Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 5, Issue, 10, pp.3121-3124, October, 2013

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

ENHANCING BIOMETRIC SECURITY WITH NEW PUBLIC KEY ALGORITHM

[1,*]Prakash Kuppuswamy and [2]Peer Mohamed Appa

[1]Department of Computer Engineering and Networks, Jazan University, KSA
[2]Department of Computer Science, Jazan University, KSA

ARTICLE INFO

Article History:
Received 17th July, 2013
Received in revised form
25th August, 2013
Accepted 05th September, 2013
Published online 23rd October, 2013

Key words:
Biometric,
Cryptography,
RSA,
Public-key cryptography,
Nlbc.

ABSTRACT

The security of bio-metric information is method of identifying a person or verifying the identity of a person based on biological characteristics. In recent years, biometric systems have assumed greater importance for information security systems. It offer reliable security, they themselves have to satisfy high security requirements to ensure authentication. Many public key algorithms such as RSA, DES and Tripple DES are concerning to construct an effective biometric security and encryption system as well. In this paper, we propose new efficient and effective mechanism for confidentiality and authentication for biometric information transmitted by using new block cipher Public key algorithm. It is an equivalent of RSA public key algorithm. It enhances the speed of encryption, decryption and authentication process. We applied this algorithm in digital signature, e-commerce and e-voting system. We bidding here, new algorithm with biometric security.

INTRODUCTION

Biometric identifiers are the distinctive, measurable characteristics used to label and describe about individuals (Jain *et al*., 2008). It is often categorized as physiological versus behavioral characteristics (Maltoni *et al*., 2003). Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition and retina. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to: typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics to describe the latter class of biometrics. Traditional biometric authentication systems store biometric templates together with the data identifying an individual in a database for later comparison. In order to authenticate an individual the biometric data presented is looked up in the database. If a record is found with biometric data that is sufficiently close to the one presented, the person is identified and hence authenticated. However, the storage of biometric data leads to considerable risks for the authentication system and raises serious concerns regarding data protection. This way of storing biometric data is often criticized as a mass storage of privacy sensitive personal data that is potentially threatened by internal or external attacks on the database (Mani Roja and Sudhir Sawarkar 2013). Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods. Biometric system can enhance user convenience and bolster security, it is also susceptible to various types of threats as discussed below (Jain *et al*., 2008; Maltoni *et al*., 2003).

Circumvention: An intruder may gain access to the system protected by biometrics and peruse sensitive data such as medical records pertaining to a legitimately enrolled user. Besides violating the privacy of the enrolled user, the impostor can also modify sensitive data.

Repudiation: A legitimate user may access the facilities offered by an application and then claim that an intruder had circumvented the system.

Covert acquisition: An intruder may surreptitiously obtain the raw biometric data of a user to access the system.

Collusion: An individual with wide super-user privileges may deliberately modify system parameters to permit incursions by an intruder.

Corresponding author: Prakash Kuppuswamy
Department of Computer Engineering & Networks, Jazan University, KSA

Coercion: An impostor may force a legitimate user to grant him access to the system.

Denial of Service (DoS): An attacker may overwhelm the system resources to the point where legitimate users desiring access will be refused service. (A.K. Jain and U. Uludag, 2003; Ratha, 2001; Pravin M. Sonsare, Shubhangi Sapkal, 2011).

A perfect image cryptosystem is required to be flexible in the security mechanism as well as be able to render high overall secure performance, and as such image security requires following characteristics (Ratha, 2001):

- The encryption system should be computationally secure. Cracking the system should require a reasonably long time thereby deterring the cracker to continue with the attack and thus barring the unauthorized user to read data.
- Encryption and decryption should be fast enough not to degrade system performance. The algorithm for encryption and decryption must be simple enough to be implemented by the user on a personal computer based platform.
- The security mechanism must be as widespread as possible and it should be flexible.
- The scheme should not lead to a large expansion of encrypted image data. This is to avoid massive storage requirements.

BACKGROUND STUDY

Pravin M. Sonsare and Shubhangi Sapkal (2011) discussed about biometric method of identification using RSA. It is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. Biometric template may be modified by attacker. To deal with this issue RSA cryptography can be used to secure Biometric Template. Cryptography and steganography provides great means for helping such security needs as well as extra layer of authentication (Pravin M. Sonsare and Shubhangi Sapkal, 2011).

S. Kavin hari, sudhan, Prof. S. Ramamoorthy (2012) proposed Double Encryption Based Secure Biometric Authentication System, In this system two different encryption algorithms have been used both in the client and server side. One is public key cryptography another one is private key cryptography. User's privacy as concern it is revealing only the identity of the user. In template protection this protocol will store the template as encrypted form. The proposed approach has no restrictions on the biometric data used and it is applicable for multiple biometrics (Kavin hari *et al*., 2012).

Dr. Manish Manoria, Ajit Kumar Shrivastava, Satyendra Singh Thakur and Debu Sinha (2011) introduced combined RSA cryptography for securely deliver biometric information to destination and it can recover the original message, without destroying the data pattern. We have explored one of the most-efficient RSA encryption algorithm and its performance with biometric information (fingerprint) using application software. This research includes the determination of appropriate key sizes and the evaluation of different matching schemes for the application of blind authentication. In our work the finger print matching performance is more than 90% with good security assurance (Manish Manoria *et al*., 2011).

Prakash Kuppuswamy, Dr. C. Chandrasekar (2011) proposed new algorithm, which is based on linear block cipher. Our goal is to build upon the new Asymmetric key algorithm based on linear block cipher or Hill cipher encryption codes of existing methods and design a set of simulation and emulation. The decryption algorithm will be there for the receiver as the private key known as k!. The concept of this new algorithm is based on modular 37 (alphabets an numerals) whereas existing algorithms are based only on modular 26 (only alphabets). We are naming this linear based algorithm as New linear block cipher or Nlbc (Prakash Kuppuswamy and Chandrasekar 2011).

Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi (2012) discussed new digital signature schemes are mostly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. This architecture is related with secure Hash Function and cryptographic algorithm. There are many other algorithms which are based on the hybrid combination of prime factorization and discrete logarithms, but different weaknesses and attacks have been developed against those algorithms. This Research paper presents a new variant of digital signature algorithm which is based on linear block cipher or Hill cipher initiate with Asymmetric algorithm (Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi 2012).

MATERIALS AND METHODS

RSA is well known public key, and use that key to send a message. The RSA method encryption using two prime number say p and q.One person multiplies two numbers and get pq which is the public key. Person also chooses another number e which must be relatively prime to $(p-1)(q-1)$. e is also part of the public key, so another person also is told the value of e. Now another person knows enough to encode a message, suppose the message is the number M. Another person calculates the value of $C = Me \pmod N$ where N=pq which is the encoding number that is to be send. The asymmetric approaches like RSA, DSA, etc. are generally known to be slower than symmetric approaches like DES, AES, etc. RSA cryptosystem can certainly eliminate several drawbacks associated with symmetric approaches. However, this cryptosystem still has some problems regarding complexity of algorithm as it works very slowly due to the fact that it is mathematically intensive and requires extra management for public keys. The new proposed linear block cipher algorithm as it works efficiently and more secure than other algorithm. In this proposed module we encode biometric code by making public key, and use that key to send a message. Our proposed algorithm based on linear block cipher, we can use different set of variables such as 2 block, 3 block, 4 block and so on. The proposed module of encryption technique mentioned below:-

Encryption technique

Step1: To encrypt acquisition image store as a digits.
Step2: Select k *k square matrix called as k.

Step3: Select any integer value say as e
Step 4: Make digits as blocks according to the k matrix. And transpose the selected block.
Step 5: Multiply blocks with selected square matrix and e value.
Step 6: Use modulation 37 with derived message. The remainder is Cipher text or decrypted message.
Announce Cipher text, e, 37 as public key, and k as private key sent to the receiver in secured channel.

Decryption technique

Step 1: Receiving Cipher digits and Private key k' and e'
Step 2: Arrange encrypted digits as r blocks.
Step 3: Calculate with encrypted using Private key and d.
Step 4: Make modulo 37 with calculated digits. The remainder value is called digits i.e encrypted image

IMPLEMENTATION

A typical biometric system is comprised of five integrated components. A sensor is used to collect the data and convert the information to a digital format. Signal processing algorithms perform quality control activities and develop the biometric template.

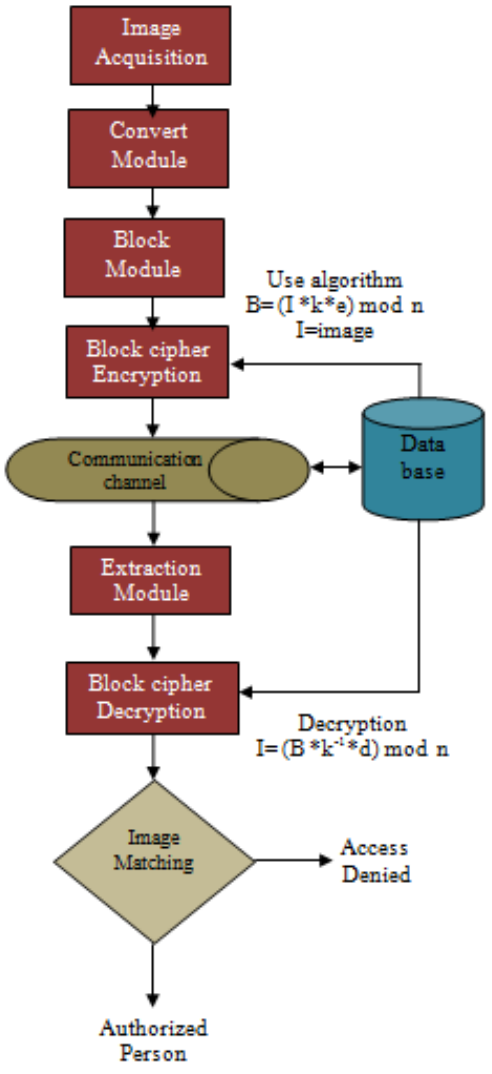

Fig. 1. Nlbc biometric system

A data storage component keeps information that new biometric templates will be compared to. A matching algorithm compares the new biometric template to one or more templates kept in data storage. Finally, a decision process uses the results from the matching component to make a system-level decision.

Image acquisition- Biometrics images acquiring by using various sensor devices. These can be sending to conversion module.

Convert Module- In this module, to hide the biometric code we use discrete cosine transformations (DCT) and transform pixel blocks to DCT coefficients and these pixel value convert as a binary digits.

Block Module-Make a binary digits into 'k' block according to the (k x k) matrix, we can make 2 block, 3 block, 4 block and so on.

Encryption algorithm- Calculate binary digital value and linear block cipher algorithm i.e. (I *k*e) mod n Here, we are assuming that the value of 'I' as a binary digit value and e is the random integer number and the value of n is 37.

Database-Database, used for storing the users bio-metric images and hidden message also for key generation algorithm. Hidden content has higher entropy.

Extraction Module -In this module, for visible representation of statistical data filters are applied to receive biometric image. To prevent loss of generality, we consider modified 2D Gabor filter. There are many algorithms to extract biometric feature in literature.

Decryption algorithm-Now in this module we want to decode biometric code. To do so, we needs to find a number d such that calculate $(B*k^{-1}*d) \bmod n$ where n=37 such that calculated value is original biometric code.

Image matching module-The decision module processes decrypted biometric code in order to either determine or verify the identity of an individual. Thus, a biometric system may be viewed as a pattern recognition system whose function is to classify a biometric signal into identification or into verification.

RESULTS

The proposed method in biometric security is the combination of the linear block cipher, Public Key. To secure transaction application, it generates tokens that are used by customer and merchant. Tokens have the different attributes like serial number, subject, hash code, issue name and public key. Customer and merchant first verify the authenticity of tokens. Then perform communication in a secure domain shown in Figure 3. Application encodes the package to transmit over the communication channel. Then, it decodes at the receiving side to achieve original data. Application also provides authentication and integrity checks to customer and merchant packages to protect against threats. The algorithm executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core.

The programs implemented using Microsoft Visual Studio 2008 (C#). It is tested with messages and with different in length of characters.

Table 1. Encryption/Decryption table

Algorithm	Key generation	Encryption (2chr)	Decryption (2chr)	Total Performance
RSA	6 seconds	4+4=8 sec	8	22 Sec
DES	10 seconds	9+9=18	18	46 Sec
3 DES	12	12+12=24	24	60 Sec
Nlbc	8	4 sec only	4	16 Sec

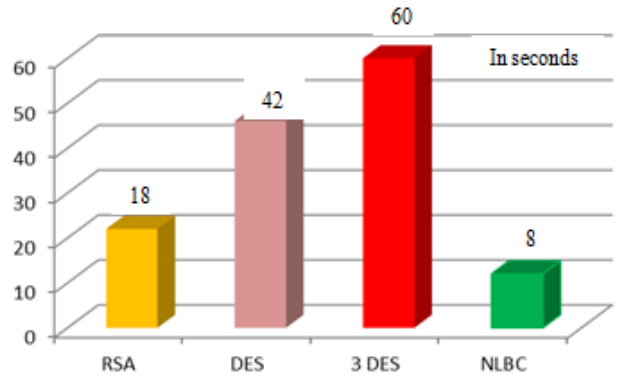

Fig. 2. Performance duration

Table 2. Comparison analysis of algorithm

	RSA	DES	3DES	New Algorithm (Nlbc)
Key length	1978-RSA Depends on number	1975 IBM 56 bit	1978 IBM 168 bit	2011 Depends on number
Rounds	1Round (for single character)	16 Round (single chr)	48 Round Single chr	1 Round 2,3,4 chars
Block size	Variable	64 bit	64 bit	Variable
Security	Normal (2)	Poor(1)	Good(3)	Good(3)

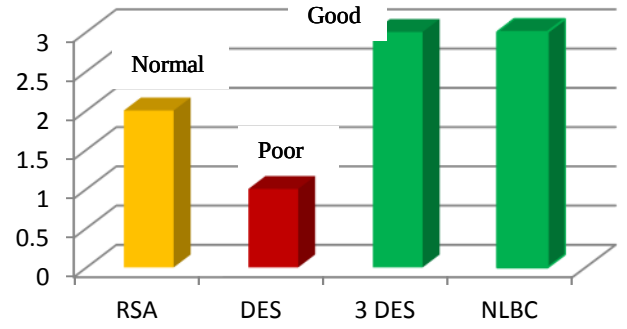

Fig. 3. Security anlysis of algorithm

Conclusion

Satisfying security requirements is one of the most important goals for biometric system security designers. In the proposed paper, it has been designed for securing biometric by using public key algorithm which is based on linear block cipher technique. The proposed method is increase the performance of biometric security rabidly. Also it will ensure the confidentiality, integrity and authentication. The experimental results shows that the proposed method is improved the interacting performance, while providing high quality of security service for desired e-commerce transactions. Several points can be concluded from the experimental results. It has been concluded that the proposed method consumes least encryption time (computing time) and others has taken maximum time in encryption for same amount of the data. It can notice that as more guards added for any information system, then more secure system is resulted. It is clear from percent of efficiency of security methods shown in the table 2. So combining more security methods with each other may increase efficiency but may increase costs.

REFERENCES

Pravin M. Sonsare, Shubhangi Sapkal, Stegano-Crypto System for Enhancing Biometric-Feature Security with RSA, International Conference on Information and Network Technology, IACSIT Press, Singapore. IPCSIT vol.4, 2011.

Kavin hari hara sudhan, S., Prof. S. Ramamoorthy, Double Encryption Based Secure Biometric Authentication System, International Journal of Engineering Trends and Technology- Volume 3. Issue1- 2012.

Jain, Anil K., Ross, Arun, "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2, 2008.

Maltoni, D., D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003

Mani Roja, M., Sudhir Sawarkar, Biometric Database Protection using Public Key Cryptography International Journal of Computer Science and Network Security, IJCSNS VOL.13 No.5, May 2013,

Jain, A.K. and U. Uludag, "Hiding biometric data," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, Nov.2003.

Ratha, N.K., J.H. Connell, and R.M. Bolle, "An Analysis of Minutiae Matching Strength," Proc. Third Int'l. Conf. Audio- and Video-Based Biometric Person Authentication, pp. 223-228, June 2001.

Pravin M. Sonsare, Shubhangi Sapkal, Stegano-Crypto System for Enhancing Biometric-Feature Security with RSA, International Conference on Information and Network Technology IACSIT Press, Singapore IPCSIT vol.4 2011.

Ratha, N., J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in Proc. Audio and Video-based Biometric Person Authentication (AVBPA), pp. 223–228, (Halmstad, Sweden), June 2001.

Dr. Manish Manoria, Ajit Kumar Shrivastava, Satyendra Singh Thakur, Debu Sinha, Exploring the Prospect of Secure Biometric Cryptosystem using RSA for Blind Authentication, International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011.

Prakash Kuppuswamy, Dr. C. Chandrasekar, Enrichment of security through cryptographic public key algorithm based on block cipher, Indian Journal of Computer Science and Engineering (IJCSE), 2011.

Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi, A New Efficient Digital Signature Scheme Algorithm based on Block cipher, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 Nov. - Dec. 2012

****