DOI 10.29042/2018-3922-3926

Helix Vol. 8(5): 3922- 3926

Enhanced RSA Key Generation Modelling Using Fingerprint Biometric

[*1]Neha Bansal, [2] Dindayal Mahto, [3] Dilip Kumar Yadav
Department of Computer Applications, NIT Jamshedpur
Email:[1]nehab.sairam@gmail.com, [2]dindayal.mahto@gmail.com,[3]dkyadav.ca@nitjsr.ac.in

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract
The RSA is a de-facto standard for public key cryptography, which provides, data confidentiality, data integrity, and authentication. However, RSA is computationally more expensive and needs longer key lengths which are very difficult to store on smaller computing devices e.g. smartphone, smartcards, palmtop, etc. Key generation using the matrix in RSA provides a way to reduce the key storage space but generating it randomly do not achieve any security goals. Biometrics can identify each person uniquely so here the matrix is generated using fingerprints. The matrix formed using fingerprints need to be stored in the database. In this paper to protect the matrix in the database from security breaches Fuzzy Vault is used which acts like a locker to provide confidentially to the matrix.

Keywords: RSA, Biometrics, Minutiae Points, Fuzzy Vault

Introduction

Since when RSA was first developed [3] it has been the most popular and widely used public key cryptosystems. The main drawbacks of RSA [1][2] compared to other cryptosystems is that it is computationally more expensive and need longer key lengths which are very difficult to store on smaller computing devices e.g. smartcards. These drawbacks have been overcome by proposing many variants of RSA [5] e.g. Multi-prime RSA [6], Common Prime RSA [7] and Dual RSA [4] to reduce the computational cost [8][9][10][11] or to reduce the key length storage space[12][13]. Now, in this paper, the authors are working on [12] which provides a way to reduce the key storage space by generating the keys using a matrix.

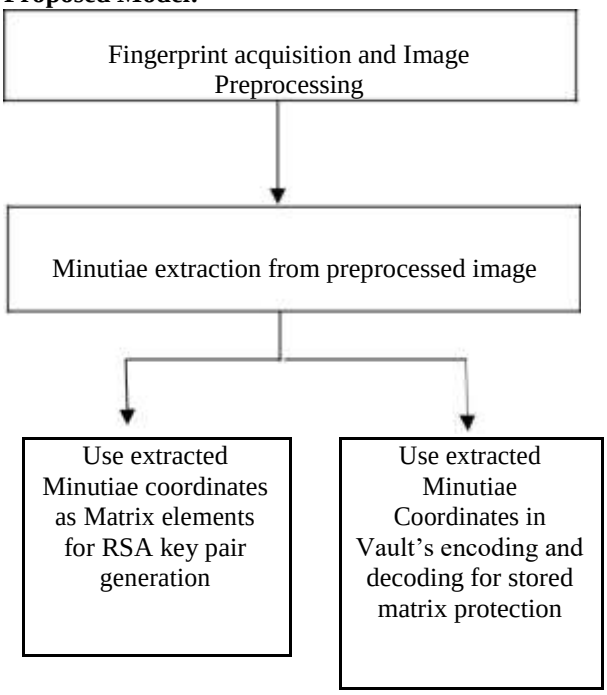
The security of any cryptographic algorithm depends upon the cryptographic keys. The keys must be strong and provide the uniqueness and randomness. Since biometrics uniquely recognize humans [15] based on physical traits like fingerprint, hand, ear, iris, and DNA or behavioral traits like talking, walking, and signature. Fingerprints are the most widely used parameter for personal identification amongst all biometrics [14].

There are many methods available to generate RSA key using a single fingerprint [20] or using a combination of two or more fingerprints [21]. In this paper, single fingerprint minutiae is used to generate the matrix elements which generate the RSA key pairs. First, the minutiae points are extracted from the fingerprint then the extracted minutiae points are used as the elements of the matrix. After the matrix is generated it must be stored so that it can be reused to regenerate the key pairs but doing so can cause the security breach. To overcome this problem a method known as the fuzzy vault is used to provide the security to the stored matrix. Fuzzy vault [19] is a crypto-biometric system which aims to secure the critical information with biometric data such as fingerprints so that only authorized user can access the data after providing the valid biometric data.[19]

The remaining part of the paper as follows:

Section 2 gives an overview of fingerprint features and minutiae extraction from the fingerprint, section 3 gives the RSA overview with key generation using matrix, section 4 gives an overview of fuzzy vault proposed by Juels and Sudan [18]. Section 5 gives implementation and conclusion of the paper.

Proposed Model:



2. Fingerprint Features

In this paper fingerprint features are extracted and used to generate the RSA key pairs. Fingerprints are the most common and widely used form of biometric Identification. What is a fingerprint means? A fingerprint is a feature pattern of a finger which is unique and remains permanent throughout one's lifetime. How is a fingerprint recognized? It is recognized using Fingerprint recognition [16] which is a method of identifying the identity of an individual based on the comparison between two fingerprints. Analysis of fingerprints to find a match requires the comparison of several fingerprint feature pattern. Let us discuss the basic fingerprint pattern.

A fingerprint is a collection of distinct numerous patterns of ridges and valleys where a ridge is a curved segment and a valley is an area between two adjacent ridges as shown in figure [1] the dark areas of the image are called ridges whereas the white area that exists between two ridges is known as valleys.

The ridge discontinuities are known as *minutiae*. Minutiae points are the important feature in the most fingerprint matching system. In case of a fingerprint identification system, we extract the minutiae features and match with the new captured fingerprint.

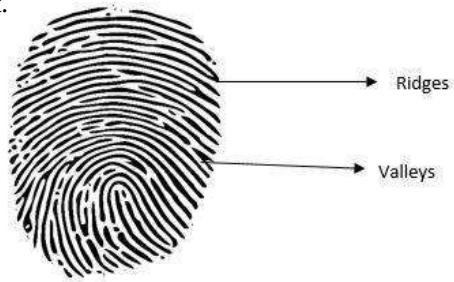


Fig. 1 Fingerprint Ridges (Dark), Valleys (White)

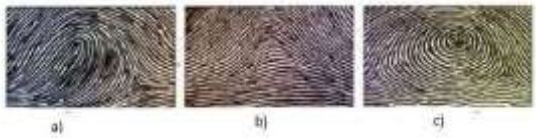


Fig. 2 Global Fingerprint Ridge Patterns. a) Loop b) Arch c) Whorl

Local level structures are called minutiae, which further classified as shown in figure 3. Local features are an important feature for fingerprint matching. A point where the ridge points end is called ridge ending.

From ridge bifurcation point, a single ridge branches from a single path and splits into two or more paths to form multiple ridges. Very small ridges are Ridge dots. Ridges that are slightly longer than dots are called Ridge Island occupying a middle space lying between two diverging ridges.

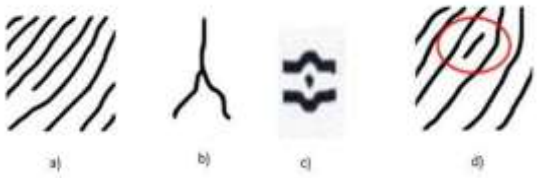


Fig. 3 Local Fingerprint Ridge Patterns. a) Ridge Ending b) Ridge Bifurcation c) Ridge Dots d) Ridge Island

There are two types of ridge pattern to detect the minutiae points:

a) Global Ridge pattern
b) Local Ridge pattern

A special pattern of ridges and valleys form the Global features. It can be used for fingerprint classification, fingerprint matching, and fingerprint alignment. It consists of many ridges to form some specific shape given below and as shown in figure 2.

Arch: From one side of the finger, the ridges enter, rise in the center to form an arc, and then exit from the other side of the finger.

Loop: From one side of the finger, the ridges enter, rise in the center to form a curve, and then exit from the same side of the finger

Whorl: Ridges form circularly on the finger around a central point.

2.1 Fingerprint acquisition and Image Preprocessing:

Preprocessing of fingerprint image means to enhance the image so that very few spurious ridges left which reduce the probability of false minutiae extraction. There are many steps for Image preprocessing as given in [17].

2.2 Minutiae extraction: The minutiae points are extracted [16]. The (x, y) coordinates of Ridge ending and ridge bifurcation are taken as minutiae points.

3. RSA Cryptosystem with Key Generation using Matrix:

Here we are referring [12] in which RSA key pairs are generated using a Matrix. The paper has various merits like it takes less space than normal RSA, It also has various demerits as given below:

1. It uses a matrix of random values which is not secure.
2. The created matrix need to store securely throughout their operational life but the paper provides no way for the security of matrix.
3. The values of private and public keys generated by the algorithm given in paper differ 32 bits only i.e. the length of a random number generated in the paper.

This paper tries to resolve the issues given above as given below:

a) Problem 1 is resolved by taking the matrix elements from features extracted by fingerprints
b) Fuzzy Vault is used to provide security to the stored matrix from security breaches to resolve problem 2.
c) Problem 3 also resolved in the modified algorithm for key generation given in 3.1.ii.

Here in this paper, we have given a modified algorithm for key generation. Encryption and decryption processes are same as given in [12].

3.1 Key generation algorithm (Modified):

This algorithm comprises of two sub-algorithm:
Create a square matrix of random numbers (i.e., 3*3) from minutiae points.

Generation of a public (P) and a private (Q) key by using the matrix obtained from the first sub-algorithm.

Generation of Square Matrix from minutiae points:

a) Put the finger on the fingerprint sensor and capture the image.
b) Apply image preprocessing and then apply the minutiae point's extraction algorithms as given in paper [16].
c) Extract the x and y coordinates of minutiae points.
d) Sort the minutiae points in ascending order and remove the duplicate points.
e) Concatenate the x and y coordinates as (x|y) taken as matrix elements.
f) Declare a matrix (KA) of size 3*3(or we can take the matrix of any order i.e. 2*2 is also capable to generate the keys pair) by using the (x|y) as matrix elements.

Generation of Square Matrix from minutiae points:
In order to generate P, Q, and N, steps are given below:

a) Takes the matrix (KA) which is obtained from Algorithm given above i.e. mat [3] [3].
b) Generate 32 bits random number R1 and add this random number to each element of the given matrix.
c) Multiply the elements in matrix with each other e.g. [a1, a2, a3] = [a1*a2*a3].
d) Generate another 32 bits random number R2 and multiply it with the resultant value obtained from (c).
e) The resultant value may not be a prime number, so the prime number can be generated by using next prime number technique which is greater than resultant value. The prime number obtained is "P".
f) In the similar manner second prime number i.e., Q is generated by using another random number R3 which is different from R2.
g) Now N=P*Q can be calculated.

4. Matrix protection using Fuzzy Vault:

The matrix (KA) needs to be stored in the database to obtain the same key each time. We provide authentication by using biometric to deduce the matrix but one of the main challenges, here is to maintain the confidentiality of the matrix in the database. So to provide the confidentiality with authentication we use fuzzy vault. Fuzzy Vault is a bio-encryption aiming to provide cryptographic security by combining biometrics and cryptography. A fuzzy vault acts like a digital locker in which we lock matrix with a set X (minutiae points are taken as elements of set X). The locker is called vault V.V can be unlocked only if a set Y (minutiae points are taken as elements of set Y) overlap largely with set X. The locking and unlocking process of vault V is given in [22].

4.1 Proposed Vault Encoding Technique:

The vault encoding scheme is given below in figure [5]:

1. Here the matrix elements (KA) are taken and concatenated(k0|k2|k3|….k8) and converted into bit form. Then the CRC of matrix elements are generated.16-bit CRC from the matrix elements is generated by dividing the matrix elements by the primitive polynomial, $CRC(a) = a16 + a15 + a2 + 1$ and the generated remainder is the required CRC. The generated CRC is appended at the end of matrix elements.
2. The first nine coordinates (x, y) of minutiae points concatenated and taken as XA from the template (T) of the fingerprint.
3. A polynomial P of degree 8 is taken which is calculated as the number of matrix elements minus one ((K)-1). Here the size of the matrix is 3*3 so K=9.
4. A polynomial (P) is generated that encodes the matrix elements (k0,k1,k2….k8) and evaluates the polynomial on all minutiae elements in the set (XA) as shown in figure[7].The resultant set is taken as set YA and is known as a set of genuine points which lies on polynomial(P).
5. Now the chaff points (X'A) are generated which do not lie on polynomial (P).
6. The union of YA and X'A forms the vault (V).

4.2 Proposed Vault Decoding Technique:

The vault decoding scheme is shown in figure [6]:

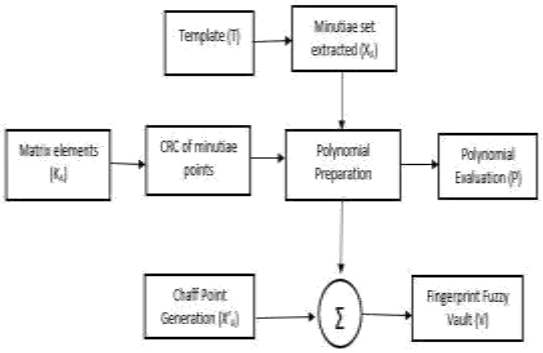


Fig. 4 Fuzzy Vault Encoding Block Diagram

1. Just like the encoding phase first, nine coordinates(x, y) of minutiae points are concatenated and taken as XB from the template (TB) of the fingerprint which may or may not be same as taken in the encoding scheme and taken as XB.
2. Only those coordinate points are selected for vault V whose value is equal or close enough to each element of XB. Fuzzy Vault (V) is taken and the possible matching points are selected and stored in the set as shown in figure [6].
3. Lagrange's Interpolation is applied. The purpose of this phase is to reconstruct all of the elements contained in *YA* to form a polynomial equation which has a degree of *8*.
4. The CRC is checked and for an authenticated person, reminder becomes zero for at least one combination of the matrix element. If at least one combination is not found, the user is an unauthenticated user and the matrix will not be released.

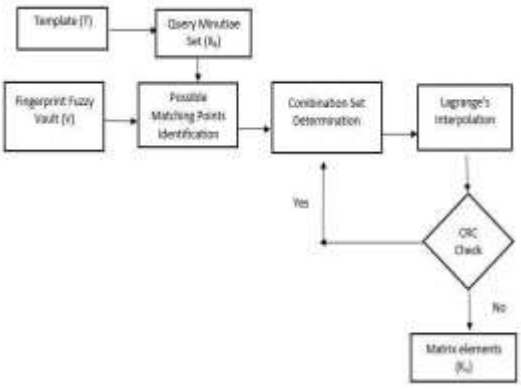


Fig. 5 Fuzzy Vault Decoding Block Diagram

Implementation

Minutiae Points are extracted from the fingerprint after preprocessing it. The extracted minutiae points are shown here:

Fig. 6 Minutiae Points Extracted

After that the minutiae points are extracted, matrix KA is formed as shown below. The matrix is used to generate a RSA key pair.

```
The Given Matrix KA of order '3' is
     2928          3635          3738
     4052          4556          5365
     5565          5975          6276
```

Comparison between RSA key generation using random matrix and enhanced RSA key generation using fingerprint biometrics based upon cryptographic security goals is given below:

Security Goals	RSA key generation using random matrix	Enhanced RSA key generation using biometrics
Key Confidentially	No	Yes
User Authentication	No	Yes
Data Integrity	No	Yes
Data Authorization	No	Yes

Conclusion

The purpose of the proposed model is to achieve cryptographic security goals i.e. Data Confidentially and User Authentication. Since the fingerprints are the most reliable method for personal identification hence we can achieve user authentication using fingerprints. Fuzzy Vault provides the confidentially to the stored matrix with the help of minutiae extracted. Random numbers are used at many levels during Keys generation to make the expected complexity of key generation high. The proposed model is very simple and can be used in small hand held devices to reduce the storage space of keys.

References

[1] M Jason Hinek ,"Low Public Exponent Partial Key and Low Private Exponent Attacks on Multi-prime RSA", A thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Master of Mathematics in

Combinatorics and Optimization, Waterloo, Ontario, Canada, 2002.

[2] M. Jason Hinek,"On the Security of Some Variants of RSA", a thesis presented to the University of Waterloo in fulfillment of the thesis requirement for the degree of Doctor of Philosophy in Computer Science Waterloo, Ontario, Canada, 2007.

[3] R. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, 21 (2), February 1978, pages 120.

[4] Sun, Hung-Min, et al. "Dual RSA and its security analysis" IEEE Transactions on Information Theory 53.8 (2007): 2922-2933.

[5] D. Boneh and H. Shacham, "Fast variants of RSA," Crypto Bytes, vol.5, no. 1, pp. 1–9, 2002.

[6] Kumar R. Santosh, Challa Narasimham, and Pallam Shetty," Cryptanalysis of Multi-prime RSA with Two Decryption Exponents", International Journal of Electronics and Information Engineering, Vol.4, No.1, PP.40-44, Mar. 2016.

[7] M. J. Hinek, "Another look at small RSA exponents," in *Topics in Cryptology-CT-RSA 2006*, ser. Lecture Notes in Computer Science, D. Point cheval, Ed. New York: Springer, 2006, vol. 3860, pp. 82–98.

[8] G. Qiao and K.-Y. Lam, "RSA signature algorithm for microcontroller implementation," in Smart Card Research and Applications, CARDIS'98, ser. Lecture Notes in Computer Sci., J.-J. Quisquater and B. Schneier, Eds. New York: Springer, 1998, vol. 1820, pp. 353–356.

[9] H.-M. Sun and C.-T.Yang, "RSA with balanced short exponents and its application to entity authentication," in Public Key Cryptology—PKC 2005, Lecture Notes in Computer Science. New York: Springer, 2005, vol. 3386, pp. 199–215.

[10] H.-M. Sun, W.-C. Yang, and C.-S. Laih, "On the design of RSA with short secret exponent," in Advances in Cryptology— ASIACRYPT'99, ser. Lecture Notes in Computer Science, K.-Y. Lam, E. Okamoto, and C. Xing, Eds. Berlin: Springer, 1999, vol. 1716, pp. 150–164.

[11] S. A. Vanstone, and R. J. Zuccherato, "Short RSA keys and their generation," J. Cryptol., vol. 8, no. 2, pp. 101–114, March 1995.

[12] Prerna Verma, Dindayal Mahto, Sudhanshu Kumar Jha and Dilip Kumar Yadav, "Efficient RSA Cryptosystem with Key Generation using Matrix", published in International Journal of Control Theory and Applications, ISSN: 0974-5572, Volume 10, Number 13, 2017.

[13] A.K. Lenstra, "Generating RSA moduli with a predetermined portion," in Advances in Cryptology—ASIACRYPT'98, ser. Lecture Notes in Computer Science, K. Ohta and D. Pei, Eds. New York: Springer, 1998, vol. 1514, pp. 1–10.

[14] Rupinder Saini, Narinder Rana," Comparison of Various Biometric Methods", International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I (March 2014).

[15] S. Prabhakar, A. Ross, A.K. Jain," An introduction to biometric recognition", Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[16] Roli Bansal, Priti Sehgal, Punam Bedi," Minutiae Extraction from Fingerprint Images - a Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011 ISSN (Online): 1694-0814.

[17] M. Usman Akram, Shoab Ahmed Khan" Fingerprint image: pre- and post-processing", International Journal of Biometrics January 2008.

[18] Ari Juels and Madhu Sudan, "A Fuzzy Vault Scheme" published in Designs, Codes and Cryptography, Springer, 2006.

[19] Karthik Nandakumar, Anil K. Jain, and Sharath Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, December 2007.

[20] Mofeed Turky Rashid, Huda Ameer Zaki,"RSA Cryptographic Key Generation Using Fingerprint Minutiae", Iraqi Commission for Computers & Informatics (ICCI) Iraqi Journal for Computers and Informatics (IJCI), Vol (1) Issue (1), 2014.

[21] Sharda Singh, J. A. Laxminarayana," RSA Key Generation Using Combination of Fingerprints", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, PP 48-53.

[22] Bambang Pilu Hartato1,2, Teguh Bharata Adji1, Agus Bejo1,"A Review of Chaff Point Generation Methods for Fuzzy Vault Scheme", 1st International Conference on Information Technology, Electrical Engineering , Yogyakarta, Indonesia,2016

