www.ijaret.org Volume 1, Issue II Mar. 2013
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Enhancing Security of Multibiometric Cryptosystem Using RSA

J.Rethna Virgil Jeny[1], Chanda Jagdish Jangid[2]

[1]Associate Professor, Dept. of IT, AVCOE Sangamner, Maharashtra.
Jenyvir20@yahoo.com

[2]Student of M. E. IT, AVCOE Sangamner, Maharashtra.
jangid.chanda@gmail.com

Abstract: *Single biometric cryptosystems were developed to obtain security and privacy. They are seriously affected by various attacks. Binding of multiple biometric cryptosystems (e.g., Fingerprint, Iris and face) together is termed as multibiometric cryptosystem. Nowadays Multibiometric systems are mostly used in many large-scale biometric applications (e.g., FBI-IAFIS) multibiometrics have several advantages over single biometric cryptosystem, it has low error rate. Multibiometric template may be modified by the attacker. To deal with this issue in this paper we propose a multibiometric cryptosystem which use RSA cryptography to secure multibiometric Template. Cryptography provides more security needs as well as authentication.*

Keywords: *Multibiometric, Cryptography, RSA.*

1. INTRODUCTION

In single biometric system a person to a computer system can be identified with three common ways, based on what you know, what you have, or who you are. “What you know” like passwords and PINs but they have less reliability they can be guessed, stolen, or lost. “What you have” like smart cards and e-tokens they also can be stolen. And Biometrics belong to the “who you are” class and which is subdivided into physiological and behavioral approaches. Signature recognition, voice recognition, keystroke dynamics, and gait analysis belong to behavioral biometric and fingerprints, iris, retina scans, hand, finger, face, ear geometry, hand vein, nail bed recognition, DNA and palm prints included in physical biometrics[1][2].

But the multi biometric systems are form from the fusion of two or more single biometric systems. Due to the presence of multiple independent features these systems are expected to be more reliable [3]. As compared with traditional single biometric authentication, multibiometric systems offer several advantages such as good recognition of accuracy, population coverage increased, provide greater security, more flexibility and user convenience. A multibiometric system contains multiple templates for the same user belongs to the different biometric sources. The exposure of a user’s biometric template information is one of the main drawbacks of a biometric system. However access to a user’s template can generate (a) physical spoofing, (b) replay attacks and (c) cross-matching across different databases to constantly track a person.

Multi biometric systems suffer the problem of non-universality, since multiple traits can ensure coverage of sufficient population. As well as, multibiometric systems give anti-spoofing measures by devising it difficult for an intruder at the same time spoof the multiple biometric traits of a legitimate user. What is more, unlike passwords or tokens, compromised biometric templates are not revocable. Due to this understanding, template security is necessary to protect both the privacy of the users and the unity of the biometric systems [4].

To overcome the above said problems, RSA algorithm is used for Public key Cryptography which is based on the presumed difficulty of factoring large integers. RSA confirms Encryption and Digital Signatures. It is universally used public key algorithm and gets its security from integer factorization problem. RSA is easy to understand and implement and also used in security protocols like IP data security, transport data security, email security, terminal connection security and many more. RSA apply two different keys with a mathematical relationship to each other. Their protection depends on the premise that knowing one key will not help you to figure out the other. For example, we multiply two large numbers together and form a product. But we cannot guess two original numbers from that product, or cannot guess one number if other is known. In RSA algorithm the public key and private keys are carefully generated

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

and they are used to encrypt the information [2]. Section II describes various attacks and existing work. Proposed system with RSA is presented in section III. Section IV describes conclusion and future work.

2. Existing Work

Person identification is not a new concept. Ancient Egyptians used body measurements to identify and differentiate people. The oldest implementation history of all biometric types had been hand geometry systems. In the late 1960's, Robert P. Miller issued patents from U. S. Patent office for a device that calculate hand characteristics and records unique features for comparison and identity verification in 1971. In 1985, David Sidlauskas developed and patented one hand geometry concept and the first commercial hand geometry recognition systems became available in 1986. As it is single biometric system they can be lost or stolen, attacker can get authentication by forming clone with same features. In [5] A Sharma and D Ojha enhanced the accuracy and security of Multi-biometric system using code-based cryptosystem. In addition of randomness cryptosystem also probabilistic, and give more susceptibility of template towards brute force attacks. It uses a public key cryptosystem to construct a commitment to achieve non-repudiability and authentication. The stored temple is easily hacked by attackers.

Nagar Jain and Nanda kumar in [6] define set of measures that facilitate a holistic security evaluation of template transformation techniques. They give six different measures to evaluate the security strength of template transformation schemes.

A biometric system can heighten user convenience and bolster security and it is also susceptible to various types of attacks as discussed below:

- Denial of Service (DoS): An attacker may overcome the system resources to the point where legitimate users desiring access will be refused service.
- Collusion: An individual with wide super-user privileges (such as an administrator) may intentionally modify system parameters to permit incursions by an intruder.
- Repudiation: A legalize user may access the facilities offered by an application and then claim that an intruder had circumvented the system.
- Covert acquisition: An intruder may snekily obtain the raw biometric data of a user to access the system.
- Circumvention: An intruder may gain access to the system protected by biometrics and examine sensitive data like medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the impostor can also change sensitive data.

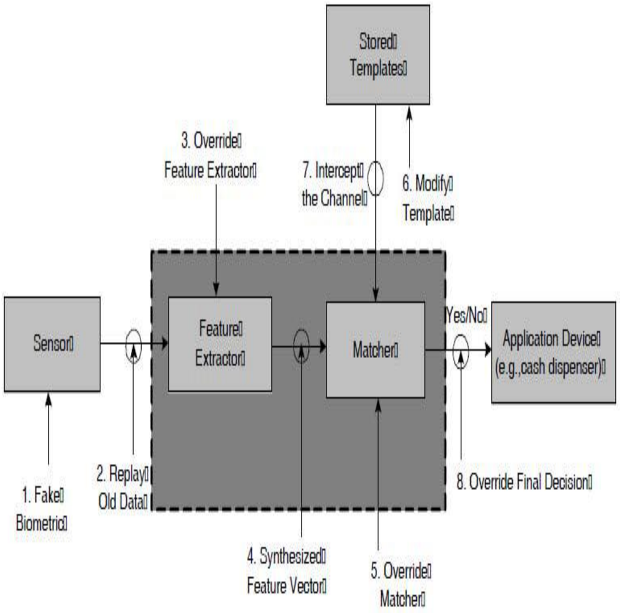

Figure 1 attack on biometrics

3. Proposed System

To secure multi biometric cryptosystem from various attacks we proposed a system consist of multibiometric module, feature extraction module, encryption module, decryption module and determination module.

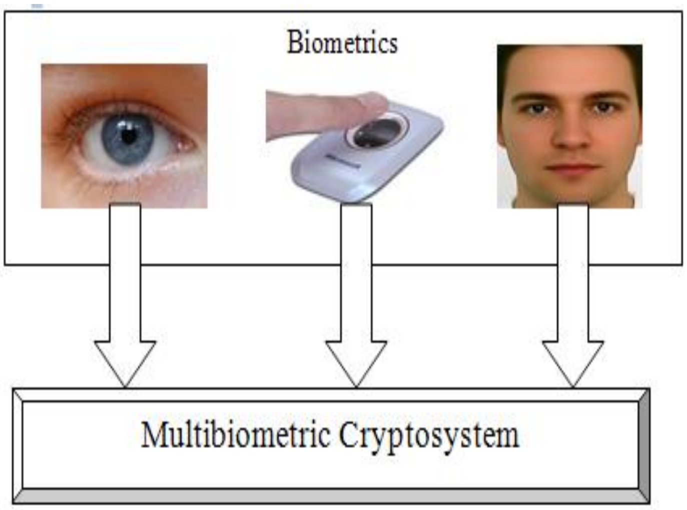

Figure.2 Multi biometric cryptosystem

Multi biometric cryptosystem is combination various biometric (e.g. face, iris, fingerprint etc) see in fig. 1. In multibiometric cryptosystem with an increasing number of templates, the speed of “a matcher” mostly decreased when those templates are given for identification. Hence, there are a couple novel directions, to overcome the disadvantages of biometrics: multibiometric systems that combine multiple biometrics for identification or verification [7].

Multi biometrics has the following advantages: like a) it improving the accuracy of the biometric verification or identification; b) it provides a certain degree of flexibility; and c) resisting spoof attacks.

3.1 Feature extraction module

Biometric feature extraction is the process in which key features of the sample biometrics are selected and enhanced. For multibiometric cryptosystem feature extraction process is done for individual biometric with different feature extraction technologies. For iris a technique for feature extraction is in [8]. A fingerprint feature extraction is located, measured and encoded ridge edgings and bifurcations in the print. Chaohong Wu gave advanced feature extraction algorithm for fingerprint in [9]. And face feature extraction is given by B. G. Bhatt1 and Z. H. Shah in [10]. There are different algorithms for feature extraction related with different biometrics [11-12].

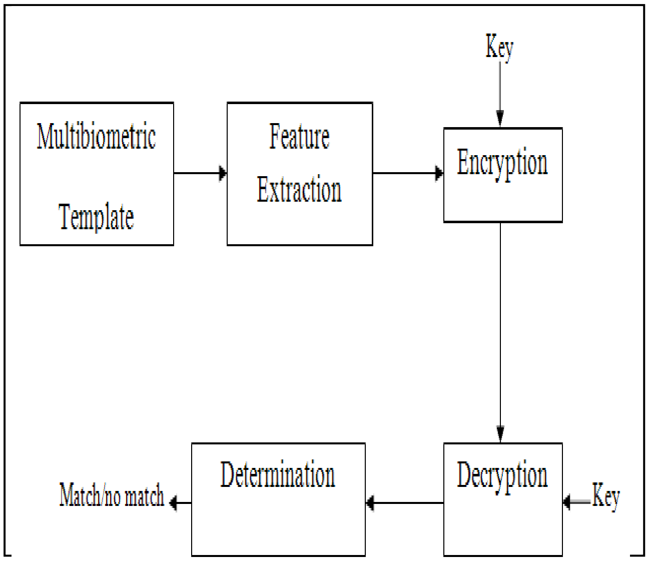

Figure 3: Multi biometric cryptosystem with RSA encryption and decryption

3.2 Encryption module

In Encryption module we encode multibiometric code by making a public key, and by using this key we send a message. For that first person selects two prime number say x and y, that person multiply xy which we called public key. Again he selects one number z which is nearly prime to(x-1) (y-1) and is a part of public key. Second person also know about value z. he has enough knowledge for encoding message A. Second person calculates value of,

$P=A^{z}(\text{mod } B)$ **(1)**

Here B=xy which we want to send.

3.3 Decryption module

In RSA decryption module we decode multibiometric code. For that we have to find a number w such that,

$zw = 1 \text{ mod}(x-1)(y-1)$ **(2)**

Then calculate, P^{w}(mod B) here B=xy that calculated value is original multibiometric code.

3.4 Determination module

In this module decrypted code show that verification or authentication is matched or not matched. It only allow authenticated person to access particular system. As it is for multiple biometrics it checks for all given input and try to provide more accurate output.

4. Conclusion And Future Work

This paper presents cryptography system with RSA algorithm to secure multibiometric template from different attacks. For RSA encryption and decryption we use same key. It is not for protecting multibiometric messages but for protecting communication parties.

Further work is to progress the security analysis by accurately modeling the biometric feature distributions.

References

[1] B. Shanthini, S. Swamynathan “A Novel Multimodal Biometric Fusion Technique for Security”, (ICIKM 2012) IPCSIT vol.45 (2012) © (2012) IACSIT Press, Singapore

[2] Pravin M.Sonsare, Shubhangi Sapkal “Stegano-CryptoSystem for Enhancing Biometric-Feature Security with RSA” IPCSIT vol.4 (2011) © (2011)

[3] Farhat Anwar, Md. Arafatur Rahman, Md. Saiful Azad “Multibiometric Systems Based Verification Technique”, ISSN 1450-216X Vol.34 No.2 (2009), pp.260-270 © EuroJournals Publishing, Inc. 2009

[4] Karthik Nandakumar and Anil K. Jain “Multibiometric Template Security Using Fuzzy Vault”, BTAS 2008

[5] Ajay Sharma , Deo Brat Ojha “ A Multi-Biometric Template Security: An Application of Code-Based Cryptosystem”, IJCIM Vol. 19. No.1 (January-April, 2011) pp 14 -24

[6] Abhishek Nagar, Karthik Nandakumar, Anil K. Jain “Biometric Template Transformation: A Security Analysis”

[7] B. Fu, S. X. Yang, J. Li, and D. Hu, “Multibiometric

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

cryptosystem: Model structure and performance analysis," IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 867–882, Dec. 2009.

[8] Rahib Hidayat Abiyev and Kemal Ihsan Kilic "Robust Feature Extraction and Iris Recognition for Biometric Personal Identification", Department of Computer Engineering, Near East University, Nicosia, North Cyprus

[9] Chaohong Wu, "Advanced Feature Extraction Algorithms for Automatic Fingerprint Recognition Systems", April 2007.

[10] Bhumika G. Bhatt, Zankhana H. Shah "Face Feature Extraction Techniques: A Survey", May 2011 B.V.M. Engineering College, V.V.Nagar,Gujarat,India

[11] Liliana Ferreira, Niklas Jakob and Iryna Gurevych "A Comparative Study of Feature Extraction Algorithms in Customer Reviews" , © 2008 IEEE DOI 10.1109/ICSC.2008.40

[12] Shailesh Kumar, Joydeep Ghosh, and Melba M. Crawford, Member, IEEE "Best-Bases Feature Extraction Algorithms for Classification of Hyperspectral Data", IEEE, VOL. 39, NO. 7, JULY 2001