International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Biometric Database Protection using Elliptical Curve Cryptography in Biometric Cryptosystem

Kushalatha.M.R. [Å*] and Ambika.D.R.[Å]

[Å]BMS College of Engineering, Bangalore

Accepted 15 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

Biometric crypto systems are being increasingly deployed in many large-scale biometric applications because they have several advantages such as lower error rates, larger population coverage, offers facility, comfort and more security to users. However in biometric Systems where the user database is stored is vulnerable to several type of attacks. As to protect these databases from attacks efficient encryption and decryption methods have to be used. The generation of direct key using these databases is also of importance. In this paper, extraction of features of face images like mouth region, eyes are done using AdaBoost Algorithm and a database is generated out of these segmented features. We also present various methods that monolithically bind a cryptographic key with the biometric templates of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. We illustrate the challenges involved in biometric feature recognition primarily due to drastic acquisition variations in the representation of a biometric identifier and the imperfect nature of biometric feature extraction and matching algorithms.

Keywords: *Adaboost, Biometric Cryptosystems, Elliptical Curve Cryptography, K- Means Algorithm*

1. Introduction

With the need to ensure security in several large applications, biometrics is presented as an alternative solution that replaces traditional authentication techniques such as the password and other identifiers; it presents simplicity to the user and can also control access to applications. However, biometric systems are also vulnerable to several attacks and especially a user template stored in the database can be used by an attacker to view confidential information or to gain access illegitimately to the system.

Biometric cryptosystems use the biometric characteristics and a secret key to generate information that does not reveal important information about the biometric data or the key. During the authentication phase the key must be generated for a successful authentication.

The objective of this work is to propose criteria for performance evaluation and vulnerability analysis of biometric cryptosystems based on *Elliptical Curve Cryptography approach*. In section 2 of this article the face detection using *Adaboost Algorithm* is described. In section 3 biometric cryptosystems based on *Elliptical Curve Cryptography approach* and the proposed criteria and the considered scenarios for the *key generation* are detailed. Conclusions and perspectives are drawn in section 4.

1.1. Encryption using ECC

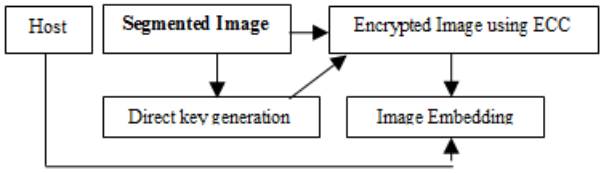

Fig 1. Block Diagram of the Encryption using Elliptical Curve Cryptography

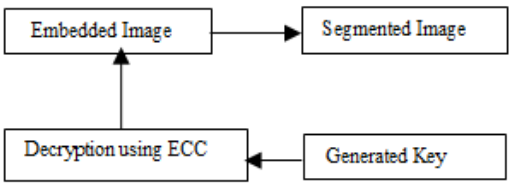

Fig 2. Block Diagram of the Decryption using Elliptical Curve Cryptography

2. ADABOOST Algorithm for Face Recognition &Feature Extraction

We implemented a face detector based on AdaBoost algorithm. We used Integral image and the AdaBoost learning algorithm (Freund and Schapire, 1995) to greatly decrease the computation time.

The following three key ideas are presented in our work.

1. Haar-like features are applied to represent image information. These features can be efficiently evaluated

*Corresponding author: **Kushalatha.M.R.**

using integral images. By varying the parameters of these Haar-like features, a large number of image features can be obtained.

2. Adaboost is used to construct a classifier. Each Haar-like feature is associated with a weak learner, providing weak evidence of the objects' existence. Adaboost selects and combines weak learners to build a strong learner. In testing, only a small set of features are evaluated, rendering an efficient computation.

3. A cascade structure is introduced to decrease computation by focusing on image regions having high probability of containing objects of interest. The cascade is formed by a set of successively more complex and hence more discriminative Adaboost classifiers. For a sub-window to be considered as a positive, namely containing an object of interest, it must pass all stages of the cascade. The computational efficiency is gained by the fact that the low-level classifiers can alter out a large number of negatives with a low computational cost. Only a small number of candidates, having high likelihood of containing object of interest, advance to higher levels, which involve more computation to differentiate between positives and negatives.

3. Elliptical curve cryptography

Elliptic curve cryptography (ECC is a public key cryptography technique, based on the concept of elliptic curves. It can be effectively deployed in environments such as pagers, PDAs, cellular phones and smart card. A user participating in public key cryptography will essentially have a pair of keys, i.e., a public key and a private key. Only the particular user is aware of the private key whereas the public keys are distributed to all users taking part in the communication. The general cubic equation of elliptic curves can be written as

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (1)$$

But for practical application the equation reduces to

$$y^2 = x^3 + ax + b \quad (2)$$

Where a, b, c, d, e are appropriately either rational numbers, real numbers or integers mod p

3.1 ECC implementation and results

1. Let m the message pixel to be encrypted. The first task in the system is to encode the plain pixel message m to be sent as the x-y point P_m. This point P_m will be encrypted as a cipher pixel and subsequently decrypted.

2. An encryption system requires a point G and an elliptic group Ep (a, b) as parameters. The encryption key is generated as

$$P_A = n_A * G \quad (3)$$

Here n_A is the primitive root of the prime number p.

3. To encrypt and send a message P_m, a random positive integer 'k' is selected and the cipher text C_m is produced as a pair of points as given in equation

$$C_m = \{kG, P_m + kP_A\} \quad (4)$$

4. To decrypt the cipher pixel, the first point in the received pair is multiplied with n_A and subtracts the value obtained from the second point as given below.

$$P_m + kP_A - n_A(k.G) = P_m + k(n_A.G) - n_A(k.G) \quad (5)$$

3.2. K means algorithm for direct key generation

Direct key generation from biometrics is an appealing template protection approach which can also be very useful in cryptographic applications. A distinct advantage of using direct key generation is that the keys need not be remembered since the keys are derived from the templates. K-means is one of the simplest unsupervised learning algorithms that solve the well known clustering problem. The procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume *k* clusters) fixed a priori. The main idea is to define *k* centroids, one for each cluster. Since the end result is a function of the centroid location, the location of the centroids is of utmost importance. Hence, a variation in the location of the centroids may give rise to a different result. So, the better choice is to place them as much as possible far away from each other.

The next step is to take each point belonging to a given data set and associate it to the nearest centroid. When no point is pending, the first step is completed and an early groupage is done. At this point we need to re-calculate *k* new centroids as barycenters of the clusters resulting from the previous step. After we have these *k* new centroids, a new binding has to be done between the same data set points and the nearest new centroid. A loop has been generated. As a result of this loop we may notice that the *k* centroids change their location step by step until no more changes can be done.

The generation of biometric key is implemented using following steps:

i. Place *k* points into the space represented by the objects that are being clustered. These points represent initial group centroids.

ii. Assign each object to the group that has the closest centroid.

iii. When all objects have been assigned, recalculate the positions of the *k* centroids

iv. Arrange the centroids as $N_1N_2N_3\ldots N_k$. If there are 8 clusters, this approach gives an 8 digit number.

v. Finally concatenate the clusters as to get the key.

3.3. Results

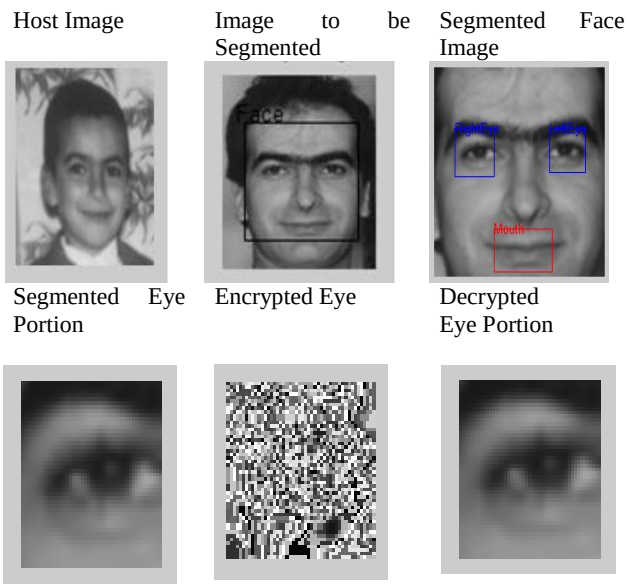

Fig 3. ECC Encryption & Decryption

4. Conclusion

In this paper, the use of Adaboost Algorithm for face detection and segmentation of features are done. The reason why the face detector obtains many false positive is the number of the non-faces in the training dataset is too small. The strong classifier is greatly dependent on the faces and non-faces in the database. However, in most case, the face detector can correctly find the face.

ECC based encryption scheme has been proposed for biometric template protection. The keys used for the encryption schemes were derived from the biometric template itself using the K-means algorithm. Even though other encryption has a faster time response, ECC based encryption performs better under noise analysis and hence it is useful for remote authentication applications.ECC uses less number of bytes to generate the key.

References

M.Mani Roja and Sudhir Sawarkar (May 2013)**,** Biometric Database Protection using Public Key Cryptography IJCSNS International Journal of Computer Science and Network Security, Vol.13 No.5, 20

Maryam Lafkih, Mounia Mikram, and Sanaa Ghouzali (2012) *Biometric Cryptosystems : Security Analysis* IEEE International Conference on Computer Science & Education, , 978-1-4673-2679-7/12.

Abhishek Nagar (Feb 2012), Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and AnilK. Jain, Fellow, IEEE *Multi biometric Cryptosystems Based on Feature-Level Fusion* IEEE Transactions on Information Forensics and Security Vol 7, No 1,

R. Ranjan and Sanjay Kumar Singh (2012) Department of Computer Engineering Indian Institute of Technology (BHU), Varanasi, India *Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems*,978-1-4673-4529-3/1

Enrique Argones R´ua , Emanuele Maiorana , Jos´e Luis Alba Castro , Patrizio Campisi *Feature Fusion for Template Stability in Biometric Cryptosystems. An Application to Face Biometrics based on Eigen-Models*, IEEE 978-1-4673-4688-7.