International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064

Encryption of Text Using Fingerprints

Abhishek Sharma[1], Narendra Kumar[2]

[1]Master of Technology, Information Security Management, Dehradun Institute of Technology, Dehradun, India
[2]Assistant Professor, Department of Computer Science and Engineering, DIT University Dehradun, Uttarakhand, India

Abstract: ***Biometrics is the science and technology of measuring and analyzing biological data of human body, extracting a feature set from the acquired data, and comparing this set against to the template set in the database. Biometric techniques are gaining importance for personal authentication and identification as compared to the traditional authentication methods. User verification systems that use a single biometric indicator often have to contend with noisy sensor data, restricted degrees of freedom, and unacceptable error rates. To represent the large amount of data in the biometric images an efficient feature extraction method is needed. In this paper we have implemented the generation of unique biometric key after Fingerprint processing. Fingerprint processing involves the feature extraction of fingerprint image processing stages such as image Preprocessing, Converting the image in to gray scale, Image Enhancement can be performed with the help of Discrete Fourier transformation, image binarization, image segmentation, image thinning, Minutiae Extraction after Minutiae Extraction again segmentation technique is used. In fingerprints images there are foreground regions and background regions where foreground region show the ridges and valleys while the background regions are to be left out.***

Keywords: Cryptography, database toolbox, oracle, and minutiae based features extraction, fingerprints matching and encryption using biometric key.

1. Introduction

Fingerprints are the oldest and most widely recognized biometric trait[1]. All human being posse fingerprint and these fingerprints are result of unique ridge and valley structure formed by skin over the fingers. Ridges and valleys are often run in parallel; these structures have bifurcation and ridge endings called as termination. The ridge structure as a whole takes different shapes, characterized by high curvature, terminations, bifurcations, crossover etc. These regions are called singularity. These singularities may be classified into three topologies; loop, delta and whorl. What makes fingerprint unique is the distribution of such structures at local level. These are called as minutiae [2]. Minutiae mean small details and this refers to the various ways that the ridges can be discontinuous. A sudden ridge end is called termination or it can divide into two ridges which is called bifurcations. Figure 1 shows a fingerprint image.

Cryptography is an important field in the area of data encryption. This paper explores a unique approach to generation of key using fingerprint. The generated key is used as an input key to various Algorithms such as DES, AES, Caesar cipher, RSA.

.

1.1. Biometric System

The term Biometric comes from the Greek word bios which mean life and metrikos which means measure. It is well known that humans intuitively use some body characteristics such as face, gait or voice to recognize each other. Since, a wide variety of application requires reliable verification schemes to confirm the ID of an individual, recognizing human on basis of their characteristics. The characteristics are as follows:

1. Voice
2. Finger Prints
3. Body contours
4. Retina & Iris
5. Face
6. Soft Biometrics.

A biometric system is fundamentally a pattern-recognition system that recognizes an individual based on an attribute vector derived from a specific physiological or behavioral characteristic that the person possesses. That feature vector is frequently stored in a database (or recorded on a smart card given to the individual) after being extracted. A biometric system based on physiological characteristics is normally more reliable than one which adopts behavioral characteristics, even if the last may be easier to integrate within certain specific application. Biometric system can than run in two modes: verification or identification. While recognition involves comparing the acquired biometric information against templates corresponding to all users in the database, verification involves comparison with only those templates corresponding to the claimed identity. This implies that identification and verification are two problems that should be deals with separately. A simple biometric system consists of four basic components:

a. Sensor module which acquires the biometric data.
b. Feature extraction module where the acquire data is processed to extract feature vectors.
c. Matching module where attribute vectors are compared against those in the template.
d. Decision-making module in which the user's identity is established or a claimed identity is accepted or rejected.

1.1.1. Fingerprint Biometrics

Fingerprints are unique for each finger of a person including identical twins. One of the most Instead; only a touch provides instant access. Fingerprint systems can also be used in identification mode. The biometric fingerprint sensor takes a digital picture of a fingerprint. The fingerprint scan detects the ridges and valleys of a fingerprint and converts them into ones and zeroes. Complex algorithms analyze this raw biometric scan to identify characteristics of the fingerprint, known as the "minutiae". Minutiae are stored in a template, but only a subset of these has to match for identification or verification. The images acquired by these sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points (ridge endings and ridge bifurcations) that are present in every fingerprint (Figure.1).

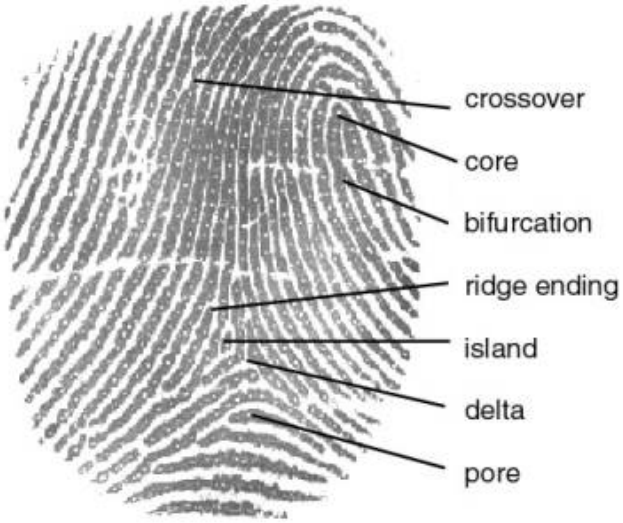


Figure 1: Ridge Endings and Ridge Bifurcations

2. Literature Review

Message authentication code is a public function of the message and a secret key that produces a fixed length value that serves as the authenticator. Protecting the secret key is major issue. We are going to use the biometrics for generating /protecting the secret key. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutia points: ridge endings and ridge bifurcations. Many types of minutiae exist, including dots. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points.

There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Loops make up 60% of all fingerprints, whorls account for 30%, and arches for 10%.Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics. Here we use Novel method of biometrics based key generation technique. Biometric crypto systems can operate in one of the following three modes 1.Key Release 2.Key binding 3.Key generation. Here we use the key generation mode in which the key is derived directly from the biometric data and is not stored in the data base.

Iwasokun G. B., Akinyokun O. C., Alese B. K. & Olabode O. compared each of the features of a template fingerprint image with each of the features in the feature sets in the reference database to determine whether the template and each of the reference images are from the same source. Comparison is done on the basis of preset parameters such as feature type, location, orientation and so on. The results obtained show that with the modified algorithm, valid and true minutiae points were extracted from the images with greater speed and accuracy[15]. Le Hoang Thai 1 and Ha Nhat Tam discusses on the standardized fingerprint model which is used to synthesize the template of fingerprints. In this model, after pre-processing step, we find the transformation between templates, adjust parameters, synthesize fingerprint, and reduce noises.[7]

3.3. Proposed Work

In this research, we have proposed a method for abstracting the minutiae points of a fingerprint and generating a biometric key to be used in Cryptographic encryption algorithm. We have used Oracle as a database for image storage and implemented the basic operations like create user, edit user, log in etc using matlab. After generation of biometric key, this is used as an input in various encryption algorithms. Later we have implemented matching of fingerprints in which it tells us the percentage matching

4. Fingerprint Processing

4.1. Edge Detection Techniques [5]

4.1.1. Prewitt

Computes the edge strength components using

$$\begin{bmatrix} 1 & 0 & -1 \\ 1 & 0 & -1 \\ 1 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ -1 & -1 & -1 \end{bmatrix}$$

4.1.2. Sobel

Computes the edge strength components using

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

This operator provides greater resilience to noise and is the best estimator of edge orientation and strength of all the "small" kernels.

4.1.3. Canny

Canny took an information theoretic approach to edge detection, stating that an edge detector should

1. Detect an edge
2. Should give a response in the correct location
3. Have a single response to an edge

4.2. Histogram Equalization

Histogram equalization increases the contrast of images. In this technique the basic idea here is to map the gray levels based on the probability distribution of the input gray levels. Histogram Equalization transforms the intensity values of the image as given by equation

$Sk=T(rk)=\Sigma\ Pr(rj)= \Sigma\ nj/n$ for j=1..k.

Where Sk is the intensity value in the processed image corresponding to intensity rk in the input image and pr (rj) =1, 2, 3…L is the input fingerprint image intensity level.

4.3. Binarization

Fingerprint image Binarization is to transform the 8-bit Gray fingerprint image with 0-value for ridges and 1value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white.

Figure 2: Sample fingerprint image

Figure 3: After Histogram Equalization

4.4. Morphological Operation

Morphological Operations are used to understand the structure or form of an image. It means identifying objects or boundaries within an image. There exists three primary morphological functions- erosion, dilation, hit or miss. Morphological operations are performed on binary images where the pixel values are either 0 or 1.Binary morphological operators are applied on binarized Fingerprint image to remove spurs, bridges, line breaks etc. A process called thinning is also applied to reduce thickness of lines. It is a process particularly used for skeletonisation.

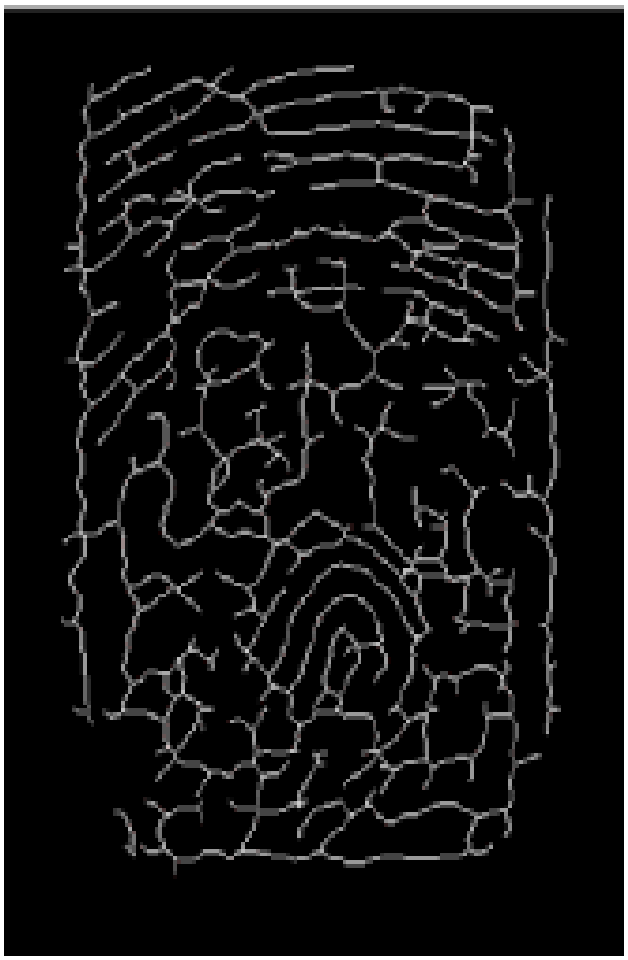


Figure 4: Morphological Operation

4.5. Minutiae points' Extraction

The binary image is thinned such that a ridge is only one pixel wide. Among all fingerprint features, minutia point features with corresponding orientation maps are unique enough to discriminate amongst fingerprint robustly; the minutiae feature representation reduces the complex fingerprint recognition problem to a point pattern matching problem. The minutiae are extracted from the enhanced, thinned and binary image. One of the minutia extraction techniques is crossing number.

4.6. Crossing Number

This method involves the use of skeleton image where the ridge flow pattern is eight-connected. The local neighborhood of each ridge pixel in the image is scanned out using a 3x3 window.

Table 1: A 3x3 neighborhood

The crossing number(CN) value is then computed as follows;

$CN=0.5\Sigma|PI - PI+1|$ for i=1... 8

Where P9= P1. It is defined as the half the sum of the differences between pairs of adjacent pixels in the eight neighborhood.

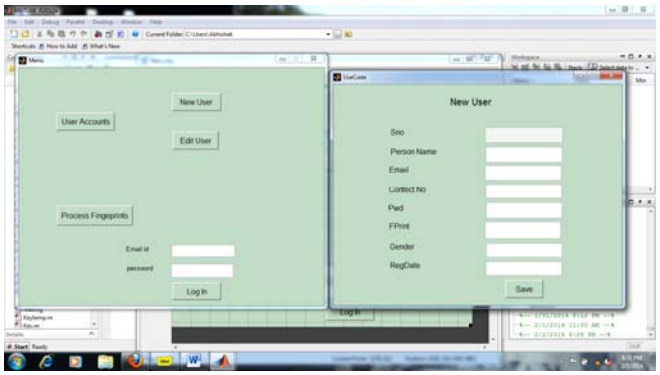
Using the properties of CN as mentioned below, ridge pixel can be classified as ridge ending, bifurcation or non-minutiae point.

Table 2: Properties of Crossing Number

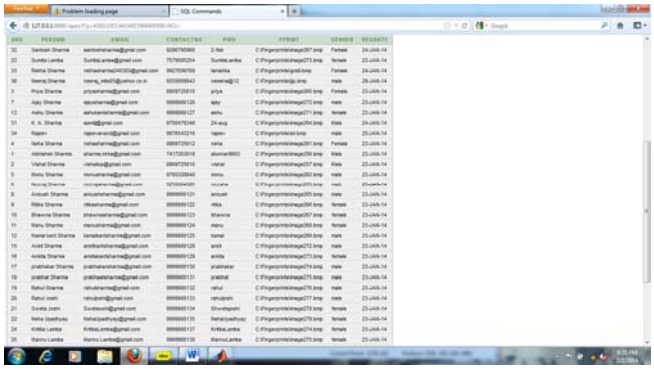
CN	*Property*
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

5. Enrollment

During the enrollment phase user account information such as User Name, Email Id, Password, Fingerprint, Contact Number, Gender etc are taken from the user and these information are saved in the database. In the project the database used is Oracle with matlab database toolbox.

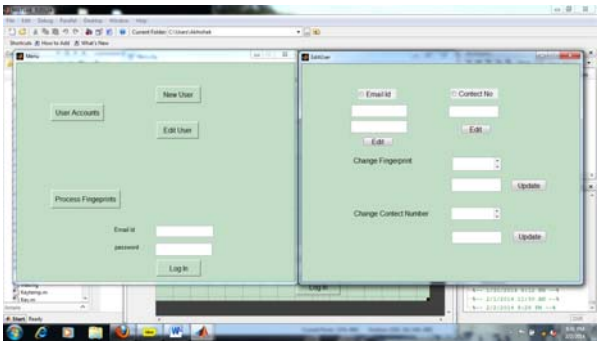


5.1. Create an Account [9]

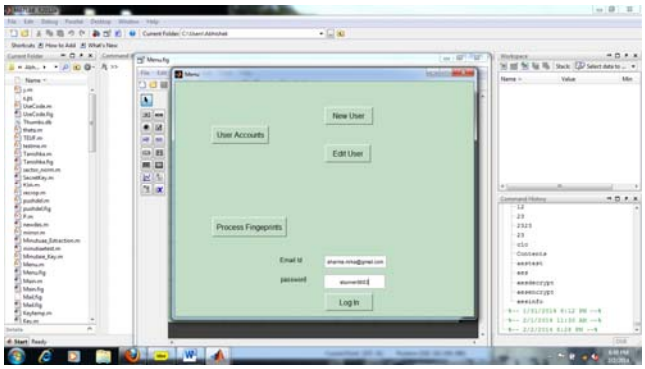


In case, if we want any change in the fingerprint template stored or contact number, we can edit the user information and update the particular record.

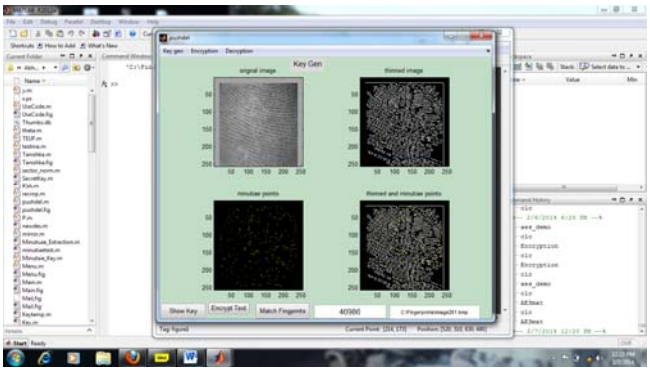
5.2. Edit Contact Number or Fingerprint



Now the biometric key from particular fingerprint can be generated using login that is called Enrollment.



5.3. Log in:



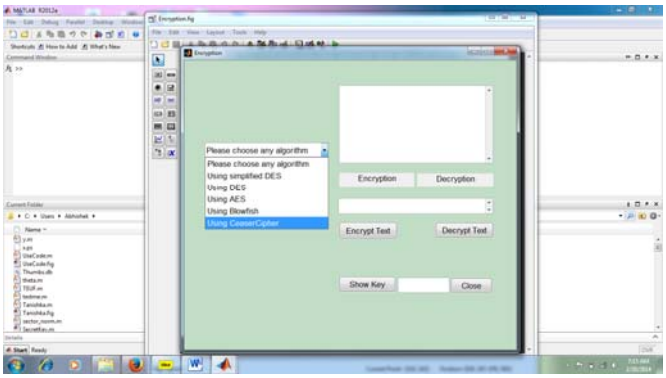
5.4. Algorithm to generate key using fingerprint

Step 1: Read the image into the memory.
Step 2: Covert to gray scale and thin image using canny edge detection.
Step 3: Minutiae Count.
Step 4: Loop through image and find minutiae, ignore 10 pixels for border.
Step 5: Make Minutiae image and create key
Step 6: Merge Thin image and minutia image together
Step 7: Plot original, thinned, minutiae image, combined image.

6. Results

Use of Generated key [10]

The generated biometric key can then be used as an input to various cryptographic algorithms like DES, Simplified DES, AES, Caesar cipher, RSA, Blowfish [10].



References

[1] Woodward, J. Orlans and P. Higgins.(2010), Biometrics, McGraw-Hill/Osborne.
[2] Kekre H. B., Bhatnagar S. ,Finger Print Matching Techniques, In Proceedings of National Conference on Applications Digital Signal Processing. (NCDSP – 2007), Mumbai, Jan 19 – 20, 2011.
[3] Raman Maini, Dr. Himanshu Aggarwal, Study and Comparison of Various Image Edge Detection Techniques.2009
[4] J. Matthews. “An introduction to edge detection: The sobel edge detector,” Available at, http://www.generation5.org/content/2002/im01.asp 2008.
[5] Raymond Thai, ‘Fingerprint Image Enhancement and Minutiae-Extraction,”, Thesis submitted to School of Computer Science and Software Engineering, University of Western Australia
[6] Counting of minutia points and generation of biometric key. http://www.math.com/school/subject2/lessons/S2U4L1DP.html
[7] Comparison of two fingerprints and calculating percent matching, FAR and FRR. http://www.bromba.com/knowhow/multiverification.htm
[8] Database Toolbox For use with matlab. Working with different kind of databases in matlab.2008.
[9] Use of oracle database to process our data through matlab. http://www.mathworks.in/help/database/ug/database.html.
[10] Kocarev, L., Jakimoski, G., Stojanovski, T., & Parlitz, U. 1998. Biometric key to encryption schemes. In Circuits and Systems, ISCAS'98. Proceedings of the 1998 IEEE International Symposium on (Vol. 4, pp. 514-517). IEEE