WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Interactive and Privacy-preserving for Online Biometric identity authentication for secure Environment

Mr.C.A.Kandasamy[1], Ms.M.Mahila[2], Ms.P.Mahalakshmi[3], Ms.B.Kokila[4], Ms.S.Kiruthika[5], Ms.S. Krishna priya [6]

[1] Assistant Professor, Department of MCA, K.S.R. College of Engineering, Tiruchengode, kandamca86@gmail.com

[2,3, 4, 5,6] Student, Department of MCA, K.S.R. College of Engineering, Tiruchengode,

cemcamahila027@gmail.com, maha.psivam@gmail.com, kokilab07@gmail.com , cemcakiruthika23@gmail.com, krishnapriyasithiyan@gmail.com

ABSTRACT :

Online Biometric identity authentication is the most important way of identity authentication for Secure Environment. More and more network services such as account login and online payment or UPI are using biometric authentication. In these scenarios, it is significant to protect efficient and the privacy of biometrics data. Such as the collection, transmission, storage and matching of biometrics data. Based on discrete Alogarithm problem and Bloom filter, this paper proposes a privacy-preserving online biometric authentication scheme. The correctness, security and computational complexity of the scheme are analyzed. Main algorithms of the scheme are implemented in python & AI to evaluate its performance. The experimental data shows that the scheme is more efficient than the existing online biometric authentication scheme.

Keywords-Privacy protection; Online biometric authentication; Discrete logarithm problem; Bloom filter

INTRODUCTION :

With the development of Internet technology, more and more online services have appeared. Privacy is a very impor- tant aspect of online services that users care about. In tradi- tional authentication methods, PIN codes, passwords or smart cards are commonly used. But users' information is at risk of being forgotten, stolen or lost. Biometric-based authentication technology relies on human biological characteristics, such as fingerprints, human face, iris and so on. In recent years, more and more attention have been focused on it. Compared with traditional authentication methods, users don't need to worry about the information loss or forgetting. Recently, many corporates have applied biometric-based authentication to their systems. And many biometric-based authentication schemes have been proposed.

Jin et al. proposed the Biohashing scheme which in 2004 [1]. In this scheme, the eigenvector of user's fingerprints is iterated with the orthogonal matrix generated by token to

This work was supported by the National Natural Science Foundation of China (Nos. 61572521, U1636114, 61772550), National Key Research and Development Plan (2017YFB0802000), UIF TDIPPM QSPjFDU (8):201906),

and Open Research Fund of State Key Laboratory of Cryptology.

Yiliang Han is corresponding author.

generate the BioCode after threshold quantization. Matching results are obtained by calculating Hamming distance between BioCodes. After the Biohashing scheme based on fingerprints, the Biohashing schemes based on human face [2], iris [3] [4] were also proposed. In 2007, Juels et al. proposed the Fuzzy Vault scheme based on fingerprints [5], which solved the contradiction between the accuracy of cryptosystem and the fuzziness of biological features. The Fuzzy Vault scheme based on iris [6], human face [7] were also proposed. But the security of the schemes above is mainly relied on the privacy of template data. This method can only be applied to local authentication and trusted two-party authentication of servers, and cannot meet the requirements of today's complex biometric authentication system.

Searchable encryption is very suitable for privacy protection of biometric authentication system in the case of template data outsourcing or server untrustworthy [8] [9] [10] [11]. Considering the characteristics of biometric authentication, Mohammad et al. proposed a privacy-preserving biometric authentication scheme CloudID based on Searchable encryp- tion [12]. But it can't provide complete privacy protection for biometric authentication system. Based on homomor- phic cryptography, some authentication schemes were pro- posed [13] [14] [15]. FingerCode scheme based on Paillier algorithm achieves privacy protection of fingerprint data in two-party interaction scenarios [16]. In 2018, Zhu et al. proposed the e-Finga scheme over outsourced data [17]. In this scheme, the user's fingerprint information registered in trust authority can be outsourced to different servers with user's authorization. And online servers can provide secure, accurate and efficient authentication service without the leak- age of fingerprint information. but this scheme still remains some problem. The users' information is directly submitted to the trusted authority. Even if *TA* is credible, user's biometric information is still not safe enough. Since the scheme is based on bilinear pairing, the scheme is still inefficient.

In this paper, we propose an efficient online privacy-

preserving biometric authentication scheme(OL-PPBA). In our scheme, the online authentication servers are considered honest-but-curious, and the trusted authority is credible, but should not get users' biometric information directly. We adopt the method of collecting the biometric information like the FingerCode scheme. Users' biometric information can be ex- tracted to a vector. We use the Euclidean distance to calculate whether the information submitted by the users matches.

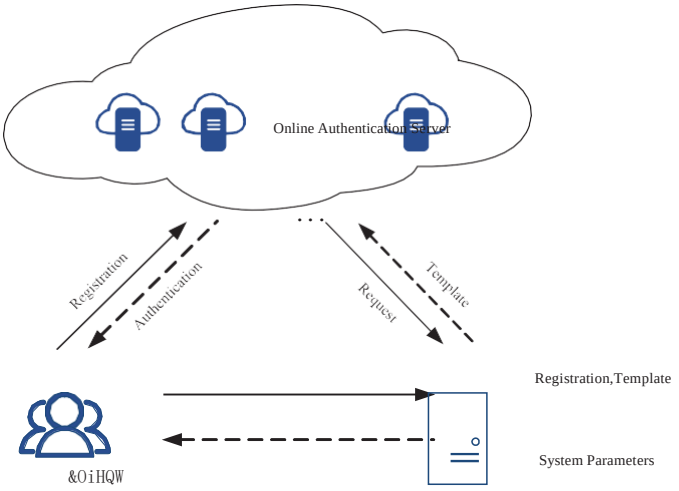


Figure 1. System Model.

SYSTEM MODEL AND SECURITY REQUIREMENTS

In this section, we formalize the system model and security requirements.

System Model

In an online privacy-preserving biometric authentication system, there are three parts involved : trusted authority(*TA*), online authentication servers(*OA*) and users, as shown in Fig. 1.

- *TA* is a trusted authority (such as government). *TA* boot- straps the system initialization by generating and sending system parameters to the registered online authentication servers (*OA*) and the users. *TA* is responsible for storage of the encrypted biometric template collected from usersand generating keys for users and *OA*.
- *OA* is responsible for online authentication service. *OA* should register in *TA* in advance. Then *OA* requests users' related templates. *OA* can provide online authen- tication service by matching the template and the usersubmitted.

Security Requirements

In our scheme, we considered the trusted authority is credible, and *TA* should hold users' encrypted biometric information. *OA* is considered honest but curious. The online authentication servers may analyze the encrypted biometric template received from *TA* to obtain the original biometric data. Besides, a *OA* may impersonate another *OA* to offer service, or conspire with other *OA*. There may also be an active adversary who may eavesdrop on all communication links to get the encrypted data, and analyze the encrypted data to obtain the plaintext. Therefore, the following securityrequirements should be satisfied.

- Privacy: The proposed scheme should ensure users' orig- inal biometric information cannot be recovered from the encrypted template, even if the adversary can get all communication data. Moreover, if two online servers try to collude to obtain user information, or an online server try to pretend to be another *OA* to provide services after getting some leaked encrypted template information, the proposed scheme can prevent their behavior.
- Confidentiality: In the real application scenario, Mali- cious users are intent to pretend another user to getting the online authentication service. The proposed scheme should ensure that nobody except the valid user couldforge a valid query.
- Unforgeability: In the system model, the trusted authority and the online server can obtain users' encrypted template legally. And the adversary can eavesdrop all communi- cation to obtain the encrypted template. The proposed scheme should protect the users' original biometric in- formation in all procedure. Even in the matching phase, nobody can get more information except the matching result. And the result should be encrypted before sendingto users.

PRELIMINARIES

In this section, we review the difficulty assumption, Eu- clidean distance and bloom filter.

A. Difficulty Assumption

- Discrete logarithm Problem(DLP):

  Let p, q be two primes such that q (p 1), and let g be the generator of Z_p^* with order q, given g, g^a Z_p^* for unknown a Z_q^* ∈ ,the DL problem in Z_p^* is to find a.

  The advantage of any probabilistic polynomial time al- ∈ gorithm in solving the DL problem in Z_p^* is defined as A

  $$AdvDL\ A = Pr[A(g, ga) = a|a\ ?\ Z^*\ q\ ]$$

- Users should register in *TA* first. Users choose the *OA* server, generate related template, and send the template to *OA*. When users want use the online authentication service, they can generate the request and send it to *OA*. In the paper [17], the encrypted templates of users' biometric information are generated by the trustedauthority *TA*. This is unsafe even *TA* is credible.

The DL Assumption is that, for any probabilistic poly-

nomial time algorithm , the advantage ^{DL} is neg-ligible. A A Adv

- Computational Diffie-Hellman Problem (CDHP):

  Given $g, g^a, g^b \in Z_p^*$ for unknown $a, b \in Z_q^*$,the CDH problem in Z_p^* is to compute g^{ab}.

359

The advantage of any probabilistic polynomial time al- gorithm in solving the CDH problem in Z_p^* is defined as

A

AdvCDH A = P r[A(g, ga, gb) = gab|a, b ∈ Z∗ q]

The CDH Assumption is that, for any probabilistic poly-

nomial time algorithm A, the advantage Adv^{CDH} is

B. Euclidean Distance

In addition, *TA* generates public key PK_{TA} and privatekey SK_{TA} for itself, and holds a list of online authenticationservers $List_{OA}$.

For biometrics representation, we adopt a bank of filters to capture biometrics' image (BioCode). A BioCode is consists of a n-dimensional feature vector, each element of which is an 8-bit integer. Given two BioCodes $x = (x_1, x_2, ..., x_n)$and $y = (y_1, y_2, ..., y_n)$, it is efficient to match them by computing Euclidean Distance and comparing with a threshold. And $d(x, y)$ can be compute as follows:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

B. Template Generation

All users should register in *T A*. Users first get their public key, private key just like *OA* gets its keys. User also gets the list of online servers list $List_{OA}$ from *T A*. Take a user with identity ID_u as an example. User ID_u gets his/her public key $PK_u =< X_u, Y_u >$ and private key $SK =< x_u, y_u >$, picks a random parameter combined with his/her terminal device d_u. User can generate his/her BioCode from his/her terminal device, which is generated as $m = (m_1, m_2, \ldots, m_n)$. After

)

1)computes $\varphi_i = m_i + H_1(ID_{OA} \| ID_u \| d_u)$.

If the Euclidean Distance between the two BioCodes is below

S efficiently. It can be simply described as follows:

$$BF_S.Test(X) \rightarrow \begin{cases} TRUE, if\ X \in S \\ FALSE, if\ X \notin S \end{cases}$$

2)chooses a random number r Z_q^*, and computes R = g^r.

3)computes $h = H_1(ID_u \ T_u \ TS_1 \ R)$, TS_1 representsis the time stamp.

4)computes $Sig_{Tu} = r(x_u + y_u + h)^{-}$.

I. PROPOSED OL-PPBA SCHEME

In this section, we propose our OL-PPBA scheme, an online privacy-preserving biometric authentication scheme, which mainly consists of 4 parts: System Initialization, Template Generation, Authentication Query Generation, and TemplateMatch.

A. System Initialization

In this phase, *TA* first chooses a security parameter λ, and outputs a set of parameters $< p, q, Z_p^*, Z_q^*, g, s, P_{pub} >$. In this set, the parameters fulfill that q (p 1), g is a generator of Z_p^* with order q, $P_{pub} = g^s$ (*mod* p). Then TA chooses 2 secure cryptographic hash function H_1() and H_2(), where H_1 : $0,1^*$ Z_q^*, H_2 : $0,1^*$ $0,1^L$. L represents the length of matching result. Finally, *TA* keeps

s as the master key, and publishes the system parameters $< p, q, Z_p^*, Z_q^*, g, P_{pub}, H_1, H_2 >$.

TA also creates a Bloom filter based on the set $DS = D_1, D_2, \ldots, D_{\Delta 2}$, where $D_i = g^i$ and Δ_d is the threshold of matching two BioCode.

5)send $< TS_1, ID_u, T_u, R, h >$ to *TA*, where $< R, h >$ is regarded as the signature of T_u.

Once recieves $< TS_1, ID_u, T_u, R, h, Sig_{Tu} >$ from user ID_u, *TA* executes as follows:

1)first verifies the time stamp TS_1.

- 2)compute $R' = (X_u Y_u P^{H_1(ID_u \| X_u \| Y_u)} g^h)^{Sig_{Tu}}$.
- 3)verifies $R? = R'$ and $h? = H_1(ID_u \| T_u \| TS_1 \| R')$.
- 4)if the time stamp and Sig_{Tu} are accepted, then saves T_u as user ID_u's template in database.

In order to simplify the description, we use *Sign*() to represents the signature process that user executes(3-6) above and use *V erify*() to represents the Verification process that *TA* executes(2-3) above.

C. Template Authorization

If the user ID_u wants to use the online biometric authentica-tion service from an online authentication server, he/she should register in the *OA* first. Then *OA* requests the template from *TA*. The Fig. 2 shows the process of template authorization phase.

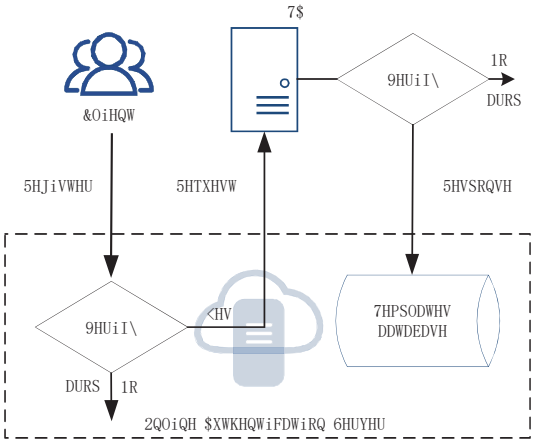


Figure 2. Template Authorization.

ensure the biometric information safe. With this method, user'sinformation is safer when user is in an untrusted network.

Besides, note that q_i $= (X_u Y_u h_1 pub$ $)^{2\vartheta_i}$, we can compute $q_i = (X_u Y_u P^{1})$

in advance to save computation when generating the query.

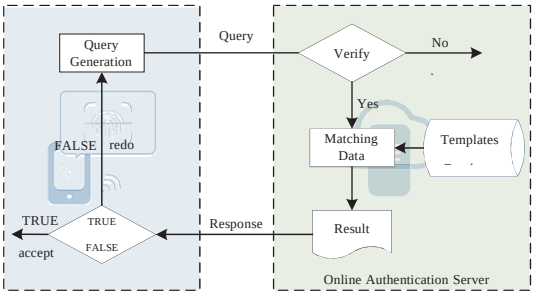


Figure 3. Query and Response.

The specific process is as follows:

1) User registers in *OA*. User ID_u generates the signature $Sig_u = Sign_{SKu}(TS_2)$, and sends $< TS_2, ID_u, Sig_u >$ to *OA*.

2) *OA* requests to *T A*. *OA* first checks whether the time stamp and the signature are valid. If both of them are valid, *OA* generates the signature $Sig_{OA} = Sign_{SKOA}(TS_3)$, and sends

$< TS_2, ID_u, Sig_u, TS_3, ID_{OA}, Sig_{OA} >$ to TA.

3) TA response to *OA*. TA first checks *OA*'s and user's Ver-

ification information. If both of them are valid, TA generatesthe signature $Sig_{TA} = Sign_{SKTA}(TS_4 \| T_u)$. Then, TA sends

E. Template Match

The Fig. 3 shows the process of authentication query gener- ation and Template Match phase. After receiving user's query request $< TS_5, ID_u, Q_u, Sig_q >$, *OA* verifies the informationuser submitted as follows:

- 1)*OA* first checks whether the time stamp and signatureare valid.
- 2)If both of them are valid. *OA* gets the related $< ID_u, T_u >$ pairs from the database.

$< TS_4 \| ID_u \| T_u \| Sig_{TA} >$ to *OA*.

Storage of Template. *OA* checks the time stamp and the signature. If both of them hold, *OA* stores $< ID_u, T_u >$ in database.

The *Result* should not use 0 or 1 to represent $TRUE$ and

$FALSE$, which may lower the security of the scheme.

a) Correctness::

$$Q_u = \begin{cases} q_1 = (X_u Y_u P_{pub}^{h_1^{(u)}})^{2\theta_1} \\ q_2 = (X_u Y_u P_{pub}^{h_1^{(u)}})^{2\theta_2} \\ \vdots \\ q_n = (X_u Y_u P_{pub}^{h_1^{(u)}})^{2\theta_n} \\ q_u = g^{\theta_1^2+\theta_2^2+\ldots+\theta_n^2-\Delta_d^2} \end{cases}$$

C. The Privacy of Users' Original Biometric Data

In the template generation phase and authentication query generation phase, users executes $\varphi_i = m_i + H_1(ID_{OA} \| ID_u \| X_u)$ and $\theta_i = m_i' + H_1(ID_{OA} \| ID_u \| X_u)$. From our analysis above, we can see that it is difficult to recover φ and θ. So the privacy of users' original biometric data can be ensured. Besides, if one user wants to revoke or replace the template he/she generates, he/she can just ask for cancelingfrom *TA* and *OA* or changing another public and private key pair.

Moreover, our scheme can guarantee the original is only known by owners, no one can recover the original data from the encrypted templates, and users generate the querywithout using their private key except an secret parameter

The Euclidean distance between the two submitted BioCodeiscan be revoked/replaced by users to protect their biometricinformation. The adversary can not acquire users' private information from eavesdropping communication even in an

untrustworthy network.

the matching data M_d must be an element of the set *DS*.

SECURITY ANALYSIS

In this section, we analyze the security properties of the OL-PPBA scheme. According to the security requirements in Section 2, this paper makes a concrete analysis from threeaspects: template confidentiality, unforgeability, privacy of users' original biometric data.

A. Template Confidentiality

In the security model, the adversary may eavesdrop on all communication to get the encrypted template, and the *OA* could get the encrypted template from TA and the request from users. In the template generation phase, $t_i = \varphi_i(x_u + y_u)^{-1}$, if the adversary wants to recover the BioCode vector $m = (m_1, m_2, \ldots, m_n)$, he/she should recover the vector φ from T_u first. According to the paper [18] [19] [20] [21], the difficulty of recovering the vector φ can be reduced to solve the discrete logarithm problem(DL). Even *TA* can not recover the vector φ without knowing user's private key, either. authentication query generating phase, $q = (X\ Y\ P^h)^{2\varphi}$

From the analysis above, we can conclude that the OL-PPBA scheme is secure and privacy-preserving.

PERFORMANCE EVALUATION

In this section, we evaluate the performance of the OL- PPBA scheme in terms of the computation and communication costs. And we select the e-Finga scheme as comparison. Main algorithms of OL-PPBA and e-Finga scheme are implemented in python to evaluate the computational performance. The OL- PPBA scheme is based on gmpy2. And the e-Finga scheme is based on pypbc.

Computation Complexity

Compared with the e-Finga scheme, the OL-PPBA scheme can provide more efficient online service for biometric authen- tication. Denote the computational costs of an exponentiation operation, a multiplication operation, and a pairing opera- tion by C_e, C_m, C_p, respectively. The computation costs of Template Generation, Authentication Query Generation and Template Match are calculated as shown in Table I. In order to simplify the description, the costs of signature and encryption for encrypted template is not calculated.

if the adversary wants to recover the BioCode vector m, he/she should recover the vector ϑ first. The difficulty of getting the vector ϑ can be reduced to solve the computational diffie-hellman problem

Algorithm	OL-PPBA	e-Finga
Template Generation	$2Ce + 2nCm$	$(2n+1)Ce + 2nCm$
Query Generation	$(n+1)Ce + nCm$	$(n+1)Ce + nCm$
Template Match	$(n+1)Ce + nCm$	$nCp + Ce + nCm$

TABLE I

COMPARISON OF COMPUTATION COMPLEXITY

can get $g^{\vartheta^2+\vartheta^2+\ldots+\vartheta^2-\Delta^2}$, but can't recover the Euclidean distance result without solving the DL problem. Besides, after getting the result, the encrypted result sent to the user is secure because the difficulty of recovering *Result* can be reduced to solve the CDH problem [21].

Template Unforgeability

In the security model, the adversary can get all commu- nication data from eavesdropping. The is curious about forging the query request. The difficulty adversary of forging a valid message comes down to recover the secret key x_u first. But as seen above, this is equal to solve the DL problem.

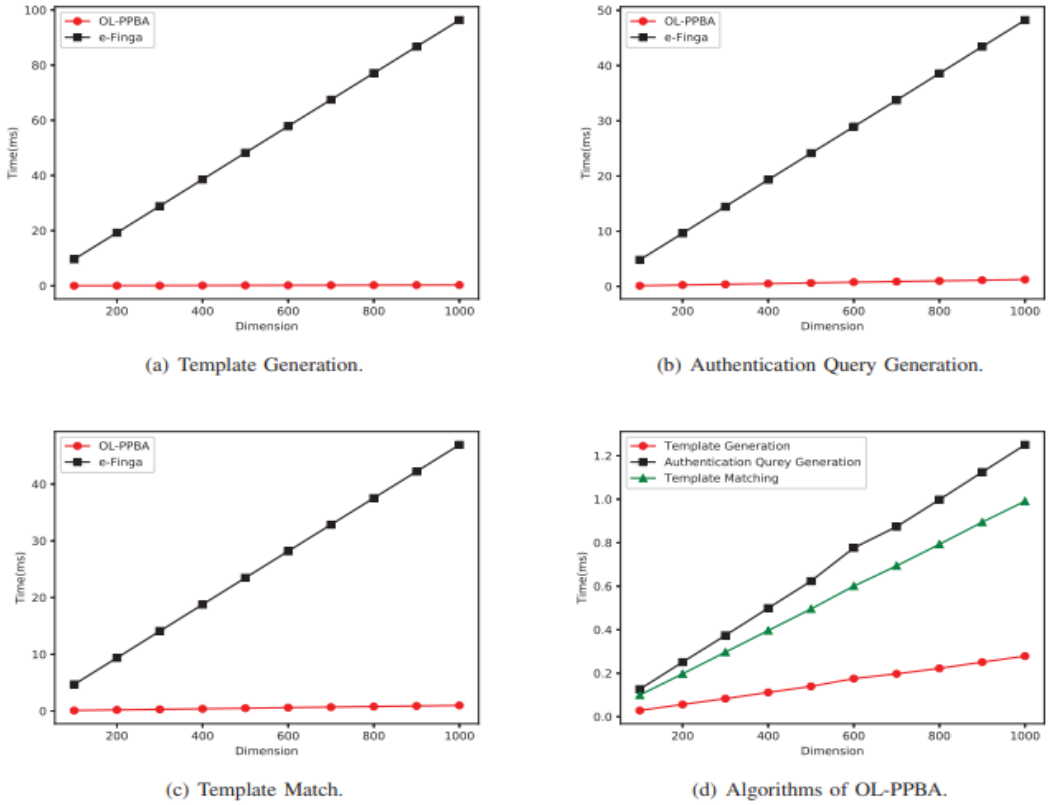
In the system model, the trusted authority and the online server can obtain users' encrypted template legally. And the adversary can eavesdrop all communi- cation to obtain the encrypted template. The proposed scheme should protect the users' original biometric in- formation in all procedure. Even in the matching phase, nobody can get more information except the matching result. And the result should be encrypted before sendingto users.

we propose our OL-PPBA scheme, an online privacy-preserving biometric authentication scheme, which mainly consists of 4 parts: System Initialization, Template Generation, Authentication Query Generation, and TemplateMatch.
In the real application scenario, Mali- cious users are intent to pretend another user to getting the online authentication service. The proposed scheme should ensure that nobody except the valid user couldforge a valid query.

In the system model, the trusted authority and the online server can obtain users' encrypted template legally. And the adversary can eavesdrop all communi- cation to obtain the encrypted template. The proposed scheme should protect the users' original biometric in- formation in all procedure. Even in the matching phase, nobody can get more information except the matching result. And the result should be encrypted before sendingto users.

In this scheme, the user's fingerprint information registered in trust authority can be outsourced to different servers with user's authorization. And online servers can provide secure, accurate and efficient authentication service without the leak- age of fingerprint information. but this scheme still remains some problem. The users' information is directly submitted to the trusted authority. Even if *TA* is credible, user's biometric information is still not safe enough. Since the scheme is based on bilinear pairing, the scheme is still inefficient.

For biometrics representation, we adopt a bank of filters to capture biometrics' image (BioCode). A BioCode is consists of a n-dimensional feature vector, each element of which is
an 8-bit integer. Given two BioCodes $x = (x_1, x_2, ..., x_n)$and $y = (y_1, y_2, ..., y_n)$, it is efficient to match them by computing Euclidean Distance and comparing with a threshold



(a) Template Generation. (b) Authentication Query Generation.

(c) Template Match. (d) Algorithms of OL-PPBA.

Figure 4. Comparison with the e-Finga scheme.

communication costs of the query and response phase asshown in table II.

TABLE II
COMPARISON OF COMMUNICATION COSTS

Procedure	OL-PPBA	e-Finga
Query	$(n+1)\|Z_p^*\|$	$n\|Z_p^*\| + \|G_T\|$
Response	L_{Result}	L_{Result}

C. Experimental Evaluation

The main algorithms of both scheme: System Initialization, Template Generation, Authentication Query Generation and Template Match are implemented. In both scheme, the per- formance is mainly determined by the computational com- plexity which is analyzed above(table I). With the increase of BioCode's dimension, the computational complexity of the schemes increases linearly. Then we select the dimension of BioCode from 100 to 1000 (with 100 interval). The test is executed on a computer with Pentium G2020 2.90 GHz, 4GB RAM. We only test 10 times per dimension because of thepoor performance of the computer. The result is shown in the Fig. 4.

From the Fig. 4, we can find that the computational costsof Template Generation, Authentication Query Generation, and Template Match in OL-PPBA scheme are too much less than that in e-Finga. It is well known that the exponential opera- tions require more computation than multiplication operations. Figure(d) shows the computational cost of the algorithms in OL-PPBA scheme. As we analyzed in Table I, Authentication Query Generation takes the longest running time, TemplateMatch take the second place and Template Generation the least.

From the analysis above, we can conclude that the OL- PPBA scheme has better performance than the e-Finga scheme.

CONCLUSION :

In this paper, we have proposed a new online biometric authentication scheme named OL-PPBA. The scheme can protect the privacy of users' biometric information and effi- ciently achieve online authentication. Nobody except user him- self/herself could get the original biometric information. Users could generate their query request with their public parameters on their own device in an untrustworthy network. In particular, *OA* can get the matching result without decryting. We have analyzed the security of the scheme. The confidentiality and unforgeability of the encrypted template could be reduced to solve the DL problem and CDH problem. And the performance

REFERENCES :

1. T. C. Meetei and S. A. Begum, "A variant of cancelable iris biometric based on biohashing," in *2016 International Conference on Signal and Information Processing (IConSIP)*, Oct 2016, pp. 1–5.

   A. Juels and M. Sudan, "A fuzzy vault scheme," *Designs, Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, Feb 2006.

A. Deshpande and P. P. Patavardhan, "Feature extraction and fuzzy- based feature selection method for long range captured iris images," in *Networking Communication and Data Knowledge Engineering*, G. M. Perez, K. K. Mishra, S. Tiwari, and M. C. Trivedi, Eds. Singapore: Springer Singapore, 2018, pp. 137–144.

2. H. G. Hong, W. O. Lee, Y. G. Kim, K. W. Kim, D. T. Nguyen, and K. R. Park, "Fuzzy system-based face detection robust to in-plane rotation based on symmetrical characteristics of a face," *Symmetry*, vol. 8, no. 8,2016.

3. Dawn Xiaoding Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000*, May 2000, pp. 44–55.

4. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *2010 Proceedings IEEE INFOCOM*, March 2010, pp. 1–5.

5. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,
6. J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryp- tion revisited: Consistency properties, relation to anonymous ibe, and extensions," in *Advances in Cryptology – CRYPTO 2005*, V. Shoup, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 205–222.

7. [8] Mr.C.A.Kandasamy, Karthickraja S "An Improved Data Hiding Method Using LZW Codes" International Journal Of
8. Multidisciplinary Research In Science, Engineering and Technology (IJMRSET), Volume 6, Issue 2, February 2023.

9. [9] C.A.Kandasamy , S.Yamini "Energy-Efficient Protocol for Wireless SensorNetworks" , Journal of Computer Applications (JCA) , ISSN: 0974-1925, Volume V, Issue 2, 2012