ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Encryption of Cryptographic key technique by crossover of Iris and Face Biometric key

Gokulakumar.A.S, Venkataraghavan.C, Kavya priya.S, Suganya.T

Student, Department of CSE, SNS College of Engineering, Coimbatore, Tamilnadu, India[1, 2]

Student, Department of IT, Info Institute of Engineering, Coimbatore, Tamilnadu, India[3]

Asst. Professor, Department of CSE, SNS College of Engineering, Coimbatore, Tamilnadu, India[4]

ABSTRACT---The security is an important aspect in our daily life whichever the system we consider security plays vital role. The biometric person identification technique based on the pattern of the human Iris and face is well suited to be applied to access control and provides Strong security. In this paper we focus on an efficient methodology of fusion of iris and face for identification and verification with total success rate. In this method, the image of the face taken is normalized and converted into binaries. The iris is localized from the facial image and then series of operations such as segmentation, normalization, feature encoding is performed and it is converted into binaries. These bits are compressed and crossed over into a combined biometric key. This combined biometric key is used to bind the each bit of the cryptographic key. This binded version of the key is used for enrollment and to release the key. Instead of storing the actual key, its hashed version is stored in order to conceal the cryptographic key to provide a secure comparison method for key verification. This binded version of the key is released only if this matches with the one which is generated lively. During enrollment, these features are used to bind a cryptographic key. The operation involved is the binary XOR. Here, the goal of the system is to reject, an unauthorized subject who does not possess the original face features used during enrollment. In contrast, a genuine subject with the correct face features will be accepted. By this spoofing can be avoided, since two kinds of keys are needed to encrypt the data and these keys are generated at once. This reduces the false acceptance rate and false rejection rate thereby the total success rate seems to be high since the key preserves security level to high.

KEYWORDS---Biometric key, Cryptographic key, Helper data, Hashed key.

I. INTRODUCTION

Biometric authentication is the primary and prevalent system for security and surveillance activities in the past several years. The automation in every field of daily life has made human identification and verification is a prime issue for ensuring the security. The biometric techniques are relates to the parts of human body which are unique, cannot be stolen and is not easily transferable compared to traditional methods such as Identification badges, Personal Identification Number (PIN), password, smartcards etc.. The commonly used biometric features include speech, fingerprint, face, Iris, voice, hand geometry, retinal identification, and body odor identification. Of this face biometrics is used throughout the world for various applications include surveillance, access control, e-passport, and human-computer interaction. And iris is a biometric feature, found to be reliable and accurate for authentication process comparative to other biometric feature available today. The fusion of this both face and iris would increase the false acceptance rate to make the application secured by preventing spoofing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. PROPOSSED ALGORITHM

The proposed algorithm contains the following steps:

a. Biometric key generation

Step 1: Images acquisition.

Step 2: Enhancement of the images.

Step 3: Feature extraction.

Step 4: Biometric key of both iris and face is generated.

b. Combined key generation

Step 1: Biometric key of iris 2048 bit of data is compressed

Step 2: Biometric key of face 248 bit of data is compressed

Step 3: Compressed biometric key of both iris and face is crossed over then combined key generated.

c. Generation of helper data and hash key

Step 1: Performing Hashing function on the cryptographic key and Store the hashed key in the database.

Step 2: Helper data is generated as a result of binding the cryptographic key with the combined biometric key.

2.1 BIOMETRIC KEY GENERATION

IRIS

IMAGE ACQUISITION

Image acquisition is considered the most critical step in our project since all subsequent stages depend highly on the image quality. In order to accomplish this, we used a CCD camera. We set the resolution to 640x480the type of the image to jpeg, and the mode to white and black for greater details.

SEGMENTATION

The main purpose of this process is to locate the iris on the image and isolate it from the rest of the eye image for further processing. Some other important tasks that are also performed in this iris segmentation block include image quality enhancement, noise reduction, and emphasis of the ridges of the iris. The image was filtered using Gaussian filter, which blurs the image and reduces effects due to noise. The iris inner and outer boundaries are located by finding the edge image using the Canny edge detector, then using the Hough transform to find the circles in the edge image. For every edge pixel, the points on the circles surrounding it at different radius are taken, and their weights are increased if they are edge points too, and these weights are added to the accumulator array. Thus, after all radiuses and edge pixels have been searched, the maximum from the accumulator array is used to find the center of the circle and its radius according to the equation

$X^{2+} Y^2 = r^2$ …..(1)

Where *X, Y* are the center of the circle and *r* is the radius of the circle. The highest two points in the Hough space correspond to the radius and center coordinates of the circle best defined by the edge points.

NORMALIZATION

This part is to enable the generation of "iris code". Normalization process involves unwrapping the iris and converting it into its polar equivalent as shown in Fig[1]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

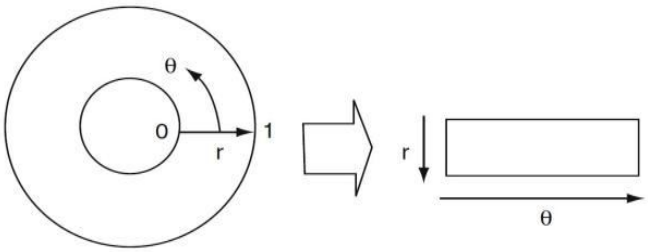

Figure 1: Generating normalized Iris Image

$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta)$ ….. (2)

With

$x(r,\theta) = (1-r)\, x_p(\theta) + r x_i(\theta)$ ……..(3)

$y(r,\theta) = (1-r)\, y_p(\theta) + r y_i(\theta)$ ……..…(4)

where

I(x,y) - iris region image, *(x,y)* –original Cartesian coordinates, *(r,* **θ***)* - corresponding normalized polar coordinates, and x_p, y_p and x_i ,y_i are the coordinates of the pupil and iris boundaries along the **θ** direction.

It was decided to use only the left and right parts of the iris area for iris recognition. Therefore, the whole iris is $[0, 360^0]$ not transformed in the proposed system. Experiments were conducted by normalizing the iris from $[-32,32^0]$ and $[148, 212^0]$, ignoring both upper and lower eyelid areas. Left and right images each one of size 112×60 are obtained. By applying this approach, detection time of upper and lower eyelids and 64.4% cost of the polar transformation are saved.

FEATURE EXTRACTION

In an iris recognition system, the 2-D Wavelet transform is only used for preprocessing. The preprocessing helps to reduce the dimensionality of feature vector and to remove noise. Nevertheless, the computational complexity is comparatively high. Thus, the paper proposes 1-D wavelet transform as filter to reduce the dimensionality of feature vector, and it can further reduce the computational complexity. The wavelet is constructed from two-channel filter bank as shown in Fig. 2(a). In wavelet decomposition of 1-D signal, a signal is put through both a low-pass filter L and a high-pass filter H and the results are both low frequency components A[n] and high frequency components D[n]. The signal y[n] is reconstructed by the construction filters *H* and *L* The wavelet filters are used to decompose signals into high and low frequency by convolution. In order to construct multi-channel filter, we can cascade channel filter banks. Fig.2(b) represents a 3-level symmetric octave structure filter bank.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

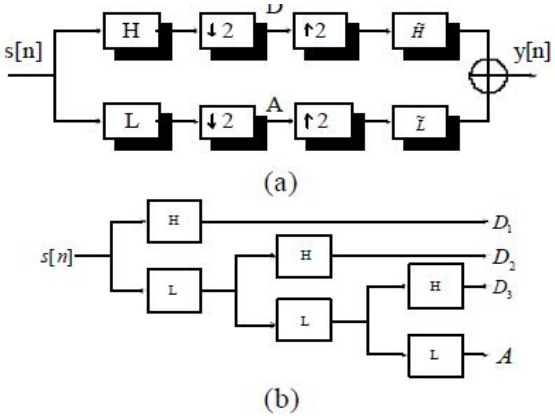

Figure.2. (a) Two-channels filter bank
(b) 3-level octave band filter bank.

2.2 FACE

IMAGE ACQUISITION

Image acquisition module is to seek and then extracts a region which contains only the face. Face detection is used to detect face and to extract the information related to facial features. The image will then be resized and corrected geometrically and it will eliminate the background and scene which are unrelated to the face so that it is suitable for recognition.

PREPROCESSING

The purpose of the preprocessing module is to reduce or eliminate some of the variations in face due to illumination. It normalized and enhanced the face image to improve the recognition performance of the system. The preprocessing is crucial as the robustness of a face recognition system greatly depends on it. By using the normalization process, system robustness against scaling, posture, facial expression and illumination is increased. The photometric normalization techniques are used in
histogram filtering[5][6].

HISTOGRAM EQUALIZATION

Histogram equalization is the most common histogram normalization or gray level transform, which purpose is to produce an image with equally distributed brightness levels over the whole brightness scale. It is usually done on too dark or too bright images in order to enhance image quality and to improve face recognition performance. It modifies the dynamic range (contrast range) of the image and as a result, some important facial features become more apparent.

The steps to perform histogram equalization are as follow:
1. For an N x M image of G gray-levels, create two arrays H and T of length G initialized with 0 values.
2. Form the image histogram: scan every pixel and increment the relevant member of H-- if pixel X has intensity p, perform
H[p] = H[p] +1 (1)
3. Form the cumulative image histogram Hc; use the same array H to store the result.
H[O] = H[O]
H[p] = H [p -1] + H[p]
For p = 1,..., G-1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

4. Set
G -1I
T[p] H[p] (2)
MN7
Rescan the image and write an output image with
gray-levels q, setting q = T[p].

FEATURE EXTRACTION

The purpose of the feature extraction is to extract the feature vectors or information which represents the face. The feature extraction algorithms used is Principal Component Analysis (PCA)

PRINCIPAL COMPONENT ANALYSIS (PCA): PCA for face recognition is based on the information theory approach. It extracted the relevant information in a face image and encoded as efficiently as possible. It identifies the subspace of the image space spanned by the training face image data and de-correlates the pixel values. The classical representation of a face image is obtained by projecting it to the coordinate system defined by the principal components. The projection of face images into the principal component subspace achieves information compression, de-correlation and dimensionality reduction to facilitate decision making. In mathematical terms, the principal components of the distribution of faces or the eigenvectors of the covariance matrix of the set of face images, is sought by treating an image as a vector in a very high dimensional face space [7][8][9].We apply PCA on this database and get the unique feature vectors using the following method .Suppose there are P patterns and each pattern has t training images of m x n configuration.

• The database is rearranged in the form of a matrix where each column represents an image.
• With the help of Eigen values and Eigen vectors covariance matrix is computed.
• Feature vector for each image is then computed.

This feature vector represents the signature of the image. Signature matrix for whole database is then computed.

•Euclidian distance of the image is computed with all the signatures in the database.
• Image is identified as the one which gives least distance with the signature of the image to recognize.

a. Generation of combined key:

- After the data of the image (iris) is converted into local binary pattern (LBP). This LBP provides 2048 bit data. This 2048 bit of data is compressed.
- After the data of the image (face) is converted into LBP. this LBP provides 256 bit of data.

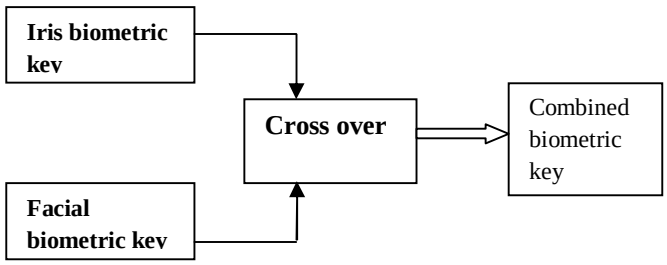

Fig 3 Illustrative of crossing the facial and iris biometric key.

The facial and iris biometric keys are crossed over to obtained the combined key. The process of crossing over includes the encryption of facial biometric key using Iris biometric key. this combined key is used for enrollment as well as verification.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

B. Generation of helper data and hash function

Enrollment/key binding

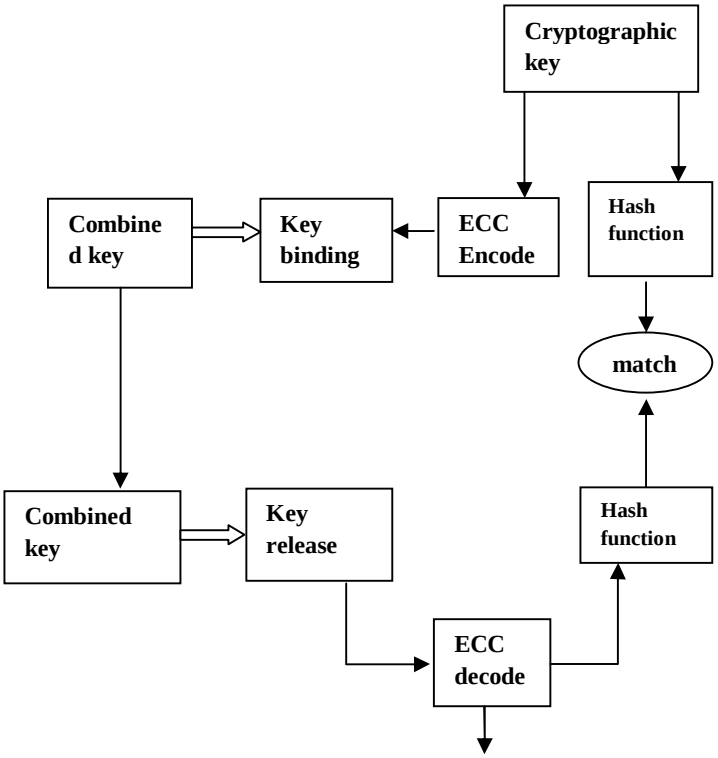

Fig. 4. The configuration of the HDS-based biometric encryption System for enrollment (key binding) and verification (key release).

From the cryptographic key module, two diverging paths are implemented: one is cryptographic hash to generate a hashed key and the other is error-correcting code (ECC) to protect against fuzzy variability and other distortions. The data obtained after ECC are then used as input to a key binding module. The key binding module utilizes feature vectors to securely embedded the encoded key and produce another helper data to be used during verification.

CRYPTOGRAPHIC HASH FUNCTION

Instead of storing the actual key, its hashed version is stored in order to conceal the cryptographic key in a helper data form suitable for storage and to provide a secure comparison method for key verification. A hash function accepts a variable-length input and produces a fixed-length output [1].

In addition, to take into account of the fuzzy variability in the extracted feature vectors, error-correcting code (ECC) is needed and we choose the BCH family of codes [2, 3].

KEY BINDING MODULE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The objective of the key binding module is to utilize a feature vector to securely bind the encoded cryptographic key, which generates a helper data for storage. In this work, each component of the PCA feature vector is used to bind one bit of the cryptographic key (after error-correcting encoding), separate the process into two sub-modules: key binding and key release, corresponding to the enrollment and verification stages, respectively. The first module performs the biometric binding process, while the second is responsible for verifying the biometric and unbindingthe cryptographic key. Figure 5(a) shows the key binding process. First, the cryptographic key is encoded for error tolerance. It is then bound to the binarized feature vector. The binding is performed using an XOR operation. This process is analogous to storing and locking the cryptographic key in a "secure box", where the "key" to this box is the biometric feature vector itself. Without access to the correct physiological features, the cryptographic key cannot be recovered. Thus, an intruder cannot feasibly produce the feature vector necessary to unlock this secure box. The theoretical basis of this form of information concealment is known as a one-time pad (OTP) [1]. Basically, as long as the mask used for XOR (i.e., the binarized feature vector) is of random nature, then the "locking" mechanism is information-theoretically secure.

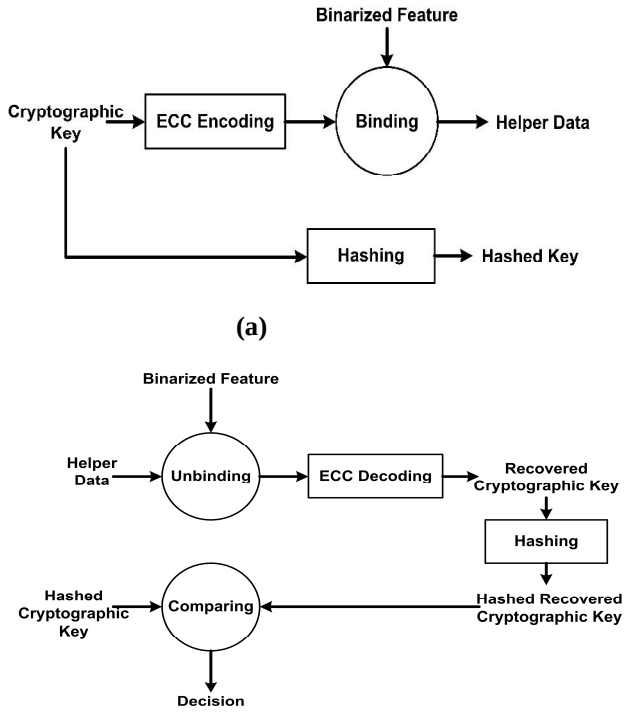

Fig 5. Illustration of (a) the key binding process, (b) the key release process

Figure 5(b) shows the steps for unbinding the key. In this case, a user claiming some identity submits his or her facial and iris features for verification, from which a binarized feature vector is extracted. The unbinding operation is also an XOR operation. If the two feature vectors, during enrollment and during verification, match exactly, then the original cryptographic key is unbound successfully. However, in a practical scenario, there are typically differences in the two vectors. Due to the XOR operation, the bit differences take the form of an aggregate "error vector". This error vector has the equivalent effect of an additive (binary) noise on the received codeword. It is characterized using the Hamming

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

distance, which is defined as the number of bit differences between two binary sequences. The ECC decoding block is responsible for eliminating these bit differences, up to some allowed Hamming distance. The result of the ECC decoder, the recovered cryptographic key, needs to be tested for authenticity. It should be noted that the original key is not stored (in plain text) anywhere; instead only its hashed value is available. Therefore, the hashed value of the recovered key is generated for comparison against the stored value. If the two hashed values match exactly, then the system declares a positive match. Otherwise, the system rejects this user.

III. BENEFITS

- As it increases the Total success rate (TSR) by reducing False Acceptance Rate (FAR) and False Rejection Rate (FRR), the performance of the system can be increased.
- The hashed key is the only data to be stored. So the unauthorized user cannot access the database hence he is unaware of the details used in hashing function.
- The security level seems to be high since both face and iris have been taken into the account.
- The probability for spoofing can be minimized. Since two techniques of biometrics are fused together, the rate of spoofing will be minimized. If an unauthorized user trying to spoof an account, even they cannot access since even the key may not released if it recognizes about the unauthenticated access.

IV. APPLICATION

It can be used in systems where high security is needed such as banking, border crossing security, criminal identification, armies, national border security forces, national security forces etc.

Nowadays, in banking, the data are to be stored in clouds. To access such data with high security and to make it secured the hashed key can be used.

It can be used to access a high secure data in personal computers, laptops or in any other devices.

V. CONCLUSION

This paper presents a combination of face recognition and Iris biometric encryption using helper data system (HDS). The HDS-based biometric encryption system is described in detail, with emphasis on the key binding module. The false rejection rate and the false acceptance rate can be minimized by this fusion technology as it increases the accuracy. The total success rate and the system performance can be increased. The main objective to avoid or prevention of spoofing can be achieved. The hardware and software for this technology is somewhat costlier when compared to others. This makes the system can't be used frequently. But while considering the agony faced by customers, the high price to be paid is worthy.

REFERENCES

[1] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[2] R. Morelos-Zaragoza, The Art of Error Correcting Coding, Wiley, 2006.

[3] S. Lin and D. Costello, Error Control Coding, Prentice-Hall, second edition, 2004.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[4] Karl Martin, Haiping Lu, F. Bui, K. N. Plataniotis, and Dimitris Hatzinakos, "A biometric encryption system for the self-exclusion scenario of face recognition," IEEE Systems Journal, 2009, under review.

[5] T. A. M. Kevenaar, G. J. Schrijen, M. v. d. Veen, A. H. M. Akkermans, and F. Zuo, "Face recognition with renewable and privacy preserving binary templates," in Proc. IEEE Workshop on Automatic Identification Advanced Technologies, October 2005, pp. 21–26.

[6] Haiping Lu, Karl Martin, Francis Bui, K. N. Plataniotis, Dimitris Hatzinakos, Face recognition with biometric encryption for privacy-enhancing Self-exclusion.

[7] Tsuyoshi Kawaguchi, Mohamed Rizon, Iris detection using intensity and edge information, Pattern Recognition 36 (2003) 549 – 562.

[8] Taranpreet Singh Ruprah, Face Recognition Based on PCA Algorithm.

[9] Rama R, PG Scholar.,Vijay albert William, Design of Iris Recognition based Authentication System in ATM, International Conference on Computing and Control Engineering (ICCCE 2012).