Secure Biometric Cryptosystem for Distributed System

Manish Manoria[1], Ajit Kumar Shrivastava[2], Satyendra Singh Thakur[3], Debu Sinha[4]
[1,2,3]Lecturer CSE Department, TRUBA Institute of Engineering & Information technology, Bhopal, India
[4]Software Engineer Accenture Technology Chennai, India
E-mail : [1]manishmanoria@rediffmail.com,
[2]ajitshrivastava@rediffmail.com, [3]satyendrathakur04@gmail.com, [4]debusinha2009@gmail.com

***Abstract*—Information (biometric) security is concerned with the assurance of confidentiality, integrity, and availability of information in all forms, biometric information is very sophisticated in terms of all, in this work we are focusing on data pattern along with all security assurance, so that we can improve the matching performance with good security assurance, here one of the most effective RSA algorithm use with biometric (fingerprint) data. Our work includes the determination of appropriate key sizes with security issues and determines the matching performance using MATLAB and JDK1.6, performance of this system is more than 86.7% and when combines this with blind authentication techniques then we get all security assurance with high performance biometric cryptosystem.**

***Keywords*—blind authentication, biometric cryptosystem, RSA, fingerprint, MATLAB.**

I. INTRODUCTION

A Biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being [1]. Statistically analyzing these biological characteristics has become known as the science of biometrics. These days, biometric technologies are typically used to analyze human characteristics for security purposes. Five of the most common physical biometric patterns analyzed for security purposes are the fingerprint, hand, eye, face, and voice. The advantage claimed by biometric systems is that they can establish an unbreakable one-on-one correspondence between an individual and a piece of data. The drawback of biometric systems is their superficial invasiveness and the general risks that can emerge when biometric data is not properly handled. There are good practices that, when followed, can provide the excellent match between data and identity that biometrics promise; if not followed; it can lead to enormous risks to privacy for an individual. Biometric system is vulnerable to a variety of attacks aimed at undermining the integrity of the authentication process. These threats are [02][3]

1. Fake biometric (e.g., finger made from silicon face mask, lens including fake iris texture) to the sensor.

2. Replay attack, because an intercepted biometric (with or without the cooperation of the genuine user) data is submitted to the feature extractor.

3. Bypassing the sensor: the feature extractor module is replaced with a Trojan horse program that functions according to its designer's specifications (henceforth, these users that try to break into systems protected by biometric authentication will be collectively called "Trudy").

4. Genuine feature values are replaced with values (synthetic or real) selected by the attacker.

5. The matcher is replaced with a Trojan horse program.

6. The attacks on the template database (e.g., addition, modification, or removal of templates) constitute.

7. The templates are tampered with (stolen, replaced, or altered) in the transmission medium between the template database and matcher.

8. The matcher result (accepts or reject) can be overridden by the attacker.

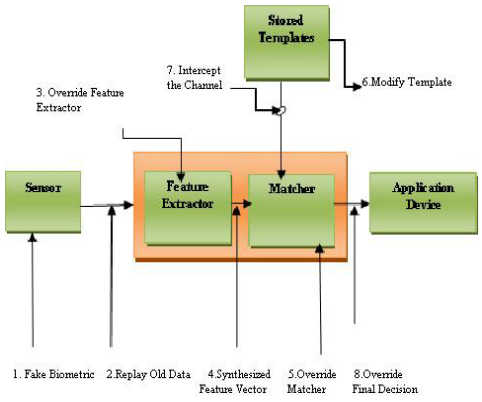

Fig.1: possible attacks in biometric system

To protect the information from these attacks an efficient method of authentication called Blind Authentication Protocol [4] came which addressed the concerns of user privacy, template protection and trust issue. Enrollment and authentication are the two

primary processes involved in a biometric security system. During enrollment, biometric measurements are captured from a subject and related information from the raw measurements is gleaned by the feature extractor, and this information is stored on the database. During authentication, biometric information is detected and compared against the database through pattern recognition techniques that involve a feature extractor and a biometric matcher working in cascade a typical automated biometrics-based identification.

2. BIOMETRIC INFORMATION CRYPTOSYSTEM

Biometrics provides security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users [6][7]. Motivation of using biometric information is that biometric system provides automatic recognition of an individual based on some unique features or characteristics possessed by the individual. Sensor technology is also improved, this is another motivation factor. Biometric systems have been developed based on common biometric traits such as fingerprint, facial features, iris, hand geometry, voice, handwriting, etc. A good biometric is characterized by use of a feature that is; highly unique - so that the chance of any two people having the same characteristic will be minimal, stable - so that the feature does not change over time, and be easily acquired - in order to provide convenience to the user, and prevent misrepresentation of the feature. Fingerprint recognition is the oldest method of biometric identification. In those time the fingerprint identification technique was used, with the name as actyloscopy[8]. The fingerprint is composed of ridges (lines across fingerprints) and valleys (spaces between ridges).The pattern of fingerprint is unique for each individual and it is immutable there are six stages involved in fingerprint cryptosystem as show in fig: 2.

A sensor takes a mathematical snapshot of the user's unique pattern, which is then saved in a fingerprint database. A fingerprint enhancement algorithm (that uses Gabor filters as band-pass filters to remove the noise and preserve true ridge/valley structures) is included in the minutiae extraction module to ensure that the performance of the system is not affected by variations in quality of fingerprint images. The continuously changing directions of the ridges constitute an oriented texture, possessing different spatial frequency, orientation, or phase; and hence, by decomposing the image in several spatial frequency and orientation channels fingerprints can be discriminated or matched. In this work we are using minutiae based matching with the ROI area concept, one of the main difficulties in the minutiae-based approach is that it is very difficult to reliably extract minutiae in a poor quality fingerprint image. So image enhancement is also done by FFT based techniques .as show in fig.3

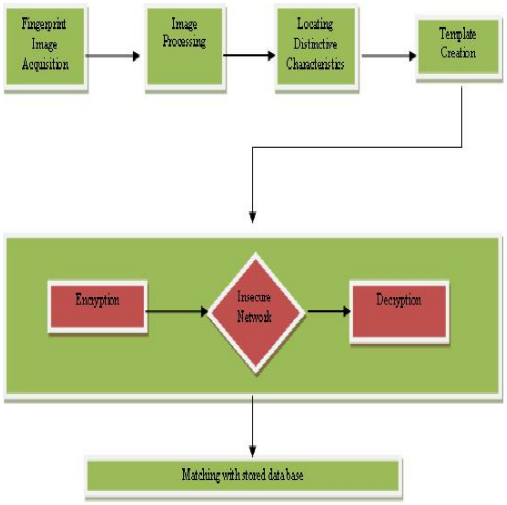

Fig: 2 Biometric Cryptosystem

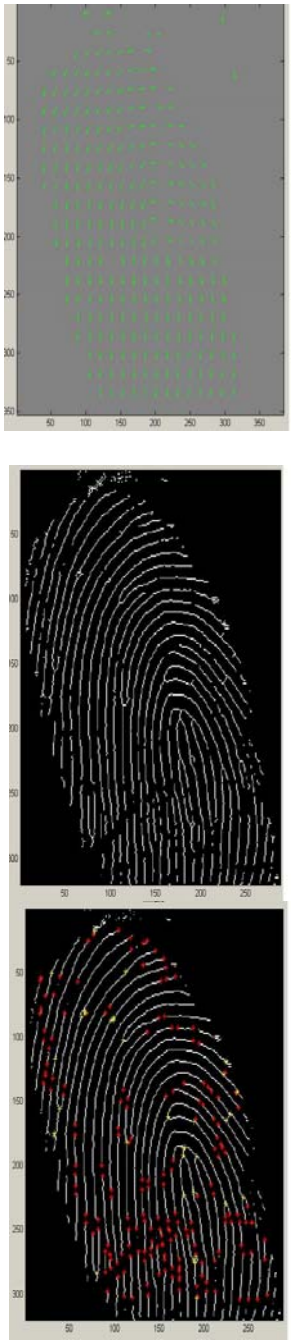

Fig.3 different processing steps for an fingerprint

3.RSA

The RSA cryptosystem is one of the well known public-key cryptosystem that offers both encryption and digital signatures (authentication). The RSA cryptosystem is the de facto standard for public-key encryption and signature worldwide. It is implemented in the most popular security products and protocols in use today, and can be seen as one of the basis for secure communication in the Internet. Its underlying function and properties have been extensively studied by mathematicians and security professionals for more than a quarter of a century. While a number of attacks have been devised during this period, exploiting special properties of the RSA function as well as details in particular implementations, it has stood up well over the years and its security has never been put into doubt. No devastating attack has ever been found and most problems appear to be the result of misuse of the system, bad choice of parameters or flaws in implementations. In fact, years of research have probably increased the trust the security community has on RSA, and we have every reason to believe that it will remain the most used public-key algorithm for years to come. [10][11][12].

For a survey of attacks on the RSA cryptosystem [10] of course, there are also attacks that aim not at the cryptosystem itself but at a given unsecure implementation of the system. These do not count as ‘‘breaking’’ the RSA system, because it is not any weakness in the RSA algorithm that is exploited, but rather a weakness in a specific implementation. RSA encryption and digital signature algorithm is considered secure if keys are 1024 - 4096 bits long [12].

The public key in this cryptosystem consists of the value **n**, which is called the modulus, and the value **e**, which is called the public exponent. The private key consists of the modulus **n** and the value **d**, which is called the private exponent. An RSA public-key / private-key pair can be generated by the following steps:

1. Generate a pair of large, random prime’s **p** and **q**

2. Compute the modulus **n** as **n** = **p×q**.

3. Select an odd public exponent e between 3 and n-1 that is relatively prime to **p-1** and **q-1**.

4. Compute the private exponent **d** from **e**, **p** and **q**.

5. Output **(n, e)** as the public key and **(n, d)** as the private key.

The encryption operation in the RSA cryptosystem is exponentiation to the **e**th power modulo **n**:

c = ENCRYPT (**m**) = **m×e** mod **n**.

The input **m** is the message; the output **c** is the resulting cipher text. In practice, the message **m** is typically some kind of appropriately formatted key to be shared. The actual message is encrypted with the shared key using a traditional encryption algorithm. This construction makes it possible to encrypt a message of any length with only one exponentiation. The decryption operation is exponentiation to the **d**th power modulo **n**:

m = DECRYPT (**c**) = **c×d** mod **n**.

The relationship between the exponent’s **e** and **d** ensures that encryption and decryption are inverses, so

that the decryption operation recovers the original message **m**. Without the private key **(n, d)** (or equivalently the prime factors **p** and **q**), it's difficult to recover **m** from **c**. Consequently, **n** and **e** can be made public without compromising security, which is the basic requirement for a public-key cryptosystem.

Sensor Type	Image Size	Size of Set	Resolution
Optical sensor "TouchViewII" by Identix	388x34 (142 k pixels)	10 users x 8 fingerprints per user	500 dpi

4. BLIND AUTHENTICATION

In the field of Information Technology the Blind Authentication is the basis for a new class of authentication schemes. The main reasons for attractiveness of blind authentication are the fact that the authentication protocol can run over public networks and provide Non-repudiable identity verification. The encryption also provides template protection, the ability to revoke enrolled templates, and alleviates the concerns on privacy in widespread use of biometrics. The proposed approach makes no restrictive assumptions on the biometric data and is hence applicable to multiple biometrics. Such a protocol has significant advantages over existing biometric cryptosystems, which use a biometric to secure a secret key, which in turn is used for authentication [4].

We define Blind Authentication as [04, 05] a Biometric Authentication Protocol that does not reveal any information about the biometric samples to the authenticating server. It also does not reveal any information regarding the classifier, employed by the server, to the user or client Blind Authentication addresses all the concerns mentioned below.

1) The ability to use strong encryption addresses template protection issues as well as privacy concerns.
2) Non-repudiable authentication can be carried out even between non trusting client and server using a trusted third party solution.
3) It provides provable protection against replay and client side attacks even if the keys of the user are compromised.
4) As the enrolled templates are encrypted using a key, one can replace any compromised template, providing revocability, while allaying concerns of being tracked. In addition, the framework is generic in the sense that this purpose. Generally false alarm is plotted on the horizontal axis whereas the correct detection rate is that it can classify any feature vector, making it applicable to multiple biometrics.

5. IMPLEMENTATION AND ANALYSIS

We have performed several experiments to evaluate the performance of RSA on biometric data template (fingerprint) using, MATLAB 7.5 and Java jdk1.6. Hardware configuration of system on which all the experiments were conducted is: - Intel Core 2 Duo processor and 100 Mbps Intranet. For the fingerprint data we have used the FVC2002 fingerprint image database.. Experimentally combined fingerprint matching and verification method was done by building a minutia extractor and a minutia matcher.

TABLE 1
Details of Biometric data base (FVC2002)

Performance evaluations:

The performance of a biometric authentication system can be measured [16] as the False Acceptance Rate (FAR) or the False Rejection Rate (FRR)) which are defined as:

FRR=Number of false rejection/Number client accesses (1) FAR= Number of false acceptance/ Number client accesses (2)

A perfect biometric authentication system would have a FRR =0 and a FAR =0 which is a little bit not achievable in reality. It is also interesting that any of the two values FRR and FAR can be reduced to an arbitrary small number, with the drawback of increasing the other value another interesting value is the Total Error Rate TER Equation (3) which is defined as:

TER = (No. of FA + No. of FR)/ total number of access (3)

The overall performance of a biometric authentication system should not be measured by the *TER* but rather by the Receiver Operation Characteristic ROC, which represents the FAR as a function of the FRR. So wherever there is a tradeoff of error types, a single performance number is inadequate to represent the capabilities of a system. Such a system has many operating points and is best represented by a performance curve. The ROC curve has been used for plotted on the vertical axis A DET curve is a modified ROC curve which is sometimes preferred for its ease of

interpretation To the using of RSA for encryption and decryption of 30 pair of fingerprint we found that the FAR and FRR the results were as follows:

No. of False Accepts = 2 (6.6%)
No. of False Rejects = 1 (3.33 %)
The total error rate = (3+1)/30=13.3%

Hence the result shows that the accuracy in this work is 86.7%.

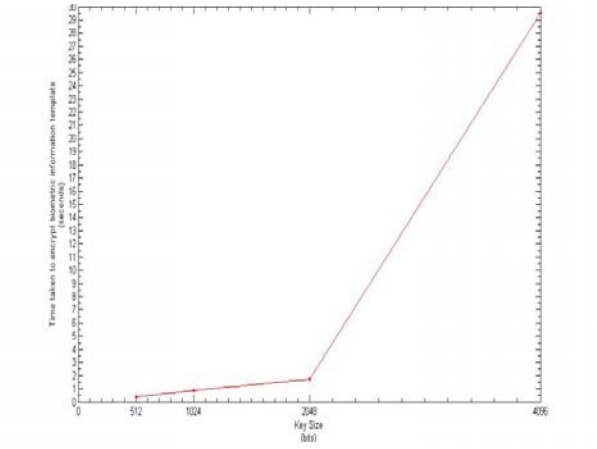

Fig.4 Graph between encrypt time and key size

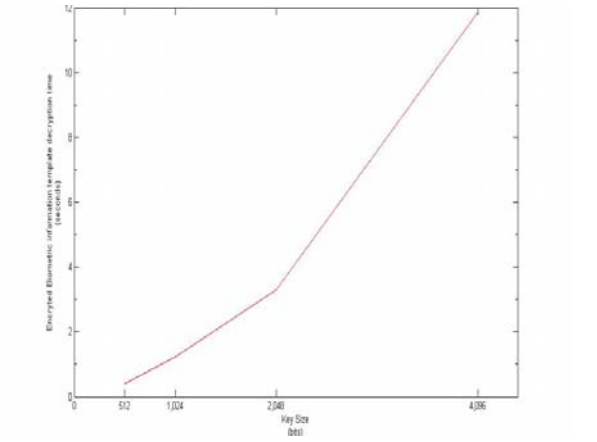

Fig5. Graph between key size and decryption time

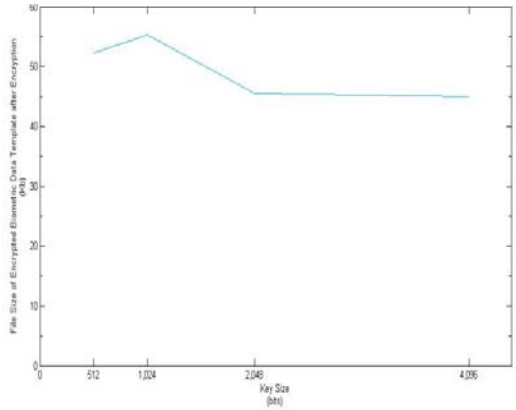

Fig5: Graph between encrypted file size and key size

5. DISCUSSION AND CONCLUSION

The result of this experiments shows that when we increase the key size then it is good for security. When the key size is increased from 2048 to 4096 bits, the data size (after encryption) will reduce. But time taken for cryptographic operations will increase. Conclusively it can be said that for secure transmission of biometric data template over an unsecured network we should increase key size, it will only affect the time to encrypt and decrypt the data without destroying the pattern of biometric data, the matching efficiency after cryptographic operation is more than 86% as show in result .When it combine the blind authentication then we will get all security assurance with good matching efficiency. The future extension to this work will be to reduce the time complexity for cryptographic purposes. To achieve this another highly secured public key encryption technique called as ECC [13][14] can be used. If we decrease the key size then we can improve the cryptographic performance of the biometric information but again we should check data pattern to improve the matching performance for any biometric authentication system.

REFERENCES:

[1] Markus Schatten,Miroslav Baca and mirko cubrilo"towards a genral definition of biometric System",IJCSI I international journal of computer science issues, Vol.2,2009

[02] Anil K. Jain Arun Ross Umut Uludag "biometric template security: challenges and solutions",eusipco turkey September 2005

[03] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar:"Biometric Template Security" Hindawi Publishing Corporation ournal on Advances in Signal Processing Volume 2008, Article id 579416, 17pages doi:10.1155/2008/579416

[04] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar "Blind Authentication: A Secure Crypto- Biometric Verification Protocol" IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010

[05] Maneesh Upmanyu, Anoop M Namboodiri, Kannan Srinathan, C.V.Jawahar "Efficient Biometric Verification in Encrypted Domain" ICB2009 (International Conference on Biometrics) Report No: IIIT/TR/2009/194

[6] Sulochana Sonkamble, Dr. Ravindra Thool, Balwant Sonkamble,"Survey of Biometric Recognition Systems and Their Applications", Journal of Theoretical and Applied Information Technology, 2005 - 2010 JATIT

[7] Anil K. Jain, Ajay Kumar, "Biometrics of Next Generation: An Overview to Appear in Second Generation Biometrics", Springer, 2010

[8] Mary Lourde R and Dushyant Khosla, "Fingerprint Identification in Biometric Security Systems", International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010, 1793-8163.

[9] C.Lakshmi Deepika1, Dr. A Kandaswamy, C. Vimal, and B. Sathish, "Invariant Feature Extraction from Fingerprint Biometric Using Pseudo Zernike Moments", Proceedings of the International Joint Journal Conference on Engineering and Technology (IJJCET 2010).

[10] Bon Boneh, "Twenty Years of Attacks on The RSA Cryptosystem a Survey on RSA attacks", dobo@cs.stanford.edu

[11] Burt Kaliski, " The Mathematics of the RSA Public-Key Cryptosystem", RSA Laboratories.

[12] Lorand Szollosi, Tamas Marosits and Gabor Feher "Accelerating RSA Encryption Using Random Precalculations", International Journal of Network Security, Vol.10, No.2.

[13] Nils Gura, Arun Patel, Arvinderpal Wander,Hans Eberle, Sheueling Chang Shantz "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs" Sun Microsystems Laboratories.

[14] Padma Bh, D.Chandravathi , P.Prapoorna Roja, "Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method" , (IJCSE) International Journal on Computer Science and Engineering, Vol.02,No.05,2010.

[15] www.bias.csr.unibo.it/fvc2002/download.asp

[16] A. Martin, T. K. G. Doddington, M. Ordowski, and M. Przybocki. . The DET curve in assessment of detection task performance., In Proceedings of EuroSpeech '97, volume 4, pages 1895.1898, 1997.