IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 1, January 2016*

# Cryptographic Fuzzy Vault with Image Processing

**Prof. Joshi Ram B**

Ph.D. Scholar, JJT University, Rajasthan, India

Associate Professor, Dept of Computer Engineering, ICEM, Pune, Savitribai Phule Pune University, Pune, India

**Abstract:** The term information security is related with the protection of information as well as the systems from unauthorized access and further misuse by disclosure, disruption, modification, inspection, recording or destruction. Information security means protecting sensitive information which is a growing concern for the body whose business mostly depends on information technology and protecting such critical data in various sectors, including the business, healthcare and defense sectors, has become the first priority of information management. The growing use of networking such as extranets and cross-organizational collaboration tools, including customers, suppliers, and business partners—increasingly need access to the required applications and data, Reviews can be collected through social media technologies. Extended networks can help organizations reduce the operational expenses through greater process efficiencies; it also promote cross-organizational innovation; and reduce the need to build costly and time-consuming point-to-point connections. In spite of tremendous benefits to this expansion of the corporate network, the need for strong security has never been more apparent. Any compromise or failing to protect this asset results in huge loss in terms of trust of customers and investors which in fact results to financial disaster. The information systems consist of three major areas communication channel, user interface and information storage; the protection of these three areas means adoption of the information security. Issues such as dynamic sensitive information ownership, group authentication and authorization and privacy protection also create challenges for the protection of information systems Biometrics has made a significant impact in forensics like identification of criminals or authentication of authorized users. In this system the main emphasis is on a pattern recognition that recognizes a person by determining the authenticity of a specific physiological constraint such as face and/or behavioral characteristic possessed by that person like audio or frequency of key stroke entered. Face recognition is highly preferable and acceptable biometrics used by humans in their visual interaction. Cryptography in conjunction with biometrics is the main objective which leads to high level of security for authentication and key retrieval and will model the secure information exchange. The challenges in face recognition system such as aging, facial expressions, variations in the imaging environment, illumination and pose of the face

**Keywords:** Information security, multi factor authentication, biometric method, binary mapping, fuzzy vault, polynomial construct.

## I. INTRODUCTION

Information security principles confidentiality, integrity, access control and availability of information/data are need to be enforced 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. Most software applications rely on the use of user-name and passwords to authenticate end users. This form of authentication, although used ubiquitously, is widely considered unreliable due to the user's inability to keep them secret; passwords being prone to dictionary or rainbow-table attacks; as well as the ease with which social engineering techniques can obtain passwords. User authentication can be carried out using something you know like the user has to remember a secret, password or pin, the second area of authentication is to use a physical device like keys, a mobile phone, or credit/debit cards i.e. something you own. The last area of authentication is a biometric for example a finger print or faces something you are. The principle of multi factor authentication is to use these three areas in conjunction to offer the stringent level of authentication. An example of two factor authentication used in our daily lives is an ATM cash machine. In order to withdraw cash from an ATM machine you must first insert or swipe your credit/debit card (something you own) and then enter your pin (something you know). If you lose your credit card you rely on the second factor (the pin) to protect your credit card until you can notify the bank that it is missing.

The Government, Military and private businesses like trading where online orders are generated 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]. Due to huge spread of network and global acceptance of the Internet most of the computers are virtually interconnected with each other. This opened up unlimited opportunities for computing and information sharing at the same it also brought the critical issue of

information security which can be solved using biometric system for authentication along with effective encryption/decryption methods. The objective is that the user need not have to remember the complex 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. Biometric methods offer a reliable solution to the problem of user authentication in identity management systems. The aim is to improve the reliability of the authentication using a multi-factor approach without incurring additional cost or making the deployment of the solution overly complex. Biometrics and cryptography are the two most prominent solutions for user authentication, data integrity preservation, and trustworthy verification.

**Key Concepts:**
Information can be protected by adopting a secure authentication systems using biometrics which confirm the username based on the physiological and/or behavioural characteristics of the individual user. Biometrics based security methods provide a secure link between the service and actual user which achieves intrinsic advantages over password based methods. There is no fear to loose or forget the password required for authentication.

Using biometrics the programmer can set the accuracy as per the threshold value which can be active parameter for customization of the vault. Current Biometric authentication systems based on physiological and behavioural characteristics of persons (known as biometrics), such as face, inherently provide solutions to many of these problems and may replace the authentication component of the traditional cryptosystems.

## II. REVIEW OF LITERATURE

A. In the review of paper [1], the focus is on biometric template security as it cannot be revoked and reissued like passwords and tokens. An overview of various biometric template protections schemes and discussed on their advantages and limitations in terms of security, revocability, and impact on matching accuracy.

B. In the review of paper [7], Factors such as age progression and other sources of variations like head pose change have adverse effects on the performance of face verification systems. In this paper, they propose to manage the influence of both the age progression and head pose change on the face verification process which uses the age and head pose as class-independent quality measures together with the scores from baseline classifiers, in order to obtain better verification performance.

This allows for improved long-term class separation by introducing a 2D parameterized decision boundary in the scores-age space using a short-term enrolment model. This new method, based on the concept of classifier stacking with age- and head pose aware decision boundary compares favourably with the conventional face verification approach, which uses age- and head-pose-independent decision threshold calculated only in the score space at the time of enrolment. In this paper, they also show the advantages of user-specific approach for the face verification task over user-independent approach.

C. In the review of 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.

D. In the review of paper [8] the focus is on a novel geometric representation for 3D faces in order to enhance distinctiveness of generally smooth range images. This novel face representation is based on Multi-Scale Extended Local Binary Patterns (ELBP) and enables accurate and fast description of local shape variations on range faces.

When associated with the SIFT-based local feature matching scheme, this novel geometric facial representation shows its discriminative power in 3D face recognition, displaying a rank-one recognition rate up to 97.2% and a verification rate of 98.4% at a 0.001 FAR respectively on the FRGC v2.0 database which demonstrate that the entire system is also robust to facial expression variations.

E. In the review of paper [9] about MFA, a combination of methods from at least two of the basic authentication factors is used to get the authorisation; for example, a bank card and Personal Identification Number (PIN). In some approaches, users are required to provide a password number from a security token.

F. In the review of paper [10] one of the motivations of using MFA is to improve the single factor based Authenticated Key Exchange (AKE) by combining two or even more factors in one system.

G. In the review of paper [11] Integrating the credit card payment system with biometrics in MFA has given support for more efficient verification.

This method proposes to employ fingerprint verification with a credit card in a MFA. Employing biometrics when using a credit card in authentication as a MFA procedure is another access control approach.

Correlation of various biometrics with different scheme [1][4][5]:

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 1, January 2016*

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

## III. 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.

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. Considering multiple users of the said system a secure fuzzy vault record is stored in the database. The details of the proposed methods are represented diagrammatically as follows:

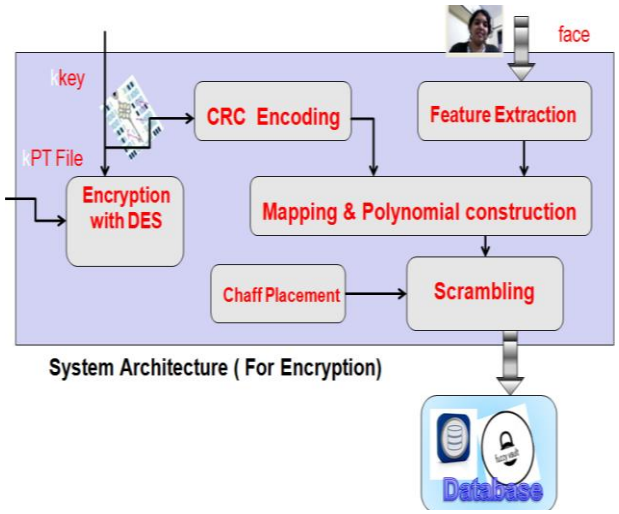


Fig:1 System Architecture for Encryption and Vault Creation

Extracted features are passes through binary mapping and polynomial construction phase. To incorporate the feature of confusion and diffusion the resultant is passed through scrambling phase and final fuzzy vault will be placed in the record format in the database.

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:

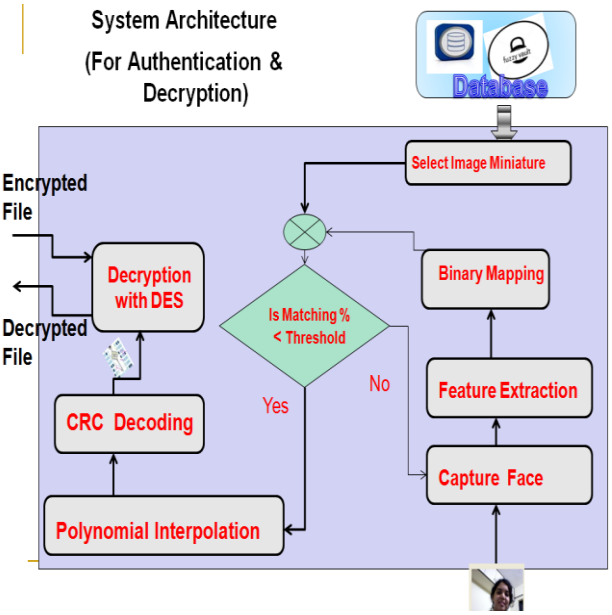


Fig:2 System Architecture for Decryption Process showing key from vault using face Authentication

## IV. DATA ANALYSIS & INTERPRETATIONS

In this phase of data analysis the major chunk of the data is in the form of n by n dimensional data sets.

A. Feature Extraction

Step 1: Collect the images of persons face and create the training set of images using Eigen value matrix. To understand the concept of Eigen value matrix first understands the definition of an eigenvector. An eigenvector of a square matrix S is a non-zero vector v that, when multiplied with S, gives a scalar multiple of itself; the scalar multiplier is often denoted by $\lambda$. That is: S v =$\lambda$v. The number $\lambda$ is called the **eigenvalue** or characteristic value of **S**corresponding to $v$.

Step 2: Now to produce the data set whose mean is zero take the average across each dimension i.e. Subtract the mean.

Step 3: To identify if there is any relationship between the data dimensions we need calculate the covariance matrix which 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. From the implementation point of view we need to calculate all the possible covariance values between the different dimensions and store them in one large two dimensional 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.

Step 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].

Step 5: Creation of feature vector using the component after getting the eigenvectors from the covariance matrix, the next step is to sort them by Eigen values highest to lowest to achieve the order of significance to the components. Principle component now can easily obtained from the data set as it turns out to be the eigenvector with the highest Eigen value.

B. Binary Mapping

The statistical procedure for elucidating the covariance structure of a set of variable i.e. Principal Component Analysis (PCA) which allows us to identify the principal directions in which the data varies. 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

Using the function for polynomial in java programming we can create a polynomial with the given coefficients. The first element of the coefficients array is the constant term. Higher degree coefficients follow in sequence. The degree of the resulting polynomial is the index of the last non-null element of the array, or 0 if all elements are null. The polynomial is in terms of some dummy variable Z, the powers are combined with binary (0 and 1) coefficients: is in terms of some dummy variable Z, the powers are combined with binary (0 and 1) coefficients:

- For a bit sequence [bk-1, bk-2… b1, b0] the associated polynomial is bk-1*Zk-1+ bk-2*Zk-2 + ...+ b1*Z + b0.

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

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

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 [rn-1, rn-2, ..., r1, r0]. Let R(Z) be the polynomial representing these appended bits. Then the codeword of length N = k + n corresponding to the message M(Z) is [bk-1, bk-2... b1, b0, rn-1, rn-2... r1, r0] for which the corresponding polynomial is clearly T(Z) = Z^n [M(Z) + R(Z)].

This follows because the original message bits now occupy more significant bit positions in the codeword; 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,

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

FINDING AND RECOMMENDATIONS

- In this system, it is observed that 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.
- During the process of encrypting, the user will select a file which is need to be encrypted, then give a password to ensure security. There would be two options for password provision. The user can manually enter password of its own, or can ask the system for generating a random key which can act as password along with real time face through web cam.
- Fuzzy Vault is created using the password and features of the face. This vault can be carried and saved wherever we want, even on smartcards, flash drives etc. So whenever the file is to be decrypted, we don't have to remember the complex password whereas we just have to give the system our real time face and the Fuzzy Vault to decrypt the file.

## REFERENCES

[1] Guha Arjun, Matthew Fredrikson, Benjamin Livshits and SwamyNikhil ,Verified Security for Browser Extensions,IEEE Symposium on Security and Privacy,2011.
[2] Jain Anil K. Shengcai Liao Fellow, IEEE and Stan Z. Li, Fellow, IEEE, 2011 on Partial Face Recognition: Alignment-Free Approach
[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] Weifeng Li ; Drygajlo, A. ; Hui Qiu on "Combination of age and head pose for adult face verification" , 2011 IEEE International Conference Publication Year: 2011, Page(s):77 – 82
[8] Di Huang ; Ardabilian, M. ; Yunhong Wang ; Liming Chen "A novel geometric facial representation based on multi-scale extended local binary patterns" 2011 IEEE International Conference
[9] E. Council, Federal Financial institutions examination council," Stat, vol. 2160, pp. 22{50, 1994.
[10] M. Hwang, S. Chong, and T. Chen, "Dos-resistantid-based password authentication scheme using smartcards," Journal of Systems and Softwareof Information Technology, vol. 8, no. 4, pp. 430{439,2011.
[11] H.-D. Ihmaidi, A. Al-Jaber, and A. Hudaib, "Securing online shopping using biometric personal authentication and steganography," in Information and Communication Technologies, 2006. ICTTA'06. 2nd, vol. 1. IEEE, 2006,pp. 233{238.

## BIOGRAPHY

**Prof. Ram B. Joshi** completed the graduation BE Computer Engineering from SGGSCE&T Nanded and ME Computer Engineering from Bharati Vidyapeeth Pune. Presently he is working as Associate Professor and HOD Computer Engineering at Indira College of Engineering &Management Pune.


DOI 10.17148/IJARCCE.2016.51108