Information Security using Cryptography and Image Processing

Avanti Deshpande[1] R. B. Joshi[2]
[1]Lecturer [2]Assistant Professor
[1, 2]Department of Computer Science & Engineering
[1, 2] MMCOE, India

Abstract—Meaning of Information security is protecting information and the systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. Therefore it is necessary to apply effective encryption/decryption methods to achieve data security. The user only needs to remember the short password to retrieve the key. The password can be forgotten and stolen. As Biometrics based authentication systems confirm an individual's identity based on the physiological and/or behavioral characteristics of the individual. It has advantages over password based methods. Biometrics based method provides direct link between the service and actual user. With biometrics, there is nothing to lose or forget, and it is relatively difficult to manipulate. Biometrics and cryptography are the two most prominent solutions for user authentication, data integrity preservation, and trustworthy verification. By combining biometrics with cryptography, high level of security can be achieved.

I. INTRODUCTION

Information security is concerned with the confidentiality, integrity and availability of information/data regardless of the form the data may take: electronic, print, or other forms [1]. Information assurance focuses on the reasons for assurance that information is protected, and is thus reasoning about information security. The Government, Military and private businesses uses or deal with confidential information about their employees, activities, products and financial status. Most of this information is now collected, processed and stored on computer in term of files or databases and transmitted across using networks to other computers [2].

A. Key Concepts

Confidentiality, Integrity, Availability, Authenticity and Non-repudiation are the core principles of information security [2].

1) Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems. For example, Sender wants to send confidential data/information to the receiver. Then information should remain confidential. That means other person except sender and receiver should not get access to the data. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

2) Integrity

Integrity means that data cannot be modified or changed. It is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality. The information must be available when it is needed. During transit, data should not get modified by an unauthorized person.

3) Authenticity

It is necessary to ensure that the data, transactions, communications or documents are genuine. It is also important for authenticity to validate that both parties involved are who they claim they are.

4) Non-Repudiation

Non-repudiation implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. For Example: Sender has sent amount of Rs. 10,000/- to the receiver electronically. After sending the amount, sender should not deny of not sending the amount electronically.

II. LITERATURE SURVEY

1) In the paper [1], biometric template security which is an important issue because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. Protecting the template is a challenging task due to intra-user variability in the acquired biometric traits. He presented an overview of various biometric template protection schemes and discussed their advantages and limitations in terms of security, revocability, and impact on matching accuracy. A biometric system is vulnerable to a variety of attacks aimed at under integrity of the authentication process. These attacks are intended to either circumvent the security afforded by the system or to deter the normal functioning of the system. Biometric recognition offers a reliable solution to the problem of user authentication in identity management systems.
2) In the paper [6], protection of fingerprint template from creation of physical spoof and replacement by imposter's template to gain unauthorized access by transformation based approaches and biometric cryptosystems. The security of the fuzzy vault depends on the infeasibility of the polynomial reconstruction and the number of chaff points. In the proposed system an even more secured fuzzy vault is generated with combined features of fingerprint and palm print to enhance the security of the template stored. One of the potential vulnerabilities in a biometric system is the leakage of biometric template information, which may lead to serious security and privacy threats. Most of the available template protection techniques fail to meet all the desired requirements of a practical biometric system like revocability, security, privacy, and high matching accuracy. In particular, protecting the fingerprint templates has been a difficult problem due to large intra-user variations.
3) Paper [3] describes about Mobile equipment (ME) which plays important role of bridge between wireless network

All rights reserved by www.ijsrd.com

and mobile user has been facing more and more security threats. Trusted mobile platform (TMP) was proposed by TCG (Trusted Computing Group) as a new mechanism to enhance the security of the resource-constrained ME. In this paper, a new study on constructing a TMP according to ME's feature, and per-forming mutual authentication in mobile user domain. A smart-phone's processor is used as an example to demonstrate the constructing of TMP, along with which three methods for adding trusted platform module (TPM) in ME are presented respectively. In the framework of TMP, we also propose a user authentication scheme combining password and fingerprint with the USIM (Universal Subscriber Identity Module). The proposed scheme is validated through a performance analysis and experimental test. The validation result shows that our approach offers better efficiency and advanced security over the authentication scheme presented in TMP's draft standard. It also outperforms TCG's user authorization scheme by providing improved security, flexibility and universality.

III. COMPARISON OF SECURITY FEATURES OF DIFFERENT SCHEME [1] [4] [5]:

Biometric	Fingerprint	Face	Hand Geometry	Voice
Barriers to universality	Hand or Finger impairment	None	Hand Impairment	Speech Impairment
Collectability	Medium	High	High	Medium
Acceptability	Medium	High	Medium	High
Potential for circumvention	Low	High	Medium	High

Table. 1: Comparison of Security features

IV. WORK PLAN AND METHODOLOGY

In this paper, the detail description about the methodology used for implementation of cryptography and fuzzy vault is mentioned. The proposed method is based on 2-dimensional quantization of distance vectors between biometrics features and pairs of random vectors. In this introduced scheme, fuzzy vault is utilized for secure binding of randomly generated key with extracted biometrics features.

V. GENERAL FRAMEWORK

In the proposed method, for face based cryptographic key generation, a set of biometrics features is first extracted from the user's face images. The extracted features are then quantized and mapped to binary representation for feature points matching. The produced binary features and the randomly generated key are bound using the fuzzy vault scheme. During authentication, the cryptographic key will be correctly retrieved if the presented authentication face features have substantial overlap with the enrolled ones. The details of the proposed methods are represented diagrammatically as follows:

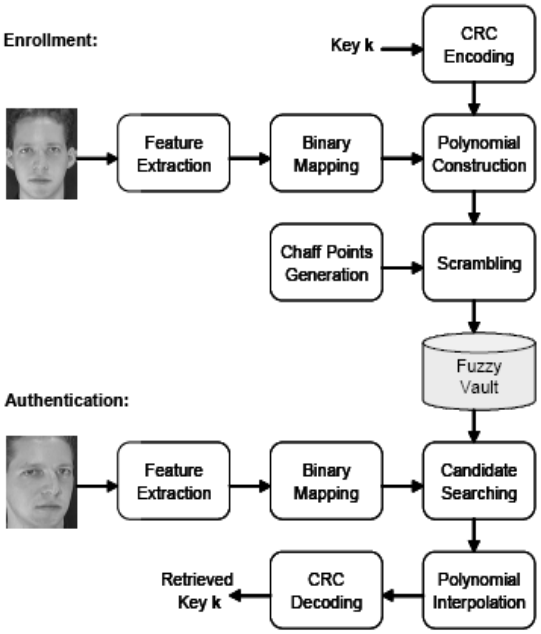

Fig. 1: Proposed Method

A. Feature Extraction

1) Store the images of persons in the organization found the training set of images using Eigen value matrix.
2) Subtract the mean: take the average across each dimension. This produces a data set whose mean is zero.
3) Calculate the covariance matrix. The aim of finding the covariance is to see if there is any relationship between the data dimensions. Covariance is always measured between two dimensions matrix. If we have a data set with more than one matrix of dimensions 2, their results that are more than one covariance measurements that can be calculated. The most practical way to get all the possible covariance values between the different dimensions is to calculate them all and put them in one big 2D matrix. The definition for the covariance matrix for a set of data with n dimensions is [3], a matrix with *n* row and *n* columns and is the Xth dimension. This formula tells [3] that if there is an n-dimensional data set, then the matrix has *n* rows and *n* columns (so it is square) and each entry in the matrix is the result of calculating the covariance between two separate dimensions.
4) Calculate the Eigenvectors and Eigen values of the covariance matrix. Eigenvectors and Eigen values always come in pairs. The eigenvector can only be found for square matrices and not every square matrix that has eigenvectors. For a given a matrix that does have eigenvectors, there must be of eigenvectors with their corresponding Eigen values. All the eigenvectors of a matrix are perpendicular [3].
5) Choosing components and forming a feature vector. Once eigenvectors are found from the covariance matrix, the next step is to order them by Eigen values highest to lowest. This gives the components in order of significance. In fact, it turns out that the eigenvector with the highest Eigen value is the principle component of the data set.

All rights reserved by *www.ijsrd.com*

B. Binary Mapping

The extracted PCA features are a set of real numbers, and generally exact matching is impossible. One method is to perform the matching of feature points based on closeness. In this work plan, a Binary Mapping method is used to produce binary representation of face features based on 2-dimensional quantization of the distance vectors between the extracted features and pairs of random vectors.

C. Polynomial Construction

The polynomial is in terms of some dummy variable *X*, the powers are combined with binary (0 and 1) coefficients:

For a bit sequence $[b_{k-1}, b_{k-2} \ldots b_1, b_0]$ the associated polynomial is

$$b_{k-1} * X_{k-1} + b_{k-2} * X_{k-1} + \ldots + b_1 * X + b_0$$

For example, for the data (message) bit sequence $[1010100101]$ of $k = 10$ bits, the polynomial representation is

$$M(X) = X^9 + X^7 + X^5 + X^2 + 1$$

Suppose *k* message or data bits are encoded into N code bits by appending to the message bits a sequence of $n = N - k\ bits\ [r_{n-1}, r_{n-2}, \ldots, r_1, r_0]$. Let $R(X)$ be the polynomial representing these appended bits. Then the code word of length *N = k + n* corresponding to the message *M(X)* is $[b_{k-1}, b_{k-2} \ldots b_1, b_0, r_{n-1}, r_{n-2}, \ldots, r_1, r_0]$ for which the corresponding polynomial is clearly

$$T(X) = X^n [M(X) + R(X)]$$

This follows because the original message bits now occupy more significant bit positions in the code word; each message bit is moved left by *n* bits to make room for the n appended bits. For example, to the above 10-bit message sequence if 3-bit sequence 111 is appended, the resulting 13-bit code sequence has the polynomial representation is as follows,

$$X^3(X^9 + X^7 + X^5 + X^2 + 1) + X^2 + X + 1$$
$$= X^{12} + X^{10} + X^8 + X^5 + X^3 + X^2 + X + 1$$

VI. FLOW OF A SYSTEM

1) In this Biometric cryptosystem, as the name suggests, it is a cryptosystem, where the any kind of files can be encrypted or decrypted using the 'DES' encryption tool and the Biometric entity (face) is used to protect the password/key used in DES.
2) While encrypting, the user will have to select a file which is to be encrypted, then give a password to ensure security.
3) There would be 2 options for password provision. The user can manually enter password of its own, or can ask the system for generating a random key.
4) But that is not sufficient; the user will also have to input its real time face through web cam.
5) Now the system will use the features of the face with the key for the formation of construct called Fuzzy Vault.
6) This vault can be carried and saved wherever we want, even on smartcards, flash drives etc.
7) So whenever the file is to be decrypted, we don't have to remember the password we entered.
8) We just have to give the system our real time face and the Fuzzy Vault to decrypt the file.

VII. CONCLUSION

This paper introduces Information Security using Cryptography and Image Processing. The proposed method utilizes fuzzy vault, for secure binding of biometrics features with randomly generated cryptographic keys. To tolerate the variations of biometrics signals, a method based on 2-D quantization of distance vectors is proposed. Experimentation shows that the proposed solution achieves promising results. However, the proposed solutions are general and can also be applied to other biometrics molarities.

REFERENCES

[1] Arjun Guha, Matthew Fredrikson, Benjamin Livshits and Nikhil Swamy, Verified Security for Browser Extensions, IEEE Symposium on Security and Privacy, 2011.
[2] Partial Face Recognition: Alignment-Free Approach, Shengcai Liao, Anil K. Jain, Fellow, IEEE and Stan Z. Li, Fellow, IEEE, 2011.
[3] Biometric Recognition: Security and Privacy Concerns, published by IEEE Computer Society, IEEE, 2009.
[4] Yu Zheng, Jingchun Xia and Dake He (2008), Trusted user authentication scheme combining password with fingerprint for mobile devices, Biometrics and Security Technologies ISBAST 2008, Page(s): 1 – 8.
[5] Biometric Recognition: Security and Privacy Concerns, published by IEEE Computer Society, IEEE, 2009.
[6] Hugh Wimberly, Lorie M. Liebrock (2011), Using Fingerprint Authentication to Reduce System Security: An Empirical Study, IEEE Symposium on Security and Privacy.
[7] William Stalling (2010), Cryptography and Network Security, Prentise Hall, Fourth Edition.
[8] Atul Kahate(2008), Cryptography and Network Security, Tata McGraw-Hill Education
[9] Paul Reid (2009), Biometrics and Network Security, Pearson Education.
[10] Digital Encoding and Decoding, By Dr. George W Benthien, March-2010.

All rights reserved by *www.ijsrd.com*