Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.377 – 387

Biometric Based Authentication Using Two-Stage Fingerprint Privacy Protection for File Storage on Server

Mrs. Afreen Fatima Mohammed

Department of Information Technology, Assistant Professor, Stanley College of Engineering & Technology for Women

fafreen@stanley.edu.in

Abstract – To enhance a security for storing files on the server, Biometric based Authentication scheme is proposed. Fingerprint is one of the most widely used biometric feature. A novel approach to protect fingerprint privacy is to generate a virtual identity. This virtual identity is generated by extracting the features from the two fingerprints given by the user. Cryptography is then applied, by applying RSA Algorithm. This generates a key, which is used for encrypting a file that has to be sent for storage on the server. Similarly, while retrieving the file from the server, the user gives his fingerprints and the filename. RSA Algorithm is again applied to generate a key. If this key match with the key stored on the server site, then the file will be decrypted with key and given to the user. Thus providing a secured way of encrypting and decrypting a file using Biometric based Authentication scheme.

Index Terms - Biometric, Fingerprint Verification, RSA, Minutiae, Orientation, Reference points, SSL

I. INTRODUCTION

Cryptography provides secured way of data transaction over the network. It is used for encrypting the data before sending over the network. This encryption is done using a key generated which are guessed or cracked down using various cryptographic algorithms discussed in [9]. A lengthy key is cracked down to encrypt and decrypt the sending and receiving messages. Maintaining and sharing lengthy, random keys is one of the critical issues in the cryptography system. This issue is solved by integrating Biometrics with cryptosystems. Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields [1]. While cryptography provides security, biometrics eliminates the need to remember passwords. In

biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

Biometrics refers to behavioral and physical characteristics of users. Physical characteristics include iris, fingerprint, DNA sequence, which are unique to each individual. In Forensic and criminal investigations, fingerprints are used as a parameter. While performing transactions using smartcards, Fingerprint Identification and Verification scheme allow the authenticated user to perform the transaction. Fingerprint of an individual contains a pattern of ridges and valleys. A single curved segment is called ridge and the valley is the region between two adjacent ridges [4]. The local ridge discontinuities are defined as the Minutiae points. Ridge Endings and bifurcations are two types of Minutiae points.

Fig1.1 Minutiae features

The Fig1.1 Shows the minutiae features of the Fingerprint. The extracted ridge endings and bifurcation features have been shown in Fig 1.2. The accurate matching of fingerprints depends largely on ridge structures.

(a)Ridge Endings (b) Bifurcations

Fig 1.2 Shows Minutiae Points

Biometric cryptosystem refer to the art of encrypting data using the information extracted from biometric information. An exclusive key generated from this extracted biometric, would be unique to each individual user. Data to be send can then be encrypted using this generated fingerprint key. Cryptography is the art of protecting data by transforming them into unreadable format called cipher text [1]. Cryptographic Systems are classified into two types: Symmetric key systems and Asymmetric key systems. Symmetric key systems use a single secret key for both encryption and decryption. This secret key is shared by both the communicating parties. Asymmetric Key systems are also known as Public key systems. Here two keys are generated: public key and private key, public key can be known widely, where as private key is known only to the user. Using the public key, any person can encrypt a message for the owner and leave it on a public server or transmit it on a public network, and such message can be decrypted only by the owner using the owner's private key [2]. Cryptography uses lengthy keys for encrypting and decrypting a message, and these keys can easily be cracked or guessed, by any attacker over the network.

If a key is generated from biometric information of the user, then such a key cannot be revealed without a successful biometric authentication [1]. The Fingerprint of the user can be taken to generate a key. It has been found that the existing techniques which make use of key for fingerprint privacy protection provided much inconvenience when the protected fingerprint image and the key were stolen. The proposed paper states Biometric based Authentication that uses a novel approach for fingerprint privacy protection. Privacy is enhanced by taking fingerprints from two different fingers instead of a single. The combined minutiae generated from the two different fingerprints of the user, will provide a new virtual identity. An RSA Algorithm can then be applied on this new virtual identity to generate a key. As we use RSA algorithm based encryption technique, the encryption lies

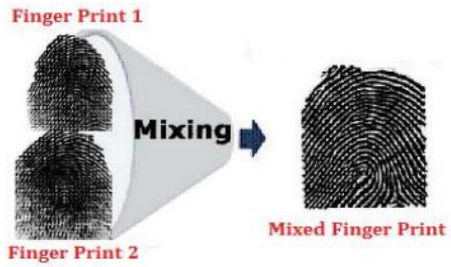
on two basic sets of keys to decrypt the message [3]. Thus having two set of keys will add security to encryption and protect the file to be sent from tampering by the unwanted parties. This paper proposes Biometric based Authentication that uses a novel approach for privacy protection of fingerprint and sending a file in a more secure manner for storage on the server.

II. LITERARTURE SURVEY

A number of techniques have been developed for secure file transfer over the network. Various cryptographic algorithms are present for providing security while the files are being transmitted. To enhance a rise in security level, a more robust scheme for incorporating biometric features were proposed. Various researches is conducted to improve and protect the privacy of fingerprint templates. Biometric based authentication techniques uses a biometric authentication system, which operates by acquiring biometric data from an individual such as fingerprints, iris scan, or facial recognition, which involves extracting a feature set from the acquired data, and comparing this feature set against the template set in the database[7]. However, this technique provides highest level of security. Since biometric identifiers cannot be shared, they represent the individual's identity [10]. In [11], Distinguishable Feature Generation is discussed to differentiate the authenticated user from the mock user. A novel system for fingerprint privacy protection by combining two fingerprints into a new identity is discussed in [12]. In the past years, researchers have done a lot of work in the field of pattern extraction from various biometric sources like iris, face, fingerprint, images and cryptography. A local key generation method is presented in [13].It proposed a unique way of generating key by combining three features: user's password, fingerprint and iris image. In [13] it is discussed that the biometric information taken by the sensors during enrolment i.e., fingerprint and iris image, undergo through hash technique. Hashing is applied to encode extracted points that distinguish users from each other. Encrypted outputs of the two biological patterns are XOR, and a secure password is created. The results show that these techniques are dynamically stable against changes in fingerprint and iris pattern in order to generate secure keys. Patterns presented in [13] are more robust against attacks compared with patterns that are solely based passwords. Another related work was done by Goh and Ngo, who combine proposed a new system in [14], based on face biometrics [15]. Usage of more than one biometrics enhances in securing the system. This is because it is mostly impossible for the theft to steal more than one biometrics. As discussed in [1], that how two set of keys adds up the security level. In [7] Token based techniques are discussed. It states that authentication can be done using key cards, bank cards and smart cards. Many Knowledge based techniques are used by token-based authentication systems to enhance security. For instance, users use PIN number to perform any transaction on ATM machine using ATM cards. These PIN numbers is used as one of the authentication techniques. Authentication techniques include both text-based and picture-based passwords.. Jo et al. [16] proposed a simple technique for the generation of digital signatures and cryptography communication with the aid of biometrics. The generation of the signature is in such a way that it becomes possible to verify the same with a cryptographic algorithm in existence like the RSA without altering its own security constraint and infrastructure. Fingerprint is one of the most widely used biometric features today. In [17] it has been discussed about the minutiae detection from the gray scale image of the fingerprint. Research is being carried out in cancellable biometrics, where the main scheme is to store an irreversibly transformed version of the biometric template which provides a high privacy and security level by allowing multiple templates to be associated with the same biometric data [18]. As the work done by Arun Ross and Asem Othman in [19], it has been shown that Mixing fingerprints can be useful in several applications: it can be used to obscure the information present in an individual's fingerprint image prior to storing it in a central database, it can be used to generate a cancellable template, i.e., the template can be reset if the mixed fingerprint is compromised, it can be used to generate virtual identities by mixing fingerprint images pertaining to an individual and it can potentially be used for fingerprint mosaicing [20].

III.PROPOSED SCHEME

In this proposed paper, fingerprint privacy is protected by using Two-stage Fingerprint matching process. Enrolment and Authentication phases are used in Fingerprint matching process. During enrolment phase, the fingerprints from two different fingers are taken. The minutiae points and reference 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.



a) Combined template taken from two different Fingerprints

b) Minutiae Image c) Orientation Image d) Combined Template

Fig 3.1 Shows Combined Minutiae template generated from two different Fingerprints

The Fig 3.1 shows the Minutiae, reference images of a fingerprint, and the combined template from both the fingerprints.

While retrieving a file from the server, the user has to give his two fingerprints, and the filename, 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.

Table 1 extracted Features of Combined Template

Features	Values
Mean	1.6572
Variance	88.452
Entropy	1.6231
Standard Deviation	1.8249
Correlation	0.5672
Energy	0.5621

The Table 1shows the extracted features of combined template. Once the features from the combined template are extracted, a vector is generated with these extracted features information and stored in a database with the name entered[6].The Enrolment Phase is shown in Fig 3.2

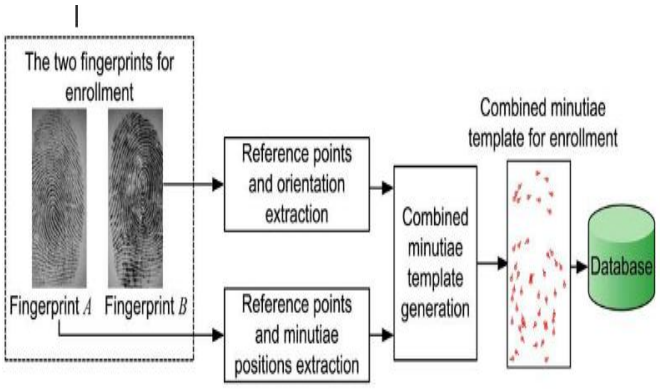


Fig 3.2 Enrolment Phase

During Authentication Phase, the extracted combined minutiae template from the two fingerprints are matched against with the corresponding template, stored in the database, as shown in the Fig 3.3. The authentication will be successful, if the matching score is over the pre-defined threshold value, as shown in Fig 3.4 Pre-processing steps like normalization, filtering , masking are already done before performing all the previous steps.

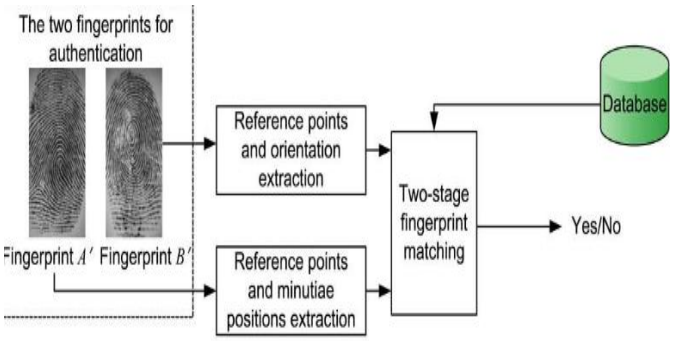


Fig 3.3 Authentication Phase

A. *TWO-STAGE FINGERPRINT MATCHING PROCESS*:

The two stage fingerprint matching process consists of the following steps:

1. *Query minutiae determination*: The local features are extracted for minutiae points.

2. *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

3. *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

4. *Protecting the database*: If a combined fingerprint is attacked or stolen by the attacker from the database, 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.

The Fig 3.4 shows the proposed two-stage fingerprint privacy protection scheme. Two different fingerprints from the user are taken, and the combined minutiae template is generated by combining the minutiae points from one finger, reference points from the other finger, and the reference points from both the fingers. This combined minutiae template represents a new virtual identity, which is normalized into binary form and then RSA is applied to generate a key from this template, and then template along with the key it is stored in a database. As shown in the Fig 3.4, during authentication phase, the same above procedure is followed to generate combined minutiae template, which is matched with the template stored in the database. The matching score is calculated using Matching score calculator. If the score is under the threshold then the match is said to be found and the user is said to be authenticated user.

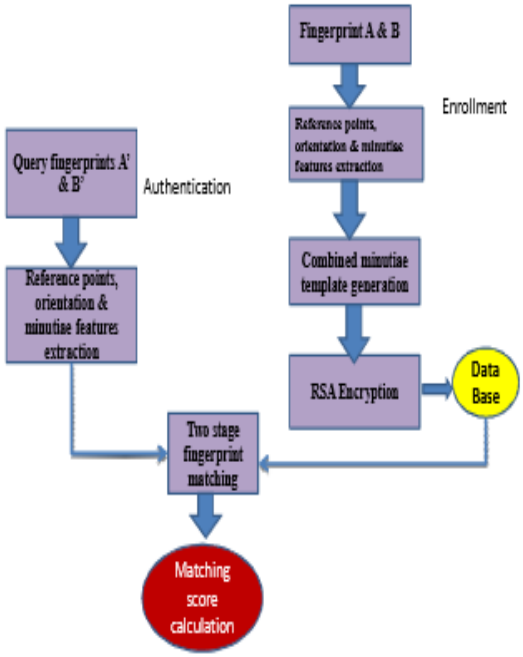


Fig 3.4 Proposed Fingerprint privacy Protection Scheme

B .KEY GENERATION PROCESS

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

C.KEY GENERATION FROM MINUTIAE POINTS

Algorithm 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

Step 1 : The Extracted minutiae points are represented as:

$Mp = \{ mi \}i=1,\ldots, Np$ (1)

Step 2 : The initial key vector is defined as follows:

$Kv = \{ xi : p(xi) \}\ i=1, \ldots.., Kl$ (2)

Where, $p(x) = Mp[I \% Np] + Mp[(i+1) \% Np] + S$ (3)

$i=1,\ldots. , Kl$

Step 3 : Initial value of S is equal to total Number of Minutiae points. The value of S will be dynamically changed as follows: $S = Kv (i) \% Sl , -1 < i< Kl$ (4)

Step 4 : Initial key vector (Kv) is converted in to a matrix Km of size $Kl / 2 * Kl / 2$ as follows: $Km = (aij) Kl / 2 * Kl / 2$ (5)

Step 5 : An intermediate key vector is generated as follows: $KIV = \{ Ki : (m(ki) \}\ i=1,\ldots. Kl$ (6)

Where $m(k) = | Aij |$, $Aij = Km\ i,j : i+size, j+size$,

$-1 < i< Kl/2$

Aij is a submatrix formed from the key matrix.

Step 6 : Final key vector (Private key) formed is:

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

$= 0$, otherwise

D. MAPPING EACH BINARY DATA PRECISELY TO EACH REGION

Although we know, that no two fingerprints are similar to one another but there's a whole lot of chances where the number of ridges may be equal to the number of furrows. An nxn matrix is used that precisely stores each furrows and ridges markings in the byte pattern accordingly to the scanned image of the fingerprint. This helps to recognize 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

$s = (d – e)$ (8)

Pb → Public key vector

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

e → public key vector

F.SECURE SOCKET LAYER SOCKETS (SSL) PROTOCOL

Secure Socket Layer (SSL) Protocol is used by the sockets. It is also referred as Transport Layer Security Protocol. Sockets are normal stream sockets. A layer of security protections are added over the underlying network transport protocol, such as TCP. SSL provides protection against modification of messages by an active wire tapper. It provides confidentiality, by encrypting the data being sent between client and server. A "cipher suite" specifies these kinds of protection, which is a combination of cryptographic algorithms used by a given SSL connection[21]. During the negotiation process, the client and server must agree on a cipher suite that is available in both environments. A negotiation process called "handshaking establishes the cipher suite used. When SSL Sockets are first created, no handshaking is done so that applications may first set their communication preferences: what cipher suites to use, whether the socket should be in client or server mode, etc. However, security is always provided by the time that application data is sent over the connection.

G.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 following steps are then performed:

Step 1: The File to be send is then encrypted using the key generated by the RSA for the combined minutiae template. RSA generates two keys, a public key and a secret key. These two keys will be stored at client's local database.

Step 2: Using public key, the client encrypts the file and sends the file to the server along with the public key.

Step 3: The server then stores the incoming file, and the public key, for a given authenticated client.

H. 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 to retrieve a file from the server, he gives the filename and the two fingerprints. The following steps are then performed:

Step 1: RSA Algorithm is applied to the combined minutiae template, generated from both the fingerprints.

Step 2: If the key generated from this combined 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.

Step 3: Hence the user can access his file securely.

IV. IMPLEMENTATION

The proposed work is implemented using J2SE 1.6 and Matlab 7.3. The various packages and technologies used are: Java Swing, Java Socket API and Matlab. Java Swing is used for the creation of Graphical User Interface (GUI). The Socket API takes care of the client server interaction. Matlab is a tool for doing numerical computations with matrices and vectors. Swing is used to create the GUI, at both the server side and the client side. The Java Socket API provides a set of function calls to establish communication between sockets on two remote machines. When messages are sent, they are queued at the sending socket until the underlying network protocol has transmitted them. When they arrive, the messages are queued at the receiving socket until the receiving process makes the necessary calls to receive them, a mentioned in [21].

V. EXPERIMENTAL RESULT

An experiment is conducted by taking one fingerprint of the thumb and another fingerprint of the index finger.

Fig 4.1 shows the fingerprint of the index finger and the thumb which were taken. The combined template was generated using by taking minutiae image and orientation image.

Fig 4.1 a) Fingerprint of the index finger b) Fingerprint of the thumb

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 shown in Fig. 4.2 represents the index and thumb fingerprint images of three different specimens along with corresponding combined templates and extracted features.

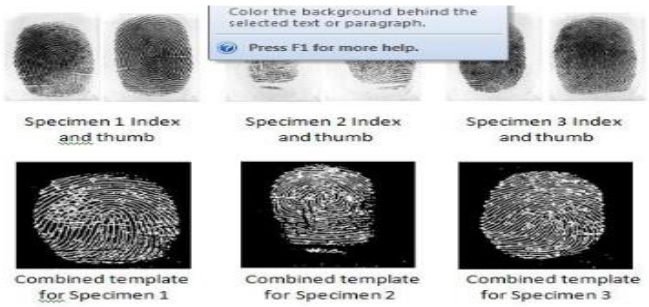


Fig 4.2 Combined templates for three different specimens

Shown in Table 2 As the features match with those stored in database the authentication system is reliable.

Table 2 extracted Features of Combined Templates taken from three different specimens

SPECIMEN 1		SPECIMEN 2		SPECIMEN 3	
Features	Values	Features	Values	Features	Values
Mean	1.6572	Mean	1.2672	Mean	1.6572
Variance	88.452	Variance	78.452	Variance	88.452
Entropy	1.6231	Entropy	1.432	Entropy	1.6231
Standard Deviation	1.8249	Standard Deviation	1.329	Standard Deviation	1.8249
Correlation	0.5672	Correlation	0.4216	Correlation	0.5672
Energy	0.5621	Energy	0.3241	Energy	0.5621

VI. CONCLUSION & FUTURE WORK

In this paper, a novel approach for protecting the fingerprint privacy is proposed using Biometric based Authentication where the two different fingerprints are taken during an enrolment phase. The minutiae and reference points from one finger, and the orientation and reference points from the other finger are taken to form a combined minutiae template. To this combined template, RSA Algorithm is applied to generate a key, using which the file to be send is encrypted. Thus this doesn't provide any

opportunity to the attacker, to crack down the key; thereby it increases the level of security. The future work might include taking fingerprints from two or more 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: 2278-8727Volume 12, Issue 1 (May.-Jun. 2013), P16-22 www.iosrjournals.org

[2]. https://en.wikipedia.org/wiki/Public-key_cryptography

[3]. Safnitha P Y, Sheena Kurian "Enhancing Security With Fingerprint Combination Using RSA Algorithm", International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages :6-65 (2014) Special Issue of ICCEIT 2014 -Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

[4]. Roli Bansal, Priti Seghal, 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

[5]. Vidya.P,Aswathy.R.S "Privacy Improvement for Fingerprint Recognition Based On RSA",

International Journal of Innovation Research in Science, Engineering & Technology, Volume 3 , Special Issue 5,July 2014

[6] Lukesh N.Jain,DR.R.G.Karindakar,."Decision Tree based Fingerprint Authentication", International Journal of Engineering and Technical Research (IJETR)ISSN: 2321-0869, Volume-3, Issue-5, May 2015

[7] Shweta Malhotra Dr.Chander Kant,"A Novel approach for securing biometric template", international Journal of Advanced Research in Computer Science and Software Engineering

[8] Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, IEEE, "Fingerprint Combination for Privacy Protection", IEEE transactions on information forensics and security, vol. 8, no. 2, February 2013

[9] Gary C. Kessler "An Overview of Cryptography", Handbook on Local Area Networks, published by Auerbach in September 1998.

[10] A. K. Jain, R. Bolle, and S. Pankanti, eds., Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999.

[11] **Yao-Jen Chang** , Wende Zhang+ , and Tsuhan Chen, "Biometric-Based Cryptographic Key Generation", ***** Advanced Technology Center, Computer & Communications Research Laboratories Industrial Technology Research Institute, Chutung, Hsinchu, Taiwan 310, R.O.C. + Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA

[12] Prabhakara Rao , Gintanjali Sahu "Protecting Fingerprint Privacy Using Combined Minutiae Template Generation Algorithm ", International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2290-2294

[13] Soroush Shiekhalhokamaii , Mohammad Amin Pirbonye" A novel Approach for regenerating a secure and reliable Password using iris and fingerprint"

[14] Mr.P.Balakumar and Dr.R.Venkatesan"Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris**"**, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, September 2011 ISSN (Online): 1694-0814 www.IJCSI.org

[15] T. Connie, A. Teoh, M. Goh, and D. Ngo, " Palm hashing: A novel approach for cancellable biometrics," Information processing letters, vol. 93, no. 1, pp. 1-5, 2005.

[16] J. G. Jo, J. W. Seo, and H. W. Lee, "Biometric digital signature key generation and cryptography communication based on fingerprint," First Annual International Workshop 2007, LNCS 4613, pp. 38-49, Springer Verlag, 2007.

[17]D.Maio and D. Maltoni, "Direct gray-scale minutiae detection in fingerprints ". IEEE Trans. Pattern Anal. And Machine Intell., Volume 19 No.1, January 1997

[18] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for face template protection," Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, vol. 6944, pp. ca. 325, 2008.

[19] Arun Ross and Asem Othman ,"Mixing fingerprints for template security and privacy,", Appeared in Proc. of the 19th European Signal Processing Conference (EUSIPCO), (Barcelona, Spain), August/September 2011

[20] A. Ross, S. Shah, and J. Shah. Image versus feature mosaicing: A case study in fingerprints. In Proceedings of SPIE Conference on Biometric Technology for Human Identification III, pages 620208–1 – 620208–12, 2006

[21] Sangheethaa Sukumaran, Swathika Rengasamy and S. Sasirekha "Critical File Access in Wireless Networks Using Multifactor Authentication ",tifac.velammal.edu.in/CoMPC

