*Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST*

# Two Level Fingerprint Privacy using RSA

Bhagya P[1] and Dr. Mahesh P.K[2]
[1-2]Don Bosco Institute of Technology/ECE, Bengaluru, India
Email: bhagya2k@gmail.com, mahesh24pk@gmail.com

***Abstract*—Authentication scheme based on Biometric is proposed to enhance security for storing information on the server. One of the biometric feature most widely used is fingerprint. A novel method to protect fingerprint privacy is to generate a virtual identity. Extracting the features from the two fingerprints given by the user, virtual identity is generated. Cryptography is applied to generate key using RSA algorithm. The generated key is used for encrypting the data that has to be stored on the server. For retrieving the file/data from the server, the key is generated by applying the RSA algorithm to fingerprint and filename given by the user. If the generated key matches with the key stored on the server, then the file/data will be decrypted with the key and used by the user. A secured way of encrypting and decrypting a data can be achieved by using Biometric based authentication scheme.**

***Index Terms*— Biometrics, Fingerprint Verification, Minutiae points, RSA.**

## I. INTRODUCTION

Cryptography with biometric are Biometric cryptosystem have strengths from both the fields. Cryptography provides high and adjustable security levels, biometrics bring in non-repudiation and eliminates the need to remember the passwords or carried tokens etc. whereas biometrics provide non-repudiation and expediency, standard cryptography provide flexible level of security and it not able to just for authentication but also for encryption. Biometric based key release refers to authentication to release a cryptographic key.

Biometric system recognizes a person through a pattern recognition system through their physical and or behavioural characteristic of a person. Fingerprints are one of many forms of Biometrics used to identify an individual and verify their identity. A fingerprint is classified based is uniquely identified based on the Local ridge and furrow minute details features and on only the Global ridge and furrow structures features (ridge endings and bifurcations, also known as minutiae, see Fig .1).

Fig. 1: Fingerprint image

*Grenze ID: 02.ICCTEST.2017.1.94*

Cryptography is the study of hiding information. Cryptography mainly deals with encryption & Decryption, where Encryption is the process of converting plain text, into cipher text .and Decryption is the reverse process, converting cipher text to plaintext. Cipher is generated by algorithm and each instance, by a key. Key will be known to the communicating persons only. Keys are made complex in such a way that the hackers cannot access the key information present in that. Cipher text are more secured, even if a hacker obtains the cipher image, he/she can't extract full information because the "key "information will be provided only to communicants. Data to be transmitted is considered as plain text. Most of algorithms provide high security of data but have the main disadvantage of key management problem. By using the cryptography algorithm along with biometric system provides more Security and overcomes the problem of key management.

Methods adopted to secure a key with a biometric: a) Remote template matching and key storage (Biometric image is compared with corresponding template) and b) Data is derived directly from a biometric fingerprint image.

## II. RELATED WORKS

In [3], to encrypt the image and transmit over the covert channel arithmetic encoding technique is used with DES. The arithmetic encoding provides coded data values in between interval of 0 and 1. That gives security and compression over the input files[3,4].The Arithmetic Coding is efficient, for providing both security and compression simultaneously is growing more important and is given the increasing ubiquity of compressed Bio-metric files in host applications of Defence, Internet and the common desire to provide security in association with these files. In [5] the RSA algorithm is used with some modifications which enhance the speed of RSA algorithm is called RSA-1 and the algorithm which provide security more than RSA algorithm is called RSA-2 algorithm which can enhance confidentiality to the sender. The problem of RSA algorithm is solved [5] through RSA-2 algorithm, it used the numbers instead of character in the plain text are represented by encoding scheme which can be able to represent special character. In case of character and number the intruder can easily know the cipher text and author can replaced it by the special symbols with the help of decimal value into their respective ASCII code character. The RSA-2 algorithm increased the speed of encryption and decryption with enhancement of security also due to special symbol. Uludag et al. [7] present their implementation of fuzzy vault, operating on the fingerprint minutiae features. They extend [7] where chaff points generated according to minutiae points and protected secret, which is clear in secret check block (cyclic redundancy check encoding), and chaff generation block. [6] differ from [2] work's in decoding implementation does not include any correction scheme, since there are serious difficulties to achieve error-correction with biometric data. Developing the necessary polynomial reconstruction via error-correction has not been demonstrated in the literature. Fuzzy vault for fingerprint decodes many candidate secrets .To identify which candidate is valid a Cyclic Redundancy Check (CRC) is used. CRC is commonly used in error correction.

Geometric hashing technique to perform alignment in a minutiae-based fingerprint fuzzy vault [8] but still has the problem of limited security. That is, the maximum number of hiding points (chaff points) for hiding the real fingerprint minutiae is limited by the size of the fingerprint sensor meanwhile the size of the fingerprint images captured and the possible degradation of the verification accuracy caused by the added chaff minutiae.

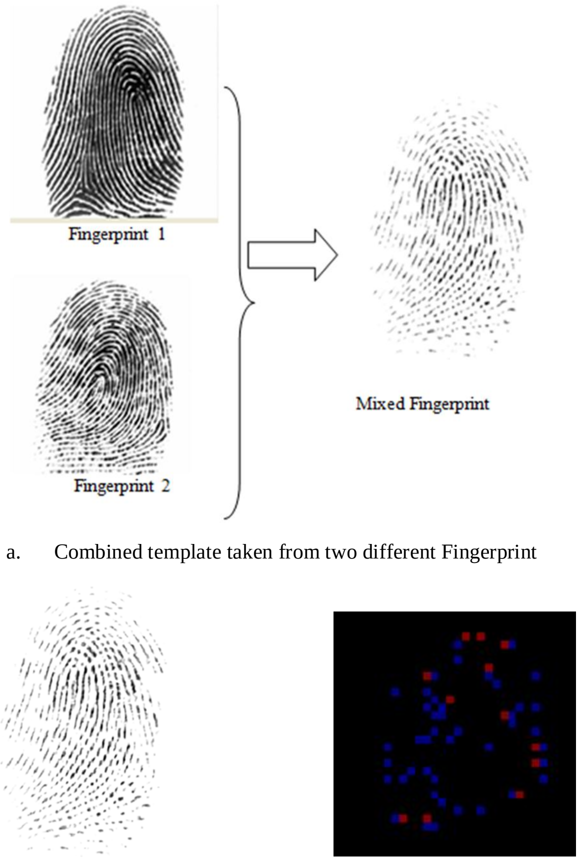
## III. PROPOSED METHOD

In this proposed method fingerprint privacy is protected by using fingerprint matching process. Emrollment and authentication phases are used in fingerprint matching process. During enrolment phase, the fingerprints from two different fingers are taken. The minutiae points from one finger, orientation and reference points from the other finger are combined to form a combine minutiae template. This generated combined minutiae template is then stored in the database, RSA is then applied to this extracted template to generate a key[5]. Using this generated key, the file to be sent to the server, is then encrypted.

While retrieving a file from the server, the user has to give his two fingerprints, and file name and again by applying RSA keys are generated. The server gets the filename and the key. If the key matches with the one stored in the server's database. It gives the file to the client. The client would then decrypt the file using the private key generated from the combined minutiae template. Thus the file is retrieved in the secure manner.

### *A. Extracting Minutiae Points from Fingerprint*

For extracting minutiae points from fingerprint, a three level approach is broadly used by researchers. These levels



a. Combined template taken from two different Fingerprint

b. Fingerprint

c. Minutiae points

Fig 2: Combined Minutiae template generated from two different Fingerprint

are listed as follows:

- Pre-processing.
- ROI selection.
- Minutia extraction.

For the fingerprint image pre-processing, Histogram Equalization and FFT are used to do image enhancement. Binarization is applied on the fingerprint image. Locally adaptive threshold method is used for this process. Then Morphological operations are used to extract Region of Interest [ROI]. In a morphological operation, the value of each pixel in the output image is based on a comparison of the equivalent pixel in the input image with its neighbors. By selecting the size and shape of the neighbourhood, we can construct a morphological operation that is sensitive to specific shapes in the input image.

### *B. Two stage Fingerprint matching process.*

Matching process consists of following steps.
-Query minutiae determination: the local features are extracted for minutiae points.
-Matching score calculation: matching score is calculated, if the matched value is under the threshold, then the person is said to be authenticated for that system.
-Fingerprint reconstruction: once a combined minutiae template is generated, it is reconstructed to form a new fingerprint, so that the attackers cannot identify the technique used.
-Protecting the database: if a combined fingerprint is attacked or stolen by the attacker from the data base, the attacker could make a fake fingerprint from the image and make an attack. For this purpose, a database is needed to be protected by using encryption. RSA is used to protect the combined minutiae template in the database.

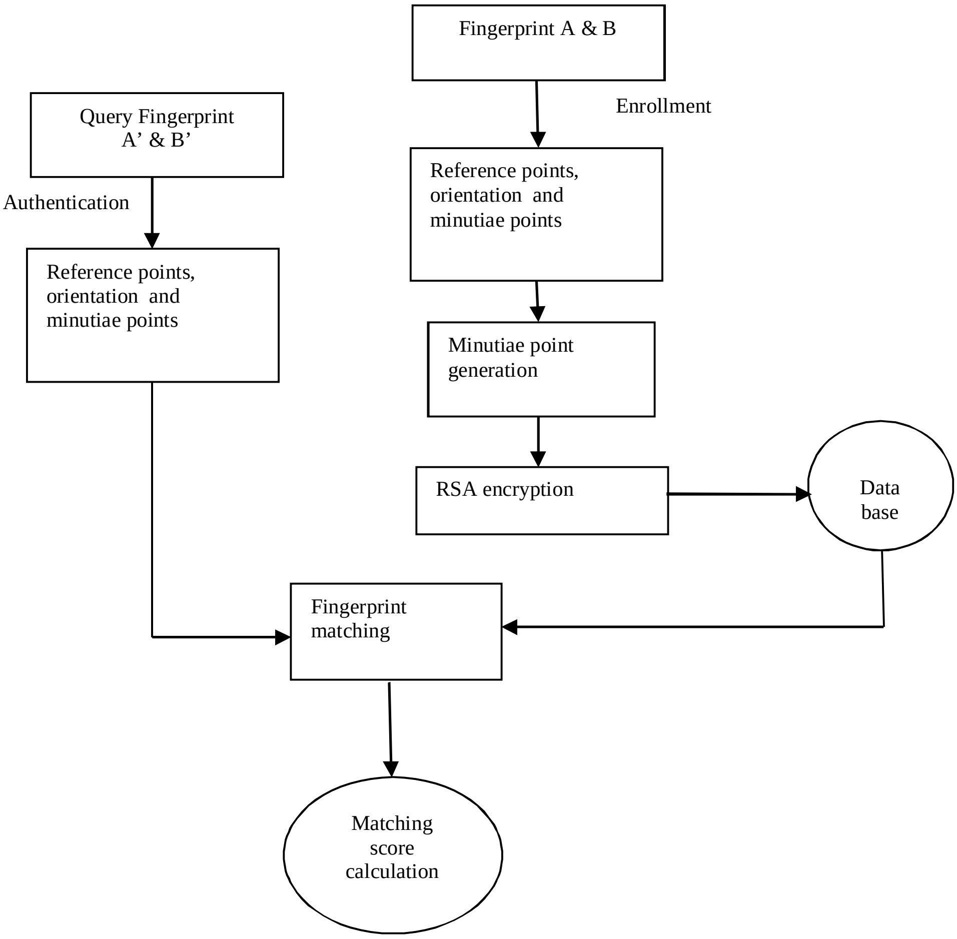

Fingerprint A & B
Enrollment
Query Fingerprint A' & B'
Authentication
Reference points, orientation and minutiae points
Reference points, orientation and minutiae points
Minutiae point generation
RSA encryption
Data base
Fingerprint matching
Matching score calculation

Fig 3 : Proposed fingerprint privacy scheme

### *C. Key generation process*

A key is generated using the RSA algorithm. Keys are generated from the minutiae template stored in the database. These are public and private keys. The keys are generated using algorithm[1] summarizes below.

Key generation from minutiae points.
Assumptions:
Mp → Minutiae point set
Kl → key length
Np → size of minutiae point set
S → Seed value Sl –seed limit
m→ (x,y) → co ordinate of a minutiae point
Kv → Key vector

Steps:

1: The extracted minutiae points are represented as
$Mp =\{ mi\}, i=1,\dots , Np$ (1)

2: The initial key vectir is defined as follows:
$Kv=\{ai:p(xi)\}, i=1, \dots Kl$ (2)
Where $p(x) =M[i\%Np] +Mp(i+1)\%Np] +S$ (3)
$i=1,\dots,Kl$

3: Initial value of S is equal to total Number of Minutiae points. The value of S will be dynamically changed as follows:

$$S =Kv(i)\%Sl, -1<i<Kl \quad (4)$$

4: Initial key vector (Kv) is converted into a matrix Km of size Kl/2 *Kl/2 as follows:

$$Km=(aij)\ Kl/2 * Kl/2 \quad (5)$$

5: An intermediate key vector is generated as follows:

$$KIV = \{ Ki : (m(ki)) \}, i=1, .... Kl \quad (6)$$

Where m(k) =| Aij |, Aij=Km i,j : i+size, j+size, -1<i<Kl/2

Aij is the submatrix formed from the key matrix.

6: Final Key vector (Private key) formed is

Kv = 1, if KIV[i] > mean (KIV) (7)

= 0, otherwise

*D. Mapping each binary data precisely to each region*

Although no two fingerprint are similar to one another but there's a whole lot chances where the number of ridges may be equal to the number of furrows. A nxn matrix is used that precisely stores each furrows and ridges marking in the byte pattern accordingly to the scanned image of the fingerprint. This helps to recognise individual fingerprint distinctively as the data in the matrix form will have different patterns of data set. This matrix contains key vector elements from the above algorithm.

*E. Calculation of public key*

Let,

d → be the total number of 1s in the data set due to furrows in the matrix Ai,j.

e → be the total number of 0s in the data set due to ridges in the matrix Ai,j.

i,j = 1,2,3, ....Np

$$s = (d-e) \quad (8)$$

Pb →Public key vector

$$Pb=Kv *(mod(s)) * e \quad (9)$$

E → public key vector

*F. Sending file to the server for the storage*

To store a file on a server, the client need to first register to the server on the network. Registration is done by creating a unique id and password. Once it is done, the client is said to be authenticated user of the server. The steps performed are: The file to be send is then encrypted using the key generated by the RSA for the combined minutiae point template. RSA generates two keys, a public key and private key. these two keys will be stored at client's local database.

Using public key, the client encrypts the file and sends the file to the server along with the public key. The server then stores the incoming file and the public key, for a given authenticated client.

*G. Retrieving file from the server*

The client when he wants to access a file from the server, he first logon to server machine by giving his id and password and then retrieve a file from the server, he gives the filename and fingerprint. The steps performed are: RSA algorithm is applied to the minutiae template, generated from the fingerprint. If the key generated from this minutiae template, matches with the one stored in the server's database, then the match is said to be found and the client can decrypt it using its secret key. Secured file can be accessed by the user.

## IV. EXPERIMENTAL RESULTS

An experiment is conducted by taking two fingerprint. The method is implemented and tested for fingerprints.Results shows that our system identifies the most of the minutiae and orientation present in the original acquired images. Formation of combined template from minutiae image and orientation image has been successful. Also the features are properly extracted from combined template. As the features match with those stored in database the authentication system is stable.

## V. CONCLUSIONS

In this paper, a novel approach for protecting the fingerprint privacy is proposed using Biometric based authentication. During enrolment phase, two different fingerprints are taken. Minutiae and reference points from one finger and orientation and reference points from other finger are combined to form minutiae template. For this

RSA algorithm applied to generate a key using which data is encrypted. The future work include taking different fingerprints from more than different fingerprints.

## REFERENCES

[1] Sayani Chandra, SAyan Paul, Bidyutmala Saha, Sourish Mitra, " Generate an Encryption Key by using Biometric cryptosystems to secure transferring of data over a network", IOSR Journal of Computer Engineering( IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume12, Issue 1 (May –Jun 2013), P16-22.

[2] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", Proc. IEEE Int'l. Symp. Inf. Theory, A.Lapidoth and E. Teletar, Eds., pp. 408, 2002.

[3] Klein, "Foiling the cracker: A survey of, and improvements to, password security," Proceedings of the 2nd USENIX Security Workshop, pp. 5-14, Aug.1990

[4] A.J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, pp.180,1997.

[5] R. Ang, R. Safavi-Naini, L. McAven, Cancellable key based fingerprint templates," ACISP 2005, pp. 242-252.

[6] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy Vault for Fingerprints," presented at Fifth International Conference on Audio-and Video-based Biometric Person Authentication, Rye Twon, USA, 2005.

[7] U. Uludag and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data " in Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop IEEE Computer Society, 2006 pp. 163.

[8] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D.Ahn, "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault," presented at Information Security and Cryptology, Beijing, China, 2005.

[9] Aniket Kore, Shiwani Gupta, Kiran Bhandari, "Generating cryptographic keys for AES encryption from Fingerprint Biometrics", 7th International Conference on Communication, Computing and Virtualization (ICCCV), 2016, p.87-92.

[10] R.Seshadri and T.Raghu Trivedi, "Efficient Cryptographic Key Generation using Biometrics", Int. J. Comp. Tech. Appl. 2016, ISSN: 2229-6093, Vol 2, p.183-187.

[11] Maragatham.S, Kanya Devi.J, "A Biometric Cryptosystem based Secured Future Level Network", ISSN 2321 - 3361, 2016, Vol 6, p.5388-5392.