Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 8 (17): 2939-2948, 2008
ISSN 1812-5654

A Secured Fingerprint Authentication System

Md. Rajibul Islam, Md. Shohel Sayeed and Andrews Samraj
Multimedia University, Faculty of Information Science and Technology,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia

Abstract: This study is a protection analysis of foremost privacy enhanced technologies for biometrics including watermark embedding technique and fixed digit encryption. A biometric authentication system is vulnerable to a mixture of attacks. These attacks are anticipated to either evade the security afforded by the system or to discourage the usual functioning of the system. Here, we briefly review some of the known attacks that can be encountered by a biometric system and some corresponding protection techniques. We explicitly focus on threats designed to extract information about the original biometric data of an individual from the stored data as well as the entire authentication system. We offer a biometric authentication scheme which uses two separate biometric features combined by watermark embedding with fixed digit encryption to obtain a non-unique identifier of the individual, in order to address security and privacy concerns. Moreover, we provide experimental results presenting the performance of the authentication system. In the client-server environment the transformed features and templates travel through insecure communication line like the internet or intranet. Our proposed technique causes security against eavesdropping and replay attacks on the internet or intranet, because the transmitted feature information and the templates are different every time.

Key words: Template protection, watermark embedding, fixed digit encryption, fingerprint, palmprint, minutiae

INTRODUCTION

Biometric systems propose numerous benefits over traditional authentication methods. Biometric information cannot be obtained by direct secret observation. It is unfeasible to share and complicated to replicate. It increases user expediency by improving the need to memorize long and random passwords. It guards against repudiation by the user. Biometrics supplies the same level of security to all users unlike passwords and is highly challenging to brute force attacks. Identification and authentication refers to two special tasks: finding the identity of a person given the biometric versus verifying the identity given the biometric data and the claimed identity.

In this study, we propose a biometric authentication scheme to address the security and privacy concerns as shown in Fig. 1. In meticulous, two biometric features (e.g., fingerprint and palmprint) are combined to obtain a non-unique identifier of the individual and stored as such

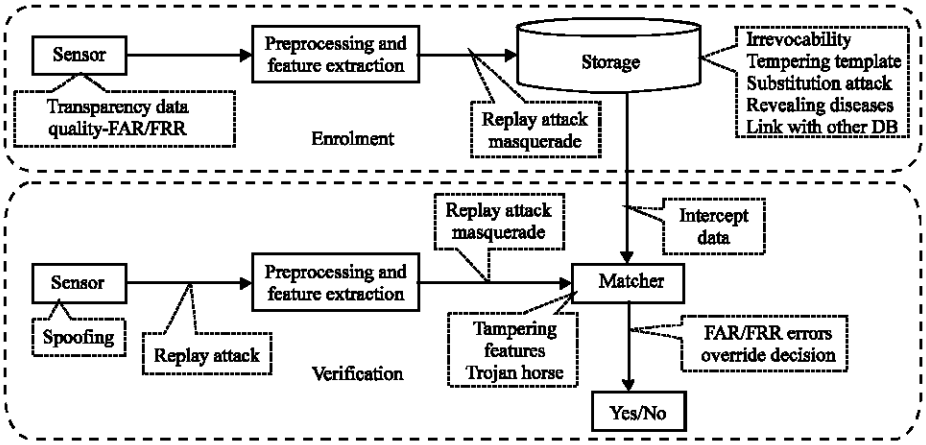

Fig. 1: Privacy and security issues concerning a biometric authentication system

Corresponding Author: Md. Rajibul Islam, Multimedia University, Faculty of Information Science and Technology, Jalan Ayer Keroh lama, 75450 Melaka, Malaysia Tel: +60162489860

Table 1: Some attacks and their temperaments

Type of attacks	Role	Area of attack
Spoofing	Fooling the authentication system by applying fake fingerprints, iris or face image, etc	Sensor
Replay attack	Injecting a recorded image in the system input, avoiding the sensor	The channel between sensor and matcher
Substitution attack	If an attacker obtains an access to the storage, either local or remote, he can overwrite the genuine user's template with his/her own	Storage database
Tempering	In order to achieve a high verification score, feature sets can be modified.	Storage database, matcher
Masquerade attack	An attacker can create a digital artifact image from a fingerprint template, if he gains an access to the templates stored on a remote server and this artifact will generate a match, if submitted to the system	During verification the channel between sensor and matcher
Trojan horse attacks	Several parts of the system, e.g., a matcher, can be replaced by a Trojan horse program that always outputs high verification scores.	Matcher
Overriding Yes/No response	The output of the system is always a binary Yes/No (i.e., match/no match) response. If an attacker were able to interject a false Yes response at a proper point of the communication between the biometrics and the application, he could pose as a legitimate user to any of the applications	During decision making after matching
Privacy issue	Insufficient accuracy of many commercial biometric systems, both in terms of FRR and FAR. High FRR causes inconvenience for legitimate users and prompts the system administrator to lower a verification threshold	During decision making after matching

in a central database. While the combined biometric ID is not a unique identifier, reducing concerns of security and privacy, we show that it can still be used in authenticating a person's identity. As a particular example, we exhibit a biometric authentication system that uses two separate biometrics of the same individual to form a combined biometric ID.

Nevertheless, it is now recognized that biometric systems are vulnerable to attacks. One of the most solemn attacks is against the stored templates. A stolen biometric template cannot be easily revoked and it may be used in other applications that utilize the same biometric feature. Table 1 shows a summary of some attacks and their role and area of attacks in the authentication system.

Security vulnerabilities of a general biometric system: Biometric authentication systems may become vulnerable to potential attacks. Some of those security vulnerabilities are presented in Table 1.

The privacy and security issues of a biometric authentication system sketched in this study are shown in Fig. 1.

Outline of biometric template security approaches: We have summarized some Biometric Template Security approaches in Table 2 which have proposed by numerous researchers. A bit briefing of their attitude, merits and drawbacks are sketched as well.

Table 2: Review of several approaches to defend templates

Template security approaches	Methodology	Benefits	Constraints
Encryption (Soutar *et al*., 1999)	Template is encrypted using well-known cryptographic techniques	Matching algorithm and accuracy are unaffected	Template is exposed during every authentication attempt
Non-invertible transform	One-way function is applied to the biometric features	Since transformation occurs in the same feature space, matcher need not be redesigned	Usually leads to increase in the FRR
Hardening/salting (Teoh *et al*., 2006)	User-specific external randomness is added to the biometric features	Increases the entropy of biometric features resulting in low FAR	If the user-specific random information is compromised, there is no gain in entropy
Key generation (Sun *et al*., 2007)	A key is derived directly from biometric features	Most efficient and scalable approach	Tolerance to intra-user variations is limited, resulting in high FRR
Secure sketch (Sutcu *et al*., 2007)	A sketch is derived from the template; sketch is secure because template can be reconstructed only if a matching biometric query is presented	More tolerant to intra-user variations in biometric data; can be used for securing external data such as cryptographic keys	Template is exposed during successful authentication. Non-uniform nature of biometric data reduces security
Hardened fuzzy vault (Nandakumar *et al*., 2007)	A hybrid approach where the biometric features are hardened (using password) before a secure sketch (vault) is constructed	Hardening increases the entropy thereby improving the vault security; also enhances user privacy	Not user-friendly; user needs to provide both the password and the biometric during authentication
Proposed watermarking with fixed digit encryption (WFDE)	An upgraded approach where two biometric features are synthesized and encrypted with a fixed digit which is derived from the biometric classification	biometric templates are never exposed anywhere in the biometric system. Thus improves the security of the biometric template and user privacy in the whole client-server model of biometric authentication system	User needs to provide two biometric data during each and every authentication session. Hence, sometimes very bothering. Not user-friendly

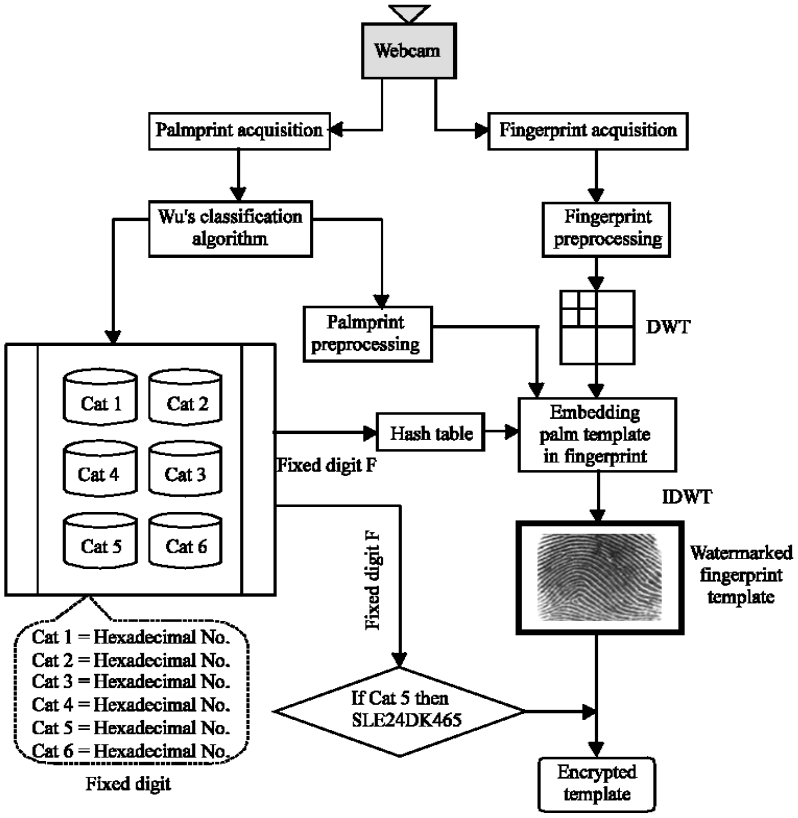

Fig. 2: Proposed watermarking with fixed digit encryption (WFDE)

Proposed approach towards enhanced authentication security: The approach based on user biometric synthesis using watermark embedded and fixed digit encryption as exposed in Fig. 2, to enhance the authentication security of the system. Biometric templates are bound with the Fixed Digits and recomputed directly from it on verification. As a result we get much stronger Biometric template security. Advantages to use fixed digit are as follows:

- Fixed digits are longer and more complex identifiers,
- No need for user memorization
- Less susceptible to security attacks

Besides, some of the security vulnerabilities of a biometric authentication system listed in Fig. 1 are addressed:

- **No substitution attack:** Without any knowledge of the Fixed Digit and other transitory data, an attacker cannot create his own template that had been used to create the genuine template.
- **No tampering:** While the extracted features are not stored, the attacker has no method to adapt them.
- **No masquerade attack:** The attacker cannot construct a digital artifact to submit to the system, since the system does not store the biometric template. Watermark with Fixed Digit Encryption provides an effective protection for remote authentication systems.
- **No Trojan horse attacks:** Watermark embedded process, Encryption or Decryption algorithm does not use any score, either final or intermediate, to make a judgment, it just retrieves (or does not retrieve) a key (as we called fixed digit in our approach). Therefore, the attacker has no means to fool the system by outputting a high score;
- **No overriding Yes/No response:** The Encryption algorithm's output is a 128-bit (or longer) fixed digit, as opposed to the binary Yes/No response. The attacker cannot obtain the fixed digit from a private template.

PROPOSED WATERMARKING WITH FIXED DIGIT ENCRYPTION (WFDE)

Present proposed scheme consists of four main steps as shown in Fig. 2. First of all, performed preprocessing and DWT (Discrete Wavelet Transform) of the fingerprint image to make it prepared for the watermark embedding process. Second step is palmprint classification, so that

the system can get a fixed digit which we have fixed according to six categories of palmprint. In third step, two different biometric images derived from the same user are applied to the watermark embedding process. The embedded template is then secured by the watermarking based on DWT and LSB. Finally, the watermarked template is encrypted using the fixed digit derived after palmprint classification from the second step. In this work, we call this approach Watermarking with Fixed Digit Encryption (WFDE).

Palmprint classification: Wu *et al.* (2004) and Huang *et al.* (2008) proposed a novel algorithm for the automatic classification of low-resolution palmprints using principle lines. The algorithm has the ability to classify palmprints into six categories according to the number of principal lines and the number of their intersections. The principal lines of the palmprint are identified first using their position and thickness. Then a set of directional line detectors is developed. After that they extract potential beginnings (line initials) of the principal lines and then, a recursive process is applied to extract the principal lines in their entirety based on these line initials. The proportions of these six categories (1-6) in the database containing 13,800 samples (Zhang *et al.*, 2003) are 0.36, 1.23, 2.83, 11.81, 78.12 and 5.65%, respectively. They have shown 96.03% of accuracy to classify palmprints.

Watermarking algorithm: For watermarking, the fingerprint image is used as the base or the cover image and the palmprint features are used as the watermark (Yeung and Pankanti, 2000; Yeung and Mintzer, 1998). These features are the palmprint template obtained by convolving the palmprint image with preprocessing.

Watermark embedding algorithm

Stage 1: Two-level Discrete Wavelet Transform (DWT) is applied on the original fingerprint image I. The coefficients of the approximation band of the DWT image contain significant details of the fingerprint image. Hence the approximation band is not modified during embedding.

Stage 2: The detailed sub-bands are divided into blocks $I_1, I_2, \ldots, I_r$ of size M×N and the coefficients in each block are numbered in raster scan order. From each block, the first wavelet coefficient that has a positive phase and whose value is less than threshold η is selected. The second LSB of the selected coefficient is replaced by one bit from the palmprint template. This process is written as follows:

$$I'_w(i,j) = \begin{cases} LSB_2(I_W(i,j)) = F(x,y) \\ I_W(i,j) \end{cases} \begin{matrix} \text{if Phase}(I_W(i,j)) \geq 0 \ \& \ I_W(i,j) < \eta \\ \text{if Phase}(I_W(i,j)) < 0 \end{matrix} \quad (1)$$

where, $I'_w(i, j)$ are the wavelet coefficients in block I_r. F(x, y) is the palmprint template, $I_w(i, j)$ is the wavelet decomposed fingerprint image, η is the threshold which decides whether the watermark bit is inserted or not and LSB_2 denotes the second LSB.

Stage 3: If the number of bits in the palmprint template F(x, y) is less than the number of blocks in the fingerprint image, then all bits of the palmprint template can be embedded. Otherwise, the following procedure is used to embed the remaining bits of the palmprint template:

- For each block I_r, a message block MB_r is formed by selecting few high order bits from each pixel of I_r. A fixed digit D is appended to message block MB_r. The value D is sufficiently large to prevent an attacker from using brute force to remove the watermark.
- The fixed digit D is used to compute a cryptographic hash of the message block

$$Hr = H(MB_r)D \quad (2)$$

- The value of $[H_r \bmod (M \times N)]$ gives the pixel position for embedding the watermark bit. The watermark bit is embedded depending on the value of the Most Significant Bit (MSB) of the hash value H_r. If the MSB of H_r is 0 then the palmprint bit is inserted unchanged; otherwise the complement of the palmprint bit is inserted.

Stage 4: After embedding all the bits from the palmprint template. Inverse Discrete Wavelet Transformation (IDWT) is applied on the watermarked fingerprint coefficients to generate the final secure watermarked fingerprint image. Figure 2 shows the watermark embedding process.

Any change in the value of I_r produces an entirely different hash and can make the watermark undetectable. Since the attacker does not know the fixed digit D, it is not possible to compute the hash value H_r. Also, high order bits are chosen for watermark insertion because any change in these values will degrade the quality of the image and hence the biometric verification performance.

Binding watermarked template using fixed digit encryption: Encryption of the watermarked template using fixed digit enhances user privacy because it enables the creation of revocable templates and prevents cross-matching of templates across different applications.

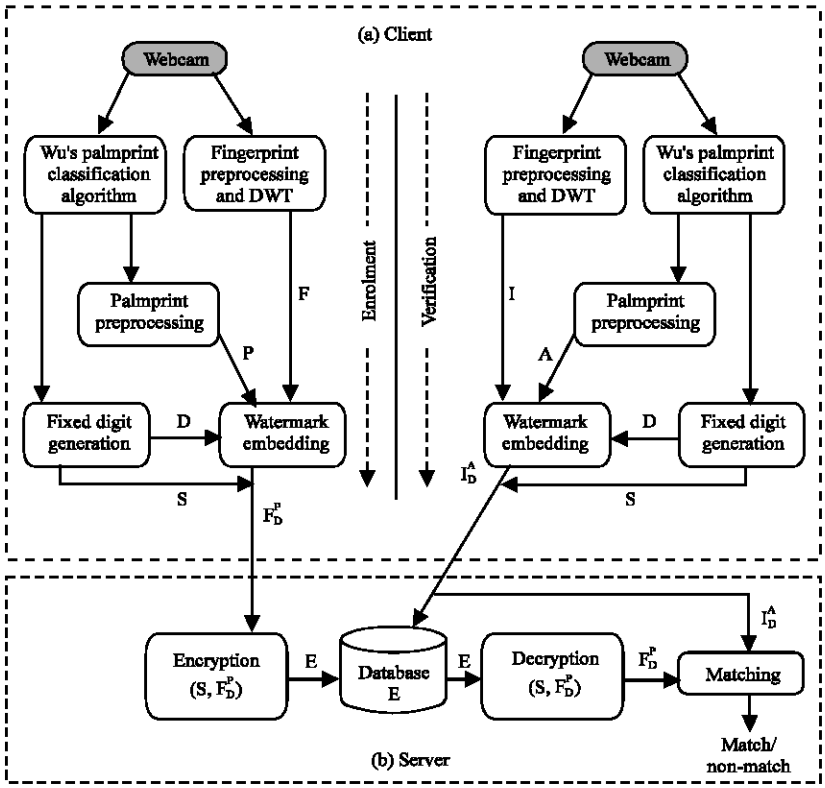

Fig. 3: Operation of WFDE, (a) client and (b) server scheme

The distribution of WFDE template is statistically more similar to uniform distribution than the distribution of original template. This offers better resistance against attacks on the WFDE template. Besides, the additional variability introduced by fixed digit-based watermark embedding reduces the similarity between WFDE templates of different users. This decreases the False Accept Rate (FAR) of the system significantly. If we imagine client-server structural design for the biometric system as shown in Fig. 3 where preprocessing, feature extraction and watermark embedding are applied at the client side and fixed digit encryption, matching is performed at the server, the server never watch the original template. Only the watermark embedded template would be exposed during successful decryption and the original template is never exposed at the server.

Two common methods for cracking a user fixed digit are dictionary attacks and social engineering techniques. In the proposed system, fixed digit is implicitly verified during authentication by matching the WFDE biometric features. Even if an adversary attempts to guess the fixed digit, it is not possible to verify the guess without knowledge of the user's biometric data. This provides resistance against dictionary attacks to learn the fixed digit. However, it is still possible to glean the user fixed digit through social engineering techniques. Therefore, fixed digit based transformation alone is not sufficient to ensure the security of the biometric template. Due to this reason, we use the watermark embedding process to secure the biometric template. Note that the fixed digit used in constructing the watermark embedding that secures the transformed template is fixed forever. Therefore, if the fixed digit is compromised, the security of the WFDE is not affected and it is computationally hard for an attacker to obtain the original biometric template. Because of the template is however synthesized by watermarking. Finally, the watermarked template is encrypted using a fixed digit derived from the palmprint classification. This prevents substitution attacks against the watermarked template because an adversary cannot modify the watermarked template without knowing the fixed digit or the key derived from it.

In Fig. 3, F and I are the fingerprint input obtained from same finger but different impressions. P and A are the palmprint preprocessing data obtained from the same user during enrolment and authentication. In Fig. 3, D represents fixed digit and S represents the encryption and decryption key generated form fixed digit. and represent the templates of enrolment phase and verification phase, respectively after watermark embedded process using fixed digit. E represents the encryption.

RESULTS

Data Collection: A number of volunteers provided their fingerprint and palmprint in the webcam of our fingerprint authentication system which takes over one month. Not all participants could provide their precise fingerprint and palmprint for every take. The webcam was located in the Image Processing and Telemedicine Laboratory with a Pentium 4 PC and took fingerprint and palmprint images from the webcam whenever a new frame was available. In each take, the participants pressed their thumbs and palms on the transparent piece of glass. And like this they put six times and after capture their fingerprint or palmprint they removed their thumbs or palm from the glass. It took five to ten seconds for per impression capture. As a result, we collected fingerprint and palmprint images where the individuals have varying fingerprints and palmprints for six impressions from the same finger and palm, respectively in different rotation angle from the webcam. We discarded all fingerprints and palmprints that were corrupted by hasty movement.

Experiments and results: Our webcam database is a database with 1200 images (100 fingers×6 impressions/finger and 100 palms×6 impressions/palm) of size 480×580. We followed the standard of FVC2000 (Maltoni *et al*., 2003), FVC2002, FVC2004 (Nanni and Maio, 2006) fingerprint databases where each database contains fingerprints from 110 fingers. Only the first two impressions of each finger and palm were used in our initial experiments, the first impressions were used as the template to WFDE and the second impressions were used as the query in the decryption of WFDE template. The output results we have shown in Fig. 5.

The final experiments are designed and performed to study effects of the watermarking on the performance of the proposed secure fingerprint-based authentication system. In this experiment the compassion of watermarking schemes on biometric images is analyzed.

To carry out the tests, we watermarked the 1200 images from present database including both 600 fingerprints and 600 palmprints, ran feature extraction and recognition on the watermarked images and compared the results to that of using the original fingerprints. In order to perform watermark embedding process we used each impression of palmprint on each fingerprint impression which are obtained from the same individual. And by following this process, we got six watermark embedded templates for single individual and like this in the whole database we got 600 templates from 100 individuals. First, to obtain a baseline performance of the authentication system, each fingerprint is matched with rest of the fingerprint database i.e., 599 fingerprints to obtain 599 normalized matching scores. Among the normalized matching scores obtained for a fingerprint, one would expect 5 high scores and 594 low scores. For each hypothesized threshold matching score, the performance of the system was characterized by the True Rejects (TR) and the True Accepts (TA). To obtain the receiver operating characteristics (ROC), the loci of the true accepts/rejects for various hypothesized thresholds were plotted.

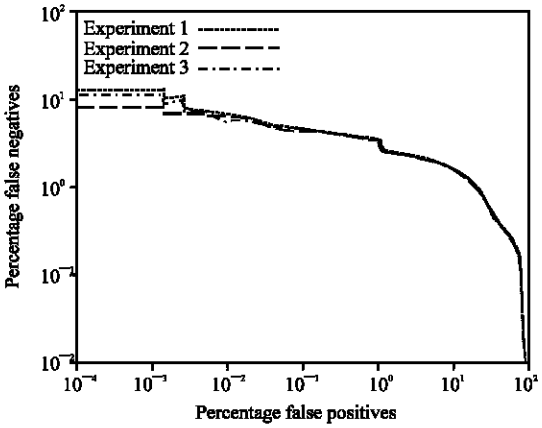

Fig. 4: Receiver Operating Characteristics (ROC) demonstrating the effects of watermarking on the performance of the fingerprint matching system

Table 3: Standard results obtained from the tests

Tests	Matching phase		TA (%)	TR (%)	Matched TA (%)
Experiment 1	Original image	Original image	92.8	7.20	94.2
Experiment 2	Original image	Watermarked image	48.7	51.3	56.4
Experiment 3	Watermarked image	Watermarked image	90.1	9.90	92.5

WFDE was performed for each fingerprint and palmprint image in the above mentioned database and the performance of the authentication was characterized using an ROC as shown in Fig. 4, for each experiment. We classified our test in three different experiments and our experiments representing the performances of the authentication system using original fingerprint database for matching in the experiment 1 and the matching performance between the original fingerprint data with watermarked fingerprints obtained by WFDE in the experiment 2 and finally the matching using the same set of watermarked fingerprint database with watermarked fingerprint data in experiment 3. We performed all these experiments and obtained the results which are shown in Table 3.

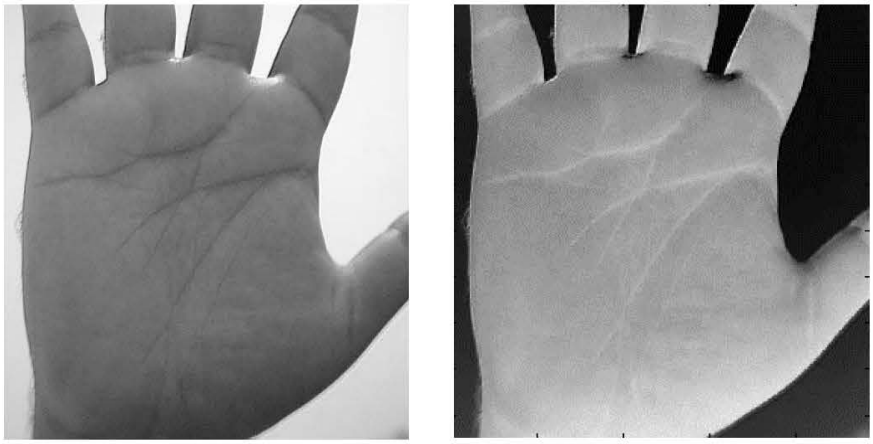

Fig. 5a: Original palmprint captured by webcam (left) and palmprint preprocessing (right)

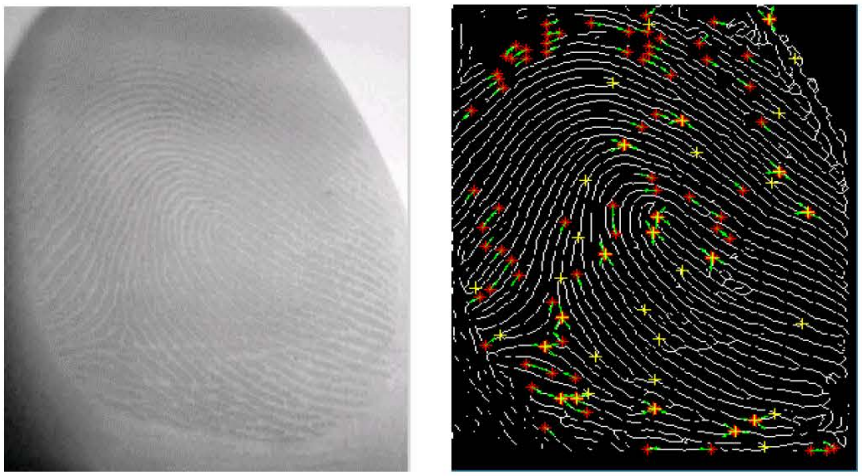

Fig. 5b: Original fingerprint image captured by webcam (left) and minutiae extracted from the original fingerprint (right)

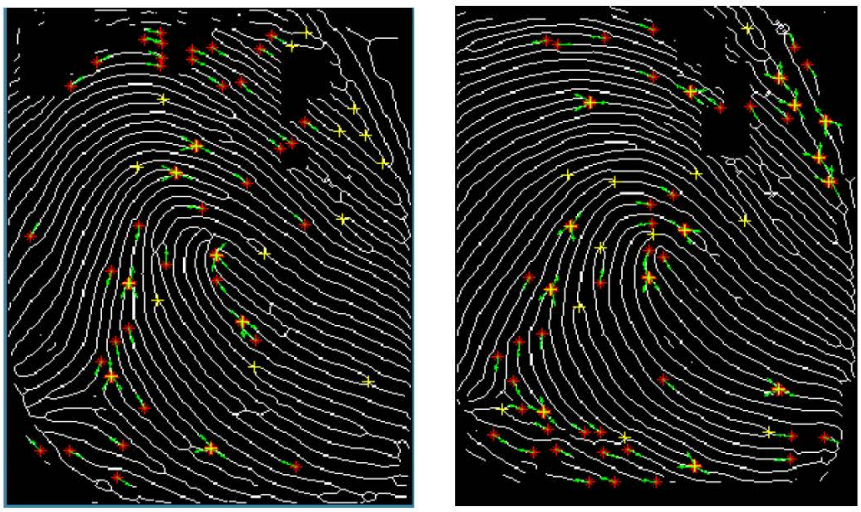

Fig. 5c: The minutiae, extracted after watermarking embedded process during enrolment phase (left) and verification phase (right)

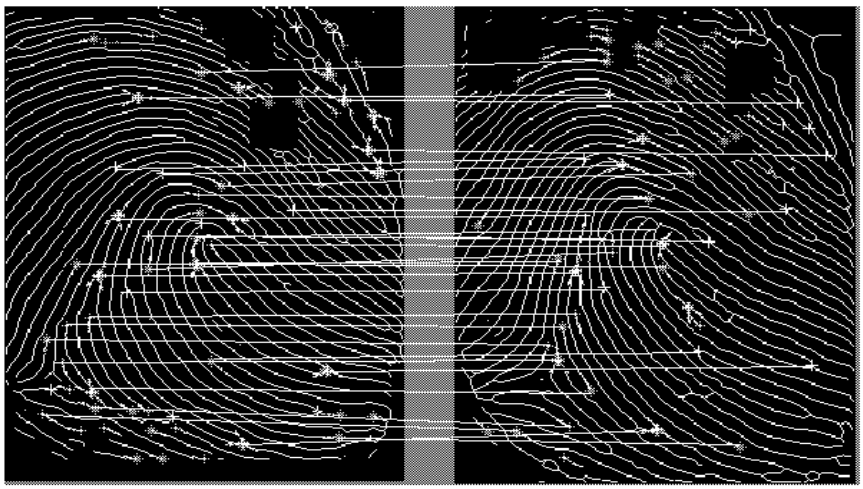

Fig. 5d: Two different impressions of the same finger embedded by watermarking in matching and illustrating our proposed scheme where templates are never exposed through authentication. Common minutiae points are marked on the templates

From a visual inspection of the matching results generated in our final experiments, we observed that experiment 1 and 3 had no significant effects on the performance of the authentication system, where experiment 2 had significant and undesirable effect. This is because; in WFDE scheme the watermark embedding affects a significant number of pixels in a local neighborhood so that some minutiae cannot be extracted during matching session. As a result experiment 2 obtained awful matching results. These results demonstrated that the watermarked images can obtain approximately the same accuracy as the original unwatermarked fingerprints in the matching/ authentication session on our proposed secure authentication system.

The averaged matched true acceptance for experiment 1 and 2 is above 90%. So we proved that our WFDE scheme will perform successfully and better. The security level also remaining strong because in our proposed scheme the original biometric is not exposed anywhere.

DISCUSSION

Although numerous techniques have been proposed to enhance the security and privacy of the biometric authentication system, but still it's a risky issue. It has been largely disregarded the study of potential vulnerability of Biometric Authentication against attacks. That means a complicated attacker could achieve access to both the embedded templates and the whole attack phases shown in Table 1 and sketched as well in Fig. 1. But a user's biometric is not obtained. Such an attacker, fully familiar with the system and exploiting its weaknesses, will not be doing just a watermark extraction process in order to break the embedded template. As a substitute, he will develop different attacks that can be run in a realistic time frame. The WFDE must be flexible against those on-line attacks.

Here, we discuss the security of the above scheme. First, we cite the security framework of the proposed authentication scheme. If challengers' success to steal the template stored in the database, they can get the encrypted template. Subsequently they attempt to extract the template and ruin the file so that it may no longer be useful. Schaathun (2006), presented some attacks in watermarking layer. A real watermarking scheme cannot be expected to be infallible. The attacks are:

- **Non-collusive watermarking attack:** Non-collusive watermarking attacks can be applied to any mark. By garbling the segment, the pirates cause the extraction algorithm to fail with some probability.
- **Collusive watermarking attack:** A collusive watermarking attack applies to detectable marks. By combining different versions of the same mark, for instance by averaging, the pirates can weaken the watermark and cause extraction to fail with some probability.
- **Cropping a segment:** A pirate can crop the file by removing certain segments. If the pirates use a very strong watermarking attack or extensive cropping, they will also ruin the file, because they have no information about the fixed digit which is used for embedding and encryption.

Suppose, the fixed digit is compromised then they can become impostor of the decryption and they will able to obtain a watermarked template which is still secured in the authentication scheme because the original template will never be exposed any where in the system, even in the matching process.

However, even if adversaries hijack the whole database, because it receives no personal information, of course including the original template and the extracted feature, the takeover does not threaten the user's privacy. Then we consider the case of a malicious authentication server collects information. In this structure, it receives watermark embedded and encrypted transformed data. As abovementioned, they imply no information before extraction the embedded and encrypted data. Besides, the malicious sever cannot know the corresponding watermark embedded process, fixed digit and encryption process. Hence, the malicious server obtains no information about original templates.

Next, we consider security of the information transformed by WFDE against hill-climbing attack (Ross, *et al*., 2007), replay attack (Jain *et al*., 2005), collusion attack. Hill-climbing attack (Jain *et al*., 2005) uses of replied matching score in order to make a fake. When the application server sends the matching score to client or adversary as shown in Fig. 3, the adversary transforms embedded feature data selected from database which the adversary constructs. The adversary sends the transformed features to the authentication server for matching. Because this system used the fixed digit to seek the corresponding data, it is difficult for the adversary to improve the fake from the replied matching score. Therefore, the probability of the adversary's success on our proposed authentication scheme becomes less than conventional biometric authentication.

Normally, replay attack is impossible, if previously obtained information is not reusable. When adversaries eavesdrop on the communication between the client and the authentication server, they obtain only embedded transformed features or encrypted data which are not reusable. Hence, no adversary successes replay attack on the proposed authentication scheme. If the adversaries can snoop to the communication from the proposed scheme and obtain the information of any embedded template or encrypted data or decrypted data, when they reuse this information, the client and the database can detect replay attack by verifying the difference among the information of the data used in WFDE scheme.

Only the attack will be established possibly when the user's biometric as well as according to our scheme the fingerprint and the palmprint both are compromised by the attacker.

CONCLUSION

In this study, we focus the problems of the current studies of the template protection. We proposed the authentication scheme to protect the biometric templates and to improve the security and privacy level of biometric authentication system. The main concept of the proposed authentication scheme is that stolen biometric information is not reusable, in every authentication for even same person. In the scheme we used fixed digit which was derived from palmprint classifications. The fixed digit concept is very similar to the password concept (Nandakumar *et al*., 2007) but here user needs to remember the password and also the password is very easy to guess. Finally, we obtained the view of the security of our proposed authentication scheme against the attacks shown in Table 1.

The performance of the authentication scheme is presented by the experiments and results. Besides, we used the palmprint classifications to split our database and the fixed digit to query the encrypted data from the database during authentication session, so that the authentication system will decrease the execution time. In this sense we can say that our proposed scheme will perform more rapidly than the conventional one.

REFERENCES

Huang, D.S., W. Jia and D. Zhang, 2008. Palmprint classification based on principle lines. Pattern Recog., 41: 1316-1328.

Jain, K., A. Ross and U. Uludag, 2005. Biometric template security: Challenges and solutions. Proceeding of 13th European Signal Processing Conference (EUSIPCO '05), September, Turkey, pp: 1-4.

Maltoni, D., D. Maio, A.K. Jain amd S. Prabhakar, 2003. Handbook of Fingerprint Recognition. Springer, New York, pp: 348.

Nandakumar, K., A. Nagar and A.K. Jain, 2007. Hardening fingerprint fuzzy vault using password. Proceeding International Conference on Biometrics, LNCS 4642, August 2007, Seoul, South Korea, pp: 927-937.

Nanni, L. and D. Maio, 2006. Combination of different fingerprint systems: A case study FVC2004. Sensor Rev., 26: 51-57.

Ross, A., J. Shah and A. Jain, 2007. From template to image: Reconstructing fingerprints from minutiae points. IEEE Trans. Pattern Anal. Mach. Translation, 29: 544-560.

Schaathun, H.G., 2006. On watermarking/fingerprinting for copyright protection. In: Proceeding of 1st International Conference on Innovative Computing, Information and Control (ICICIC '06), 5-7 September, 50-53.

Soutar, C., D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, 1999. Biometric Encryption™. In: Bioscrypt Inc. ICSA Guide to Cryptography, Randall, K., (Eds.). Nichols, McGraw-Hill, New York, pp: 1.

Sun, S.W., C.S. Lu and P.C. Chang, 2007. Biometric template protection: A key-mixed template approach. In: Proceeding IEEE International Conference Consumer Electronics 2007, 10-14 January, Las Vegas, NV, pp: 1-2.

Sutcu, Y., Q. Li and N. Memon, 2007. Protecting biometric templates with sketch: Theory and practice. IEEE Trans. Inform. Forensics Security, 2: 503-512.

Teoh, A.B.J., A. Goh and D.C.L. Ngo, 2006. Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs. IEEE Trans. PAMI, 28: 1892-1901.

Wu, X., D. Zhang, K. Wang and B. Huang, 2004. Palmprint classification using principle lines. Pattern Recog., 37: 1987-1998.

Yeung, M. and F.C. Mintzer, 1998. Invisible watermarking for image verification. J. Elect. Imaging, 7: 578-591.

Yeung, M. and S. Pankanti, 2000. Verification watermarks on fingerprint recognition and retrieval. J. Elect. Imaging, 9: 468-476.

Zhang, D., W.K. Kong, J. You and M. Wong, 2003. On-line palmprint identification. IEEE Transa. Pattern Anal. Mach. Intel., 25: 1041-1050.