IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 31, 2021, accepted June 18, 2021, date of publication June 24, 2021, date of current version July 1, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3092018

Privacy-Preserving Cancelable Biometric Authentication Based on RDM and ECC

LEI WU[1,2,3], LINGZHEN MENG[1], SHENGNAN ZHAO[1], XIA WEI[1], AND HAO WANG[1,2]

[1]School of Information Science and Engineering, Shandong Normal University, Jinan 250358, China
[2]Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250358, China
[3]Shandong Provincial Key Laboratory for Software Engineering, Jinan 250101, China

Corresponding author: Lei Wu (wulei@sdnu.edu.cn)

This work was supported in part by the Natural Science Foundation of Shandong Province under Grant ZR2020MF056 and Grant ZR2020KF011, in part by the Natural Science Foundation of China under Grant 62071280, and in part by the Major Scientific and Technological Innovation Project of Shandong Province under Grant 2020CXGC010115.

ABSTRACT Biometric authentication is getting increasingly popular and demands a wide range of solutions to against increasing cybercrimes and digital identity thefts. This paper proposes a new privacy-preserving cancelable biometric authentication key agreement scheme, which improves the existing authentication scheme based on ECC. We are going to integrate the fuzzy commitment and cancelable biometrics to guarantee the security for user's biometric information. The cancelable biometrics named as the random distance method (RDM) which can generate non-invertible and privacy-preserving revocable pseudo-biometric identities. The proposed scheme realizes the mutual authentication of participants, and the privacy of biometric information and also can resist the vast majority of existing attacks. We use the widely accepted BPR adversary model to formally prove the safety features of our scheme. Further, the comparison of other existing related schemes shows that the performance of this scheme has greater advantages in terms of computation and communication costs. The experiments demonstrate that this scheme can achieves higher accuracy, while preserving biometric information privacy.

INDEX TERMS Biometric authentication, privacy preservation, cancelable biometrics, elliptic curve cryptography (ECC), RDM.

I. INTRODUCTION

In recent time, the advancement of the Internet and mobile technology provides various convenient online services for our life, such as banking, electronic commuting, games, E-health, etc. However, users access these services through an insecure channel, which makes it easy to become the target of adversaries. To avoid sensitive information theft and illegal use, the demand for identity authentication between users and servers is increasing. Biometric authentication has become increasingly mature, such as face recognition, fingerprint recognition and iris recognition have been widely used in mobile intelligent terminals. At the same time, biometric information has the risk of privacy leakage, the privacy-preserving biometric authentication has become a hot spot for many scholars.

In the process of biometric authentication, biometric information is directly stored and transmitted as digital entities which are in danger due to malicious activities, so the preservation of biometric information is crucial. Reference [1]–[3] proposed a privacy-preserving biometric authentication scheme based on homomorphic encryption that can directly add or multiply the ciphertext without exposing the information in the plaintext, but it requires a complicated computational process on the ciphertext, so the efficiency will be very low. In response to this problem, the auxiliary vector is introduced for approximate matching, which relatively improves efficiency [4]. Therefore, homomorphic encryption is not widely used in practical applications. Elliptic curve cryptography is a lightweight cipher with short key length and high efficiency. Yoon and Yoo [5] presented biometric-based remote user authentication scheme, which uses ECC in a multi-server environment. Reference [6] proved that Yoon's scheme is insecure against insider attack and impersonation attack.

The associate editor coordinating the review of this manuscript and approving it for publication was Tony Thomas.

A biometric-based authentication scheme for client-server networks was proposed by Yeh *et al*. [7]. Reference [8] found that Yeh's scheme failed to achieve session key agreement, mutual authentication. The biometric authentication schemes for health care system using ECC was proposed by Sahoo *et al*. [9]. Reference [10] proposed the ECC-based secure three-factor authentication protocol with forward secrecy for Wireless Medical Sensor Network Systems and it utilizes a fuzzy commitment scheme to handle the biometric information. Reference [11] presented a biometric-based authentication approach for mobile devices and used ECC. In order to establish a secure channel on the open network and ensure the authenticity of the user and server, mutual authentication and session keys play a vital role. The mentioned above schemes are based on the ECC biometric authentication scheme, which cannot provide perfect forward secrecy or resist user anonymity and replay attacks, and use only simple hash algorithms to protect the privacy of biometric information. Therefore, it is a new challenge to develop a novel and reliable biometric authentication key agreement scheme that can overcome most of the existing attacks. The main contributions of this paper can be summarized as follows:

(1) In response to the analysis of the security deficiencies of the above mentioned ECC-based biometric authentication schemes, we propose a new biometric authentication scheme, privacy-preserving cancelable biometric authentication based on RDM and ECC. On the basis of using the elliptic curve cryptography to establish a shared session key, we use a cancelable feature to protect the original biometric information.

(2) For the existing ECC-based key agreement authentication schemes, most of the biometric information is preserved only by simple hash algorithm. We employ a novel template transformation technique namely Random Distance Method (RDM) to generate pseudo-biometric templates and use fuzzy commitment to preserve the pseudo transformed template, so that the privacy of biometric information is effectively preserved.

(3) We compare this scheme with other related scheme in terms of security, computational cost and communication cost, demonstrate that we have a significant improvement in security with lower computation and communication costs. We also analyze the accuracy of this biometric authentication scheme, and this scheme is compared with other methods and expressed by ROC curve, which proves that this scheme has better accuracy.

The remaining part of this paper is organized as follows. The related work discussed in Section 2, it describes the corresponding preliminary information such as Cancelable transforms, Fuzzy Commitment and ECC. In Section 3, we propose a biometric-based authentication scheme using ECC, the implementation process of the scheme is introduced in detail. Then the security analysis of the proposed scheme is demonstrated in Section 4. The performance analysis of the scheme is presented in Section 5. Finally, Section 6 presents the conclusion.

II. RELATED WORK

A. CANCELABLE TRANSFORMS

In literature, the four main approaches in biometric template protection are: fuzzy commitment, secure sketch, secure multiparty computation, and cancelable biometrics [12]. Fuzzy commitment and secure sketch are often used in biometric cryptography systems, which are usually implemented by error-correcting codes [13]–[16]. Secure multi-party attempts to determine the distance between registration and probe biometrics using computationally secure cryptographic tools such as garbled circuits and homomorphic encryption. A secure template must satisfy important properties such as non-invertibilty and revocability. Non-invertibilty means that it must be computationally difficult to recover the original biometric data from a template. Revocability means that if a biometric template is corrupted, the corrupted template can be undone and a new template can be generated using a different transformation. Cancelable biometric transforms the original biometric identity of a user to a pseudo-biometric identity that is used for storage and matching purposes. In [17], cancelable biometrics was first defined, and cancellable biometric features have been a hot topic in recent years. There are many schemes to study the generation of templates, and non-invertible transforms is the main method. At present, the commonly used method is Random Projection (RP) which is based on the feature vectors extracted from biometrics and projected onto a random subspace, such that pair-wise distances between points before and after projection are approximately preserved. Reference [18]–[21] describes this method in detail. Reference [22] proposed a locality sensitive hashing based approach, dubbed as locality sampled code (LSC), to generate cancelable IrisCodes features. However, this technique was limited to unimodal biometric systems having binary feature representations. A novel palmprint template protection scheme based on random comparison and noise data was proposed by Qiu *et al.* [23]. Abeer and Ghada [24] presented effective methods based on different discrete transforms, such as Discrete Fourier Transform (DFT), Fractional Fourier Transform (FrFT), in addition to matrix rotation to generate cancelable biometric templates. The implementation of this technology is limited to face or fingerprint, and cannot be used for multi-mode use.

In response to the shortcomings of the above technologies, this scheme employs a novel template transformation technique named as Random Distance Method (RDM). Compared with RP, the RDM not only has simple calculation, but also generates non-invertible, revocable, and diverse pseudo-biometric templates, which reduces the dimension of the features by 50% [25]. The concept of random distance is shown in figure 1. RDM maps biometric features as points in cartesian space, let (x_0, y_0) is the user's feature point. RDM is proposed to use the distance of feature point from some random point for matching purposes, such as the Euclidean distance between dx_1 and dy_1 of (x_0, y_0) and (x_1, y_1), if both

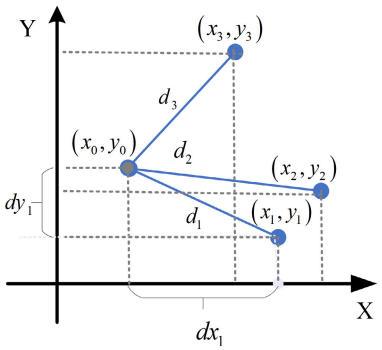


FIGURE 1. The concept of random distance.

$dx_1 < \delta$ and $dy_1 < \delta$ are satisfied, the difference between them is particularly small and belongs to the same user.

B. FUZZY COMMITMENT

Fuzzy commitment scheme belongs to the key-binding, the security of pseudo-transformed templates is guaranteed by employing fuzzy commitment protocol, which was first proposed by Juels and Sudan [14] and has been widely applied to the privacy-preserving biometric templates by binding encoded keys to biometric data. Fuzzy commitment is mainly a combination of cryptography and error-correcting code that plays a key role [26]. If the biometric information is a corrupted code word, the error-correcting code can check and correct the information. At the registration stage, the server S employs the fuzzy commitment scheme to input the user's biometric information B and the randomly selected key K, S outputs the helper data HD. In the authentication phase, the user's biometric query information B' and the helper data HD are put into the recovery module to extract the key K'. If the difference between B and B' is less than the error correction capability of ECC in the fuzzy commitment scheme, the recovery module can completely recover the same key, and then perform Hash matching. This process is shown in Figure 2.

In [27], Chang *et al.* proposed a multi-biometric fusion framework BIOFUSE, that combines fuzzy commitment and fuzzy vault using the format-preserving encryption scheme. Fuzzy commitment and homomorphic encryption are used in bio-encrypted identity verification to achieve blind authentication [28]. Reference [29] proposed a new multi-server authentication protocol for using fuzzy commitment scheme. In [30], Rehman *et al.* found that Barman *et al.*'s protocol [29] is still vulnerable to anonymity violation attack and impersonation based on stolen smart card attack. Reference [30] proposed an enhanced protocol to overcome the security weaknesses of Barman *et al.*'s scheme.

C. OVERVIEW OF ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is one of the safest and most effective encryption in public key cryptosystems. RSA is also a public key encryption algorithm and the longer

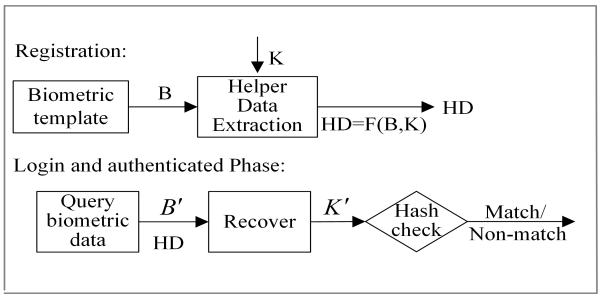


FIGURE 2. The fuzzy commitment scheme.

the key, the lower the efficiency. Compared with RSA, ECC has the same security, but the length of key is much smaller and the efficiency is higher. Therefore, ECC as a lightweight password is widely used in identity authentication schemes in IoT communications. A novel authentication scheme using ECC's lightweight password-based authentication technology for internal attack protection was proposed [31]. Reference [32] combined Physical Unclonable Function (PUF) and ECC to propose an access control and authentication scheme suitable for Telecare Information System. ECC is used in smart grids and implemented secure authentication protocols [33]. Reference [34] proved that [33] had incorrect login and authentication phase and proposed a quick solution to fix the pertinent flaws of the PALK. A robust authentication and access control protocol for securing wireless healthcare sensor networks with ECC [35].

First, the notations and their descriptions throughout this article are listed in Table 1.

Definition 1: Denote a non-singular elliptic curve over a prime finite field, as in

$$y^2 = x^3 + ax + b \bmod p \tag{1}$$

where all the points on the elliptic curve $(x, y) \in F_p$, $a, b \in F_p$. This equation must be satisfied $4a^3 + 27b^2 \bmod p \neq 0$. In ECC, the scalar multiplication is defined as the repeated addition. Let G be a base point on elliptic curve $E_p(a, b)$, whose order be n. If $G \in F_p$, then $nG = G + G + \cdots n$ (n times).

Definition 2 (Elliptic Curve Discrete Logarithm Problem (ECDLP)):

Given a prime number P, $G \in F_p$, $P = kG$. For the known K and G, it is easy to find the value of P, but when P and G are known, it is computational infeasible to derive integer $k \in [1, n-1]$.

Definition 3: Elliptic curve computational Diffie-Hellman (ECDH)

When Alice and Bob want to exchange information but do not want a third party to get it, they can use ECDH. Let Alice and Bob have their own private keys $a, b \in F_p$, they first calculate their respective public keys $aG, bG \in E_p(a, b)$, and then calculate the same shared key $s = a(bG) = b(aG)$, but it is infeasible for the middleman to try to calculate.

TABLE 1. Notations and descriptions involved in this article.

Notation	Description
F_p	A prime finite field
$E_p(a,b)$	A non-singular elliptic curve group
S	A server
U_i	The ith user
s	The server's private key
SC_i	U_i's smart-card
P_{pub}	The server's public key
$ID_i/PW_i/B_i$	U_i's identity, password and biometrics
Z_n^*	The interval $[1, n-1]$
SK	The session key
$E_k(\cdot)/D_k(\cdot)$	A symmetric encryption/decryption algorithm
$\oplus$	The bitwise XOR operation
$\|$	The concatenation operation

III. THE PROPOSED SCHEME

This section specifically introduces the detailed phases of the scheme, including the system initialization phase, registration phase, login authenticated and key agreement phase.

A. SYSTEM INITIALIZATION PHASE

In this phase, the required parameters are generated by the server S. An elliptic curve $E_p(a,b)$ is selected in the finite filed F_p, where p is a large prime number, G s a base point and n is the order of G. S selects a random number $s \in Z_n^*$ as the private key, and calculates $P_{pub} = sG$ as the public key. Finally, S sets $\{E_p(a,b), n, G, P_{pub}\}$ as the public parameters.

B. USER REGISTRATION STAGE

A new user U_i who wants to enjoy the service provided by the server S needs to register the user's information with S, including the user's identity ID_i, password PW_i and biometric information B_i. First, U_i uses the random distance method (RDM) to convert the biometric information to generate a pseudo-biometric template and store it in the database, while the conversion parameters are stored in the smart card SC_i. S processes the user's identity information anonymously, and uses the fuzzy commitment scheme to generate helper data HD, and stores HD in the database for using in the verification phase. The specific process is given below from both the U_i and the S.

(1) User U_i

1) U_i inputs his identity ID_i, password PW_i and biometric information B_i, then generates a random number r_i to calculate $MP_i = H(ID_i \| PW_i) \oplus r_i$, sends ID_i and MP_i to the server S.
2) U_i generates a random key K_T, and uses the random distance method (RDM) to convert the biometric information to generate a pseudo-biometric template, and puts the template Tf in the database. At the same time, the user puts the conversion parameters into the smart card SC_i. The detailed process is shown in Table 2.

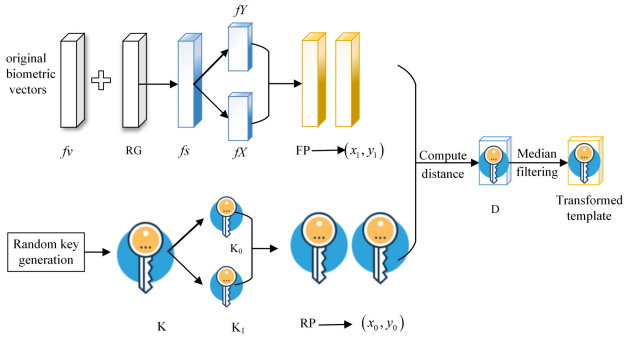


FIGURE 3. Random distance method to generate pseudo-biometric template.

For the biometric information input by the user, the filter is used to extract the characteristics of the biometric information, and the pseudo-identities is generated by the random distance method as shown in Figure 3. The specific process is as follows:

Step 1: U_i uses the log-Gabor filter to calculate and extract the features of biometric information and process them in different directions and different scales to obtain a one-dimensional vector $fv \in R^{N'}$.

Step 2: Generate the value of a specific user as the random network $RG \in R^{N'}$. The random network RG has the same size as the one-dimensional vector fv. The original feature vector is salted with the random network RG, that is $fs = fv + RG$, which increases the entropy of the template;

Step 3: Divide the salted into two equal vectors $fX = fs(1 : N'/2)$ and $fY = fs(N'/2 + 1 : N')$ and use the values corresponding to these two points to define the mapping $FP_j(x_1 = fX(j), y_1 = fY(j))$, where $j = 1 \cdots N'/2$;

Step 4: Generate the user's private key $k \in R^{N'}$, divide the key k into two equal parts k_0 and k_1, define a random point mapping $RP_j(x_0 = k_0(j), y_0 = k_1(j))$ and calculate the distance d between the user's characteristic point $FP_j(x_1, y_1)$ and the random point (x_0, y_0) as a vector $D(j) = d$;

Step 5: Perform median filtering on the vector D to generate a pseudo-biometric template Tf, and the median filtering is used to provide an irreversible operation.

It is observed that the conversion parameters in this process are RG and K. By changing the conversion parameters, different pseudo-biometric templates can be generated. Even if both RG and K are known to the attacker at the same time, the original biometric information will not be disclosed because the process is non-invertibilty.

(2) Server S

1) The server S receives ID_i and MP_i sent by the U_i. Firstly, S checks whether $H(ID_i)$ exists in the database. If not, it generates a random number N_0 and calculates $R_i = Q_i \oplus MP$, $V_i = H(ID_i \| Q_i)$, $Q_i = H(ID_i \| s)$, $eID_i = E_s(ID_i \| N_0)$.
2) S generates a key K and obtains the pseudo-biometric template Tf from the database. S uses the fuzzy commitment scheme to generate helper data HD

TABLE 2. User registration phase.

User Registration phase:		
User(U_i)/Smart-card (SC_i)		Server (S)
Input ID_i, PW_i and B_i random number r_i $MP_i = H(ID_i \parallel PW_i) \oplus r$ $B_i \xrightarrow{RDM} Tf$	$\xrightarrow{ID_i, MP_i}$	random nonce N_0 $Q_i = H(ID_i \parallel s)$ $eID_i = E_s(ID_i \parallel N_0)$ $R_i = Q_i \oplus MP$ $V_i = H(ID_i \parallel Q_i)$ Fuzzy Commitment $Fc = (K, Tf) = HD$ Store $\{H(ID_i), HD, H(K)\}$ in its database Store $\{eID_i, R_i, V_i, E_k(\cdot)/D_k(\cdot), H(\cdot)\}$ into SC_i
Store $\{RG, K_T\}$ into SC_i	$\xleftarrow{SC_i}$	

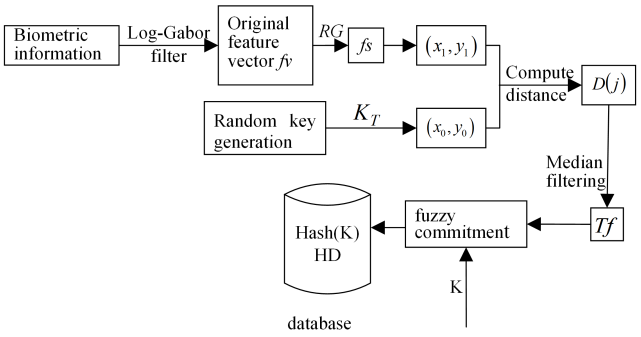


FIGURE 4. The process of generating auxiliary data with fuzzy commitment.

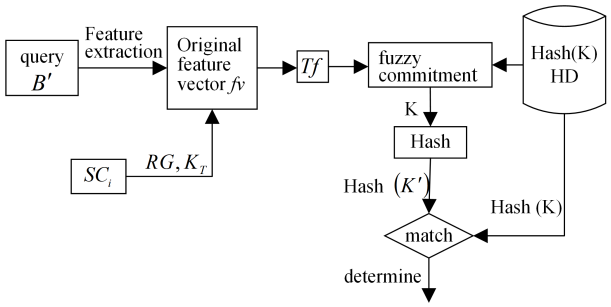


FIGURE 5. Fuzzy commitment scheme for the determination of biometric information.

and store it in the database. This process is shown in figure 4. S puts $\{H(ID_i), HD, H(K)\}$ in the database and $\{eID_i, R_i, V_i, E_k(\cdot)/D_k(\cdot), H(\cdot)\}$ in the smart card SC_i.

C. LOGIN AUTHENTICATED AND KEY AGREEMENT PHASE

For a legal user, the login authenticated and key agreement phase is as the following steps:

1) U_i inputs the user's identity ID_i, password PW_i and imprints biometric B_i by using his smart-card SC_i, and generates a random number r_i. Then SC_i calculates $MP_i' = H(ID_i \parallel PW_i) \oplus r_i$, $Q = R_i \oplus MP_i'$, and verifies $V_i? = H(ID_i \parallel Q_i)$ whether is established to determine the authenticity of the user's identity. If not, U_i terminates the session; else, U_i goes to the next step.

2) U_i generates a random number $x \in Z_n^*$, and calculates $A_1 = H(ID_i \parallel Q_i \parallel X \parallel t_1)$, where t_1 is the current timestamp of the user. U_i uses RG and K_T in SC_i to perform RDM conversion of B_i and generates a pseudo-biometric template Tf'. Finally, Finally, U_i sends $\{eID_i, X, A_1, t_1, Tf'\}$ to S.

3) The server S first checks the validity of the timestamp t_1 and verifies whether $t_1' - t_1? < \Delta t$ is established, which t_1' is the time when the message is currently received. If not, S terminates the session; else, S calculates $ID_i \parallel N_0 = D_s(eID_i)$, $Q_i' = H(ID_i \parallel s)$ and checks $A_1? = H(ID_i \parallel Q'_i \parallel X \parallel t_1)$. So that S can verify the authenticity of the user. If not, S terminates the session; else S goes to the next step.

4) S applies the fuzzy commitment scheme and inputs and Helper data thereby recovering the key Tf' and Helper data HD thereby recovering the key K'. S verifies whether $Hash(k')? = Hash(k)$ is established, as shown in figure 5. After establishment, S generates a random number $y \in Z_n^*$ and a random number δ, then S calculates $C_2 = E_{Q_i'}(ID_i \parallel \delta)$, $NID_i = E_s(ID_i \parallel \delta)$, $Y = yG$, and $A_2 = H(C_2 \parallel Q_i' \parallel t_2)$, Finally, S sends $\{C_2, A_2, t_2\}$ to U_i.

5) Firstly, U_i checks the validity of the timestamp t_2 and verifies whether $t_2' - t_2? < \Delta t$ is established, where t_2' is the time when the message is currently received. After establishment, U_i then checks whether $A_2 = H(C_2 \parallel Q_i \parallel t_2)$ is established. If not, U_i terminates the session; else, U_i calculates $NID_i \parallel Y = D_{Q_i}(C_2)$ and replaces eID_i with NID_i, then U_i establishes a session key $SK_i = H(Q_i \parallel X \parallel Y \parallel xY)$ and calculates $A_3 = H(NID_i \parallel Y)$. Finally, U_i sends A_3 to S.

6) S verifies whether $A_3? = H(NID_i \parallel Y)$ is established, if not, S terminates the session; else, S calculates session key $SK_j = H(Q_i' \parallel X \parallel Y \parallel yX)$. U_i and S share the same session key SK_j and complete the authentication.

TABLE 3. Login authenticated and key agreement phase.

Login authenticated and key agreement phase:		
User(U_i)/Smart-card (SC_i)		Server (S)
Input ID_i, PW_i and B_i random number r_i $MP_i' = H(ID_i \parallel PW_i) \oplus r_i$ $Q = R_i \oplus MP_i'$ $V_i? = H(ID_i \parallel Q_i)$ random number $x \in Z_n^*$ $X = xG$ $A_1 = H(ID_i \parallel Q_i \parallel X \parallel t_1)$ $B_i \xrightarrow{RDM} Tf'$	$\xrightarrow{eID_i, X, A_1, t_1, Tf'}$	$t_1' - t_1? < \Delta t$ $ID_i \parallel N_0 = D_s(eID_i)$ $Q_i{}' = H(ID_i \parallel s)$ $A_1? = H(ID_i \parallel Q'_i \parallel X \parallel t_1)$ $Fc(HD, Tf') = k'$ $Hash(k')? = Hash(k)$ random number $x \in Z_n^*$ and a nonce δ $Y = yG$ $Y = yG$ $NID_i = E_s(ID_i \parallel \delta)$ $C_2 = E_{Q_i'}(ID_i \parallel \delta)$ $A_2 = H(C_2 \parallel Q_i' \parallel t_2)$
$t_2' - t_2? < \Delta t$ $A_2 = H(C_2 \parallel Q_i \parallel t_2)$ $NID_i \parallel Y = D_{Q_i}(C_2)$ Replace eID_i with NID_i $SK_i = H(Q_i \parallel X \parallel Y \parallel xY)$ $A_3 = H(NID_i \parallel Y)$	$\xleftarrow{C_2, A_2, t_2}$	$A_3? = H(NID_i \parallel Y)$ $SK_j = H(Q_i' \parallel X \parallel Y \parallel yX)$

IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME

A. FORMAL SECURITY ANALYSIS

This section first gives the formal security analysis in the random oracle model under the BPR adversary model, and then analyses the vast majority of possible attacks, which proves that the security of this solution has been improved.

1) SECURITY MODEL

In this paper we demonstrate the security of this scheme using the widely used BPR model, where the two entities in the scheme are the server and the user. When there are multiple instances at the same time, we denote the *ith* user instance and *jth* server instance by U^i and S^j. The BPR model uses session identifier (sid) to define the relationship of partners. For two oracles to be partners with one another they should have the same SID and the same SK, one should be a client and the other a server, each should think itself partnered with the other, and, finally, no third oracle should have the same SID. U^i and S^j are partnered, holding (sid, sk, pid), (sid', sk', pid') (i.e., session id, session key, and partner id), respectively, and the conditions: $sid = sid'$, $sk = sk'$, $pid = S^j \wedge pid' = U^i$ hold. Let A be a probabilistic polynomial time (PPT) adversary. This scheme allows adversaries to monitor, delay, replay and modify messages at will. We define the security of the key agreement authentication protocol through games between the challenger and the adversary. In the game, adversary A is allowed to make the following oracle query:

send (U, i, m): This query sends message m to oracle Π_u^i. The oracle computes what the protocol says to, and sends back the response. The adversary can require one of the participants (such as server A) to initiate a session with the other party (such as client A).

Reveal (U, i): This query allows adversary A to obtain the session key sk.

Corrupt (U, d): This query reveals the secret parameters of U according to the value of d:

$-$d $= 0$, reveals the password PW of U.

$-$d $= 1$, reveals the parameters stored in the smart-card of U.

Execute $\left(U^i, S^j\right)$: This query allows A to completely breaches a participant or U^i and S^j obtains all the exchanged information of the compromised party.

Test (sid): At any time, A can only perform this kind of query once and then get a challenge that is either a real session key value or a random value. This challenge value depends on the value of bit b randomly selected by the *Test* oracle. If no session key is agreed or sid is not fresh, returns the invalid symbol $\perp$; else, flips a coin. If b $= 0$, this query returns the real session key, if b $= 1$, this query will return a randomly selected key with the same bit length as the actual session key.

2) SEMANTIC SECURITY

The purpose of adversary A is to distinguish the real session key from the random key. A is allowed to do a *Test* query, and the result of the real session key and the random key is

1/2. If A correctly guesses whether the key is random or not, then A wins, outputs a bit b', and $b = b'$, b is the random bit selected in the *Test* query. A's advantage in breaking protocol Π and violating semantic security is defined as:

$$Adv_{\Pi}^{m} = |2pr\left[b = b'\right] - 1| \tag{2}$$

If Adv_{Π}^{m} is only negligibly larger than $O\left(\frac{q_s}{|D|}\right)$, then the protocol Π is called semantically secure, where q_s is the number of *send* queries, $|D|$ is the size of a uniformly distributed password dictionary D.

3) SECURITY PROOF

Theorem 1: Let A be a PPT adversary that attacks the semantic security of our privacy-preserving biometric-based key agreement scheme Π. Then,

$$Adv\,(A) \leq \frac{q_f^2}{2^{l_f}} + \frac{q_h^2}{2^{l_h}} + \frac{(q_s - q_e)^2}{n-1} + \frac{q_s}{2^{l_h-1}} + 2q_h Adv_G^{ECDH}\,(C) + 2\frac{q_s}{|D|} \tag{3}$$

where q_f, q_h, q_s, q_e denote the number of encryption/decryption, hash, Send and Execute oracle queries, respectively. l_h, l_f are the bit length of the output of hash and encryption oracles. The $Adv_G^{ECDH}\,(C)$ denotes the probability of successfully solving the ECDH problem with C.

Proof: Define four consecutive games G_i $(i = 0, 1, 2, 3)$ to describe the process of proof, Let Su_i be the event that the adversary A correctly guessed the value of b in G_i.

Game G_0: This game model is A's real attack on the key agreement, according to the definition of semantic security, we have

$$Adv_{\Pi}\,(A) = |2\Pr[Su_0] - 1| \tag{4}$$

Game G_1: This game model excludes the collision resistance of the scheme compared to G_0. According to the birthday paradox, the probability of collision in the hash oracle, encryption/decryption oracle and transcripts are bounded by $\frac{q_h^2}{2^{l_h+1}}$, $\frac{q_f^2}{2^{l_f+1}}$, $\frac{(q_s-q_e)^2}{2(n-1)}$. Thus,

$$|\Pr[Su_1] - \Pr[Su_0]| \leq \frac{q_h^2}{2^{l_h+1}} + \frac{q_f^2}{2^{l_f+1}} + \frac{(q_s - q_e)^2}{2(n-1)} \tag{5}$$

Game G_2: This game model is the same as G_1, without making hash oracle, adversary A guesses instances of A1, A2, A3. Thus,

$$|\Pr[Su_2] - \Pr[Su_1]| \leq \frac{q_s}{2^{l_h}} \tag{6}$$

Game G_3: This game uses the method of calculating the session key $SK = H\,(Q_i \parallel X \parallel Y)$. Therefore, in this game, A has no advantage in guessing the value of b in the *Test* query. Thus,

$$\Pr[Su_3] = \frac{1}{2} \tag{7}$$

G_3 and G_2 are indistinguishable unless the operator C can safely solve the ECDH problem. In addition, the scheme has three influencing factors, in which the biometric information employs privacy-preserving RDM. A can obtain two factors at most, but not knowing the information of the smart card is useless. Assuming a *Corrupt* $(U, 1)$ is queried, there are the following examples:

Corrupt $(U, 0)$ is queried, the success probability is at most $\frac{q_s}{|D|}$. Thus,

$$|\Pr[Su_3] - \Pr[Su_2]| \leq q_h Adv_G^{ECDH}\,(C) + \frac{q_s}{|D|} \tag{8}$$

Finally, the theorem 1 can be easily proved by the above formulas.

B. SECURITY ANALYSIS AGAINST OTHER POSSIBLE ATTACKS

This section presents the informal security analysis of the proposed scheme, discusses possible attacks and demonstrates that the scheme is resistant to the vast majority of attacks and its security has been significantly improved [36].

1) ACHIEVE USER ANONYMITY

On the public channel, the original identity ID_i is not transmitted. In the registration phase, S uses its own private key s to encrypt the user's identity ID_i and generate a pseudo-identity eID_i. In the login authenticated and key agreement phase, according to $ID_i \parallel N_0 = D_s\,(eID_i)$, only legal S can decrypt eID_i. Moreover, a random number is used to encrypt ID_i in every session. Therefore, this scheme can realize user anonymity during the entire communication process.

2) ACHIEVE MUTUAL AUTHENTICATION BETWEEN U_i AND S

S can verify the authenticity of the user through the formula $A_1? = H\left(ID_i \parallel Q'_i \parallel X \parallel t_1\right)$, and only provides services to legitimate users. Therefore, we need to analyze the situation where the equation $A_1 = H\,(ID_i \parallel Q_i \parallel X \parallel t_1)$ is established, in which we only need to analyze whether Q_i is easy to be stolen. According to $Q_i = H\,(ID_i \parallel s)$, the adversary can directly calculate Q_i by obtaining the ID_i and the server's private key s, but it is obvious that this method cannot be realized. The ID_i is encrypted with the server's private key s to achieve user anonymity. Moreover, the other way is to obtain the information in the smart card SC_i. According to $Q_i = R_i \oplus H\,(ID_i \parallel PW_i) \oplus r_i$, there is a random number r_i, so it is too difficult for the adversary to obtain Q_i. Similarly, U_i can verify the legitimacy of S through $A_2? = H\,(C_2 \parallel Q_i \parallel t_2)$, only the legitimate S has the private key s, and then decrypts to obtain ID_i. As a result, U_i and S can achieve mutual authentication each other and then share the same session key protocol $SK_i = H\,(Q_i \parallel X \parallel Y \parallel xY)$.

3) FORWARD SECRECY

Forward secrecy means that even if the long-term key used by U_i and S to generate the session key is compromised, the previously established session key and communication information should be preserved. The session key agreement

of this scheme is defined by $SK_i = H(Q_i \| X \| Y \| xY)$, where $X = xG$, $Y = yG$, x, and y are random numbers generated by the U_i and the S, respectively. Moreover, even if the adversary intercepts the values of X and Y, it is not possible to calculate the value of xyG in the common session key SK_i. Because of the difficulty of discrete logarithm problem based on ECDH, this scheme can achieve forward secrecy.

4) RESIST THE REPLAY ATTACK

Replay attack means that the adversary steals the data that has been sent and re-sends it to the authentication server intact. This scheme resists replay attacks by adding timestamps, and S is allowed to accept a uniquely limited time for a reply. In this scheme, the user's authentication information $\{eID_i, X, A_1, t_1, Tf'\}$ is sent to S. S checks the validity of the timestamp t_1 by verifying ${t_1}' - t_1? < \Delta t$, that is, the user's current timestamp and the time of receiving the message are less than Δt. If this formula does not hold, the session will be terminated. S can also resist replay attacks by verifying whether $A_1? = H(ID_i \| {Q'}_i \| X \| t_1)$ is established. Similarly, when the server sends $\{C_2, A_2, t_2\}$ to the user, it verifies the validity of the timestamp through the formula ${t_2}' - t_2? < \Delta t$, so our scheme can resist replay attacks.

5) LOST SMART-CARD ATTACK

In the smart card SC_i of this scheme, there are conversion parameters $\{RG, K_T\}$ for RDM of biometric information. Because RDM is non-invertibilty, even if the smart card is lost, the adversary cannot get the original biometric information B_i. In addition, the SC_i includes parameters $\{eID_i, R_i, V_i, E_k(\cdot)/D_k(\cdot), H(\cdot)\}$. According to $eID_i = E_s(ID_i \| N_0)$, $R_i = Q_i \oplus MP_i$, $V_i? = H(ID_i \| Q_i)$, eID_i is preserved by a random number N_0 and the server's private key. From Section 4.2.2, it is impossible to get the value of Q_i, so even if the smart card is lost, the privacy of user will not be leaked.

6) INSIDER ATTACK

According to $MP_i = H(ID_i \| PW_i) \oplus r_i$, even if there is a malicious administrator inside the server who wants to steal user's information. Because of the existence of the random number r_i, the adversary cannot get the user's password from MP_i. And the original biometric information is converted into pseudo-identities. Therefore, this scheme can resist insider attack.

7) DENIAL OF SERVICE (DoS) ATTACK

When the user U_i sends a request to the server S, U_i is first authenticated by the smart card SC_i locally. If the user U_i is illegal, SC_i will terminate the procedure. A message can only be sent to the server S by a legitimate U_i. Therefore, our scheme can resist the denial of service attack.

8) RESIST IMPERSONATION ATTACK

In this scheme, the adversary wants to realize this attack only by sending valid information $\{eID_i, X, A_1, t_1, Tf'\}$ to the server S, then the adversary must get parameter Q_i. According to the section B. 2), it is very difficult for the adversary to steal Q_i. Therefore, this scheme can resist impersonation attack.

9) CLOGGING ATTACK

The adversary can try to launch a clogging attack by changing message $\{eID_i, X, A_1, t_1, Tf'\}$. The adversary obtains valid information by computing $A_1? = H(ID_i \| {Q'}_i \| X \| t_1)$ and $eID_i = E_s(ID_i \| N_0)$. According to the above analysis, it is very difficult for the adversary to get Q_i and eID_i. Therefore the adversary cannot send a large number of service requests to the server S continuously, and there is no network congestion. Even if the adversary gets the information sent by the user U_i, it cannot pass the authentication checks by $A_1? = H(ID_i \| {Q'}_i \| X \| t_1)$. S only accepts messages that match timestamp t_1. Otherwise, S will terminate the procedure. Therefore, this scheme can resist clogging attacks [37].

V. PERFORMANCE ANALYSIS

This section shows security analysis and performance analysis of the scheme in terms of security features, communication cost, computational cost and accuracy, and compares it with other existing related biometric authentication schemes.

A. ANALYSIS OF SECURITY FEATURES

Table 4 summaries the comparison of this scheme with other relevant ECC-based biometric authentication schemes in terms of security. From the analysis of various security aspects and attack levels, we can find that our scheme has higher security. Compared with the authentication scheme that uses a simple hash to preserve biometric information, our scheme uses RDM to generate non-invertible and revocable pseudo biometric template and uses the fuzzy commitment scheme to preserve the generated biometric template. Therefore, it can be concluded that the scheme has high security and can resist most of the existing attacks.

B. ANALYSIS OF COMPUTATIONAL COST

This section mainly compares the computational cost of this scheme with the mentioned above schemes. Table 5 describes the different symbols used in the analysis of computational cost. Table 6 shows the results of comparison between this scheme and other related schemes. Compares with reference [39] scheme, although our scheme increases the template conversion time of RDM, RDM is not only computationally simple and consumes a very short time, but also improves the privacy preservation of the biometric information in this scheme. The computation cost of our scheme is within an acceptable range for practical applications. In [43], they also used cancelable biometrics, but RP has complex multiplication calculations, and the computational cost is obviously high. In contrast, our solution has a significant advantage in terms of computational cost. As shown in Figure 6.

TABLE 4. Comparison of security features.

Schemes	SF_1	SF_2	SF_3	SF_4	SF_5	SF_6	SF_7	SF_8	SF_9	SF_{10}	SF_{11}	SF_{12}
Wazid [38]	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes
Banerjee [39]	yes	yes	yes	no	yes	yes	no	yes	yes	yes	yes	yes
Sharma [40]	yes	yes	yes	yes	yes	yes	yes	yes	no	yes	yes	no
Lu [41]	yes	yes	no	yes	yes	no	yes	yes	no	yes	no	yes
Chaudhry [42]	yes	yes	yes	yes	yes	yes	yes	no	no	yes	yes	yes
Our scheme	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes

SF_1: Mutual authentication, SF_2: Session key agreement, SF_3: User anonymity, SF_4: User impersonation attack, SF_5: server impersonation attack, SF_6: Man in the middle attack, SF_7: Replay attack, SF_8: Lost smart card attack, SF_9: Privacy-preserving biometric information SF_{10}: Privileged insider attack, SF_{11}: Untraceability, SF_{12}: Perfect forward secrecy

TABLE 5. The description of different notations.

Notation	Description
T_{EM}	ECC scalar multiplication
$T_{S/D}$	Symmetric encryption/decryption
T_H	One-way hash function
T_{RDM}	RDM generates pseudo-biometric template
T_{RP}	RP generate pseudo-biometric template

C. ANALYSIS OF COMMUNICATION COST

In this section, it is mainly to analyze and compare the communication costs of this scheme. Obviously, communication costs are low and there is no need to transmit too much information. The timestamp is 64 bits (8 bytes), the hash digest is 160 bits (20 bytes), the size of an elliptic curve point is 320 bits (40 bytes), the symmetric encryption algorithm is AES with 128 bits (16 bytes) packet length and the user's identity is 32 bits (4bytes), respectively.

In the registration phase, the first piece of information transmitted phase of this scheme is the $\{ID_i, MP_i\}$ that the user sends to the server. Its communication cost of $4 + 20 = 24$. In the Login authenticated and key agreement phase, the information in the second paragraph is $\{eID_i, X, A_1, t_1, Tf'\}$ that the user sends to the server, and the communication cost is $16 + 40 + 20 + 8 + 10 = 94$. The information transmitted for the third time is $\{C_2, A_2, t_2\}$, that incurs cost of $16 + 20 + 8 = 44$. The information transmitted for the fourth time is $\{A_3\}$, that incurs cost of 20. Table 7 compares the message exchange and communication cost of our scheme with other related schemes. As shown in Figure 7, this scheme has a significant advantage in terms of lower communication cost.

D. ANALYSIS OF THE ACCURACY

The metrics used in this section to evaluate the accuracy of identity authentication are FAR, FRR and ERR. The meaning of these ratios is explained as follows:

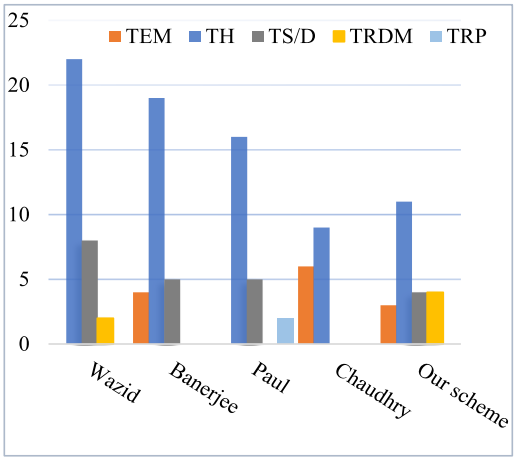


FIGURE 6. Analysis of computational cost.

False Acceptance Rate (FAR): This parameter is described from how many times authentication systems deny an imposter as a legitimate user and defined as the ratio of the number of False Acceptances to the number of authentication attempts:

$$FAR = \frac{FP}{TN + FP} \tag{9}$$

False Rejection Rate (FRR): This parameter is determined from how multiple times authentication systems allowed a legitimate user as an imposter and defined as the ratio of the number of False Rejections to the number of authentication attempts:

$$FRR = \frac{FN}{TP + FN} \tag{10}$$

Equal Error Rate(EER): This parameter shows that the value of FAR and FRR is equal, the less the equal error rate value and the better the performance of the scheme.

Where, False Positive (FP) is the number of imposter acceptance, True Negative (TN) is the number of imposter

TABLE 6. Analysis of computational cost.

Schemes	User	Server(S)	total
Wazid [38]	$2T_{RDM}+13T_H+2\ T_{S/D}$	$9\ T_H+6T_{S/D}$	$2T_{RDM}+22T_H+8T_{S/D}$
Banerjee [39]	$2T_{EM}+10T_H+2\ T_{S/D}$	$2T_{EM}+9T_H+3T_{S/D}$	$4T_{EM}+19T_H+5\ T_{S/D}$
Chaudhry[42]	$3T_{EM}+4T_H$	$3T_{EM}+4T_H$	$6T_{EM}+8T_H$
Paul [43]	$2T_{PR}+7T_H+T_{S/D}$	$9T_H+4T_{S/D}$	$2T_{PR}+16T_H+5T_{S/D}$
Our scheme	$2T_{RDM}+1T_{EM}+6T_H+T_{S/D}$	$2T_{EM}+5T_H+3T_{S/D}$	$2T_{RDM}+3T_{EM}+11T_H+4T_{S/D}$

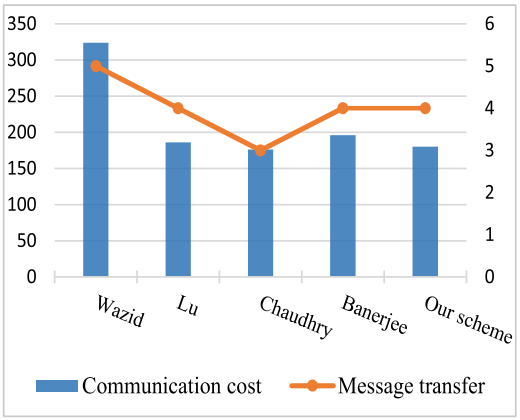


FIGURE 7. Random distance method to generate pseudo-biometric template.

TABLE 7. Analysis of communication cost.

Schemes	Message transfer	Communication cost
Wazid *et al*[38]	5	324bytes
Lu *et al*[41]	4	186bytes
Chaudhry *et al*[42]	3	176bytes
Banerjee *et al*[39]	4	196bytes
Our scheme	4	180bytes

TABLE 8. Comparison of performance between this scheme and other methods on CASIA-Face V5 database.

CASIA-Face V5	Best Testing		Worst Testing	
Methods	EER	FAR (FRR = 0)	EER	FAR (FRR = 0)
XOR	0.3	0.41	0.3	0.41
GraySalt	0.23	0.27	0.31	0.39
Our scheme	0.09	0.12	0.09	0.12

TABLE 9. Databases used for experimentation.

Modality	Database	Subjects
Fingerprint	FVC2006	300
Face	CASIA-Face V5	500
IRIS	IRIS(LWIR)	197

rejection, False Negative (FN) is the number of legitimate rejection and True Positive (TP) is the number of legitimate acceptance.

The first sample of each subject is compared with the second sample of the same subject to calculate FRR, and the first sample of each subject is compared with the first sample of all remaining subjects to calculate FAR. This paper uses two scenarios, the first is the best-test scenario, when each user is assigned a different random point, the distances d_1 and d_2 may tend to be the same. The worst-test scenario is the distance d_1 and d_2 between the random point (RP_j) and the feature point $\left(FP_j^1, FP_j^2\right)$ of two different users. Tables 8 shows that EER and FAR values of this scheme and other methods on CASIA-Face V5 database in both scenarios. It is evident that our scheme has the lowest EER and the best performance.

Table 9 describes the databases used in this paper. This paper conducts experiments. on three different databases on fingerprint, face and iris to analyze the performance of this scheme, and the method used in this scheme is compared with XOR and GraySalt. In GraySalt, a completely artificial pattern equal to the size of original image is added to the original image to get the cancelable biometric image. For XOR based salting, the original features are xored with random patterns followed by non-linear median filtering, desampling, and binarization to generate transformed templates. Figure 8 shows the worst-case comparison of ROC curves for experiments on three databases. The ROC curve plot is a function of the decision threshold, which plots the rate of the False Positive Rate on the x-axis against the True Positive Rate on the y-axis. The larger the area under the curve, the better the performance of the system. In figure 8, we find that the performance of our scheme implemented on three different databases is much better than the other two methods.

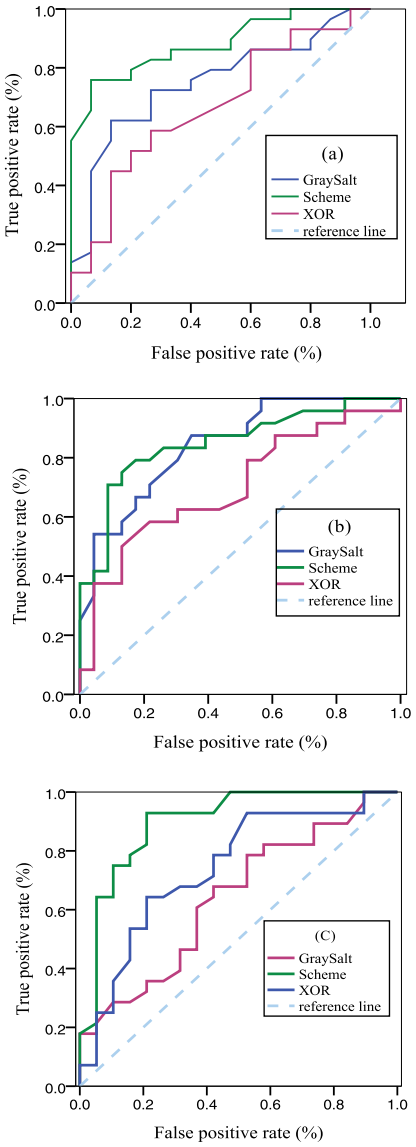


FIGURE 8. ROC curves in the worst-case scenario (a) FVC2006, (b) CASIA-Face V5, (c) IRIS(LWIR).

VI. CONCLUSION

This paper proposed a privacy-preserving biometric authenticate scheme based on ECC and cancelable biometric. A secure communication channel is established between the user and the server, and the elliptic curve cryptography is used to share the same session key protocol to achieve mutual authentication. This scheme showed the detailed process of the entire session key in detail, and employed a novel template transformation technique (RDM) to generate pseudo-biometric templates. This scheme used fuzzy commitment to preserve the generated pseudo-biometric template. The original biometric information does not appear during the authentication process and is adequately preserved. Further, the security of this scheme is analyzed compared with existing relevant schemes, and it is proved that the security of this scheme has been greatly improved and can resist all kinds of huge numerous attacks such as replay attacks, user anonymity and impersonation attacks. We performed a performance analysis of the solution in terms of communication cost, calculation cost and accuracy. Based on the difficulty of the elliptic curve discrete problem, well forward secrecy is realized. Under the same level of security, the key length of the elliptic curve cryptography is much smaller. RDM reduces the dimension of biometric characteristics by 50%, which greatly reduces the pressure of the entire program to transmit information, so the communication cost is lower. Meanwhile, we evaluated the accuracy of this scheme and the ROC curve shows that our scheme has higher accuracy in biometric authentication.

ACKNOWLEDGMENT

(Lei Wu and Lingzhen Meng contributed equally to this work.)

REFERENCES

[1] G. B. Marta, E. Maiorana, and J. Galbally, "Multi-biometric template protection based homomorphic evaluations," *Pattern Recgnition*, vol. 67, pp. 149–163, Jan. 2017.

[2] M. K. Morampudi, M. V. N. K. Prasad, and U. S. N. Raju, "Privacy-preserving iris authentication using fully homomorphic encryption," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 19215–19237, Jul. 2020.

[3] Y. Lin and J. H. Liang, "Research on secure identity authentication based on homomorphic encryption and biometric," *Netinfo Secur.*, vol. 18, no. 4, pp. 1–8, 2018.

[4] M. Yasuda, "Secure Hamming distance computation for biometrics using ideal-lattice and ring-LWE homomorphic encryption," *Inf. Secur. J. Global Perspective*, vol. 26, no. 2, pp. 85–103, Mar. 2017.

[5] E.-J. Yoon and K.-Y. Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," *J. Supercomput.*, vol. 63, no. 1, pp. 235–255, Jan. 2013.

[6] D. He and D. Wang, "Robust biometrics-based authentication scheme for multi-server environment," *IEEE Syst. J.*, vol. 9, no. 3, pp. 816–823, Feb. 2015.

[7] H. Yeh, T. Chen, K. Hu, and W. Shih, "Robust elliptic curve cryptography-based three factor user authentication providing privacy of biometric data," *IET Inf. Secur.*, vol. 7, no. 3, pp. 247–252, Sep. 2013.

[8] F. Wu, L. Xu, S. Kumari, and X. Li, "A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks," *Comput. Electr. Eng.*, vol. 45, pp. 274–285, Jul. 2015.

[9] S. S. Sahoo, S. Mohanty, and B. Majhi, "A secure three factor based authentication scheme for health care systems using IoT enabled devices," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 1, pp. 1419–1434, Jan. 2021.

[10] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems," *IEEE Syst. J.*, vol. 14, no. 1, pp. 39–50, Mar. 2020.

[11] J. J. Hathaliya, S. Tanwar, and R. Evans, "Securing electronic healthcare records: A mobile-based biometric authentication approach," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102528.

[12] S. Rane, Y. Wang, S. C. Draper, and P. Ishwar, "Secure biometrics: Concepts, authentication architectures, and challenges," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 51–64, Sep. 2013.

[13] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 503–512, Sep. 2007.

[14] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proc. IEEE Int. Symp. Inf. Theory*, Aug. 2002.

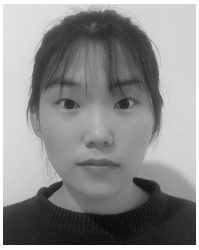
[15] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, Dec. 2007.

[16] S. Barman, H. P. H. Shum, S. Chattopadhyay, and D. Samanta, "A secure authentication protocol for multi-server-based E-healthcare using a fuzzy commitment scheme," *IEEE Access*, vol. 7, pp. 12557–12574, 2019.

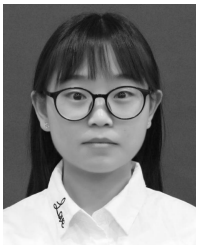
[17] C. Soutar, D. Roberge, A. Stoianov, and R. R. Gilroy, "Biometric encryption using image processing," *Proc. SPIE*, vol. 3314, pp. 178–189, Apr. 1998.
[18] V. Rajasekar, J. Premalatha, and K. Sathya, "Cancelable iris template for secure authentication based on random projection and double random phase encoding," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 2, pp. 747–762, Mar. 2021.
[19] Z. L. Li and L. J. Huang, "Security algorithm of face recognition based on binary pattern and random projection," in *Proc. IEEE Int. Conf. Cogn. Inform.*, Jul. 2010, pp. 733–738.
[20] M. Deshmukh and M. K. Balwant, "Generating cancelable palmprint templates using local binary pattern and random projection," in *Proc. 13th Int. Conf. Signal-Image Technol. Internet-Based Syst. (SITIS)*, vol. 13, Dec. 2017, pp. 203–209.
[21] P. Punithavathi and S. Geetha, "Dynamic sectored random projection for cancelable iris template," in *Proc. 9th Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, Beijing, China, Sep. 2016, pp. 7–9.
[22] D. Sadhya and B. Raman, "Generation of cancelable iris templates via randomized bit sampling," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2972–2986, Nov. 2019.
[23] J. Qiu, H. Li, and C. Zhao, "Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication," *Comput. Secur.*, vol. 82, pp. 1–14, May 2019.
[24] A. D. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. E. A. El-Samie, and N. F. Soliman, "Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications," *Entropy*, vol. 22, no. 12, p. 1361, Nov. 2020.
[25] H. Kaur and P. Khanna, "Random distance method for generating unimodal and multimodal cancelable biometric features," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 709–719, Mar. 2019.
[26] A. Stoianov, "Security of error correcting code for biometric encryption," in *Proc. 8th Int. Conf. Privacy, Secur. Trust*, Ottawa, ON, Canada, Aug. 2010, pp. 231–235.
[27] D. Chang, S. Garg, M. Ghosh, and M. Hasan, "BIOFUSE: A framework for multi-biometric fusion on biocryptosystem level," *Inf. Sci.*, vol. 546, pp. 481–511, Feb. 2021.
[28] P. Failla, Y. Sutcu, and M. Barni, "A privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics," in *Proc. 12th ACM Workshop on Multimedia and Security*, Roma, Italy, 2010, pp. 241–246.
[29] S. Barman, A. K. Das, D. Samanta, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Provably secure multi-server authentication protocol using fuzzy commitment," *IEEE Access*, vol. 6, pp. 38578–38594, 2018.
[30] H. U. Rehman, A. Ghani, S. A. Chaudhry, M. H. Alsharif, and N. Nabipour, "A secure and improved multi server authentication protocol using fuzzy commitment," *Multimedia Tools Appl.*, vol. 80, no. 11, pp. 16907–16931, Jul. 2020.
[31] S. Shamshad, K. Mahmood, S. Kumari, and M. K. Khan, "Comments on 'Insider attack protection: Lightweight password-based authentication techniques using ECC,'" *IEEE Syst. J.*, vol. 15, no. 1, pp. 877–880, Mar. 2021.
[32] L. Xiao, S. Xie, D. Han, W. Liang, J. Guo, and W.-K. Chou, "A lightweight authentication scheme for telecare medical information system," *Connection Sci.*, vol. 9, pp. 1–17, Mar. 2021.
[33] A. A. Khan, V. Kumar, M. Ahmad, S. Rana, and D. Mishra, "PALK: Password-based anonymous lightweight key agreement framework for smart grid," *Int. J. Electr. Power Energy Syst.*, vol. 121, Oct. 2020, Art. no. 106121.
[34] S. A. Chaudhry, "Correcting 'PALK: Password-based anonymous lightweight key agreement framework for smart grid,'" *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106529.
[35] Z. Ali and A. Ghani, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102502.
[36] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi, and M. Shafiq, "A provably secure and efficient authenticated key agreement scheme for energy Internet based vehicle-to-grid technology framework," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4425–4435, Jul./Aug. 2020.
[37] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107731.
[38] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and M. Conti, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
[39] S. Banerjee, C. Chunka, S. Sen, and R. S. Goswami, "An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards," *Wireless Pers. Commun.*, vol. 107, no. 1, pp. 243–270, Jul. 2019.
[40] G. Sharma and S. Kalra, "A lightweight multi-factor secure smart card based remote user authentication scheme for cloud-IoT applications," *J. Inf. Secur. Appl.*, vol. 42, pp. 95–106, Oct. 2018.
[41] Y. Lu, L. Li, H. Peng, and Y. Yang, "An enhanced biometric-based authentication scheme for telecare medicine information systems using elliptic curve cryptosystem," *J. Med. Syst.*, vol. 39, no. 3, pp. 1–8, Mar. 2015.
[42] S. A. Chaudhry, H. Naqvi, and M. K. Khan, "An enhanced lightweight anonymous biometric based authentication scheme for TMIS," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 5503–5524, Mar. 2018.
[43] P. P. Paul and M. Gavrilova, "Multimodal cancelable biometrics," in *Proc. IEEE 11th Int. Conf. Cognit. Informat. Cognit. Comput.*, Aug. 2012, pp. 43–49.

LEI WU was born in 1980. He received the Ph.D. degree in applied mathematics from Shandong University, China, in 2009. He is currently an Associate Professor with Shandong Normal University, China. His research interests include cryptology and cloud computing security.

LINGZHEN MENG was born in 1996. She received the B.S. degree from the Department of Computer Science and Technology, Qilu Normal University, Jinan, China, in 2019. She is currently pursuing the master's degree in information science and engineering with Shandong Normal University. Her research interest includes privacy-preserving in biometric authentication systems.



SHENGNAN ZHAO was born in 1995. She received the B.S. degree in computer technology and engineering from the Jining Medical College, China, in 2019. She is currently pursuing the master's degree in information and engineering with Shandong Normal University. Her research interests include privacy preservation in social networks and cloud computing security.



XIA WEI was born in 1996. She received the B.S. degree in computer science and technology from the Jiangxi Science and Technology Normal University, Nanchang, China, in 2019. She is currently pursuing the master's degree in information science and engineering with Shandong Normal University. Her research interest includes privacy preservation in location-based service.

HAO WANG received the Ph.D. degree in computer science from Shandong University, China, in 2012. He is currently an Associate Professor with Shandong Normal University. His primary research interests include public key cryptography, in particular, designing cryptographic primitives and provable security. His current research interests include attribute-based cryptography, security in cloud computing, and blockchain.