ISSN(ONLINE) : 2319-3069

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.70

Vol.6 Issue 2
Feb. 2014

Performance Analysis of Fingerprint Based Biometric Authentication System using RSA

Dr. Rajiv Srivastava[1], Satyendra Singh Thakur[2]
Professor & Director SIRT, Bhopal,462023, India[1]
Ph.D. Schaller, Department of CSE, Mewar University, Chhitorghar, Rajasthan, India[2]
drrajiv_sri@yahoo.com[1], satyendrathakur04@gmail.com[2]

Abstract

Biometric information offers a reliable and secure solution to the problem of user authentication but, biometric systems themselves are vulnerable to a number of attacks. It is needed to secure firstly the biometric information, The available biometric template protection schemes are not yet sufficiently mature for large scale deployment; they do not meet the requirements of diversity, revocability, security, and high-recognition performance. Cryptography is one of the techniques to secure biometric information but the implementation of cryptographic systems presents several requirements and challenges. for example the performance of algorithm often crucially, and guaranteeing security is a formidable change, one needs encryption algorithms to run at the transmission rates of the communication links at the speed that are achieve through to designing a cryptographic algorithm . In this work the main focus is on the data pattern, so that we can improve the matching performance after cryptographic operation with good security assurance and channel efficiency.

Keywords: *Biometric Security, Biometric Template, Channel efficiency, Bio-cryptosystem, template privacy.*

1. Introduction

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, iris, 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. Biometrics provides security benefits across the spectrum, from IT vendors to end users, and from security system developers to security system users [1][2]. 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 times the fingerprint identification technique was used, with the name as actyloscopy [3]. Biometrics-based

authentication systems that use physiological and/or these advantages of biometric systems over traditional systems, there are many unresolved issues associated with biometric authentication system. For example, how secure are biometric systems against attacks? How can we guarantee the integrity of biometric templates? How can we use biometric components in traditional access control frameworks? How can we combine cryptography with biometrics to increase overall system security? What will be the matching performance after cryptographic operation? In this work the main focus is on the data pattern, so that we can improve the matching performance after cryptographic operation with good security assurance and channel efficiency.

2. Literature Review

2.1 Biometric Information

Biometric authentication relies on any automatically measurable physical characteristic or personal trait that is distinctive to an individual for a biological measurement to qualify as a biometric it should fulfill the following desirable property [4]:

- Universality: Every person should have the characteristic.
- Uniqueness: No two people should be the same in terms of the characteristic, i.e. it should be distinct.
- Permanence: The characteristic should not change over time.
- Robustness: The characteristic can be measured consistently.

2.2 Biometric Authentication Systems

Looking at biometric systems in a more general way will reveal certain things all biometric-based authentication systems [5] [6] have in common. In general such systems work in two modes:

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.70
Vol.6 Issue 2
Feb. 2014
ISSN(ONLINE) : 2319-3069

2.2.1 Enrollment mode: In this mode biometric user data is acquired. This is mostly done with some type of biometric reader. Afterwards the gathered information is stored in a database where it is labeled with a user identity (e.g. name, identification number) to facilitate authentication.

2.2.2 Authentication mode: Again biometric user data is acquired first and used by the system to either verify the users claimed identity or to identify who the user is. While identification involves the process of comparing the user's biometric data against all users in the database, the process of verification compares the biometric data against only those entries in the database which are corresponding to the users claimed identity.

In general one can consider the verification of the identity of a person a two-class problem: either the person is who he/she claims to be (client) or the person fails to be the one he/she claims to be impostor).So we are basically dealing with a binary-decision scheme where we either accept or reject a person. Simple biometric systems usually consist of the following four components as shows in fig 2.1:

Sensor modules: This module acquires biometric user data. Examples of sensor modules would be a retina-scanner or a fingerprint sensor.

Feature extraction modules: This module is responsible for extracting feature values of a biometric trait. If hand geometry would be used as a biometric trait then feature values would include width of fingers at various locations, width of the palm, thickness of the palm, length of fingers etc.

Matching modules: The matching modules compare the acquired biometric features against those stored in a database.

Decision-making modules: The user's identity is either established or a claimed identity is accepted or rejected. This is done based on the results of the matching modules.

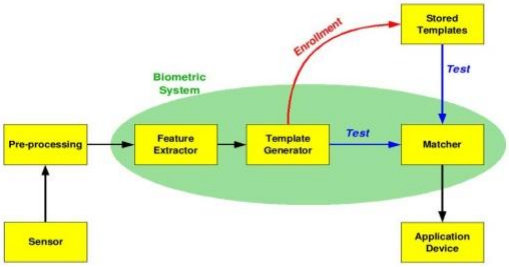

Fig.1 Biometric Authentication system

2.3 Performance Evaluation for Biometric Authentication System: Since we are dealing with a binary decision scheme it is obvious that the decision-making module can make two kinds of errors [7]. The errors, which can be made in the process of verification, are called:

False Rejection (FR) : when an actual client gets identified as an impostor.

False Acceptance (FA): when an actual impostor gets identified as a client.

The performance of a biometric authentication system can be measured as the False Acceptance Rate (FAR) equation (2), or the False Rejection Rate (FRR) equation (1) 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 this purpose. Generally false alarm is plotted on the horizontal axis whereas the correct detection rate is plotted on the vertical axis.

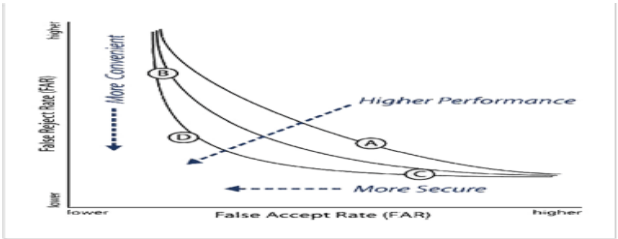

Fig.2 The Security/Convenience Trade-Off

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.70
Vol.6 Issue 2
Feb. 2014
ISSN(ONLINE) : 2319-3069

2.4. Security Enhancement of Biometrics by Combination with Cryptography

The biometric characteristics that have been widely used in various applications are human face, iris, retina, hand geometry, signature, voice etc. Each biometric characteristic have its merits and demerits, and the choice of implementation is based on the type of application. No single biometric is expected to meet all the essential requirements. Some important requirements of biometrics are acceptability, performance, and accuracy. The properties of biometric characteristics and the requirements of applications determine the match between the specific biometric and an application [8]. Protecting biometric templates with cryptography with the

convenience of information exchange across the Internet, the storage of sensitive data on open networks calls for many security concerns [9]. A straightforward method of protecting the biometric templates is to encrypt the biometric data before storage or transmission. The hard-to-invert function is commonly used in cryptographic scheme, for it is computationally impossible to find the original data from a transformed one. There are some cases in the robust hash functions that small changes in a biometric sample would yield the same hash value. Instead of storing the original biometric data *x* in the database, only its value generated by a hash function *H(x)* is stored [9]. Hence, if the biometric data is compromised or attacked, we can change for another new representation, which also provide the same authentication information. Furthermore, we could apply different hash functions on different applications. We just need to adopt another new transformation for the system if the biometric template is compromised. Authentication systems that are based on password or tokens (ID card) are not able to meet strict security performance requirements for a number of modern applications. These applications generally based on Internet, control financially valuable and privacy related tasks (e.g., e-commerce).

2.5 RSA a Public key Cryptosystem

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:

Step 1: Select two prime no’s **p** & **q**
Step 2: Calculate n as product of **p** & **q**, i.e. **n=pq**
Step 3: Calculate m as product of **(p-1)** & **(q-1)**
Step 4: Select any integer **e<m** such that it is co- prime to m, i.e gcd(**e,m**) =1
Step 5: Calculate d such that **de** mod **m** = 1 ,
i.e. $d = e^{-1} \bmod m$
Step 6: The public key is **{e,n}**
The private key is **{d,n}**
(Cipher text) **C** = $P^{e} \bmod \mathbf{n}$
(Plaintext) **P**= $\mathbf{C}^{\mathbf{d}} \bmod \mathbf{n}$.

3. Proposed Work

In the proposed system we analyze Performance of Fingerprint Based Biometric Authentication System**.** In spite of this work address determination of appropriate key sizes with security issues and determines the matching performance for fingerprint data using MATLAB 7.5, JDK1.6 and JCE 1.2 The work is divided in three parts, first part is data pre-processing in which the fingerprint images pre-processes and convert to the template the basic function of preprocessing is to improve the image such that it increases the chances of success for the other processes. The pre-processing techniques are actually used to enhance the contrast of the image, removal of the noise and isolating the objects of interest in the image, in second

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.70
Vol.6 Issue 2
Feb. 2014
ISSN(ONLINE) : 2319-3069

part cryptographic operation will perform and the last part show the matching efficiency. All these work shown in fig.3 the following are the steps involved in proposed work.

Step1. Take a fingerprint image from the database.

Step2. Perform image Histogram equalization is to expand the pixel value distribution of an image so it will increase the perceptional information and the visualization Effect.

Step3. Perform Fast Fourier Transformation: In this method we divide the image into small processing blocks (32 x 32 pixels) and perform the Fourier transform.

Step4. Perform image binarigation process which transforms the 8-bit Gray image to a 1-bit image with 0-value for ridges and 1-value for furrows.

Step5. Fingerprint Image Segmentation: After image enhancement the next step is fingerprint image segmentation. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image.

Step6. Block direction estimation: Here the fingerprint image is divided into blocks of size 16 x 16 pixels (W x W) after which the block direction of each block is calculated according to the algorithm:

Calculate the gradient values along x-direction ($\mathbf{g_x}$) and y-direction ($\mathbf{g_y}$) for each pixel of the block. Two Sobel filters are used to fulfill the task. For each block, use following formula to get the least Square approximation of the block direction.

$$\tan 2ß = \frac{2\,\Sigma\,\Sigma\,(g_x * g_y)}{\Sigma\,\Sigma\,(g_{x^2} - g_{y^2})}$$

For all the pixels in each block. The formula is easy to understand by regarding gradient values along x-direction and y-direction as cosine value and sine value. So the tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula.

$$\tan 2\theta = \frac{2Sin\theta\ Cos\theta}{Cos^2\theta - Sin^2\theta}$$

After finished with the estimation of each block direction, those blocks without significant information on ridges and furrows are discarded based on the following formulas:

$$E = \frac{2\Sigma\,\Sigma\,(gx * gy) + \Sigma\,\Sigma\,(g_{x^2} - g_{y^2})}{W * W * \Sigma\,\Sigma\,(g_{x^2} + g_{y^2})}$$

Step7. Perform the region of interest in the enhanced fingerprint image. In the fingerprint image, the region of interest (ROI) is the area of an image, which is important for extraction of minutiae point.

Step8. Perform Minutiae Extraction using four operations: Ridge Thinning, Minutiae Marking, False Minutiae Removal and Minutiae Representation.

Step9. Perform cryptographic (RSA) operation using JDK 1.6 and Java Cryptographic Extension.

Step10. Perform minutiae Match**:** An elastic string (x, y, θ) match algorithm is used to find number of matched minutiae pairs among $I_{1'}$ & $I_{2'}$ According to the elastic string match algorithm minutiae m_i in $I_{1'}$ and minutiae m_j in $I_{2'}$ are considered "matching," if the spatial distance (SD) between them is smaller than a given tolerance r_0 and the direction difference (DD) between them is smaller than an angular tolerance Θ_0.

SD= $\sqrt{(xi - xj)^2 + (yi - yj)^2} \leq \mathbf{r_0}$

DD= min $(|\theta i - \theta j|, 360 - |\theta i - \theta j|) \leq \Theta_0$

Let mm (.) be an indicator function that returns 1 in the case where the minutiae m_i and m_j match according to above equations.

$$mm(mi,mj) = \begin{cases} 1, \mathbf{sd(mi,mj)} \leq \mathbf{r0\ and\ dd(mi,mj)} \leq \Theta\mathbf{0} \\ \mathbf{0}\ otherwise \end{cases}$$

Now the total number of matched minutiae pair given by,

$$\text{Num (matched minutiae)} = \Sigma mm\,(mi,)$$

And final match score is given by, Match Score

$$= \frac{\text{Num (match hed minutiae)}}{Max\,(num\ of\ minutiae\ \ I_{1'}, I_{2'})}$$

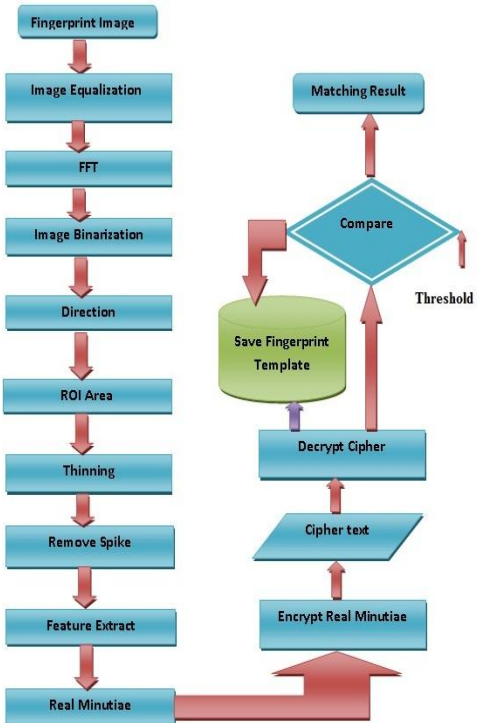

Fig.3 Praposed Model For secure authentication

Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.70
Vol.6 Issue 2
Feb. 2014
ISSN(ONLINE) : 2319-3069

4. Results

We have performed several experiments to evaluate the performance of Biometric (fingerprint) Authentication System using MATLAB 7.5 and Java JDK1.6 and JCE 1.2. 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 [13] the details of data based is given in table no. 3.1. Experimentally combined fingerprint matching and verification method was done by building a Minutiae extractor and a Minutiae matcher. To the using of RSA for encryption and decryption of 50 pair of fingerprint we found that the FAR and FRR the results were as follows:
No. of False Accepts = 2 (4%)
No. of False Rejects = 1 (2 %)
The total error rate = (4+2)/50=12%
Matching performance of this system is 88 %**.**

TABLE 1: Details of Biometric data base (FVC2002)

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

5. Conclusion and future scope

The result of these 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 88% as shown in result. The future extension to this work will be to reduce the time complexity for cryptographic purposes. To achieve this highly secured public key encryption technique called as ECC 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] Sulochana Sonkamble, Dr. Ravindra Thool, Balwant Sonkamble, "Survey of Biometric Recognition Systems and Their Applications". Journal of Theoretical and Applied Information Technology, 2010 JATIT.

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

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

[4] Anil K. Jain, Arun Ross, Sharath Pankant, "Biometrics: A Tool for Information security". IEEE transactions on information forensics and security, vol. 1,No. 2, June 2006.

[5] George Chellin Chandran .J, Dr. Rajesh. R.S., "Performance Analysis of Multimodal Biometric System Authentication" .IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.

[6] Igor Bohm, Florian Testor, "Biometric Systems". In paper for biometrics Department of Telecooperation University of Linz 4040 Linz, Austria

[7] George Chellin Chandran .J, Dr. Rajesh. R.S., "Performance Analysis of Multimodal Biometric System Authentication" .IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.

[8] K. Saraswathi, Dr. R. Balasubramaniam, "BioCryptosystems for Authentication and Network Security-A Survey". Global Journal of Computer Science and Technology Page 12 Vol. 10, Issue 3, April 2010.

[9] Jing Dong and Tieniu Tan, "Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations". In National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, 10190,Beijing,China.

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

[11] Burt Kaliski, "The Mathematics of the RSA Public-Key Cryptosystem" .In 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] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman, A. K. Jain,
"FVC2002: Second Fingerprint Verification Competition".