International Journal of Advances in Engineering Research http://www.ijaer.com

(IJAER) 2014, Vol. No. 8, Issue No. III, Sep **ISSN: 2231-5152**

SECURITY USING CRYPTOGRAPHIC TECHNIQUES FOR IMAGE PROCESSING

***V.RaviKishore, ** Dr.V.Venkata Krishna**

**Research Scholar KL University*

ravikishore1985@yahoo.co.in

***Professor & Principal GIET,Rajahmundry* vakula_krishna@gmail.com

ABSTRACT

This paper focuses mainly on the different kinds of image security techniques. The digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are lots of other techniques which enhance the security of images in the field of encryption and decryption Image security is protecting image 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. In this paper a Survey of different secure image techniques and Biometrics are the two most prominent solutions for user authentication, data integrity preservation, and trustworthy verification. By combining biometrics with image security techniques, high level of security can be achieved. It additionally focuses on the functionality of Image encryption and decryption techniques.

INTRODUCTION

The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging. Image 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]. Securable image assurance focuses on the reasons for assurance that is protected, and is thus reasoning about image security. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information. Encryption will be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text [1]. Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read [1].

Encryption of data [2] has become an important way to protect data resources especially on the internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources. The image encryption algorithms can be classified into three major groups: (i) position permutation based algorithm [3] (ii) value transformation based algorithm and [4,5] (iii) visual transformation based algorithm [3].

Key Concepts A.

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.

LITERATURE SURVEY

1) In the paper [1], 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 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.

1. *New Mirror-Like Image Encryption Algorithm and Its VLSI Architecture.*

Jiun-In Guo and Jui-Cheng Yen [3] have presented an algorithm which was mirror like. In this algorithm there were 7 steps. In the first, 1-D chaotic system is determined and its initial point x (0) and sets k = 0.

Then, the chaotic sequence is generated from the chaotic system. After that binary sequence is generated from chaotic system. And in last 4 stages image pixels are rearranged using swap function according to the binary sequence.

2. Lossless Image Compression and Encryption Using SCAN.

S.S. Maniccam and N.G. Bourbakis [4] have presented a new algorithm which does two works: lossless compression and encryption of binary and gray-scale pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

3. New Encryption Algorithm for Image Cryptosystems.

Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [6] used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. . Then traditional cryptosystems from commercial applications can be used.

4. Technique for Image Encryption using Digital Signatures.

Aloka Sinha and Kehar Singh [4] have proposed a new technique in which the digital signature of the original image is added to the encoded version of the original image. A best suitable error code is followed to do encoding of the image, ex: Bose- Chaudhuri Hochquenghem (BCH) code. At the receiver end, after decryption of that image, the digital signature verifies the authenticity of the image.

5. Technique for Image Encryption using multi-level and image dividing technique.

Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha Wmn Lee, and SmJmng Kim[7] proposed an algorithm which was multilevel form of image encryption using binary phase exclusive OR operation and image dividing technique. The same grey level multi-level image is divided into binary images. Then binary pictures is regenerate to binary phase encoding and then these images are encrypt.

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

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.

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:

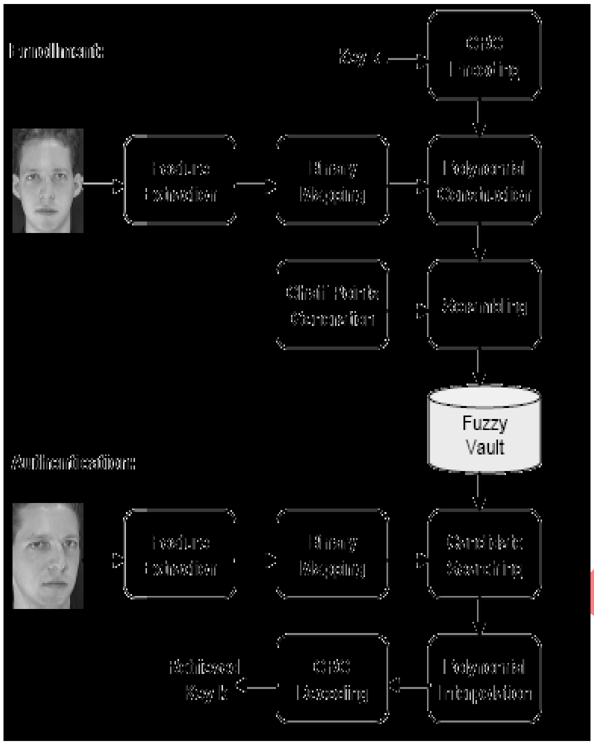

Figure 1: Proposed Method

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.

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.

Polynomial Construction C.

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

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

M(X)=x9+x7+x5+x2+1 bit sequence representation

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.

CONCLUSION

The security for the digital images has become highly important since the communication by transmitting of digital products over the open network occur very frequently .Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. Newly proposed image encryption techniques and also enhance the security level by introducing more than one chaotic scheme for image encryption algorithms. 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. **[1]** John Justin

[11] M, Manimurugan S , "A Surve on Various Encryption Techniques ", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012***.**

[12] Ephin M, Judy Ann Joy and N. A. Vasanthi, " Survey of Chaos based Image Encryption and Decryption Techniques " , *Amrita International Conference of Women in Computing (AICWIC'13)Proceedings published by International Journal of Computer Applications (IJCA).*

[13] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", *Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000.*

[14] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203),229-234.

[15] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", *Pattern Recognition 34,1229- 1245,2001.*

[16] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems ", *The Journal of Systems and Software 58 , 83-91,2001.*