Multimodal Biometric Key Generation for Cryptographic Security using Face and Iris

Balamurugan, G., Dr. K.B. Jayarraman, Arulalan, V., Lokesh, V.

ABSTRACT
To incorporate the user’s convenient for utilization of biometric feature for the cryptographic security. In order to reduce the effort of remember a memorable password. To generate the key from the biometric features for security is so as to make the key unpredictable to an intruder lacking the knowledge about the user’s biometrics. Multimodal key generation so as to obtain a cryptographic optimal security. In this paper, we propose an efficient technique based on Multimodal Biometric (FACE and IRIS) for generation of secure key generation. The proposed technique is composed of three main modules namely Feature Extraction, Multimodal biometric template generation, Cryptographic key Generation. Initially, the features like Texture properties are extracted from the face and iris respectively. Consequently, the extracted features are fused together at the feature level to obtain the multi-modal Biometric Template. As a final 256-bit secure cryptographic key is generated from the multi-Biometric template.

INTRODUCTION
The requirement for the reliable user authentication approach has been arised for high-end to the security issues in networking and communication modalities (Beng et al 2008). The generalized security standard to maintain for protection of the user information using some cryptographic standard mechanism like symmetric and asymmetric methodologies and using key authorities. The security mechanism provided by the cryptographic analysis is not more precise for the protection; the general authentication technique can be altered by cracking the password obtained by the cryptography; so we need an additional security based on the cryptographic analysis. Biometrics plays an important role for the protection system (Jagadeesan et al 2010). The major recognition and the security protection is depend only on the biometric system. Additionally new concept called multimodal biometric system has been imported to specify the security mechanism for the protection. The term multimodal Biometric plays a vital role for joining, the two modalities which perform fusion and also the feature level technique for the template construction. From this methodology an important functional properties for security is obtained; where a cryptographic key generation is carried from the feature level biometric template (Anil Jain et al 2005). From this the obtained key value can be used for the encryption and decryption purpose.

II. The Contribution of the Proposed System
1. Feature extraction from face and iris
2. Multimodal template generation
3. Cryptographic key generation

A. Feature Extraction From Face Image:
Face recognition is considered to be noticeable biometric authentication system which can be processed by using various functional properties and algorithms like PCA, LDA etc (Yan et al 2008). Hence in this facial
recognition technique, we perform texture analysis based on local mapping binary pattern (LMBP); in this it follows two main functions like
1. Computational Efficiency
2. Robustness

B. Working of LMBP Algorithm:
Step1: Facial images divided into small regions
Step2: a texture description for sub images is then intended using LMBP
Step3: then texture descriptions are combined to form histograms
Steps4: Finally histogram encoded to the exterior and the spatial relations of facial regions.

LMBP is known as an ordered set of uniform patterns at a given pixel position. To extract the LMBP texture descriptor of a region, the operation begins by assigning a label to each pixel of a region by the 5x5 neighborhood of a pixel with the pixel representation.
The decimal form of 8-bit (LMBP) is given by
\[
\text{LMBP}(X_c, Y_c) = \sum_{n=0}^{5} S(n - ic)2^n
\]

Where:
- \(X_c\) and \(Y_c\) are the center pixel
- \(I_n\) is the value of the 8 surrounding pixels
- \(S(x) = \begin{cases} 1 & \text{if} \ x \geq 0 \\ 0 & \text{if} \ x < 0 \end{cases}\)

The local neighborhood is defined as the set of evenly spaced sampling points on a circle centered at the pixel; a sampling point which does not fall at the center of a pixel is calculated through bilinear interpolation; to compare histograms, we employ the chi-squared distance defined as
\[
X^2(u, v) = \sum_{i=1}^{m} \left( \frac{(u_i-v_i)^2}{(u_i-v_i)} \right)
\]

As LMBP approach is taken as an advance for the texture analysis which provide the property of tolerance against illumination changes is termed as “FACE HISTOGRAMS”.

**Fig. 1:** Block Diagram for the proposed System.
Were $u$ & $v$ are histogram which is normalized, $n$-is the number of elements in the histogram. This pair of histograms was measured by the chi-squared distance.

$$x^2 + y^2 = r^2$$

**Fig. 2:** Neighbourhood Circular format with 8 sampled points radius of 2.

**C. Feature Extraction From Iris Image:**

Iris recognition is an approach for the biometric authentication that uses pattern-recognition method which is based on high resolution images of the irises of an individual user. The human iris, which is said to be an annular part between the pupil (generally, visible black in an image) and the white sclera has an extraordinary structure and that provides many intermingle minute characteristics such as freckles, stripes, etc. These are the visible characteristics, which are generally defined as the texture of the iris, are unique. While most biometric value has 13 to 60 distinct characteristics, the iris is defined to have 266 unique spots. Each eye is supposed to be unique and remain stable over time. In this we perform canny edge detection and then Hough Transform for the identification of arbitrary shapes.

**D. Basic Steps in Iris Recognition:**

The first step, image acquisition deals with captures the sequence of iris images from the cameras and sensors. These images should clearly display the entire eye particularly iris and pupil, and preprocessing operation may be carried to enhance the value of image e.g. histogram equalization, noise removal using filtering etc. The next step of iris recognition is to isolate the iris part from the eye image, called segmentation. It is a technique necessary to isolate and exclude the object as well as locating the circular region of iris. The inner boundaries and the outer boundaries of the iris are calculated. Segmentation of iris relies on the quality of the images of eye. An automatic algorithm for segmentation based on the circular Hough transform is employed.

**Fig. 3:** Steps involved in iris.

In third step segmented iris is normalized. The normalization procedure will produce iris regions, which have stable dimensions, so that two images of the identical iris under different constrains will have characteristic features at the same spatial location. In order to deliver accurate recognition of individual users, the most selective information available in an iris pattern must be extracted in the fourth step. Only the salient features of the iris must be encoded so that comparisons between templates can be processed. Once the features of iris are extracted we are used to match the iris template with the available template in the database. Hamming distance is calculated between two iris templates. The Hamming distance algorithm is also employed as integrate noise
masking, so that only salient bits are used for calculating the Hamming distance between two iris templates (Gang et al 2006).

E. Extraction of Iris Texture:

The normalized 2d form image is converted into 1D signal, and these signals are used to convolve with 1d Gabor wavelets.

\[
G(f) = \exp \left( -\log \left( \frac{f}{f_0} \right) \right) / 2 \log \left( \frac{f}{f_0} \right)
\]

III. Fusion of Face and Iris Features:

In this step, two sets of features are fused together at the feature level to obtain a multi-modal biometric template which can be performed for Biometric-authentication (Balamurugan G et al 2014).

A. Feature Representation:

Facial - The normalized histograms are obtained such as (u, v) co-ordinates [10, 11]; we store these extracted value as vectors. Vector F1 contains all the u co-ordinate values and vector F2 contains all the v co-ordinate.

\[
F1 = [u1 \ u2 \ u3 \ \ldots \ \ldots \ u_n] \ |F1|=n
\]

\[
F2 = [v1 \ v2 \ v3 \ \ldots \ \ldots \ v_n] \ |F2|=n
\]

Iris – The texture properties obtained from the log-Gabor filter are complex numbers (a+ib); we store the iris texture features in two different vectors.

\[
I1 = [a1 \ a2 \ a3 \ \ldots \ a_n] \ |I1|=m;
\]

\[
I2 = [b1 \ b2 \ b3 \ \ldots \ \ldots \ b_n] \ |I2|=m.
\]

The input to the fusion process will be four vectors F1, F2, I1, and I2. The fusion process results with the multi-modal Biometric feature are

1. Individual Shuffling feature vectors.
2. Shuffled Concatenation of feature vectors.
3. Merging of the concatenated feature vectors.

1) Individual Shuffling Feature Vectors:

The first step in the fusion process is the shuffling of each of the individual feature vectors F1, F2, I1 and I2. The steps involved in the shuffling of vector F1 are,

i. A random vector R of size F1 is generated. The random vector R is controlled by the seed value.
ii. For shuffling the i\textsuperscript{th} component of face feature vector 1 F,
   a) The i\textsuperscript{th} component of the random vector R is multiplied with a large integer value.
   b) The product value obtained is modulo operated with the size of the face feature vector F1.
   c) The resultant value is the index say ‘j’ to be interchanged with. The components in the i\textsuperscript{th} and j\textsuperscript{th} indexes are interchanged.
iii. Step (ii) is repeated for every component of F1. The shuffled vector F1 is represented as S1.

The above process is repeated for every other vectors F2, I1 and I2 with S2, S3 as random vectors respectively, where S2 is shuffled F2 and S3 is shuffled I1. The shuffling process results with four vectors S1, S2, S3 and S4.

2) Shuffled Concatenation of Feature Vectors:

The next step is to concatenate the shuffled vectors process S1, S2, S3 and S4. Here, we concatenate the shuffled face S1 and S2 with the shuffled iris features S3 and S4 respectively. The concatenation of the vectors S1 and S3 are carried out as follows:

i. A vector M1 of size S1 S3 is created and its first S3 values are filled with S3.
ii. For every component 1 S ,
   a) The corresponding indexed component of M1 say ‘t’ is chosen.
   b) Logical right shift operation is carried in M1 from index ‘t’.
   c) The component of S1 is inserted into the emptied i\textsuperscript{th} index of M1. Therefore said process is carried out between shuffled vectors S2 and S4 to form vector M2. Thereby, the concatenation process results with two vectors M1 and M2.

3) Merging of the Concatenated Feature Vectors:

The last step in generating the multimodal biometric template BT is the merging of two vectors M1 and M2. The steps involved in the merging process are as follows.
I. For every component of M1 and M2,
   a. The components M11 and M21 are converted into their binary form.
   b. Binary NOR operation is performed between the components M11 and M21.
   c. The resultant binary value is then converted back into decimal form.
   ii. These decimal values are stored in the vector $B_T$, which serves multimodal biometric template.

IV. Generation of Cryptographic Key From the Multi Modal Template:

The final step of the proposed technique is the generation of the k-bit cryptographic key from multimodal biometric Template $B_{T_{(6,7)}}$. The template vector $B_T$ can be represented as,

$$B_T = [B1, B2, B3, \ldots, B_T]$$

The set of distinct components in the template vector $B_T$ are identified and are stored in another vector $U_{BT}$.

$$U_{BT} = [u_1, u_2, u_3, \ldots, u_d \mid |U_{BT}| < |B_T|$$

The vector $U_{BT}$ is then resized to k components suitable for generating the k-bit key [12, 13, 14]. The resize procedure employed in the proposed approach,

$$B = \left\{ \left[\begin{array}{c} u1 \\ u2 \\ \vdots \\ uk \end{array}\right] \right\}; \text{if } |U_{BT}| > k$$

$$B = \left\{ \left[\begin{array}{c} u1 \\ u2 \\ \vdots \\ u_d \end{array}\right] \right\}; \text{if } |U_{BT}| < k$$

Where $u_i = \frac{1}{2^d} \sum_{j=1}^{k} u_j$

Finally, the key $K_S$ is generated from the vector $B$, $K_S << B_i \mod 2^i$, $1 = 1, 2, 3, \ldots k$

Conclusion:

In this paper, we propose a technique to generate a secure cryptographic key for by incorporating multiple biometrics modalities of human being, so as to provide better security. An efficient approach for generation of secure cryptographic key based on multi-modal Biometric (Face and Iris) proposed in this paper. The proposed technique consist of 3 modules namely feature Extraction, Multimodal Biometric template and Cryptographic key generation. Firstly, the features of texture descriptors have been extracted from Face and Iris; then the extracted features have been combined together at the feature level to obtain the multi-biometric template. Lastly, a 256-bit secure cryptographic key has been generated from the multimodal biometric template.

REFERENCES

Anil Jain, Karthik Nandakumar and Arun Ross, 2005. Score normalization in multimodal biometric systems, Pattern Recognition, 38: 2270-2285.


