2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC) August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

Encrypted Fingerprint Authentication at Untrusted Servers

Motahareh Taheri
Electrical and Computer Engineering Department
Semnan University ,Semnan, Iran
Email: tahery_motahareh@yahoo.com

***Abstract*—This paper presents effective encrypted fingerprint authentication based on outsourced correlation filter computation. The privacy of fingerprint data raises important concerns at untrusted servers. In this work, we propose a framework for privacy preserving fingerprint authentication in untrusted server with outsourcing computation. The privacy of fingerprint authentication is preserved by three state. Firstly, all training images are encrypted. Secondly, all correlation filter computation and verification stage is performed over encrypted fingerprint images in server side. Thirdly, Privacy of the fingerprint authentication result is preserved by sending it to the client. We prove that our scheme is secure in untrusted server and has high accuracy. We show evaluations of our method on a standard fingerprint database FVC2002 to demonstrate its reliability.**

***Index Terms*—Fingerprint Authentication, Untrusted Server, Privacy Preserving.**

1. Introduction

Fingerprint techniques have advanced over the past years to a reliable means of authentication, which have been deployed in various application domains. The widespread use of fingerprint authentication systems, however, it will bring privacy risks because biometric information can be collected and misused to profile and track against their will. These issues raise the desire to construct privacy-preserving fingerprint authentication systems [1].

Cloud computing is the delivery of computing services over the Internet [5]. It has attractive features such as unlimited storage, high processing capabilities, and low cost. These properties create a new computing model and motivate clients to outsource their computation to cloud [9]. However, clients have no control over outsourced data and will not realize what is being derived from their data. So, security and privacy of sensitive data being handled by the cloud become an important issue. The problem of privacy–preserving fingerprint authentication has been studied for decades and numerous techniques have been proposed [2], [6].

In this paper, privacy of input data, verification model, and verified output are preserved. Correlation filters are generated from encrypted training images in the server side. Outsourcing correlation filter computation to a cloud server reduces computation cost of the client. To protect the output, encrypted verified results are sent back to client for decryption and comparison with a predefined threshold for verification.

The remainder of this paper is organized as follows. Section 2 explains background studies to designing the proposed method. Section 3 gives the details of the proposed method step by step. Experimental results on fingerprint database is given in section 4 and finally section 5 draws the conclusions.

2. Background Study

Encrypted fingerprint authentication at untrusted server is presented in this paper. For privacy preserving, all computation including generation CFs, cross- correlation , Peak to sidelobe ratio (PSR) measurement are performed in encrypted domain. To do this, linear and nonlinear operations should be transformed to the encrypted domain by additively homomorphic encryption properties and secure algorithm.

2.1. Correlation Filter

Correlation filters have ability to handle some recognition tasks, good speed and scaling. One of the important class of correlation filters is the use of biometric recognition such as fingerprint images for person verification. CF has a good mathematical foundation with low computational time. It has a greater robustness and higher accuracy compared to traditional appearance based methods.

Unconstrained minimum average correlation energy filter (UMACE) is made of linear combination of training samples. The peak value in UMACE filter is free to increase according to the input data by maximizing the square of the average magnitude of the peak. Response of correlation filter to Fourier transformed of i^{th} image $X_i(i = 1, ..., K)$ is represented by $g_i = X_i^* H$, where diagonal matrix X_i contains Fourier transformed of i^{th} image and H represents the correlation filter. Energy of the i^{th} correlation output is $E_i = \frac{1}{d} g_i^\dagger g_i$, where $d, (d = d_1 \times d_2)$, is the dimension of g_i and $\frac{1}{d}$ is used for normalization. Since all $E_i\{i = 1, \ldots, K\}$ cannot be simultaneously minimized, the average correlation energy (ACE) is minimized instead. The ACE can be expressed as follows.

978-1-5386-7582-3/18/§31.00

$$
\begin{aligned}
ACE &= (\frac{1}{K \times d}) \sum_{i=1}^{K} \sum_{u=1}^{d1} \sum_{v=1}^{d2} |H_i(u,v)|^2 |X_i(u,v)|^2 \\
&= (\frac{1}{K \times d}) \sum_{i=1}^{K} (H^\dagger X_i)(X_i^\dagger H) \\
&= H^\dagger [(\frac{1}{K \times d}) \sum_{i=1}^{K} X_i X_i^\dagger] H \\
&= H^\dagger D H \qquad (1)
\end{aligned}
$$

Where † shows the transpose. Diagonal matrix $D_i = X_i X_i^\dagger$ contains the power spectrum of i^{th} image, and $D = (\frac{1}{K}) \sum_{i=1}^{K} D_i$ .Diagonal matrix D contains the average power spectral density of the training images. The average peak intensity can be expressed as:

$$|H^\dagger m|^2 = H^\dagger m m^\dagger H \qquad (2)$$

If we consider $m = (\frac{1}{K \times d}) \sum_{i=1}^{K} X_i$ as the average of training images, CF maximizes $|H^\dagger m|^2$ and minimizing $H^\dagger D H$, hence, the objective function is given by

$$J(H) = (H^\dagger m m^\dagger H)/(H^\dagger D H) \qquad (3)$$

This leads to the closed-form solution for CF H.

$$H = D^{-1} m \qquad (4)$$

Computation of H is trivial as D is a diagonal matrix constructed by averaging the power spectra of training fingerprint images.

2.2. Paillier Cryptosystem

The Paillier cryptosystem is an additively homomorphic public-key encryption scheme. By homomorphic encryption, server can perform some computations on encrypted data while user's privacy are preserved [7].

The operations of the Paillier cryptosystem can briefly be described in three parts:

1) **Key Generation:** Two large prime numbers *p* and *q* randomly and independently are chosen, such that greatest common divisors (gcd) between them is one. We also select $N = pq$ and $gcd(L(g^\lambda \bmod N^2), N) = 1$, where λ that is the private key, defined as $\lambda = lcm(p-1, q-1)$. The pair of *N* and *g* defines the public keys.
2) **Encryption:** The ciphertext (corresponding to m) $\in Z_{N^2}$ is derived as:

$$c = E(m,r) = g^m r^N \bmod N^2 \qquad (5)$$

Where $r \in Z_N^*$ is the uniformly chosen key and is not fixed.
3) **Decryption:** For decrypting the ciphertext *c*, the private key λ is used and the plaintext *m* is obtained as:

$$m = D(c, \lambda) = \frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N \qquad (6)$$

where $L(u) = \frac{u-1}{N}$.

Because of these three properties, the Paillier cryptosystem is said to be homomorphically additive:

After decrypting the Eq. 7 and Eq. 8, $m_1 + m_2$ can be get. Means, the Paillier cryptosystem provides plaintext addition.

$$
\begin{aligned}
c_1 \times c_2 &= E(m_1, r_1) \times E(m_2, r_2) \\
&= g^{(m_1+m_2)} (r_1 r_2)^N \bmod N^2. \qquad (7) \\
c_1 \times g^{m_2} &= E(m_1, r_1) \times g^{m_2} \\
&= g^{(m_1+m_2)} (r_1)^N \bmod N^2 \qquad (8)
\end{aligned}
$$

The Paillier cryptosystem provides plaintext multiplication.

$$D([E(m_1, r_1)]^{m_2} \ mod \ N^2) = (m_1 \times m_2) \bmod N. \qquad (9)$$

2.3. SecureOperation

Multiplication algorithm: Multiplication can be executed without revealing any information. Suppose that c_1 and c_2 are two numbers in ciphertext domain, where $c_1 = E(m_1)$ and $c_2 = E(m_2)$ in which E(.) denotes Paillier cryptosystem. We try to obtain a number c_3 in ciphertext domain, which satisfy $D(c_3) = m_1 \times m_2$. Where D(.) denotes Paillier decryption.

Division algorithm: For dividing encrypted data in the semi-honest mode, we assume that the divisor is known for client and server. c_1 and c_2 are two numbers in ciphertext domain, where $c_1 = E(m_1)$, $c_2 = E(m_2)$. We try to obtain a number c_3 in encrypted domain, in which $D(c_3) = (\frac{m_1}{m_2})$.

Fast Fourier Transform (Secure-FFT): Discrete Fourier transform (DFT) can be performed in the encrypted domain, by using the homomorphic properties. It is called as secure-FFT in proposed method [10]. The DFT and inverse DFT of a one dimensional real value signal $x(m)$ is defined as:

$$
\begin{aligned}
X(k) &= \sum_{m=0}^{M-1} x(m) W^{mk}, \quad k = 0, 1, 2, 3, ..., M-1 \\
x(m) &= \frac{1}{M} \sum_{k=0}^{M-1} X(k) W^{-mk}, \quad m = 0, 1, 2, 3, ..., M-1
\end{aligned} \qquad (10)
$$

Where $W = e^{-j2\pi/M}$ and x(m) is a finite duration sequence with length M. In order to process W^{mk} in the encrypted domain, it must be approximated by suitable integers as:

$$
\begin{aligned}
C(u) &= \lceil Q_2 W^u \rfloor = \lceil Q_2 (W_R + j W_I) \rfloor \\
&= \lceil Q_2 cos(2\pi u/M) \rfloor + j \lceil Q_2 sin(2\pi u/M) \rfloor = C_R + j C_I
\end{aligned} \qquad (11)
$$

Where $\lceil . \rfloor$ is the rounding function and Q_2 is a suitable DFT coefficient scaling factor. Based on the above defini-

tion, the integer approximation of the DFT and $IDFT$ are defined as:

$$\begin{aligned} DFT: X(k) &= \sum_{m=0}^{M-1} C(mk)x(m) \\ &= \sum_{m=0}^{M-1} [x(m)C_R(mk) + jx(m)C_I(mk)], \\ & k = 0, 1, 2, 3, ..., M-1 \\ IDFT: x(m) &= \sum_{k=0}^{M-1} [\Big(X_R(k)C_R(mk) - X_I(k)C_I(mk)\Big) \\ &+ j\Big(X_R(k)C_I(mk) + X_I(k)C_R(mk)\Big)], \\ & m = 0, 1, 2, 3, ..., M-1 \end{aligned} \tag{12}$$

Since the above equation requires only integer multiplications and integer additions, they can be executed in the encrypted domain by relying on homomorphic properties. In the following, we will consider the encryption of $s(n)$ as the separate encryption of both $s_R(n)$ and $s_I(n)$: $E[X(m)] = \{E[x_R(m)], E[x_I(m)]\}$. We assume that x is a real-valued signal. So, the secure DFT (SDFT) and secure IDFT (SIDFT) can be computed as:

$$\begin{aligned} E[X(k)] &= \prod_{m=0}^{M-1} E[x(m)C_R(mk) + jx(m)C_I(mk)] \\ &= \{\prod_{m=0}^{M-1} E[x(m)]^{C_R(mk)}, \prod_{m=0}^{M-1} E[x(m)]^{C_I(mk)}\}, \\ & k = 0, 1, 2, 3, ..., M-1 \end{aligned} \tag{13}$$

$$\begin{aligned} E[x(m)] &= \prod_{m=0}^{M-1} E[\Big(X_R(k)C_R(mk) - X_I(k)C_I(mk)\Big) \\ &+ j\Big(X_R(k)C_I(mk) + X_I(k)C_R(mk)\Big)] \\ &= \{\prod_{m=0}^{M-1} E[X_R(k)]^{C_R(mk)} E[X_I(k)]^{-C_I(mk)} \\ &, \prod_{m=0}^{M-1} E[X_R(k)]^{C_I(mk)} E[X_I(k)]^{C_R(mk)}\}, \\ & m = 0, 1, 2, 3, ..., M-1 \end{aligned} \tag{14}$$

3. Privacy-preserving fingerprint authentication at untrusted server

In this section, we describe the proposed method. This method is conducted based on Paillier cryptosystem. In order to make use of servers computational power, all processing of designing CFs and verification are done in server side by exploiting the properties of homomorphic encryption and the two-party computation process. This method is done without leaking any information about the original images. Fig.1 illustrates parameters transmision between the client and server in our method. Details of modification in both client and server stages are carried out in the following four steps and shown in Fig.2. They will be explained in details later.

1) *M* encrypted training images that are chosen randomly from each of *C* classes in client side are stored in the database in the server side.
2) Encrypted CF is designed from *M* encrypted training images by the server.
3) Secure cross-correlation between encrypted test and encrypted CF is computed in encrypted domain by the server.
4) To measure similarity between encrypted test image and encrypted CF, PSR measurement is applied on correlation output plain in encrypted domain.
5) Comparison between decrypted PSR result and PSR threshold is done in client side to decide whether the encrypted test image is authentic or imposter.

Encrypted Correlation Filter: Firstly, encrypted CF is built by server from encrypted training images ($E(s_i)$) in the server side. Corresponding encrypted CF ($E(H)$) for each classes is designed according to Eq.4 and Fig.2.

Secure Cross-Correlation: Secure cross-correlation in encrypted domain is executed between encrypted correlation filter ($E(H)$) and encrypted test image ($E(t)$). This operation is performed with secure multiplication and Paillier cryptosystem properties. Cross-correlation in Plaintext frequency domain is defined as:

$$\begin{aligned} C &= T^*H = (T_R - jT_I)(H_R + jH_I) \\ &= (T_RH_R + T_IH_I) + j(-T_IH_R + T_RH_I) \end{aligned} \tag{15}$$

where T and H are Fourier transform of the t and h and "*" refer to conjugate operation. Cross-correlation in encrypted domain is defined as:

$$\begin{aligned} E(C) &= E\Big((T_RH_R + T_IH_I) + j(-T_IH_R + T_RH_I)\Big) \\ &= [E(T_RH_R)E(T_IH_I)] + j[E(-T_IH_R)E(T_RH_I)] \end{aligned} \tag{16}$$

where E[.] denotes the Paillier cryptosystem, as indicated in Eq.5. With real and imaginary part of E(T)$\Big($secure-FFT(E(t))$\Big)$ and E(H) $\Big($secure-FFT(E(h))$\Big)$ and four secure multiplicative, we can calculate Eq. 16 in encrypted frequency domain. Finally, to transform cross-correlation from encrypted frequency domain to encrypted domain, secure-IFFT must be performed.

Secure PSR measurement : To discriminate authentic from impostor images, the peak of output correlation plain is measured by peak-to-sidelobe ratio (PSR) criterion. The definition of PSR in plain domain is:

$$PSR = \frac{peak}{mean} \tag{17}$$

The peak parameter is the largest value in the correlation output between the filter and test image. The mean is obtained from the sidelobe region around the peak. Fig. 3 illustrates PSR computation in small windows with $W_1 = 5$ and $W_2 = 20$. According to Eq.3, to compute PSR in encrypted domain, server must have the encrypted peak and encrypted mean of the sidelobe region around the peak. Correlation output plane in encrypted domain is encrypted form of correlation output plane in plaintext domain, so encrypted peak is located at the center of that.

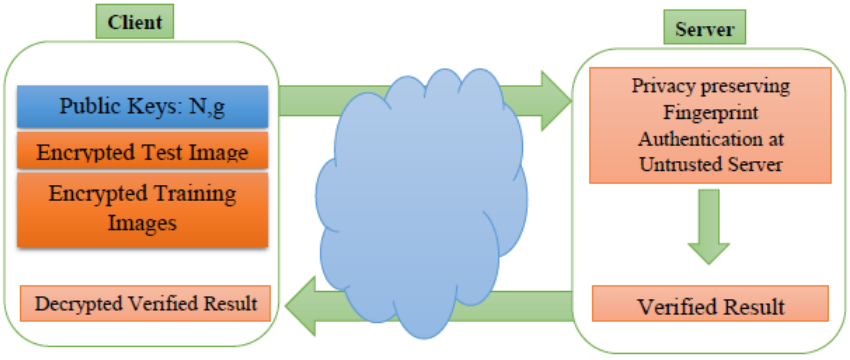


Figure 1. Parameter communication between client and server in proposed method.

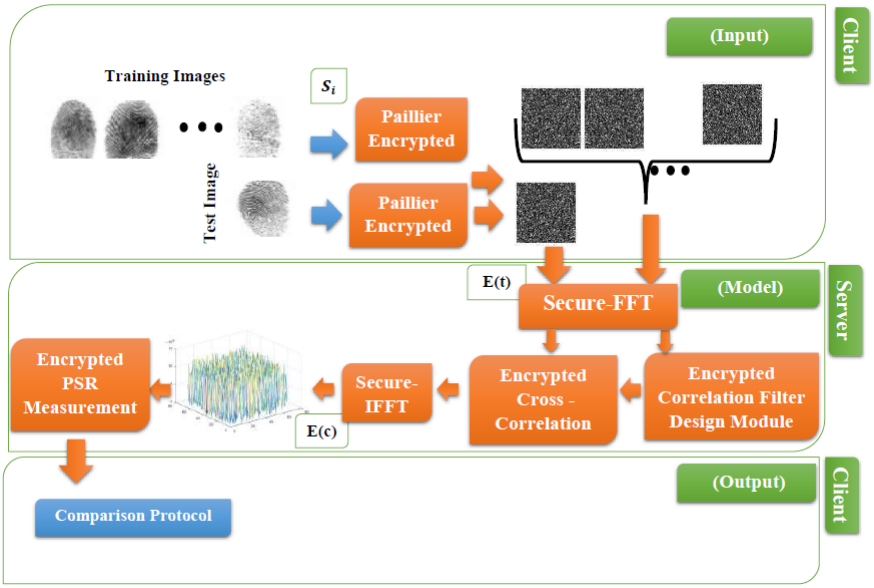


Figure 2. Schematic of the proposed secure fingerprint authentication.

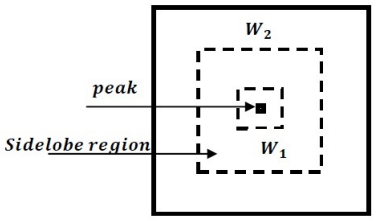


Figure 3. Illustration of peak to sidelobe ratio (PSR) computation.

To obtain encrypted mean value, a sidelobe region around the encrypted peak is considered and it is calculated as follows:

$$E(mean) = E(\sum_{x,y} c_{sidelobe}(x,y)/M) = [\prod_{x,y} E(c_{sidelobe}(x,y))]^{1/M} \bmod N^2 \quad (18)$$

Where $c_{sidelobe}$ is the sidelobe region around the peak according to the Fig.3, and M is the size of $c_{sidelobe}$. We use division algorithm that is described in section 2.3, to calculate PSR (Eq.3) in encrypted domain as:

$$E(PSR) = E(\frac{peak}{mean})$$

4. Experimental Results

Privacy preserving correlation filter for fingerprint authentication is evaluated in this section. First, fingerprint dataset is introduced. Then, biometric information protection requirements are examined in the proposed method. These parameters include authentication accuracy and complexity.

4.1. Database

FVC2002 has four different databases (DB1, DB2, DB3 and DB4) were collected by different sensors. In this paper, a standard fingerprint database FVC2002-DB1 is used. It should be noted that all of the images are normalized to have the same size of 64×64. Sample fingerprint images are shown in Fig.4.

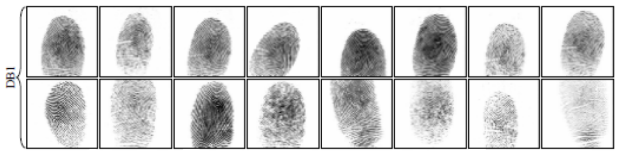


Figure 4. Fingerprint images of FVC2002-DB1.

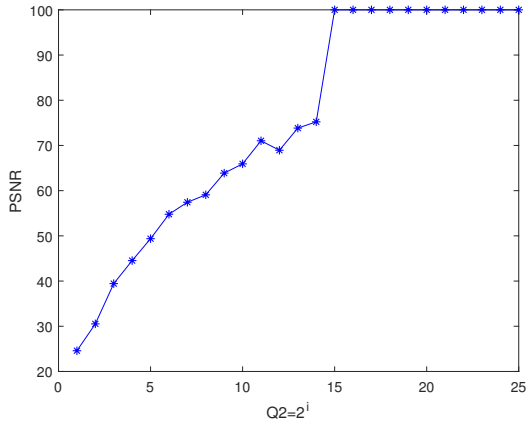


Figure 5. PSNR between decrypted secure FFT and FFT in plain domain vis different scaling factor.

4.2. Optimum scaling factors

For the sake of simplicity we will assume Q_2 is powers of two, ($Q_2 = 2^{n_2}$). Finally, we will indicate the bit length of the modulus used by Paillier as $n_P = \lceil log_2 N \rfloor$. For security reasons, usually requires $n_P \geqslant 1000$. FFT coefficient scaling factor (Q_2) in Eq.11 effects on FFT precision in encrypted domain. The larger Q_2, the smaller quantization effects on FFT output. Fig.5 shows peak signal-to-noise ratio (PSNR) between decrypted secure FFT (DF) and FFT in plain domain (OF) against various values of the Q_2. It can be observed that, when Q_2 is 2^{16} the decrypted secure FFT is equal to FFT in plain domain. So, scaling factor is set to 2^{16}. The PSNR (in dB) is defined as:

$$PSNR = 10 * log_{10} \frac{MAX_{OF}^2}{\frac{1}{m*n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [OF(i,j) - DF(i,j)]^2}$$

4.3. Optimum PSR threshold value

To verify an input image, its PSR value is calculated. If this value is larger than a predefined threshold, then it is considered as authenticated person. Otherwise it belongs to imposter category. PSR value is critical hyperparameter that determines the performance of the authentication system. To determine the optimum value of the PSR threshold, false accept rate (FAR) versus false reject rate (FRR) for all persons in each database when PSR threshold (Thr) varies is plotted. The point where both FAR and FRR are equal to zero represents the optimum value. As Fig.6 shows optimum PSR threshold is 20 for database. The definition of FAR and FRR are as follow:

$$FAR = \frac{\text{number of imposter image with PSR} > Thr}{\text{total number of imposter images}}$$

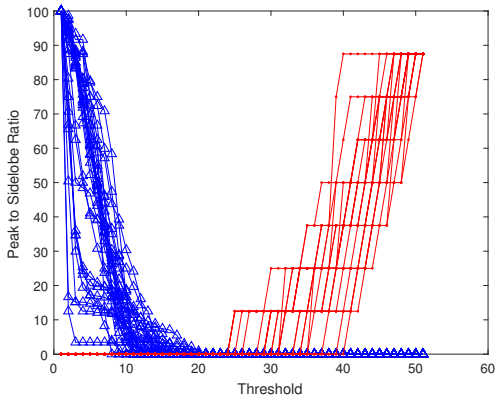


Figure 6. FAR and FRR versus PSR threshold plot

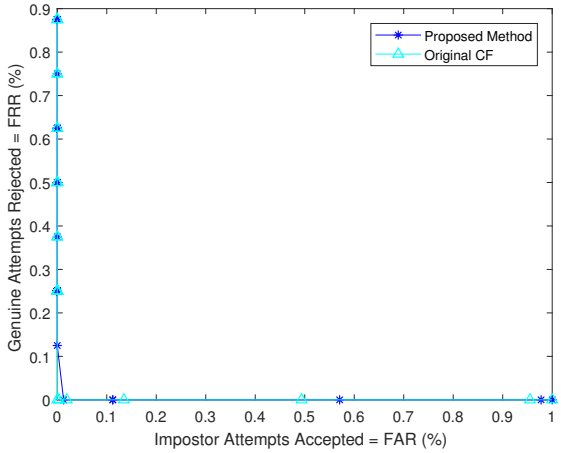


Figure 7. ROC in FVC2002 database.

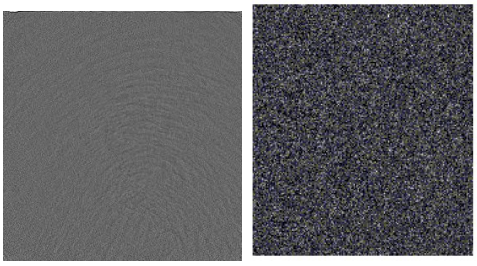
$$FRR = \frac{\text{number of authentic image with PSR} < Thr}{\text{total number of authentic images}}$$

4.4. Accuracy evaluation

Biometric template protection schemes should preserve the verification performance similar to plaintext scheme. In this section, we evaluate the performance of the proposed scheme for fingerprint authentication. For generating correlation filter in plaintext and protected schemes, 5 training images of each subject in each database were selected. The remaining fingerprint images were used as test samples. The receiver operating curve (ROC) is depicted in Fig.7 on fingerprint databases for the plaintext and protected schemes. The x-axis denotes the FAR results and the y-axis is the FRR. It can be seen that the proposed method results are comparable with plaintext results and transforming correlation filter in to encrypted domain does not degrade the performance of fingerprint verification. According to Fig.7, small difference between these methods due to the fact that the Paillier cryptosystem can only operate in the integer domain. Table1 shows recognition between the proposed method and other privacy preserving fingerprint method.

TABLE 1. COMPARISON OF ACCURACY EVALUATION.

Ref	Database	Accuracy
Proposed method	FVC2002	98.5%(RR)
[11]	FVC2002	90.4%(RR)
[4]	UPEK	1.39%(EER)
[3]	FVC2002	6%(EER)
[8]	FVC2002	8.68%(EER)



(a) (b)

Figure 8. Result of point spread function (PSF) attack. (a) Filter obtained from plain images. (b) Filter obtained from encrypted images.

4.5. Security analysis

The security of our algorithm is based on the security of homomorphic encryption and correlation filter schemes. Homomorphic encryption is secure which has been proved in [7]. Thus, our system is secure. Correlation filter that is designed by original training images in plain domain is not robusted against point spread function (PSF) attack. It reveals their private training sets. Fig. 8 (a) shows this fact. However, facial features in the result of PSF attack on CF obtained from encrypted images are unrecognizable (Fig.8 (b)).

5. Conclusions

In this paper, we present a encrypted fingerprint authentication scheme at untrusted server. Privacy of fingerprint images are preserved in three states: privacy of the input images, privacy of the computation, and privacy of the authentication result. Our method allows the client to securely outsource some computation task to an untrusted server by encrypting all information, either stored in the database or exchanged between the client and the server. Furthermore, the client can verify the correctness of the authentication result. Experiments on FVC2002 database showed that authentication can be carried out in the encrypted domain with no degradation in its performance.

References

[1] F.-J. Gonzalez-Serrano, A. Amor-Martin, and J. Casamayon-Anton, "Supervised machine learning using encrypted training data," *International Journal of Information Security*, pp. 1–13, 2017.

[2] h. C. J. Bringer and A. Patey, "Privacy-preserving biometric identification using secure multiparty computation," *IEEE Signal Processing Magazine*, vol. 9386, 2013.

[3] C. Li and J. Hu, "A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, vol. 11, no. 3, pp. 543–555, 2017.

[4] Y. Lin, Y. Ling, Y. Wangke, and W. Zhendong, "A cancelable fuzzy vault algorithm based on transformed fingerprint features," *Chinese Journal of Electronics*, vol. 26, no. 2, pp. 260–267, 2017.

[5] M. Nassar, N. Wehbe, and B. Al-Bouna, "K-nn classification under homomorphic encryption application on a labeled eigen faces dataset," *Intl Conference on Computational Science and Engineering (CSE)*, pp. 546–552, 2016.

[6] E. Pagnin and A. Mitrokotsa, "Privacy-preserving biometric authentication: challenges and directions," *Hindawi Security and Communication Network*, 2017.

[7] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 223–238, 1999.

[8] M. Sandhya and M. Prasad, "Securing fingerprint templates using fused structures," *IET Biometrics*, vol. 6, no. 3, pp. 173–182, 2017.

[9] R. Shokri, "Privacy-preserving deep learning," *22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 1310–1321, 2015.

[10] A. S. T. Shortell, "Secure fast fourier transform using fully homomorphic encryption," *International Conference on Advanced Concepts for Intelligent Vision Systems*, vol. 9386, 2016.

[11] Y. Zhang, "Robust privacy preserving fingerprint authentication," *Master of Science Rice university*, 2015.