Crypto Key Generation based on Naive Bayes Classification of Biometric Fingerprint Features for Image Encryption

Jisha Nair.B.J.
Research Scholar Mphil ,
RVS College of Arts & Science,Sulur,India

Ranjitha Kumar.S
Associate Professor, Department of Computer Science
RVS College of Arts & Science, Sulur,India

Abstract — Protection and security of images are a major issue in this modern era of digital technology. Due to the fast growth of information technology, communication and storage of images are to be dealt with great concern. Encryption is one of the ways to ensure high security to images and are used in many fields such as medical science, military etc. Contemporary cryptography provides necessary techniques for securing information and protecting multimedia data .This paper proposes a way of encrypting and decrypting images using a unique key generated from biometric features of fingerprint. The key is generated based on naive bayes classification method applied on biometric fingerprint features extracted while authentication. Three feature extraction methods are discussed in this paper. Major security issues like confidentiality, integrity and authentication are addressed by the use of image encryption. Symmetric cryptographic algorithm which uses a secret key for both encryption and decryption is used in this work.

Keywords — biometrics, classification, crypto system, encryption , decryption, naive bayes.

I. INTRODUCTION

A biometric is defined as a unique biological feature of an individual used for the purpose of identification and verification. The combination of biometrics and cryptography provides better security and authentication. Biometric cryptosystems emerged as a new branch of research combining the benefits of both the technologies. Nowadays biometric fingerprint features are not only used for identification but is used in the field of cryptography for the purpose of encryption and decryption of documents and images. Data is secured using symmetric cryptographic system in this work.

With the increasing explosion of multimedia applications, security is a significant issue in communication and storage of images, and encryption is a general practice to maintain image security. Image encryption techniques intend to convert original image to another image that is very difficult to understand, so that the confidentiality is preserved between users. Nobody can identify the content without a key for decryption. The process of encoding plain data into cipher data is called encryption and the reverse process of converting cipher data back to plain data is called as decryption.

II. THE PROPOSED WORK

The proposed system generally includes the following steps: Fingerprint Image Preprocessing & Feature Extraction, Key generation, Encryption and decryption.

- Fingerprint Image preprocessing & Feature Extraction
- Key Generation
- Encryption and Decryption(Crypto Module)

In this work, biometric features of fingerprint images are collected from the user. Eight images of the thumb finger are collected from each user and are stored in the database.

A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are some abnormal points on the ridges. Before starting the actual feature extraction techniques fingerprint is preprocessed.In the proposed work three techniques of feature extraction methods are used[1][2]. They are

- Ridge Bifurcation method

- Ridge Ending method
- Orientation field method

A. Ridge Bifurcation Method

A ridge bifurcation (encoded as valley skeleton end point) has three arms of ridges meeting in one point. Two ridges encompass an acute angle. The tangent to the third ridge lying opposite of the enclosed valley defines the direction of a ridge bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right.[3]

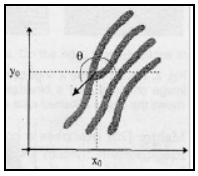

Fig. 1 Ridge Bifurcation

B. Ridge Ending Method

The minutiae point for a ridge ending is defined as the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the valley area were thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia.

In simple, the point where the valley "Y"'s, or (equivalently) where the three legs of the thinned valley area intersect. A ridge ending (encoded as valley skeleton bifurcation point) has three arms of valleys meeting in one point.

Two valleys encompass an acute angle. The tangent to the third valley lying opposite of the enclosed ridge defines the direction of a valley bifurcation. The direction is again measured as the angle the tangent forms with the horizontal axis to the right

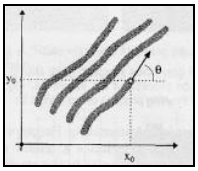

Figure. 1 Ridge Endings

C. Orientation Field Method

Fingerprint image is an oriented texture.The orientation field of a fingerprint image represents the direction of ridges.The local dominant orientation is computed as an optimal estimate of direction vectors at each pixel in a local window. Fingerprint image typically divided into number of non-overlapping blocks and an orientation representative of the ridges in the block is assigned to the block based on grayscale gradients in the block. The block size depends on the inter-ridge distance, i.e. it should include at least one ridge and one valley in a block. The block orientation can be determined from the pixel gradients by averaging or voting (optimization).

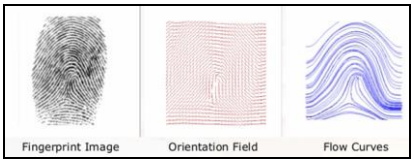

Figure 3 Orientation Field

III. METHODOLOGY

A. Feature Extraction

Based on the above three feature extraction methods important and significant features are collected after preprocessing steps are done[4][5]

Different classes are generated based on the users having similar features.Whenever a user needs to encrypt an image , his fingerprint image is collected and features are extracted based on any one of the methods.Using naive bayes classifier the class is identified.[6][7]

B. Classification

Naive Bayes is a probability based classific-ation algorithm which is the classifier used in this work.

The probability of a fingerprint d being in class c is computed as:

$$P(c \mid d) \propto P(c) \prod_{1 \le k \le n_d} P(t_k \mid c)$$

Where P (tk|c) is the conditional probability of a fingerprint tk occurring in a class c. This thesis interprets P (tk|c) as a measure of how much evidence tk contributes that c is the correct class. P (c) is the prior probability of a fingerprint occurring in class c.

Naive Bayes serves better for multiclass pre- diction. Performance can be evaluated by using classification efficiency because the decryption performance solely depends on the classification efficiency.

C. Key Generation

After classification, depending on the class an unique key is generated. This key is circularly shifted to generate corresponding keys for respective classes.

D. Image Encryption and Decryption

The above generated key is used to encrypt and decrypt the image which is to be secured before exchange or storage.

IV. PRACTICAL RESULTS

Experimental environment used : The experiment was carried out on an pentium i3 machine (3.33GHz) with 4GB RAM. MATLAB (R2013b) version in windows (64-bit) platform was used for the analysis and performance evaluation.

Datasets used : Our algorithm was tested on the standard database: FVC 2008[8]. These databases totally consist of large number of fingerprint images from 120 different fingers, of varying classes. However, only hundred images were chosen for experimentation from FVC 2004 database. These images are used for performance evaluation. The significant minutia feature points are obtained from the gathered biometric fingerprint images using the techniques presented in this work.

Evaluation Techniques: The performance evaluation of the proposed biometrics techniques used for image encryption is described. Based on the features extracted, fingerprint images are classified using popular classifier Naïve Bayes method. Kernel Distribution is appropriate for predictors that have a continuous distribution. It does not require a strong assumption such as a normal distribution. This can be used in cases where distribution of a predictor may be skewed .

A. *FAR and FRR Analysis*

The proposed system is evaluated using the parameters such as False Rejection Rate (FRR) andFalse Acceptance Rate (FAR).

(See Table 1 **)**

Table 1

Feature point selection method	FAR & FRR		
	Samples Testes	FAR	FRR
Ridge Bifurcation	100	11	14
Ridge Ending	100	10	12
Orientation Field	100	30	35

The most important metrics in examining an encrypted image is the visual inspection. The more the hidden the features of the image are, the better the encryption algorithm is.

B. Histogram Deviation Analysis

In this work Histogram Deviation is visualized to evaluate the performance of encryption. Histogram representation of both the original image P1 (see Fig 4(a) &(b)) and Encrypted image P2 (Fig 5(a) &(b) are visualized. The steps for calculating this metric are as follows:

1. Estimate the histogram of both the original image and encrypted image.
2. Absolute difference between both histograms are estimated
3. Estimate the area under the absolute difference curve divided by the total area of the image.

It is clear that the histogram of the encrypted image is nearly uniformly distributed, and extensively different from the histogram of the original image. Hence the encrypted image does not provide any clue to employ any statistical attack on the projected image encryption procedure, which makes statistical attacks complex.

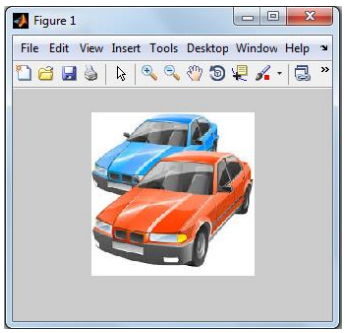

Figure 4 (a)

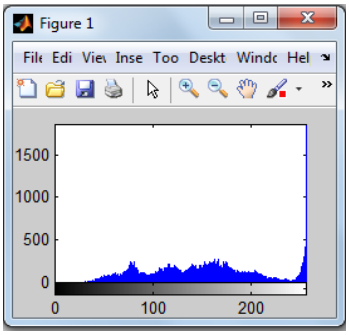

Figure 4(b)

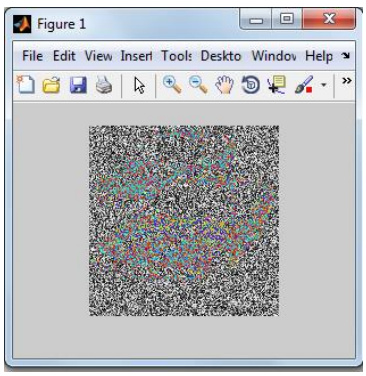

Figure 5 (a)

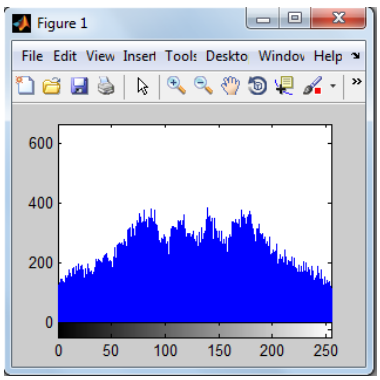

Figure 5 (b)

C. Spectrum Analysis

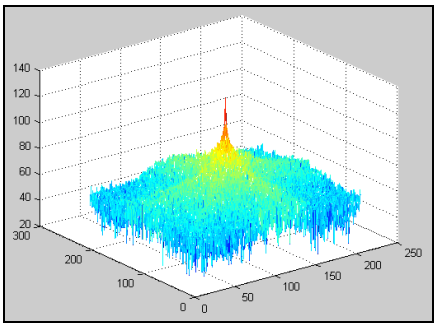

Figure 6(a)

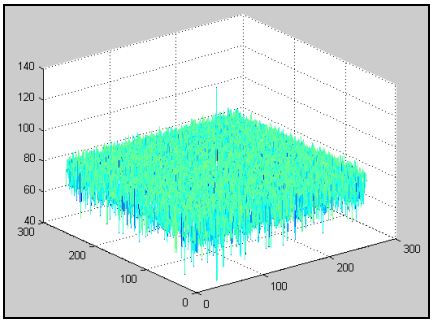

Figure 6(b)

V . CONCLUSIONS

Securing the data and images has become one of the most challenging tasks because of the increased number of cyber crimes. The conventional image encryption system uses a secret key for encryption and decryption. The key is to be stored securely in the system. Securing crypto keys is an important area of research. One solution to this issue is the generation of secret key from biometric features extracted while it is required for encrypting or decrypting data or images. The proposed security scheme results in better security if fusion of multimodal features are used.

REFERENCES

[1] S. Pankanti, S. Prabhakar, and A. K. Jain, “On the individuality of fingerprints”, IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(8), 2002, pp. 1010–1025.
[2] A. K. Jain, F. Patrick, A. Arun, “Handbook of Biometrics. Springer science and Business media”, I edition, 2008 pp. 1-42.Nyongesa H. O., et. al. “Fast Robust Fingerprint Feature Extraction and Classification," Journal of Intelligent and Robotic Systems, vol. 40, no. 1, pp. 103-112, 2004.
[3] Park C., and Park H., “Fingerprint classification using fast Fourier transform and nonlinear discriminant analysis," Pattern Recognition, vol. 38,no. 4, pp. 495 – 503, April, 2005.
[4] Hong L., Wan Y., and Jain A., “Fingerprint Image Enhancement: Algorithm and Performance Evaluation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no.8, pp. 777-789, 1998.
[5] L. Hong, Y. Wan, and A. K. Jain, “Fingerprint image enhancement: Algorithms and performance evaluation”, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20(8), 1988, pp. 777–789.
[6] FVC2002. http://bias.csr.unibo.it/fvc2002/
[7] FVC2004. http://bias.csr.unibo.it/fvc2004/
[8] Kaur M., et. al., “Fingerprint Verification System using Minutiae Extraction Technique," Proceedings of World Academy of Science, Engineering and Technology, vol. 36, December, ISSN 2070-3740, 2008.
[9] Wei L., Yonghui C., and Fang W., “Fingerprint Classification by Ridgeline and Singular Point Analysis," Congress on Image and Signal Processing, 2008.