A Biometric Solution to Cryptographic Key Management Problem using Iris based Fuzzy Vault

Mrunal Fatangare
M.E. CS IInd D.Y.Patil College of Engg.
Akurdi, Pune-411044, Maharashtra, India

K.N.Honwadkar
Asst. Prof.(IT) D.Y.Patil College of Engg
Akurdi, Pune-411044, Maharashtra, India

ABSTRACT

Reliable information security mechanisms are required in the today's era of cyber theft. Traditional Cryptography is a powerful mechanism to achieve information security. Current cryptographic algorithms (e.g., Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA) have a very high proven security but they suffer from the key management problem. Human identification is also a challenging field. That is why if we can make a blend of cryptography and biometric then it becomes a upcoming security tool. Using unique biometric identity of a person the keys for cryptosystem can be made secure. Iris is one of the proven and accurate means to identify person and it does not change throughout life of a person. This paper presents a biometric solution to cryptographic key management problem using iris based fuzzy vault.

Key words:

Biometrics, cryptosystem, fuzzy vault, encoding, decoding, chaff points, polynomial projection, Lagrange interpolation

1. INTRODUCTION

In cryptography keys are very important; as if keys are lost the reliability of the algorithm is lost. All cryptographic algorithms require that the keys must be securely stored and reasonably long. Though biometric authentication can be used to ensure that only the legitimate user has access to the secret keys, a biometric system itself is vulnerable to a number of threats. Traditional cryptography does not allow fuzziness whereas when biometric is included in the security system it is required that fuzziness should be allowed by the system. Fuzziness means while encrypting or decrypting system should allow a key to be released using a nearer biometric feature extraction. A intermingle of these two techniques can produce a high level security system. This system can be called as a biocrypto system or Fuzzy vault [4].

There are different ways to achieve the bio crypto system [12],

- Biometric based key release – keys are secured using system, this system let the user to use traditional key system. If biometric match is successful then the keys are released.
- Biometric key generation – in this system the biometric template is stored and features are extracted and used as cryptographic key.

The later sections of the paper are as follows: section II describes related work done by different scholars, section III describes the proposed method with its block diagram, section IV describes the future of fuzzy vault and section V concludes the paper.

2. RELATED WORK

A number of research works have been reported toward effective combination of biometrics with cryptography. Bodo [1] first proposed to use the data derived from the biometrics templates as the cryptographic key directly in his German patent. Juels and Wattenberg [2] proposed a fuzzy commitment scheme to combine CRC of Polynomial and Key. Error correction coding methods are used to tolerate variations of biometrics features. Juels and Sudan [4][8] introduced the basic fuzzy vault scheme. This scheme is based on the difficulty of polynomial reconstruction problem. During enrollment, a user selects a polynomial and encodes his cryptographic key into the polynomial's coefficients. The encoding of key can be achieved by dividing key into non-overlapping chunks and mapping to the coefficients. This system can compensate for intraclass variations in the biometric data. It is based on fingerprint minutiae extraction.

Chang et al [6] introduced a method to map the extracted face features to bits, and the bit stream is used as the cryptographic key. A major problem with their methods Generation is that the biometrics data is usually subject to drastic variation, and in general can not produce exactly the same key. Karthik Nandakumar, A.K.Jain[7][9][10] had worked a lot on the fingerprint based fuzzy vault. They implemented the system in encoding and decoding phase with CRC calculation, polynomial projection and adding noise to the system. Later they extracted helper data from the biometric and used it in decoding of fuzzy vault. They also proved that the fuzzy vault can be used in biometric template protection. They also have suggested that multiple fingerprints from same finger and multiple biometrics could be used for the greater security of fuzzy vault. E.S.Reddy and I.R.Babu[12][13] have worked on iris based fuzzy vault. In the system, they carry on work using iris data as password. This is not secure as it may contain much information about the template and expose it. They suggested the steps like iris localization, normalization, generation of secret key using iris data, then extracting locking elements and gerating fuuzy vault. Black and white images are used to carry out the work. It is totally minutiae based system. Implementation of fuzzy vault is carried out in three stages a. Transformation b. Encoding and finally c. Decoding.

In general the security of the fuzzy vault scheme lies in difficulty of polynomial reconstruction. Even though the biometric is compromised (the most dangerous situation) then also one could not get the secret code easily. As it will require sufficiently large time and expenditure required will be huge. Due this time and cost constraints ‘Fuzzy Vault’ is almost unbreakable.

The later sections of this paper presents a biometric cryptosystem construct called ‘fuzzy vault’ which is based on iris and which was originally proposed by Juels and Sudan[4] in “A fuzzy vault scheme,” in 2002 for fingerprints. This paper aims to show how biometric cryptosystem is used for providing authentication and in turn security to cryptographic keys.

3. PROPOSED METHOD

Proposed method that is iris based fuzzy vault involves two phases 1. Iris Feature extraction and 2. Fuzzy Vault construction (encoding and decoding). In our system it is allowed to use user defined 16 character long secret key. CRC is also used to decode the vault correctly. Iris once taken need not be normalized. We avoid it as translation and rotation may cause error. Statistical feature analysis is used to extract locking and unlocking elements.

3.1 Implementation

This section illustrates implementation of iris based fuzzy vault. Fig. 1 depicts diagrammatic representation of overall fuzzy vault scheme. For the implementation of the system few steps we have to carry. First eye image is preprocessed to get iris image. A set biometric future is first extracted from iris and analyzed on the ground of statistical analysis. Thus we obtain locking/unlocking units which are used to create vault. Thus normal iris template is not stored anywhere but in the transformed form (vault) it gets stored. Encoding includes CRC calculation, polynomial projection, chaff point generation (noise) and vault generation. Unlocking units are taken out from iris as same as the locking units. Decoding includes genuine point identification, Lagrange interpolation and CRC decoding.

3.2 Iris preprocessing

First eye image is taken and from the eye image iris image is taken out. Using canny edge detection iris from eye and pupil from iris is separated. Radius for iris is assumed to be between 60 – 100 pixels and 12 – 30 pixels for pupil. This radius is calculated manually. It is always assumed that the center of iris and pupil is same but sometimes it is found that the center is shifted by 2-4 pixels. Once you are able to get the iris image separated then proceed towards iris feature extraction. Figure 2 illustrates the extraction of iris from the eye image.

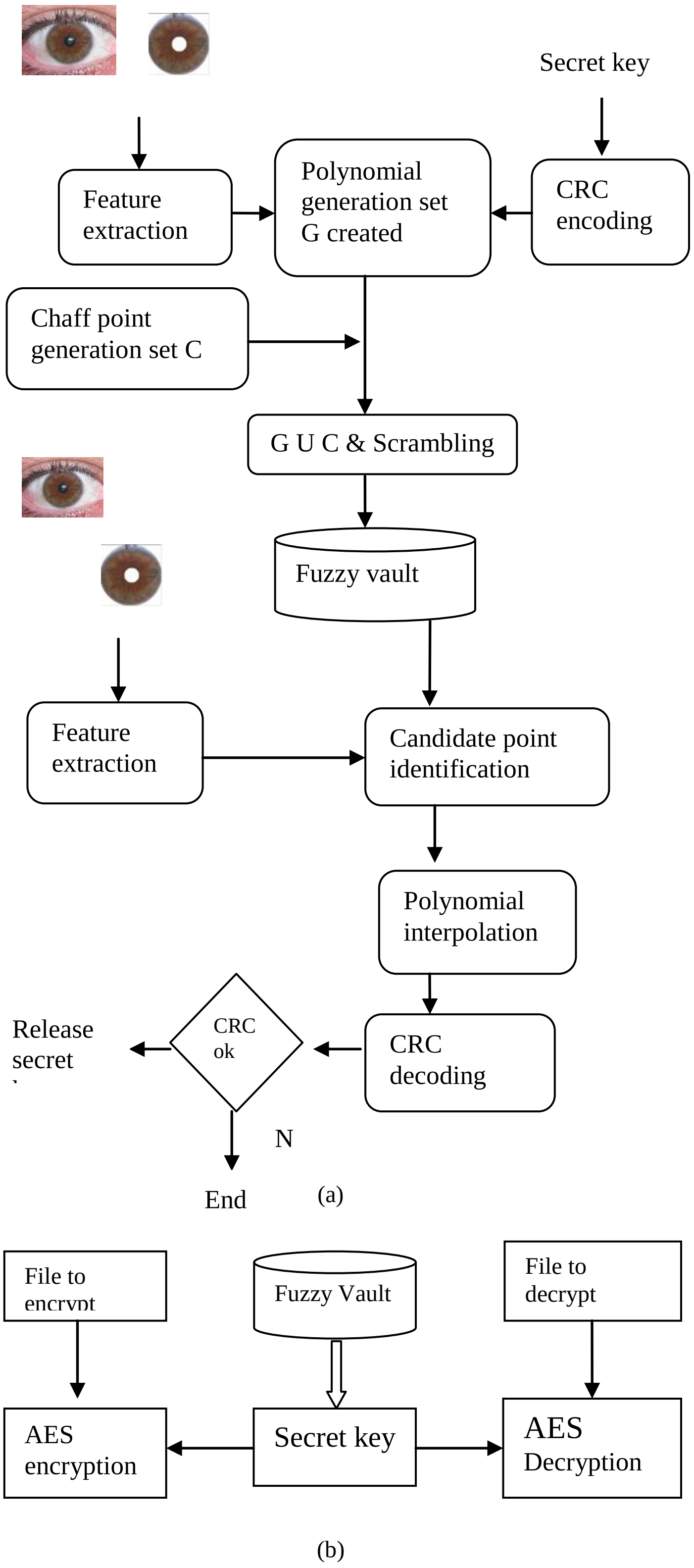
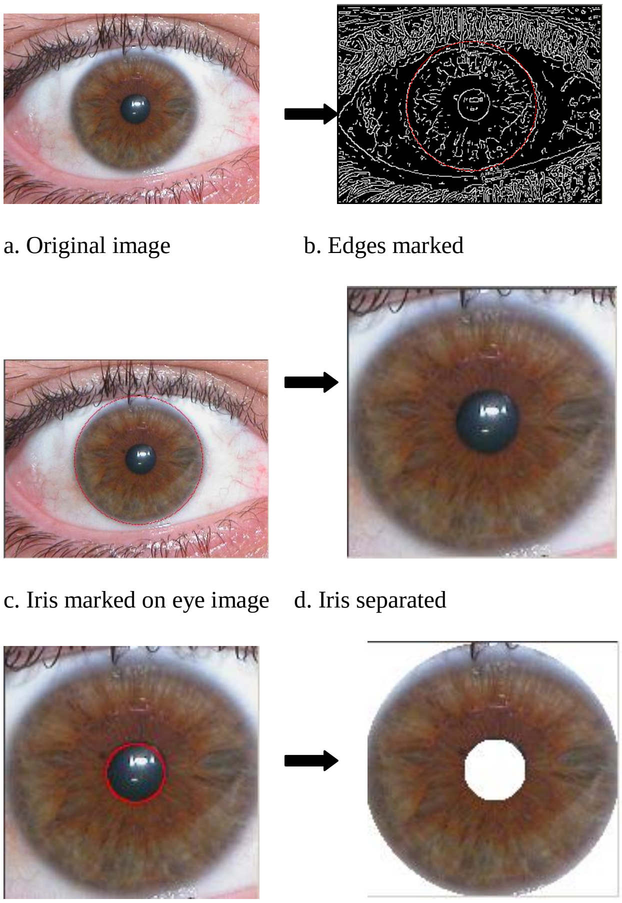


Figure1. (a) Overall fuzzy vault system architecture (b) Overall system architecture



a. Original image b. Edges marked

c. Iris marked on eye image d. Iris separated

e. Pupil marked on iris f. Iris separated from pupil

Figure 2: Iris preprocessing a. Original image b. result of canny edge detection c. Iris marked on eye image d. Iris separated e. result of canny edge detection f. Pupil marked on iris g. pupil separated h. Iris separated from pupil

3.3 Color histogram analysis

This is an important step in making fuzzy vault. Color histogram is a representation of the distribution of colors in an image. The histogram of an image is a statistical description of the distribution in terms of occurrence frequencies of pixel intensities, it can be considered as a feature vector representing the image in a lower dimensional space. Color image is converted to gray scale image. RGB values are analyzed and converted to equivalent y, u, and v values. This conversion is required because the RGB values cannot be taken directly while compressing. [15]

y = B * 0.114 + G*0.587 + R*0.299 + 128

u = B * 0.5 - G*0.33126 - R*0.16875 + 128

v = B * (-0.08131) - G*0.41869 + R*0.5 + 128

(128 added for the purpose of normalization of value as it should not fall below zero)

3.4 Iris feature extraction

It has been proven that the statistical data about iris can be used for iris recognition system [14]. That is why in our system statistical analysis of iris data is done first. For which following definitions are calculated:

1. Mean
2. Median
3. Mode
4. variance
5. Standard deviation of the circle's mean

On the iris image the circles are marked at the distance of 5 pixels each as shown in fig. 3. For every circle marked the above mentioned definitions are calculated.

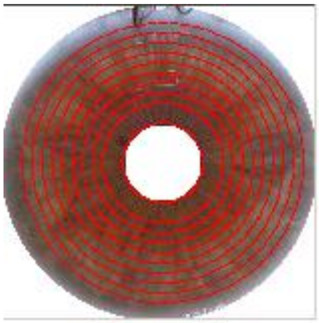


Figure3: Concentric circles marked on iris for feature extraction

To calculate **mean**

$$\overline{X^{2}} = \sum_{i=1}^{N} X_i^c , c = \overline{1,C}$$

Where

C – Number of circles in the separated iris

X^{c}_{i} – intensity value of the ith pixel of the cth circle

To calculate **variance**

$$S^{c^2} = \frac{1}{N^c - 1}\sum_{i=1}^{N^c}(X_i^c - \overline{X_i^c})$$

Where

N^c - number of pixels along the cth circle.

To calculate **Standard deviation**

$$SD = \sqrt{\frac{1}{N-c}\sum_{i=1}^{N}(X_i^c - \overline{X_i^c})}$$

Now these statistical features are stored in the database for further processing. Using these features, an image can be viewed as a feature vector. These statistical features are used for iris recognition process and extracting the locking elements from the iris.

As shown in fig.3 features are extracted from the concentric circles. From each circle 3 locking elements are taken. Hence from 6 circles, 18 locking elements can be collected. From 18 if 9 elements [(D +1)] matched then matching process becomes successful. To extract features concentric circles are used because it is observed that color pattern remains similar in circular fashion.

Algorithm to extract locking units

- Get original image
- Apply Canny edge detection, Gaussian smoothening
- Apply Hough transform to detect iris boundaries (Rmin = 60 and Rmax = 100)
- Separate iris with pupil from original image.
- Apply Canny edge detection on separated image
- Apply Hough transform to locate pupil (Rmin = 12 and Rmax = 30)
- Perform statistical analysis of separated iris image.
- Extract locking element as follows

Mode = 3 mean – 2 median

Standard deviation = sq. root of variance

Mode **|** standard deviation = 16 bit locking element.

3.5 Design issues:

The parameters used in the implementation of fuzzy vault are g, c, and d. Following table 1 shows the meaning and requirement of the parameters.

Table 01: Parameters used to design a Fuzzy Vault

Parameter	Meaning	Required
g	Number of genuine points Locking units Unlocking units	>D+1 (3 / circle) D+1 (9)
c	Number of chaff points	10 times g
d	Degree of polynomial	8
t	Total points in the vault	g + c

Genuine points are obtained from the biometric template and for this purpose it is required that the template should be clear enough to extract the features required.

As the numbers of chaff points are increased the security of the vault is generally increased. In some cases the attacker can take the advantage of greater number of chaff points to add his own biometric feature to break the vault. But generally the chaff points are used to confuse the attacker.

The degree of polynomial is depending on the secret length. For 16 character secret (128 bit) the polynomial is with degree 8. The whole security of system lies in the infeasibility of polynomial reconstruction.

The implementation of proposed work has been carried out on UBIRIS color iris database. Database is composed of 1877 images collected from 241 persons Camera Model used is Nikon E5700, Software E5700v1.0, Color Representation RGB, Focal Length 71 mm Exposure Time 1/30 sec. Image Width 2560 pixels, Height 1704 pixels, Horizontal Resolution 300 dpi, Vertical Resolution 300 dpi, Bit Depth 24 image format JPEG.

4. CONCLUSION

Fuzzy vault is one of the most comprehensive mechanisms for secure biometric authentication and cryptographic key protection. We have discussed a fully automatic and practical fuzzy vault system based on iris that can easily secure secrets such as 128-b AES encryption/decryption keys. In this paper we have elaborated the fuzzy vault based on statistical analysis of color iris. From the ring wise statistical analysis of iris it becomes easy to capture locking and unlocking elements. Also it improves the FAR of system. However the proposed method can be used for other biometric also. The performance of the fuzzy vault can be further improved by using multiple biometric sources, such as multiple modalities (e.g., iris and face, iris and fingerprint).

5. ACKNOWLEDGEMENT

I wish to thank all the people who gave me an unending support right from the stage the idea was conceived. I am also grateful to UBIRIS team for providing us with the huge database for work, without which implementation was just impossible. I express my profound thanks to **Prof. Mrs.M. A. Potey,** DYPatil C.O.E. who have guided and helped me in preparation of this paper.

6. REFERENCES

[1]. A. Bodo, Method for producing a digital signature with aid of biometric feature, German Patent DE 42 43 908 Al, 1994

[2]. Juels, and M. Wattenberg, "A fuzzy commitment scheme", Proc. of sixth ACM Conf. on Computer and Communication Security, pp. 28-36, 1999

[3]. N. K. Ratha, J. H. Connell, and R. M. Bolle, “An Analysis of Minutiae Matching Strength,” in Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), Halmstad, Sweden, June 2001,pp. 223–228.

[4]. Jules and M. Sudan, “A fuzzy vault scheme”, in Proc. IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, 2002, p. 408.

[5]. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, “Biometric cryptosystems: Issues and challenges,” Proc. IEEE (Special Issue Multimedia Security for Digital Rights Management), vol. 92, no. 6, pp. 948–960, Jun. 2004

[6]. Y J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation", Proc. of IEEE Int. conf. on Multi-media and Expo, pp. 2203-2206, 2004

[7]. Anil K.Jain, Sharath Pankanti,Umut Uludag Department of Computer Science and Engineering, “Fuzzy vault for fingerprint”, Michigan State University, East Lansing, MI, 48824 2.Exploratory Computer Vision Group, IBM T.J. Watson Research Center, Yorktown Heights, NY, 10598

[8]. Ari Juels RSA laboratories, 174 middlesex turnpike, bedford, ma 01730, USA ,Madhu Sudan Massachusetts Institute of Technology, 32 Vassar street, Cambridge, MA 02139, USA, “A Fuzzy Vault Scheme” , RSA Lab,

Received November 27, 2002; Revised January 12, 2005; Accepted February 16, 2005

[9]. Karthik Nandakumar, Student Member, IEEE, Anil K. Jain, Fellow, IEEE, and Sharath Pankanti, Senior Member, IEEE, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", IEEE transactions on information forensics and security, vol. 2, no. 4, December 2007.

[10]. Karthik Nandakumar, Abhishek Nagar and Anil K. Jain, "Hardening Fingerprint Fuzzy Vault using Password", International Conference on Biometrics, pp.927-938, 2007.

[11]. Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008

[12]. E. Srinivasa Reddy, Ramesh Babu; "Performance of Iris Based Hard Fuzzy Vault" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008

[13]. E. Srinivasa Reddy, Ramesh Babu; "authentication using fuzzy vault based on iris texture" Second Asia international Conference on Modeling & Simulation 2008, pp 361-368

[14]. Khin Sint Sint Kyaw "iris recognition system using statistical features for Biometric identification", international conference on electronic computer technology, pp 554 – 556, 2009

[15]. Book- digital Image Processing – Rafael C. Gonzalez, Richard E.Woods, Pearson Education. Pg.no.522