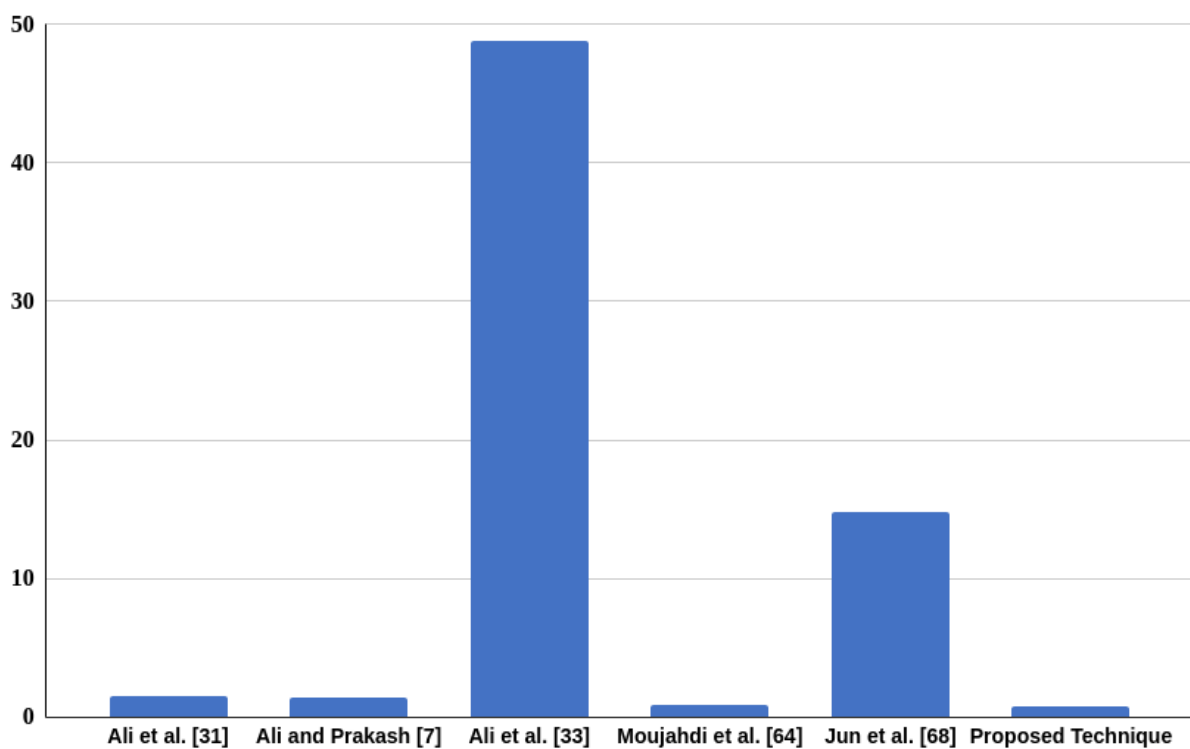
**Table 4.** Average time taken comparison of various techniques (values milliseconds).

| Techniques                | Template Generation | Template Matching |
|---------------------------|---------------------|-------------------|
| Ali et al. [31]           | 79                  | 1.5               |
| Ali and Prakash [7]       | 73                  | 1.4               |
| Ali et al. [33]           | 253                 | 48.8              |
| Moujahdi et al. [64]      | 52                  | 0.9               |
| Jun et al. [74]           | 5257                | 14.8              |
| <b>Proposed Technique</b> | <b>48</b>           | <b>0.8</b>        |





(a)

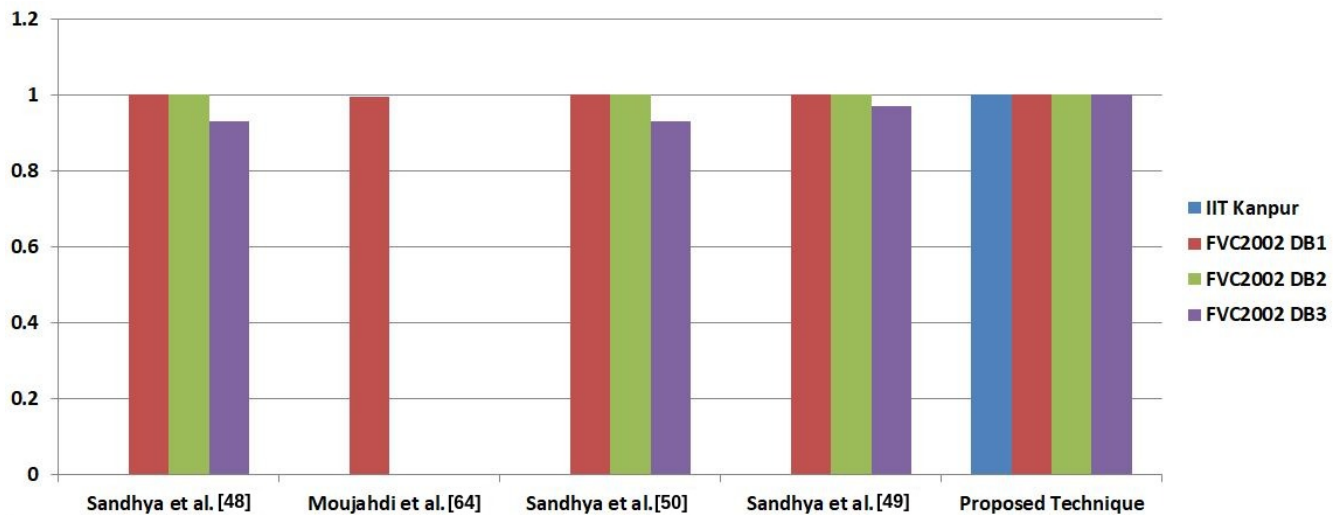


(b)

**Figure 9.** Average time taken (in milliseconds) by various techniques for (a) template generation, (b) template matching.

It can be observed from Table 2 that FVC2002 DB1, DB2, and DB3 are the most extensively used databases, and we know that IIT Kanpur is a large database [7]. Hence, for the rest of the analysis, these databases have been chosen. The KS test values obtained

for FVC2002 (DB1, DB2, and DB3) and IIT Kanpur fingerprint databases are shown in Table 5. As the KS test value ranges between 0 to 1, and the value closer to 1 means better separation between the genuine user and the imposter, so it can be observed that the proposed technique has good separation between the genuine and the imposter scores; as it achieved KS test value as 1. Figure 10 depicts the superior performance of the proposed technique for the KS test.



**Figure 10.** Kolmogorov–Smirnov (KS) test graph for the proposed technique and the other techniques, signifying a good separation between the imposter and genuine scores for the proposed technique.

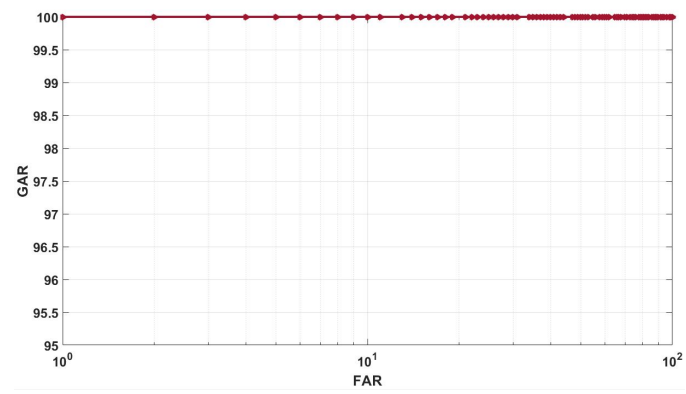
**Table 5.** KS test values comparison.

| Techniques                | IIT Kanpur | FVC2002 DB1 | FVC2002 DB2 | FVC2002 DB3 |
|---------------------------|------------|-------------|-------------|-------------|
| Sandhya et al. [48]       | -          | 1           | 1           | 0.93        |
| Moujahdi et al. [64]      | -          | 0.9934      | -           | -           |
| Sandhya et al. [50]       | -          | 1           | 1           | 0.93        |
| Ali et al. [31]           | 1          | 1           | 1           | 1           |
| Ali and Prakash [7]       | 1          | 1           | 1           | 1           |
| Sandhya et al. [49]       | -          | 1           | 1           | 0.9691      |
| <b>Proposed Technique</b> | <b>1</b>   | <b>1</b>    | <b>1</b>    | <b>1</b>    |

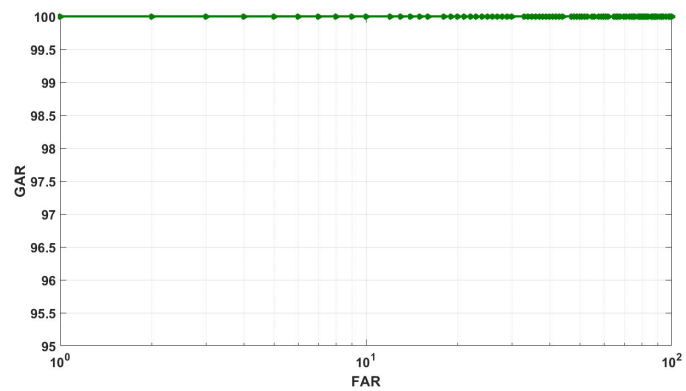
Note: “-” means that the result is not reported by the authors of the technique, for that particular database.

The ROC curve shows the relationship between FAR and GAR. The better value of GAR for different values of FAR means a better performing framework. The ROC curve plots obtained using FVC protocol on FVC2002 (DB1, DB2, and DB3) and IIT Kanpur fingerprint databases are shown in Figure 11. It can be observed that the ROC curve plots obtained for the proposed technique are highly encouraging, hence, the performance of the proposed technique is exceptionally and achieved 100% accuracy [31].

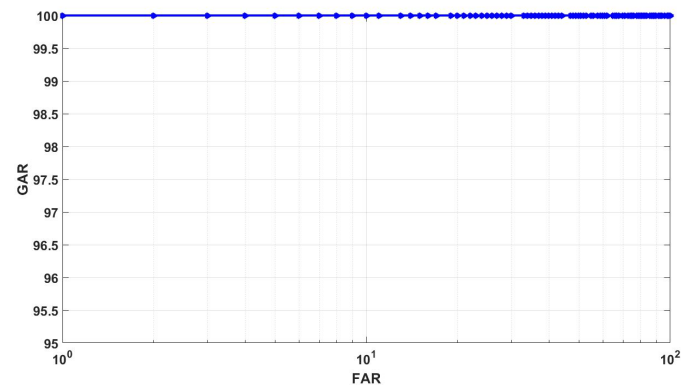
As the proposed technique uses the secure fingerprint features and uses only good-quality minutiae points for the template generation, from the experimental results it can be concluded that the proposed technique is highly robust and is extremely efficient in terms of user recognition.



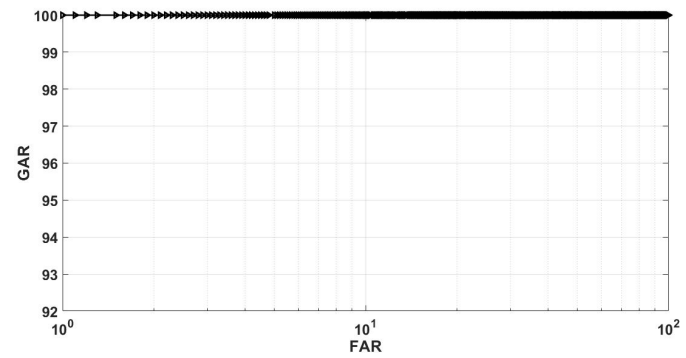
(a) FVC2002 DB1.



(b) FVC2002 DB2.



(c) FVC2002 DB3.



(d) IIT Kanpur.

Figure 11. The proposed technique’s ROC curves.

## 5. Conclusions

There are various issues related to security and privacy in the fingerprint-based authentication systems. In an insecure fingerprint-based biometrics, an adversary can even reconstruct the original fingerprint of a user. Ali et al. in [31] have designed a framework for a secure fingerprint-based biometrics; however, the technique proposed by them has various limitations. In this paper, a highly robust technique is proposed that constructs an efficient and optimized user template, which has a shape of the 3D spiral curve. Only good-quality minutiae points have been used for the template construction. All the features used to generate the user template are secure as well as revocable. The proposed technique is fast and can generate user template in just 48 milliseconds and for matching the template it requires only 0.8 milliseconds. The proposed technique achieved 0% EER as well. Nothing useful about the original fingerprint of the user can be obtained by adversary even after getting the user template. The technique designed is found to be extremely efficient with respect to revocability, diversity, security, and performance.

In future, we would like to extend the proposed technique for touch-less 3D fingerprint and sensor interoperability; so that it can work with different types of sensors during verification. We will analyze the proposed technique in terms of entropy [75–79] and will compare with other authentication modules [72,80,81]. It will be interesting to combine the other biometric traits in the human body with the proposed technique to develop a multi-modal biometric system. We would also like to use other fingerprint features such as ridge density, texture, etc. with the proposed technique.

**Author Contributions:** U.S. and S.S.A. designed and performed the experiments, conceptualization and methodology, and analyzed the data. U.S. and S.S.A. wrote the manuscript in consultation with P.T., N.S. and R.S.B. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Huh, J.-H. Surgery Agreement Signature Authentication System for Mobile Health Care. *Electronics* **2020**, *9*, 890. [[CrossRef](#)]
2. Munilla, J.; Hassan, A.; Burmester, M. 5G-Compliant Authentication Protocol for RFID. *Electronics* **2020**, *9*, 1951. [[CrossRef](#)]
3. Tidrea, A.; Korodi, A.; Silea, I. Cryptographic Considerations for Automation and SCADA Systems Using Trusted Platform Modules. *Sensors* **2019**, *19*, 4191. [[CrossRef](#)] [[PubMed](#)]
4. Saxena, N.; Hayes, E.; Bertino, E.; Ojo, P.; Choo, K.-K.R.; Burnap, P. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics* **2020**, *9*, 1460. [[CrossRef](#)]
5. Kaveh, M.; Martín, D.; Mosavi, M.R. A Lightweight Authentication Scheme for V2G Communications: A PUF-Based Approach Ensuring Cyber/Physical Security and Identity/Location Privacy. *Electronics* **2020**, *9*, 1479. [[CrossRef](#)]
6. Ali, S.S.; Baghel, V.S.; Ganapathi, I.I.; Prakash, S. Robust biometric authentication system with a secure user template. *Image Vis. Comput.* **2020**, *104*, 104004. [[CrossRef](#)]
7. Ali, S.S.; Prakash, S. 3-Dimensional Secured Fingerprint Shell. *Patt. Recogn. Lett.* **2019**, *126*, 68–77. [[CrossRef](#)]
8. Zhang, J.; Wu, M. Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine. *Electronics* **2020**, *9*, 1746. [[CrossRef](#)]
9. Tan, H.; Kim, P.; Chung, I. Practical Homomorphic Authentication in Cloud-Assisted VANETs with Blockchain-Based Healthcare Monitoring for Pandemic Control. *Electronics* **2020**, *9*, 1683. [[CrossRef](#)]
10. Noh, J.; Jeon, S.; Cho, S. Distributed Blockchain-Based Message Authentication Scheme for Connected Vehicles. *Electronics* **2020**, *9*, 74. [[CrossRef](#)]
11. Knežević, M.; Tomović, S.; Mihaljević, M.J. Man-In-The-Middle Attack against Certain Authentication Protocols Revisited: Insights into the Approach and Performances Re-Evaluation. *Electronics* **2020**, *9*, 1296. [[CrossRef](#)]
12. Iyappan, G.I.; Ali, S.S.; Prakash, S. Multi-resolution Local Descriptor for 3D Ear Recognition. In Proceedings of the BIOSIG 2019, Darmstadt, Germany, 18–20 September 2019; pp. 1–8.
13. Iula, A.; Micucci, M. Experimental Validation of a Reliable Palmprint Recognition System Based on 2D Ultrasound Images. *Electronics* **2019**, *80*, 1393. [[CrossRef](#)]
14. Nakanishi, I.; Maruoka, T. Biometrics Using Electroencephalograms Stimulated by Personal Ultrasound and Multidimensional Nonlinear Features. *Electronics* **2020**, *9*, 24. [[CrossRef](#)]
15. McGoldrick, L.K.; Halánek, J. Recent Advances in Noninvasive Biosensors for Forensics, Biometrics, and Cybersecurity. *Sensors* **2020**, *20*, 5974. [[CrossRef](#)] [[PubMed](#)]

16. Iyappan, G.I.; Prakash, S.; Dave, I.R.; Joshi, P.; Ali, S.S.; Shrivastava, A.M. Ear recognition in 3D using 2D curvilinear features. *IET Biom.* **2018**, *7*, 519–529.
17. Cavoukian, A.; Stoianov, A. Biometric encryption. In *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2009.
18. AlMajed, H.; AlMogren, A. A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things. *Sensors* **2020**, *20*, 6158. [[CrossRef](#)] [[PubMed](#)]
19. Ali, S.S.; Prakash, S. Fingerprint Shell Construction with Prominent Minutiae Points. In Proceedings of the COMPUTE 2017, Bhopal, India, 16–17 November 2017; ACM: New York, NY, USA, 2017; pp. 91–98.
20. Qiu, S.; Wang, D.; Xu, G.; Kumari, S. Practical and Provably Secure Three-Factor Authentication Protocol Based on Extended Chaotic-Maps for Mobile Lightweight Devices. *IEEE Trans. Dependable Secur. Comput.* **2020**, *1*. [[CrossRef](#)]
21. Ali, S.S.; Prakash, S. A Few Techniques for Fingerprint Template Protection. Ph.D. Thesis, Discipline of Computer Science & Engineering, IIT Indore, Madhya Pradesh, India, 2019.
22. Ratha, N.K.; Connell, J.H.; Bolle, R.M. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* **2001**, *40*, 614–634. [[CrossRef](#)]
23. Ilyas, M.; Othmani, A.; Fournier, R.; Nait-ali, A. Auditory Perception Based Anti-Spoofing System for Human Age Verification. *Electronics* **2019**, *8*, 1313. [[CrossRef](#)]
24. Ali, S.S.; Iyappan, G.I.; Mahyo, S.; Prakash, S. Polynomial Vault: A secure and robust fingerprint based authentication. *IEEE Trans. Emerg. Top. Comput.* **2019**. [[CrossRef](#)]
25. Nandakumar, K. A fingerprint cryptosystem based on minutiae phase spectrum. In Proceedings of the WIFS 2010, Seattle, WA, USA, 12–15 December 2010; pp. 1–6.
26. Ross, A.A.; Shah, J.; Jain, A.K. Toward reconstructing fingerprints from minutiae points. In Proceedings of the SPIE Conference on Biometric Technology for Human Identification, Orlando, FL, USA, 28 March 2005; pp. 68–80.
27. Ross, A.; Shah, J.; Jain, A.K. From Template to Image: Reconstructing Fingerprints from Minutiae Points. *IEEE Trans. PAMI* **2007**, *29*, 544–560. [[CrossRef](#)]
28. Chen, F.; Zhou, J.; Yang, C. Reconstructing Orientation Field From Fingerprint Minutiae to Improve Minutiae-Matching Accuracy. *IEEE Trans. Image Process.* **2009**, *18*, 1665–1670. [[CrossRef](#)] [[PubMed](#)]
29. Feng, J.; Jain, A.K. Fingerprint Reconstruction: From Minutiae to Phase. *IEEE Trans. PAMI* **2011**, *33*, 209–223. [[CrossRef](#)]
30. Breebaart, J.; Yang, B.; Buhan-Dulman, I.; Busch, C. Biometric template protection. *Datenschutz Datensicherheit DuD* **2009**, *33*, 299–304. [[CrossRef](#)]
31. Ali, S.S.; Iyappan, G.I.; Prakash, S. Fingerprint Shell construction with impregnable features. *J. Intell. Fuzzy Syst.* **2019**, *36*, 4091–4104. [[CrossRef](#)]
32. Mohanraj, V.; Chakkaravarthy, S.S.; Gogul, I.; Kumar, V.S.; Kumar, R.; Vaidehi, V. Intelligent, smart and scalable cyber-physical systems. *J. Intell. Fuzzy Syst.* **2019**, *36*, 3935–3943.
33. Ali, S.S.; Iyappan, G.I.; Prakash, S. Robust technique for fingerprint template protection. *IET Biom.* **2018**, *7*, 536–549. [[CrossRef](#)]
34. Baghel, V.S.; Ali, S.S.; Prakash, S. A non-invertible transformation based technique to protect a fingerprint template. *IET Image Process.* **2021**. [[CrossRef](#)]
35. Cappelli, R.; Ferrara, M.; Maltoni, D. Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition. *IEEE Trans. PAMI* **2010**, *32*, 2128–2141. [[CrossRef](#)] [[PubMed](#)]
36. Ferrara, M.; Maltoni, D.; Cappelli, R. Noninvertible Minutia Cylinder-Code Representation. *IEEE Trans. IFS* **2012**, *7*, 1727–1737. [[CrossRef](#)]
37. Ferrara, M.; Maltoni, D.; Cappelli, R. A two-factor protection scheme for MCC fingerprint templates. In Proceedings of the BIOSIG 2014, Darmstadt, Germany, 10–12 September 2014; pp. 1–8.
38. Liu, E.; Zhao, Q. Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with  $l_1$  minimization. *Neurocomputing* **2017**, *259*, 3–13. [[CrossRef](#)]
39. Nurtantio, A.P.; Catur, S.; Septino, N. Image compression based on SVD for BoVW model in fingerprint classification. *J. Intell. Fuzzy Syst.* **2018**, *34*, 2513–2519.
40. Feng, R.; Wang, Z.; Li, Z.; Ma, H.; Chen, R.; Pu, Z.; Chen, Z.; Zeng, X. A Hybrid Cryptography Scheme for NILM Data Security. *Electronics* **2020**, *9*, 1128. [[CrossRef](#)]
41. Trivedi, A.K.; Thounaojam, D.M.; Pal, S. Non-Invertible cancellable fingerprint template for fingerprint biometric. *Comput. Secur.* **2020**, *90*, 101690. [[CrossRef](#)]
42. Azzakhnini, S.; Ballihi, L.; Aboutajdine, D. Combining Facial Parts For Learning Gender, Ethnicity, and Emotional State Based on RGB-D Information. *ACM Trans. Multimed. Comput. Commun. Appl.* **2018**, *14*, 19:1–19:14. [[CrossRef](#)]
43. Yang, H.; Lin, B.; Chang, K.; Chen, C. Joint Estimation of Age and Expression by Combining Scattering and Convolutional Networks. *ACM Trans. Multimed. Comput. Commun. Appl.* **2018**, *14*, 9:1–9:19. [[CrossRef](#)]
44. Balazia, M.; Sojka, P. Gait Recognition from Motion Capture Data. *ACM Trans. Multimed. Comput. Commun. Appl.* **2018**, *14*, 22:1–22:18. [[CrossRef](#)]
45. Dave, I.R.; Iyappan, G.I.; Prakash, S.; Ali, S.S.; Shrivastava, A.M. 3D Ear Biometrics: Acquisition and Recognition. In Proceedings of the INDICON 2018, Coimbatore, India, 16–18 December 2018.

46. Kumar, G.; Tulyakov, S.; Govindaraju, V. Combination of symmetric hash functions for secure fingerprint matching. In Proceedings of the ICPR 2010, Istanbul, Turkey, 23–26 August 2010; pp. 890–893.
47. Iyappan, G.I.; Ali, S.S.; Prakash, S. Geometric statistics-based descriptor for 3D ear recognition. *Visual Comput.* **2020**, *36*, 161–173.
48. Sandhya, M.; Prasad, M.V.N.K. k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection. In Proceedings of the ICB 2015, Phuket, Thailand, 19–22 May 2015; pp. 386–393.
49. Sandhya, M.; Prasad, M.V.N.K.; Chillarige, R.R. Generating cancellable fingerprint templates based on Delaunay triangle feature set construction. *IET Biom.* **2016**, *5*, 131–139. [[CrossRef](#)]
50. Sandhya, M.; Prasad, M.V.N.K. Securing fingerprint templates using fused structures. *IET Biom.* **2017**, *6*, 173–182. [[CrossRef](#)]
51. Wang, S.; Deng, G.; Hu, J. A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognit.* **2017**, *61*, 447–458. [[CrossRef](#)]
52. Derman, E.; Keskinöz, M. Normalized cross-correlation based global distortion correction in fingerprint image matching. In Proceedings of the IWSSIP 2016, Bratislava, Slovakia, 23–25 May 2016; pp. 1–4.
53. Wang, S.; Hu, J. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach. *Pattern Recognit.* **2012**, *45*, 4129–4137. [[CrossRef](#)]
54. Si, X.; Feng, J.; Yuan, B.; Zhou, J. Dense registration of fingerprints. *Pattern Recognit.* **2017**, *63*, 87–101. [[CrossRef](#)]
55. Jiang, Q.; Zhang, N.; Ni, J.; Ma, J.; Ma, X.; Choo, K.K.R. Unified Biometric Privacy Preserving Three-Factor Authentication and Key Agreement for Cloud-Assisted Autonomous Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 9390–9401. [[CrossRef](#)]
56. Wang, D.; Wang, P. Two Birds with One Stone: Two-Factor Authentication with Security beyond Conventional Bound. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 708–722. [[CrossRef](#)]
57. Wang, S.; Hu, J. A blind system identification approach to cancelable fingerprint templates. *Pattern Recognit.* **2016**, *54*, 14–22. [[CrossRef](#)]
58. Ahn, D.; Kong, S.G.; Chung, Y.S.; Moon, K.Y. Matching with secure fingerprint templates using non-invertible transform. In Proceedings of the CISP 2008, Sanya, China, 27–30 May 2008; Volume 2, pp. 29–33.
59. Tran, M.H.; Duong, T.N.; Nguyen, D.M.; Dang, Q.H. A local feature vector for an adaptive hybrid fingerprint matcher. In Proceedings of the ICIC 2017, Hanoi, Vietnam, 26–28 June 2017; pp. 249–253.
60. Wang, S.; Yang, W.; Hu, J. Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs. *Pattern Recognit.* **2017**, *66*, 295–301. [[CrossRef](#)]
61. Boulton, T.E.; Scheirer, W.J.; Woodworth, R. Revocable fingerprint biotokens: Accuracy and security analysis. In Proceedings of the CVPR 2007, Minneapolis, MN, USA, 18–23 June 2007; pp. 1–8.
62. Khan, T.M.; Bailey, D.G.; Khan, M.A.U.; Kong, Y. Efficient Hardware Implementation For Fingerprint Image Enhancement Using Anisotropic Gaussian Filter. *IEEE Trans. Image Process.* **2017**, *26*, 2116–2126. [[CrossRef](#)]
63. Ali, S.S.; Iyappan, G.I.; Prakash, S.; Consul, P.; Mahyo, S. Securing biometric user template using modified minutiae attributes. *Pattern Recognit. Lett.* **2020**, *129*, 263–270. [[CrossRef](#)]
64. Moujahdi, C.; Bebis, G.; Ghouzali, S.; Rziza, M. Fingerprint shell: Secure representation of fingerprint template. *Pattern Recognit. Lett.* **2014**, *45*, 189–196. [[CrossRef](#)]
65. Ali, S.S.; Prakash, S. Enhanced Fingerprint Shell. In Proceedings of the SPIN 2015, Noida, India, 19–20 February 2015; pp. 801–805.
66. Lee, S.; Jeong, I.R. On the Unlinkability of Fingerprint Shell. *Secur. Commun. Netw.* **2020**, *2020*, 8256929. [[CrossRef](#)]
67. Taha, A.A.; Hanbury, A. An Efficient Algorithm for Calculating the Exact Hausdorff Distance. *IEEE Trans. PAMI* **2015**, *37*, 2153–2163. [[CrossRef](#)]
68. NIST; NBIS. 2017. Available online: <https://www.nist.gov/services-resources/software/nist-biometric-image-software-nbis> (accessed on 1 December 2020).
69. Lam, H.K.; Hou, Z.; Yau, W.Y.; Chen, T.P.; Li, J. A systematic topological method for fingerprint singular point detection. In Proceedings of the ICCARV 2008, Hanoi, Vietnam, 17–20 December 2008; pp. 967–972.
70. Zhu, E.; Guo, X.; Yin, J. Walking to singular points of fingerprints. *Pattern Recognit.* **2016**, *56*, 116–128. [[CrossRef](#)]
71. Wilcoxon, R. Kolmogoro-Smirnov Test. In *Encyclopedia of Biostatistics*; John Wiley & Sons, Ltd.: Hoboken, NJ, USA, 2005.
72. Eberz, S.; Rasmussen, K.B.; Lenders, V.; Martinovic, I. Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS'17), Abu Dhabi, United Arab Emirates, 2–6 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 386–399.
73. Maio, D.; Maltoni, D.; Cappelli, R.; Wayman, J.L.; Jain, A.K. FVC2000: Fingerprint verification competition. *IEEE Trans. PAMI* **2002**, *24*, 402–412. [[CrossRef](#)]
74. Jun, B.K.; Jaijie, K.; Ig-Jae, K.; Teoh, A.B.J. Cancelable fingerprint template design with randomized non-negative least squares. *Pattern Recognit.* **2019**, *91*, 245–260.
75. Wang, D.; Gu, Q.; Huang, X.; Wang, P. Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS'17), Abu Dhabi, United Arab Emirates, 2–6 April 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 372–385.
76. Sadeghi, K.; Banerjee, A.; Sohankar, J.; Gupta, K.S.S. Geometrical Analysis of Machine Learning Security in Biometric Authentication Systems. In Proceedings of the 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA), Cancun, Mexico, 18–21 December 2017; pp. 309–314. [[CrossRef](#)]

- 
77. Feng, Y.C.; Yuen, P.C. Binary Discriminant Analysis for Generating Binary Face Template. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 613–624. [[CrossRef](#)]
  78. Wang, D.; Cheng, H.; Wang, P.; Huang, X.; Jian, G. Zipf's Law in Passwords. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2776–2791. [[CrossRef](#)]
  79. Inthavisas, K.; Lopresti, D. Secure speech biometric templates for user authentication. *IET Biom.* **2012**, *1*, 46–54. [[CrossRef](#)]
  80. Bonneau, J.; Herley, C.; van Oorschot, P.C.; Stajano, F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 20–23 May 2012; pp. 553–567.
  81. Wang, D.; Li, W.; Wang, P. Measuring Two-Factor Authentication Schemes for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4081–4092. [[CrossRef](#)]