ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm

Mohammad Shahnawaz Nasir[1], Prakash Kuppuswamy [2]

Lecturer, Department of Computer Science, Jazan University, KSA[1]

Lecturer, Department of Computer Engineering & Networks, Jazan University, KSA[2]

ABSTRACT: The objective of this research proposal is to design new bio metric security protocol using hybrid encryption system. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques. The security of bio-metric information transfer through unreliable channel is challenging, because of external attacks. Therefore, Security of biometric information is essential requirement in this current trend and technology. The various protocols such an AES, DES, 3 DES are currently using biometric solution. But, the key distribution and encryption and decryption cycle is major problem. The new protocol solves make more secure and easy to encrypt and decrypt the data. Thus, in this paper, we propose new efficient and effective mechanism for confidentiality and authentication for biometric security system by using RSA and simple symmetric key algorithm. Also it examines the possibility of using a combination of biometric attributes to overcome common problems in having a biometric scheme for authentication. It also investigates possible schemes and features to deal with variations in Biometric attributes.

Keywords: Biometric, RSA, AES, DES, Triple DES, SSK, Encryption, Decryption.

I. INTRODUCTION

Cryptography is the science and art of secret writing that it cannot form without creativity actions with entrepreneurial talent [4][5][6]. It studies some mathematical techniques and provides mechanisms necessary to provide aspects related to information security like confidentiality, data integrity, entity authentication, and data origin authentication [6].

Biometric cryptography comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance [11].

Hybrid model biometric system offers several advantages compared to other symmetric security systems. First, a hybrid system can increase the reliability of the verification process. Second, a hybrid system can capture the unique, biometric characteristics of a much larger and more varied target population third, the system is much more difficult to spoof than a single biometric system [1].

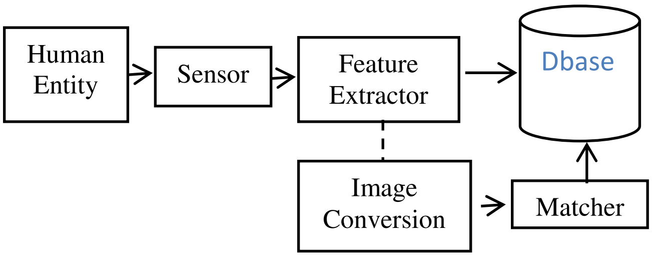

Fig. 1 Simple biometric system model

Symmetric algorithms are cryptosystems that either a secret key will be shared for both encryption and decryption [7][8]. The algorithms of symmetric cryptosystems are very strong against possible attacks, but mainly weakness of symmetric cryptosystems is brute-forcing the secret key. This characteristic creates the biggest critical act in any cryptosystem that uses symmetric algorithms which is distribution of the shared secret between the two parties like DES algorithms [8] [9].

Asymmetric algorithms use different values for encryption and decryption and do not need to share secret between two parties. Each party only has to keep a secret of its own. The earliest foundation of asymmetric algorithms known as public key cryptosystems comes from key exchange problem of symmetric algorithms. RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. The RSA cryptography algorithm using in various application in the security aspects.

II. LITERATURE REVIEW

Arun Rossa, Anil Jaina, James Reismanb (2003) discussed hybrid technique which has the entire image is taken into account while constructing the ridge feature map. Minutiae matching are used to determine the translation and rotation parameters relating the query and the template images for ridge feature map extraction. Itering and ridge feature map extraction are implemented in the frequency domain thereby speeding up the matching process. ltered query images are catched to greatly increase the one-to-many matching speed. The hybrid matcher performs better than a minutiae-based Fingerprint matching system [2].

Sonam Shukla, Pradeep Mishra (2012) in this their proposal issues associated with identity usurpation are currently at the heart of numerous concerns in our modern society. Establishing the identity of individuals is recognized as fundamental to the numerous administrative operations. Identity documents (IDs) are tools that permit the bearers to prove or confirm their identity with a high degree of certainty. Also they discuss fingerprint and face biometric systems, decision and fusion techniques used in these systems [1].

K.Kavitha1 , Dr.K.Kuppusamy (2012), they proposed facial recognition system is a computer based application for automatically identifying or verifying a person from a digital image. One of the ways to do this is by comparing the selected facial features from the image and a facial database. Some facial recognition algorithms identify faces by extracting landmarks, or features, from an image of the subject's face[10].

Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi (2012), proposed new symmetric key algorithm. They proposed a modular 37 function and select any number and calculate inverse of the selected integer using modular 37. The symmetric key distribution should be done in the secured manner. Also, they examined the performance of our new SSK algorithm with other existing symmetric key algorithm [3].

Shweta Malhotra, Chander Kant Verma(2013) proposed Multimodal biometrics, many unimodal have several problems such as noisy data, spoof attacks etc. which cause data insecure. To overcome these problems multimodal biometrics is used. Multimodal biometrics allows fusing two or more characteristics into single identification. It leads to more secure and accurate data. In this paper, we have combined two characteristics one physical and one behavioral and further a key is added to the template to make it more secure. The template is finally stored in database [4].

III. PROPOSED ALGORITHM STRUCTURE

We are proposing a new technique for best security possible using a combination of simple symmetric key algorithm and RSA asymmetric key algorithm techniques. Available cryptography protocols use potential advantages of symmetric and public cryptography. As we know, private key cryptography is strong in terms of their algorithms and public key cryptography can be used to protect symmetric algorithm by distributing its key.

A. Simple Symmetric key algorithm

Symmetric key is implemented in two ways either as a block cipher or stream cipher. Block cipher transforms a fixed length block of plaintext say a fixed size of 64 data into a block of ciphertext (encrypted text) data of the same length. We know that, whatever user ID consist of Alphabets between A to Z and numbers which is between 0-9. Here, In New symmetric key algorithm, we introduce synthetic data, which is based on the user ID. Normally the synthetic data value consists of equivalent value of alphabets and numbers. Alphabet value A is assigned as integer number 1 and B=2 ……so on. Next we consider integer value 0 assigned as 27 and 1=28……9=36 also the space value considers as an integer number 37.

1) Key generation method

(i) Select any natural number say as n
(ii) Find the Inverse of the number using modulo 37(key 1) say k.
(iii) Again select any negative number (for making secured key) n1.
(iv) Find the inverse of negative number using modulo 37(key 2) k1.

2) Encryption method

(i) Assign synthetic value for user ID
(ii) Multiply synthetic value with random selected natural number
(iii) Calculate with modulo 37
(iv) Again select random negative number and multiply with it
(v) Again calculate with modulo 37 CT = (PT* n*n1) mod 37

3) Decryption method

(i) Multiply received text with key1 & key2
(ii) Calculate with modulo 37
(iii) Remainder is Revealed Text or Plain Text PT = (CT*n^{-1}*$n1^{-1}$) mod 1

B. RSA Asymmetric key Algorithm

The RSA algorithm is based on the assumption that integer factorization is a difficult problem. This means that given a large value *n*, it is difficult to find the prime factors that make up *n*. It is most popular asymmetric key algorithm**.**

1) Key Generation

(i) Choose two very large random prime integers p and q
(ii) Compute n and φ(n):n = pq and φ(n) = (p-1)(q-1)
(iii) Choose an integer e, 1 < e < φ(n) such that: gcd(e, φ(n)) = 1(where gcd means greatest common denominator)

(iv) Compute d, $1 < d < \varphi(n)$ such that:$e*d \equiv 1 \pmod{\varphi(n)}$, the public key is (n, e) and the private key is (n, d) the values of p, q and φ(n) are private; e is the public or encryption exponent; d is the private or decryption exponent

2) Encryption

ciphertext $CT = M^e \pmod{n}$

3) Decryption

Message M= $CT^d \pmod{n}$

IV. IMPLEMENTATION

The typical setting of a hybrid biometric authentication system will be wide spread and include individual sub-systems to derive vital data from some specific user attribute. Based on registration and identification, proposed hybrid algorithm is developed. Following picture shows the block diagram biometric system, it consists of two phases, namely Registration and Authentication phases. In Registration phase, each user's image is captured and extracted. Every user identified by the unique user I.D. with their relevant feature.

Proposed approach of implementation structure described as in figure.2. The entire implementation structure has two phases: registration phase and authentication phase. In Registration phase the biometric traits are extracted and a random key is generated which is bound with the features using key binding algorithm and helper data is created. The proposed new algorithm architecture consists following phases:-

- Registration phase
  - User Identification
  - Feature extraction
  - Data conversion
  - Symmetric key encryption
  - Asymmetric key generation
  - Encryption
  - Database module

- Authentication phase
  - Cipher text
  - Decryption
  - Symmetric key decryption
  - Matching algorithm
  - Feature extraction
  - Decision module

It could be noted that the consolidate function is first applied per individual at the enrolment process. Subsequently, it is applied for every authentication session. Complex consolidate functions could also embed extra security transformations to resist attacks. For example it could add extra bits to prevent key generation from being straight-forward.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 8, October 2013

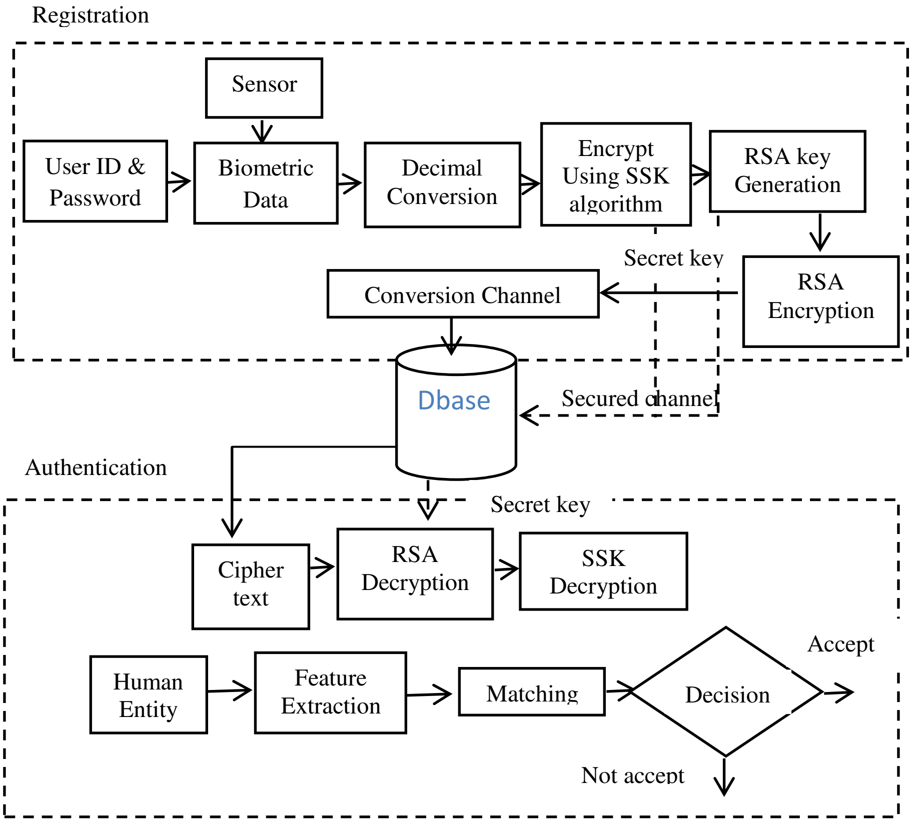

Fig. 2 Proposed hybrid architecture of RSA & SSK

V. RESULT ANALYSIS

In this paper, the popular secret key algorithms including DES, 3DES, AES, were analyzed, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were implemented in a uniform language (C++), using their standard specifications, and were tested on two different hardware platforms, to compare their performance.

Table 1 describe about comparison of algorithm performance, Here we selected different algorithm including symmetric key DES, Triple DES and Public key algorithm Advanced Encryption Standard. From the Table 1 and Figure 3, it is clear that performance speed very high comparing to AES and 3DES algorithm.

Table I
Performance analysis of algorithm

Input Size	DES	3DES	AES	New algorithm RSA+SSK
20527	24	72	39	30
36002	48	123	74	56
45911	57	158	94	78
102440				
Bytes/Sec	795/sec	290/sec	494/sec	624/sec

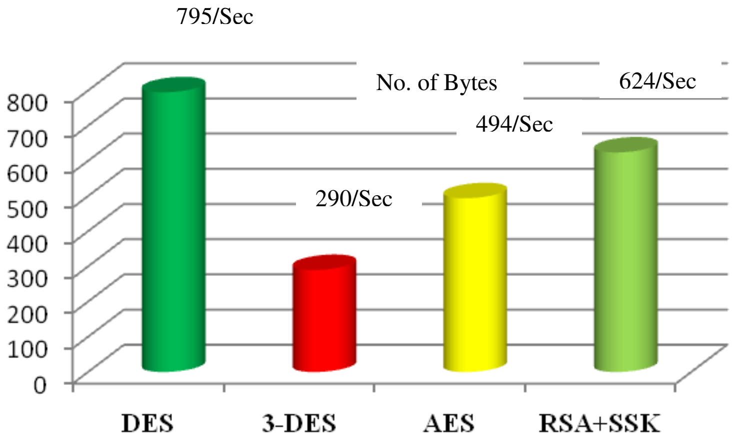

Fig. 3 Algorithm performance chart

Table 2 shown below describe about Key size in bits, We are comparing here our proposed new algorithm key size with symmetric key DES, Triple DES and Public key algorithm Advanced Encryption Standard. From the Table 2 and Figure 4, it is clear that generation of key size is just 32 bit only, So that we can perform encryption and decryption technique rapidly.

Table II
Comparison of key size

Algorithm	**Key Size (Bits)**	**Block Size (Bits)**
DES	64	64
3DES	192	64
AES	256	128
RSA+SSK	32	Flexible

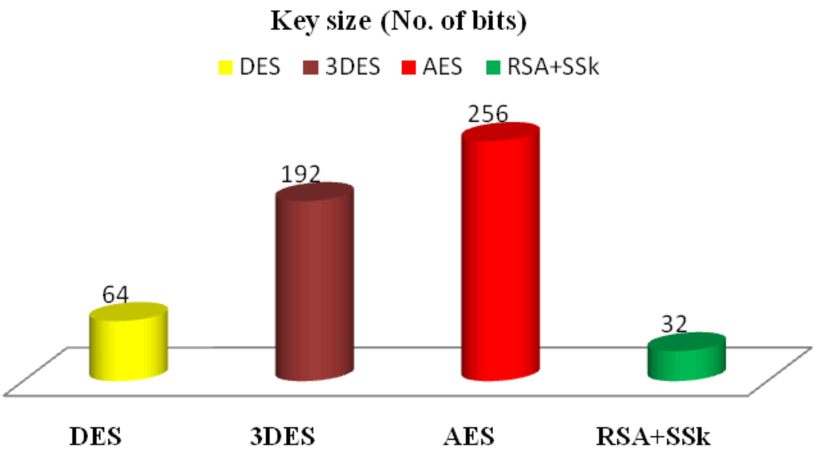

Fig. 4 Comparison of key size

The security of our algorithm is strengthened by the RSA encryption which gives very high security standard given the state of art.

VI. CONCLUSION

Satisfying security requirements is one of the most important goals for biometric system designers. In the proposed paper, it has been designed for securing biometric transaction by using most familiar RSA asymmetric key and simple symmetric key algorithm. The proposed method is increase the performance of security, key generation and rapidity. The experimental results shows that the proposed method is improved the interacting performance, while providing high quality of security service for desired biometric security system. Several points can be concluded from the experimental results. It has been concluded that the proposed method consumes least performance time (computing time) and key generation time others has taken maximum time in encryption for same amount of the data.

REFERENCE

1) Sonam Shukla,Pradeep Mishra, "A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits", International Journal of Soft Computing and Engineering (IJSCE),ISSN: 2231-2307, Volume-2, Issue-1, March 2012.

2) Arun Rossa, Anil Jaina, James Reismanb, "A hybrid Fingerprint matcher", 2003 Published by Pattern Recogninition, Elsevier Science Ltd 36 (2003) 1661 – 1673, Elsevier Publication.

3) Prakash Kuppuswamy, Dr. Saeed Q Y Al-Khalidi, "Implementation of Security through simple symmetric key algorithm based on modulo 37", International Journal of Computers & Technology www.ijctonline.com ISSN: 2277-3061 Volume 3 No. 2, OCT, 2012.

4) Shweta Malhotra, Chander Kant Verma , "A Hybrid Approach for Securing Biometric Template", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.

5) Lin, H. S., "Cryptography and Public Policy, Journal of Government Information", (1998) 135–148.

6) Alia, M.A., Yahya, A., "Public–Key Steganography Based on Matching Method", European Journal of Scientific Research,(2010) 223-231.

7) Schneier, B., “Applied Cryptography”, New York : John Wiley & Sons, 1996.

8) Kumar, S., & Wollinger T., “Fundamentals of Symmetric Cryptography, Embedded Security in Cars”, (2006) 125-143.

9) Burke, J., McDonald, J., & Austin, T., Architectural support for fast symmetric-key cryptography, Independent Component Analysis: A Tutorial Introduction. MIT Press, Cambridge, MA (2004).

10) K.Kavitha, Dr.K.Kuppusamy, “A Hybrid biometric authentication algorithm”, International Journal of Engineering Trends and Technology- Volume-3Issue3- 2012 ISSN: 2231-5381 http://www.internationaljournalssrg.org Page 311.

11) A.K. Jain, P.Flynn, A.Ross, “Handbook of Biometrics”, Springer, 2008.

12) Rosenberger, Dorizzi B, “Hybrid template update system for unimodal biometric systems”, E-ISBN :978-1-4673-1383-4, Arlington conference, Sept. 2012.

BIOGRAPHY

Mohammad Shahnawaz Nasir, Lecturer in College of Computer Science and Information System, Jazan University, Jazan, Kingdom of Saudi Arabia. He received his Master in Computer Science & Applications (MCA) and Master in Science (M.Sc.) Physics, Electronic Specializations Degrees from Aligarh Muslim University, India. Previously he worked as faculty with AOU (KSA), JMI (New-Delhi) and AMU (Aligarh, India). His work experience in Saudi Arabia also includes Web, Network, and Database Administration. His research areas are Data Mining and Biometrics.

Prakash Kuppuswamy Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar-Doctorate Degree yet to be awarded by ‘Dravidian University’. He has published 15 International Research journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.