Secured User Authentication using Encrypted Palmprint

T. P. Kamatchi
III Year ME Biometrics & Cyber Security
PSG College of Technology

K. Gokila Meena
Assistant Professor (S.G)
PSG College of Technology

ABSTRACT

Securing personal privacy and deterring identity theft are national priorities. Biometrics, an emerging set of technologies, provides an effective solution. Foremost examples of are biometric technologies that identify and authenticate faces, hands, palmprints, fingers, signatures, irises, voices, and fingerprints. The biometric data whenever transmitted across the network can be stolen and misused, which provides a fear over the personal privacy. In order to provide personal privacy over palmprints we propose an idea using encryption scheme over the image. In this paper, the palmprint images are obtained from the user, then encrypted and stored in the database server thereby the personal privacy of palmprints can be provided.

Keywords

Biometrics, Cryptography, Public-key Cryptography, Revocability, Security, Encryption

1. INTRODUCTION

Biometric Technology drives the future direction of strong authentication. The promise of biometric is to protect your data and safeguard your identity from being stolen. The industry and technology have matured, and the applications of biometrics growing every day. Almost all the biometric systems are considered secure but it still possesses ample chances of getting hacked. Majorly, two places are keen to be attacked: (i) one is on the channel of communication in the network and another (ii) is on the server’s database. For getting protected from such attacks this system is proposed. Many applications of authentication still require working over networks such as Internet or ATM networks. The major concern is with unsure servers and insecure public internet. Hence there arises authentication, privacy and security problems. True (Unencrypted) biometric templates are easily compromised and substituted. Many systems have been implemented to address the problem of privacy concerns over the years. Proposed work addresses all the features for good biometric authentication system.

1) In both client and the server side strong encryption algorithm is used which addresses the security concerns.

2) Authentication can be carried out between non trusting client and server by using a public key cryptography solution.

3) Protection against replay and client side attacks is achieved even if the keys of the user are compromised.

4) When authentication takes place in the decrypted domain, accuracy of the system can also be maintained.

2. LITERATURE SURVEY

Early researches on fast palmprint identification can be roughly classified into two categories, hierarchical matching and palmprint classification. Hierarchical matching approaches typically involve first extracting multiple kinds of features and then searching in a layered fashion. Simpler features which can be quickly extracted and matched are used at higher layers because they allow a large number of candidates to be discarded. The drawback is that the templates discarded at higher layers may contain the target. Classification strategies often make use of expert knowledge to design the classification rules. They proceed by dividing palmprints into several classes and matching the query only with the templates in its class. The drawback here is that the initial classification may have put the query and its target template into different classes, making a successful match impossible. Therefore, while both strategies speed up the identification process, they do so at the expense of accuracy.

A. Gyaourova and A. Ross have proposed an indexing technique [1] that can either employ the biometric matcher that is already present in the biometric system or use another independent matcher. Index codes are generated for each modality using the corresponding matcher. During retrieval, the index code of the probe is compared against those in the gallery using a similarity measure to retrieve a list of candidate identities for biometric matching. The proposed indexing technique on a multimodal database resulted in a reduction of the search space by an average of 84% at a 100% hit rate. The main factor for the amount of speedup during identification was the penetration rate of the indexing.

Dai and Zhou introduces high resolution approach for palmprint recognition with multiple features extraction[2]. Features like minutiae, density, orientation, and principal lines are taken for feature extraction. For orientation estimation the DFT and Radon-Transform based orientation estimation are used. For minutiae extraction Gabor filter is used for ridges enhancement according to the local ridge direction and density. Density map is calculated by using the composite algorithm, Gabor filter, Hough transform. And to extract the principal line features Hough transform is applied. SVM is used as the fusion method for the verification system and the proposed heuristic rule for the identification system.

Jiaa, Huanga and Zhang have proposed palmprint verification based on robust line orientation code [3]. Modified finite Radon transform has been used for feature extraction, which extracts orientation feature. For matching of test image with a training image the line matching technique has been used which is based on pixel-to-area algorithm.

D. Huang, W. Jia, and D. Zhang proposed a novel algorithm for the automatic classification of low-resolution palmprints [4]. First the principal lines of the palm are defined using their position and thickness. Principal lines are defined and characterized by their position and thickness. A set of directional line detectors is devised for principal line extraction. By using these detectors, the potential line initials of the principal lines are extracted and then, based on the extracted potential line initials, the principal lines are extracted in their entirety using a recursive process. The local information about the extracted part of the principal line is used to decide a ROI and then a suitable line detector is chosen to extract the next part of the principal line in this ROI. After extracting the principal lines, some rules are presented for palmprint classification. The palmprints are classified into six categories considering the number of the principal lines and their intersections.

Zhang, Kong, You and Wong have proposed Online Palmprint Identification. The proposed system takes online palmprints [5], and uses low resolution images. Low pass filter and boundary tracking algorithm is used in pre processing phase. Circular Gabor filter used for feature extraction and 2-D Gabor phase coding is used for feature representation. A normalized hamming distance is applied for matching.

J. You, W. Kong, D. Zhang, and K. Cheung proposed a dynamic selection scheme by introducing global texture feature measurement and the detection of local interesting points [6]. Our comparative study of palmprint feature extraction shows that palmprint patterns can be well described by textures, and the texture energy measurement possesses a large variance between different classes while retaining high compactness within the class. The coarse-level classification by global texture features is effective and essential to reduce the number of samples for further processing at fine level. The guided searching for the best matching based on interesting points improves the system efficiency further.

W. Li, J. You, and D. Zhang, have proposed an effective indexing and searching scheme [7] for an image database to facilitate fast retrieval when the size of a palmprint database is large. There are three key issues to be considered: feature extraction, indexing, and matching. In general, in an image database, the extracted features are often associated to the original images as indices. A search for the best matching is conducted in a layered fashion, where one feature is first selected to lead the search by reducing the set of candidates. Then other features are used to reduce the candidate set further. Such a process will be repeated until the final output is determined based on the given matching criteria. The selection of features plays an important role for efficient search.

Prasad, Govindan and Sathidevi, have proposed Palmprint Authentication Using Fusion of Wavelet Based Representations [8]. Features extracted are Texture feature and line features. In proposed system pre-processing includes low pass filtering, segmentation, location of invariant points, and alignment and extraction of ROI. OWE used for feature extraction. The match scores are generated for texture and line features individually and in combined modes. Weighted sum rule and product rule is used for score level matching.

Cappelli, Ferrara, and Maio proposed high resolution palmprint recognition system [9] which is based on minutiae extraction. Pre-processing is formed by segmentation of an image from its background. To enhance the quality of image, local frequencies and local orientations are estimated. Local orientation is estimated using fingerprint orientation extraction approach and local frequencies are estimated by counting the number of pixels between two consecutive peaks of gray level along the direction normal to local ridge orientation. Minutiae feature is extracted in feature extraction phase. To extract the minutiae features contextual filtering with Gabor filters approach is applied. Minutiae cylinder code has been used for matching the minutiae features.

3. PALMPRINT AUTHENTICATION

Palmprint authentication system can operate in two modes, enrollment and verification. In the enrollment mode, a user is asked to provide several palmprint samples to the system. The samples are captured by palmprint scanner and passed through preprocessing and textured feature extraction to produce the templates stored in a given database. In the verification mode, the user is asked to provide his/her user ID and his/her palmprint sample. Then the palmprint sample passes through preprocessing and textured feature extraction. The extracted features are compared with templates in the database belonging to the same user ID. The figure 1 shows the Palmprint Authentication System.

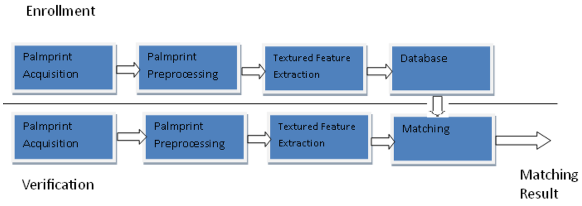


Fig 1: Palmprint Authentication System

4. PUBLIC- KEY CRPTO SYSTEMS

Public-key cryptography is also known as asymmetric-key cryptography, to distinguish it from the symmetric-key cryptography, Encryption and decryption are carried out using two different keys. The two keys in such a key pair are referred to as the public key and the private key. With public key cryptography, all parties interested in secure communications publish their public keys. The figure 2 shows the simplified view of the public-key encryption.

- User 1, if wanting to communicate confidentially with User 2, can encrypt a message using User 2's publicly available key. Such a communication would only be decipherable by User 2 as only User 2 would have access to the corresponding private key

- User 2, if wanting to send an authenticated message to user 2, would encrypt the message with User A's own private key. Since this message would only be decrypted with User 1's public key, that would establish the authenticity of the message - meaning that User 1 was indeed the source of the message

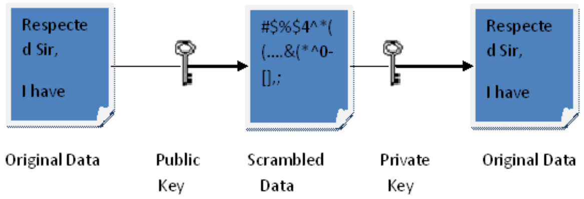


Fig 2: Public Key Encryption

5. PROPOSED WORK

The proposed system works with the following scenario. The client and server communicate with each other, while doing the enrollment and authentication. During enrollment, individual's palm print is obtained with unique user name and password. In order to provide security to the palmprint both in network and database, encryption algorithm is used in both client and server side. RSA algorithm is used with some modifications which is called RSA-2. It provides more security and also to enhance confidentiality than RSA algorithm. The problem of RSA algorithm is that it uses the numbers instead of characters in the plain text, which is also able to represent special characters. If it is of characters and numbers, the intruder can easily calculate the cipher text by trying some replacement and possibly may enter into the system. It can be solved through RSA-2 algorithm. The RSA-2 algorithm increases the speed of encryption and decryption with enhancement of security also due to special symbols. RSA-2 algorithm will reduce the denial of service problem since it is a public key cryptography. During authentication, one who wants to authenticate himself has to give his username, password and his palm print to the authenticating server. If matching is success, authentication is confirmed. This is implemented through the following algorithm.

5.1 Algorithm

5.1.1 Enrollment Process

Step 1: Start

Step 2: Palm prints are taken from user

Step 3: Image Preprocessing is performed to get the sub area of palm

Step 3: Textured features are extracted from palm prints

Step 4: Encryption algorithm RSA-2 is performed on the client side

Step 5: Encrypted data is stored in the database

5.1.2 Authentication Process

Step 1: Start

Step 2: User is asked to provide palm prints along with the User ID and Password

Step 4: Image preprocessing is performed

Step 5: Textured features are extracted from the preprocessed palm prints

Step 6: Encryption algorithm RSA-2 is performed on the client side for encryption

Step 7: Forward the RSA-2 encrypted palm print to the server side

Step 8: RSA-2 decryption algorithm is performed on the server side

Step 9: Matching algorithm is performed

Step 10: If Yes, Authentication is confirmed

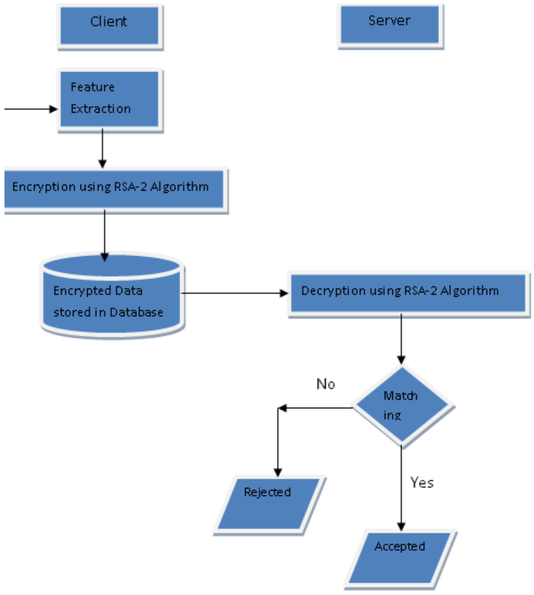

Client
Server
Feature Extraction
Encryption using RSA-2 Algorithm
Encrypted Data stored in Database
Decryption using RSA-2 Algorithm
No
Match ing
Yes
Rejected
Accepted

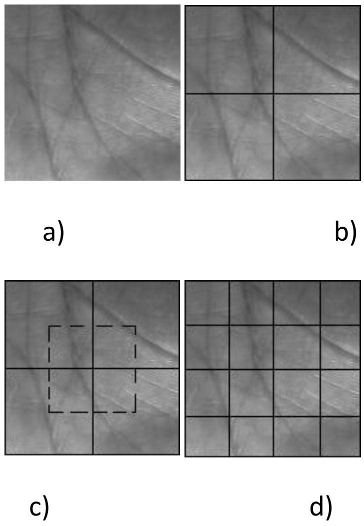
Fig 3: Proposed System

5.2 Textured Feature Extraction

Step1: Read ROI images

Step2: Crop Original ROI image into 64 X 64, 32 X 32 and 16 X 16 non-overlapping and intersect of previous sub images as shown in figure 4.

Step3: Calculate, Variance for all sub images and store the values into Feature Vector.



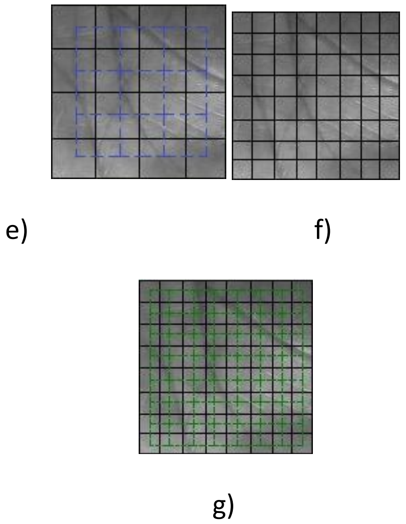


Fig 4. Textured Feature Extraction

[a] Extraction of ROI.

[b] Cropping 64X64 non-overlapping sub-images.

[c] Cropping 64X64 intersect sub-images.

[d] Cropping 32X32 non-overlapping sub-images.

[e] Cropping 32X32 intersect sub-images.

[f] Cropping 16X16 non-overlapping sub-images.

[g] Cropping 16X16 intersect sub-images.

7. RESULTS

After developing this system, we have taken different palmprint images and encrypted using RSA-2 Algorithm. There are various measures to test the system performance. Two of the major measures are False Acceptance rate (FAR) and False Rejection Rate (FRR). In this system the False Acceptance Rate is zero when the threshold value is above 30%. Similarly the False Rejection Rate is zero when the threshold value is below 16%.

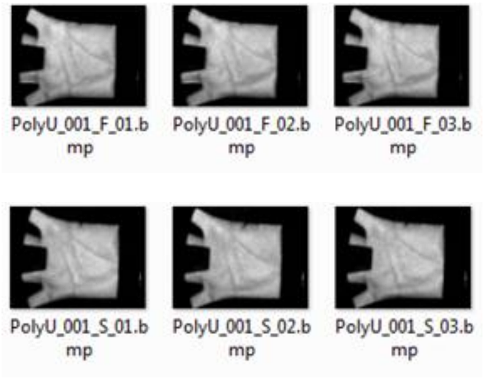


Fig 5: Six Input Images are obtained from PolyU Database for training

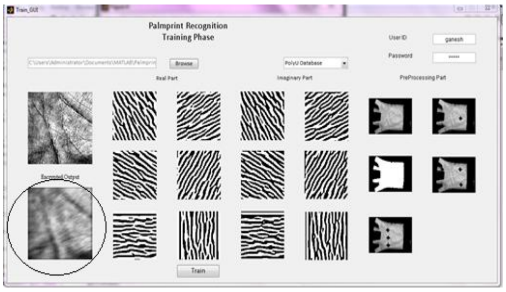


Fig 6: Encrypted Output

Table 1. Different Threshold values and the corresponding FAR

Threshold (%)	FAR (%)
10	53.33
12	51.78
14	49.56
16	42.22
18	37.11
20	27.78
22	17.33
24	10.44
26	4.89
28	0.44
30	0
32	0
34	0

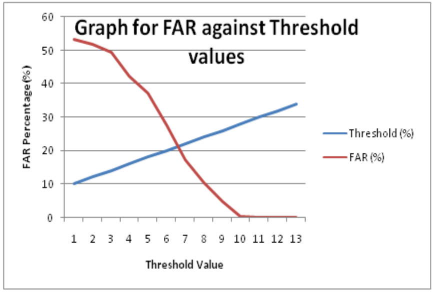
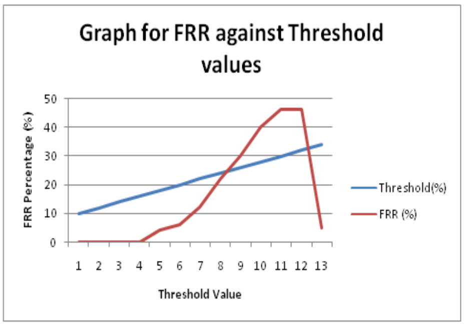


Table 2. Different Threshold values and the corresponding FRR

Threshold (%)	FRR (%)
10	0
12	0
14	0
16	0
18	4
20	6
22	12
24	22
26	30
28	40
30	46
32	46
34	5



7. CONCLUSIONS AND FUTURE WORK

7.1 Conclusion

Several existing methods have been reviewed for palmprint recognition. An additional layer of security in authentication is provided by using encryption scheme when compared with the existing systems. Palmprint recognition is an emerging field and limited works were carried which paves way for the researchers to invent new methods to reduce the error rates and to improve the accuracy and speed of the system.

7.2 Future Work

The future work can be extended to apply two-level of encryption and can be achieved by employing two different encryption algorithms in the system. Also inorder to overcome from the replay attack cancellable biometrics technique can be applied.

8. REFERENCES

[1] A. Gyaourova and A. Ross, A Novel coding scheme for indexing fingerprint patterns" Proceedings of S+SSPR Workshop, December 2008

[2] J. Dai, J. Feng, J. Zhou, "Robust and Efficient Ridge-Based Palmprint Matching," IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.34, No. 8, pp. 0162-8828, August 2012

[3] Jiaa, Huanga and Zhang, "Palmprint Verification based on robust line orientation code" Science Direct, May 2008

[4] D. Huang, W. Jia, and D. Zhang, "Novel algorithm for the automatic classification of low-resolution palmprints", IJARCSSE, January 2014

[5] D. Zhang, W. K. Kong, J. You, M. Wong, "Online Palmprint Identification," IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.25, No. 9, pp. 0162-8828,September 2003

[6] J . You, W. Kong, D. Zhang, and K. Cheung, "On hierarchical palmprint coding with multiple features for personal identification in large databases," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 2,pp. 234–243, February 2009

[7] W. Li, J. You, and D. Zhang, "An effective indexing and searching scheme for an image database" , IJDL, 1997

[8] S. M. Prasad, V. K. Govindan , P. S. Sathidevi, "Palmprint Authentication Using Fusion of Wavelet Based Representations," IEEE, pp. 978-1-4244-5612-3, 2009

[9] Cappelli, Ferrara, Maio, "High resolution Palmprint Recognition System", IEEE, June 2012

[10] ShikhaWadha and Monika Malhotra, "Enhancing security in palmprint recognition systems using Encryption algorithms" International Journal of Engineering and Computer Science, June 2014

[11] David Zhang, Guangminglu, Lei Zhang and Nan Luo, "Palmprint Recognition using 3D Information", IEEE, August 2009

[12] Wei Li Zhang, D. ; Zhang, D. ; Guangming Lu ; Jingqi Yan "Efficient joint 2D and 3D palmprint matching with alignment refinement", IEEE, June 2010

[13] Naidu Swathi, Chemudu Satish, Vaddi Seshu Satyanarayana, Pillem Ramesh, Hanumakumar, NareshBhuma, CH.Himabin du, "New palm print authentication system by Using wavelet based method" , AIRCCSE, March 2011

[14] Nageshkumar, Mahesh.PK and M.N. ShanmukhaSwamy, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image", IEEE, June 2009