www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6291-6295

ENHANCING SECURITY IN PALM PRINT RECOGNITION SYSTEMS USING ENCRYPTION ALGORITHMS

Shikha Wadhwa, Monika Malhotra

Student
Department Of Computer Science Engineering
WCTM, Gurgaon
Haryana, India
Wadhwa.shikha13@gmail.com
Asst. Professor
Department Of Computer Science Engineering
WCTM, Gurgaon
Haryana, India
gudiyadudeja@gmail.com

Abstract: ***Nowadays, the use of biometric characteristics (e.g., palmprints, irises, fingerprints) is incrementing for individual recognition and many applications of biometrics are already available. Biometrics recognition has many advantages over the traditionally used methods (e.g., password, smart card), because biometric characteristics cannot be shared or forgotten, as it is inherently associated with the individual.***

The main focus of Biometrics authentication system is on revocability, security, privacy, accuracy and privacy. In this fast developing communication world, one of the essential requirement is security of biometrics information. In this paper, a biometric authentication system with 2-way security is being proposed, which basically concerns with user's privacy, network security, trust issues, template protection, and accuracy. Encryption of biometric details is done twice. That's why; we called the system two way secured. None of the extra information is being disclosed to any unsafe network or any server's database about the biometrics or user. Two different encryption algorithms are used at the client and server side. Modified version of RSA algorithm, i.e., RSA-2 algorithm is used at one side which is a public key cryptography and other encryption algorithm used is private key cryptography, 3DES algorithm.

No restrictions are possessed on the biometric data used in the proposed approach and it is also applicable for different biometrics (palm print, face, iris, and finger print). An additional layer of security in authentication is being provided by using two way encryption schemes when compared with existing systems.

Keywords: Biometrics, Cryptography, Public Key Cryptography, Revocability, Security

I. INTRODUCTION

Biometrics are being used for secure recognition and certification for more than two decades since biometric data is unforgettable, non-transferable, unique, and always with us.

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 link of communicating network and another (ii) on server's database. For getting protected from such attacks this system is proposed. Many applications of authentication still require to work over networks such as Internet or ATM networks. More concerns in privacy and security are raised while performing authentication with unsure servers or over insecure public networks. Security of the unencrypted biometric templates is the principal concern because once they are compromised, they cannot be substituted.

To clarify our problem, let us consider the following usage scenario:

"X" wants an account to be created in "Y's bank", where palm print authentication is required. "X" does not trust "Y" that it can handle his palm print data securely, and also does not trust the communication link for plain palm print to be sent. The main concentration is that, for both "X", "Y" can be incapable to provide security to his palm print or even peculiar to try and benefit his palm print data, while the

process of authentication continues. Hence, "X" is reluctant for giving his plain palm print data to "Y". Whereas, the client is not trusted by "Y" as shammer could be there. He can also disown his service at a later time. The network is not secure for both the parties. A variety of applications like using remote servers to internet shopping over the Internet can work firmly and faithfully under using palm print based systems.

For many applications, where the authentication of user is done using a powerful encrypted data of his palm print (say using RSA [2]), then many concerns on security and privacy can also be dealt. However, the authentication requires the accomplishment of all the calculations in the encrypted domain of server. But, eradication of similarity among the data is done by using encryption algorithms, while similarity of data is done by matching algorithms [1] which are required to maintain and attain high accuracy. Hence, we can also state that security/privacy and accuracy appears opposing factors. Sensible trade-off between security and accuracy is being made by a variety of secure authentication systems. This inescapable problem can be overcome if the system is projected in such a way that the matching is performed in the plain feature space which also permits us for maintaining the palm prints performance. It is demonstrated that acquiring a solution to this problem is possible by dispersing the work between client and server, using our proposed scheme. Strong public key encryption is used at client side, known as RSA-2 algorithm, it is the modified version of RSA [5] algorithm and private key cryptography is used at server side, known as triple DES.

II. RELATED WORK

Validation of identity of individuals is done by authentic recognition schemes. To determine whether the legitimate user is using the system or not is the aim of such schemes. Examples of such applications are computer systems, laptops, secure access to buildings, cellular phones and ATMs. Above mentioned applications are vulnerable to different types of attacks due to lack of this personal biometric authentication system. Biometrics signifies that the persons are recognised automatically by characterising them with their behavioural or physiological characteristics. It is possible to establish an individual's identity with the help of biometrics. Although hacking chances of plain biometric details from the database or from the communication link is there. To overcome this problem, we are proposing that encrypted version of the palm print to be used.

The second work in the area of encryption which is developed is based on security [4] of biometric templates which are used to formulate the problem as that of distinguishing the actual and imposter samples in the encrypted domain. But, deterioration of pattern in data can be experienced by using a strong encryption, and accuracy of verification is affected due to this. Hence, a compromise among template security (strong encryption) and accuracy (retaining patterns in the data) is being made by matching mechanisms. The primary difference in this approach is that they are capable to project the matching in the plain feature space, which allows us to assert the performance of the biometric itself, while carrying out the authentication on data with strong encryption, which provides high security / privacy.

Many attempts have been made to address the problem of privacy concerns over the years.

Our proposed work addresses all the features for good biometric authentication system mentioned above.

1) Two different strong encryptions are used in client and server side and which also addresses security concerns.

2) By using a public key cryptography solution, authentication can be carried out between non trusting client and server.

3) Security is also enhanced by two way encryption schemes. 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.

III. PROPOSED WORK

The proposed system works with the following scenario. The client and server communicate with each other, while doing the enrollment and authentication [6]. A unique user name, password is being assigned to every person. During enrolment, individual's palm print is being added with unique user name and password. The palmprint is being provided security in order to provide security to the palmprint both in network and database by using two different encryption algorithms in both client and server sides. At client side, the RSA [9] algorithm is used with some modifications which is called RSA-1[10] and it enhances the speed of RSA algorithm and the algorithm which provides more security than RSA algorithm is called RSA-2 [3] algorithm which can also enhance confidentiality to the client. The problem of RSA algorithm is solved through RSA-2 algorithm; it uses the numbers instead of characters in the plain text, which is also able to represent special characters. In case of character and numbers the intruder can easily know the cipher text and author can replace it by the special symbols with the help of decimal value into their respective ASCII code character. The RSA-2 algorithm increases the speed of encryption and decryption with enhancement of security also due to special symbols. At server side we are using 3DES algorithm. 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. To maintain accuracy matching has been done with plain biometric details. After matching took place in the server and if success, authentication is confirmed. This is implemented through the following algorithms.

3.1 Algorithm

Enrollment Process

Step 1: Start

Step 2: Palm prints are taken from user.

Step 3: Features are extracted from palm prints like ridges etc.

Step 4: RSA-2 encryption algorithm is performed on client side.

Step 5: RSA-2 decryption algorithm is performed on server side.

Step 6: 3DES encryption algorithm is performed on the server side.

Step 7: Encrypted data is stored in the database.

Authentication Process

Step 1: Start

Step 2: User is asked to provide palm prints alongwith User ID, Password

Step 3: Features are extracted from palm prints like ridges etc.

Step 4: RSA-2 encryption algorithm is performed on client side for encryption.

Step 5: Forward the RSA-2 encrypted palm print to the server side.

Step 6: RSA-2 decryption algorithm is performed on server side.

Step 7: Get 3DES encrypted equal data from database.

Step 8: 3DES decryption algorithm is performed on server side.

Step 9: Matching algorithm is performed.

Step 10: Reply with authentication confirmation.

Above steps are diagrammatically shown in following figures, i.e. Fig. 1 & Fig. 2:

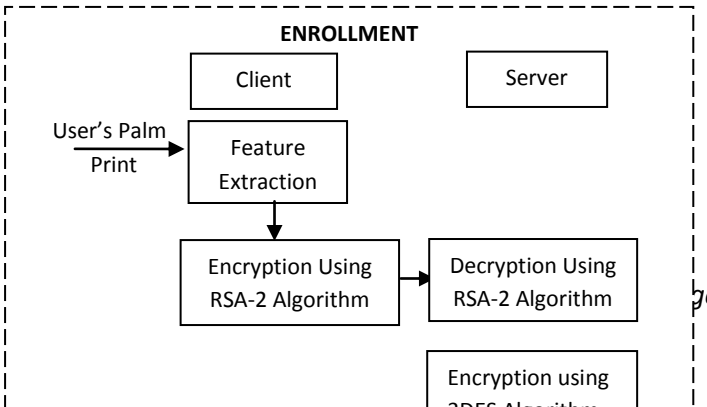


Fig 1: Enrollment Process

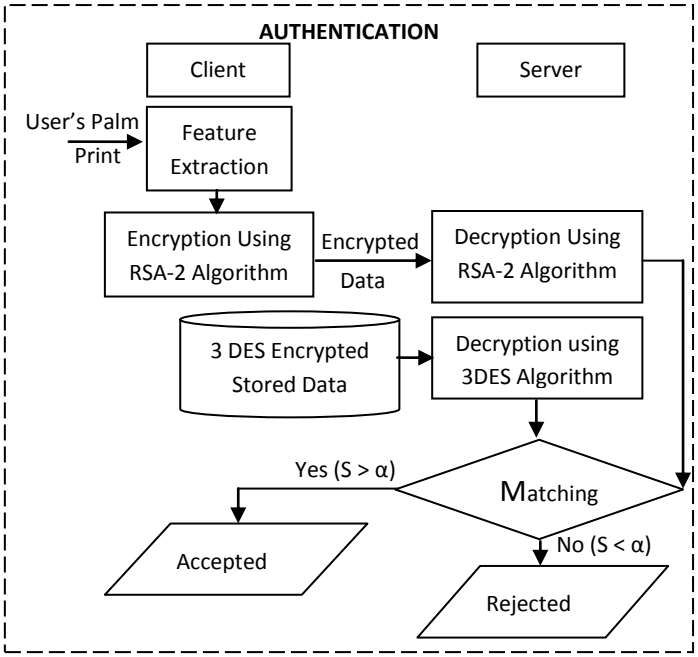


Fig 2: Authentication Process

IV. RESULTS

4.1 Effect of different versions of RSA algorithms

The comparison between three algorithms is represented in Fig 3**.** The file size is taken to be in X axis and the execution time in Y axis. The execution time of all the algorithms is represented simultaneously in chart.

In this chart, three different lines are displayed. From this graph, the RSA1 has high speed when compared to RSA and RSA2. The RSA2 requires more time for execution.

To put it in nutshell, the execution depends on the file size of the referred two algorithms, RSA2 is better than RSA in case of security. However, RSA1 deals an entirely different aspect which is not dealt by other algorithms. It is based on the repeated occurrence of a character instead of file or key size in the case of RSA algorithm.

It is observed that RSA1 gives better performance based on the execution time whereas the RSA2 is better based on security. The time is directly proportional to the file size.

RSA ANALYSIS CHART

.

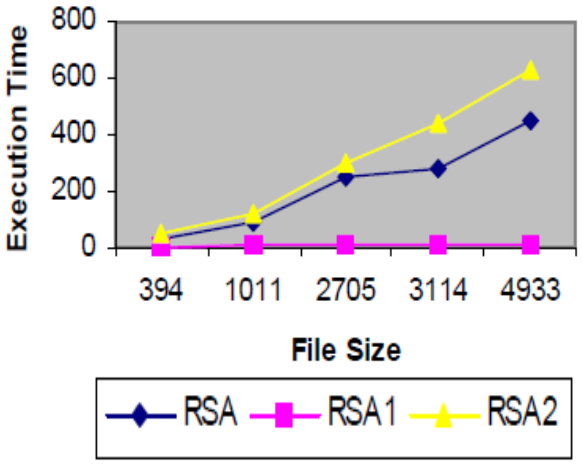


Fig 3. Effect of different versions of RSA algorithm

False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the measures of system performance. The result (Fig 4) shows that the FAR of the existing system is 0.09 and of the proposed system is 0.03.

It is also concluded in Fig 5 that the FRR of existing system is 0.11 and of proposed system is 0.06.

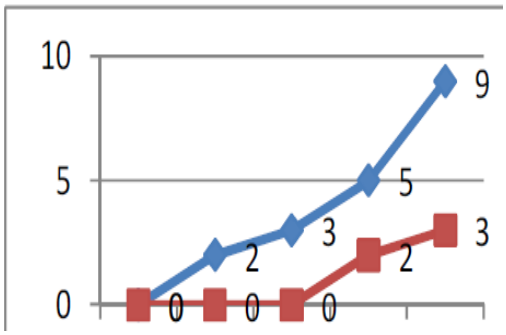


Fig 4 False Acceptance Rate

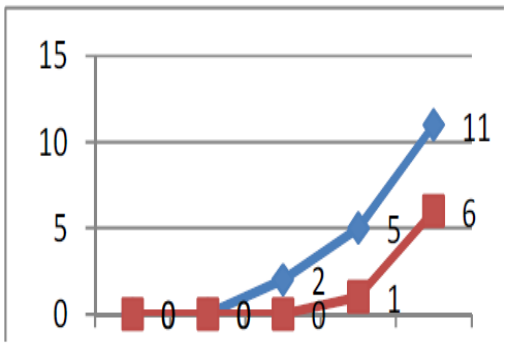


Fig 5 False Rejection Rate

V. CONCLUSION AND FUTURE WORK

5.1 Conclusion

Two level security and accuracy is the main advantage of the proposed system. To provide more security two very strong encryption schemes (RSA2 and 3DES) are being used. By means of matching algorithms the accuracy can be achieved.

In our system we used dynamic matching algorithm and variable length features of palm print. The proposed work is extremely secure under a variety of attacks and it can be used in various biometric traits.

5.2 Future Work

In Future work we would like to conduct further experiments using Diffie-Hellman Algorithm for key exchange between Client and Server. It can be applied to other biometrics like iris, finger print, and face recognition systems in future. It can also be implemented with any other strong cryptographic algorithms.

VI. REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1,pp. 4–20, Jan. 2004.

2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol.40, no. 3, pp. 614–634, Mar. 2001.

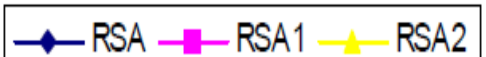
[3] RSA-2 Algorithm "Speed and Security enhancement through public key cryptography", International Journal of Engineering Science & Technology Vol.2 (8), 2010, 3551-3556, J. SaiGeetha et. al.

[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security,"EURASIP, vol. 8, no. 2, pp. 1–17, 2008.

[5] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no.2, pp. 120–126, 1978.

[6] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. V. Jawahar,"Efficient biometric verification in the encrypted domain," in 3rd Int.Conf. Biometrics, Jun. 2009, pp. 906–915.

[7] J. Dai and J. Zhou, "Multifeature-Based High-Resolution Palmprint Recognition", IEEE Transactions



On Pattern Analysis And Machine Intelligence, Vol. 33, No. 5, 2011, pp. 945-967.

[8] You D. Zhang, W. K. Kong and M. Wong. On-line palmprint identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(9):1041-1050, 2003.

[9] Algorithm for software implementations of RSA, A .Mitchell C. Trinity coll, Cambridge as appears computer and Digital Techniques, IEEE May 1989 (Vol 136, No: 3- PP 166-170).

[10] RSA Speedup with Chinese Remainder Theorem Immune against Hardware Fault cryptanalysis, December 11- International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.2, March 2011 75 15, 2000-New Orleans, Louisiana Sung-Ming Yen, Sang-Jae.