Encryption of Text Using Fingerprints as Input to Various Algorithms

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 248001, India

Abstract: ***Human fingerprints are rich in details called minutiae, which can be used as identification marks for fingerprint verification. The goal of this project is to develop a complete system for fingerprint verification through extracting and matching minutiae. To achieve good minutiae extraction in fingerprints with varying quality, preprocessing in form of image enhancement and binarization is first applied on fingerprints before they are evaluated. Many methods have been combined to build a minutia extractor and a minutia matcher. Minutia-marking with false minutiae removal methods are used in the work. An alignment-based elastic matching algorithm has been developed for minutia matching. This algorithm is capable of finding the correspondences between input minutia pattern and the stored template minutia pattern without resorting to exhaustive search. Performance of the developed system is then evaluated on a database with fingerprints from different people.***

Keywords: Cryptography, database toolbox, oracle, fingerprint, image enhancement, filtering, minutiae extraction, image post-processing, fingerprints matching and encryption using biometric key.

1. Introduction

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society, in which questions related to identity of an individual such as "Is this the person who he or she claims to be?", "Has this applicant been here before?", "Should this individual be given access to our system?" "Does this employee have authorization to perform this transaction?" etc are asked millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, etc. With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming more critical. A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user, and not anyone else. Examples of these systems include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of an impostor.

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.

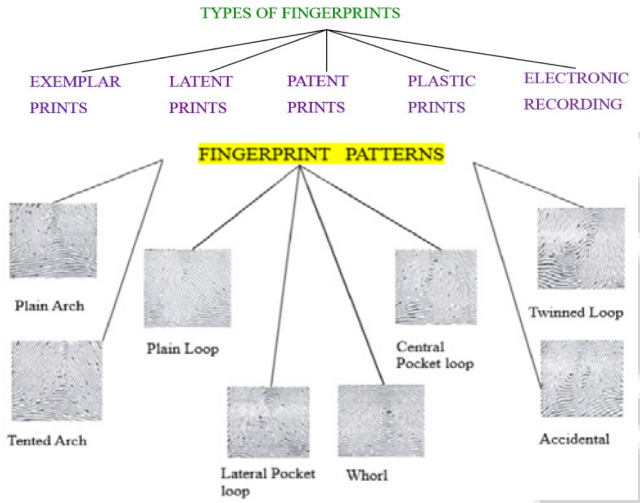
While recognition involves comparing the acquired biometric information against templates corresponding to all users in the database, verification involves comparison with only those templates corresponding to the claimed identity. This implies that identification and verification are two problems that 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).



2. Literature Review

Fingerprint identification is based upon unique and invariant features of finger prints. Finger prints are graphical flow like ridges present in human fingers which are formed during embryonic development, caused by ridges underneath the skin. According to FBI, the odds of two people sharing the same fingerprints are one in 64,000,000,000. Fingerprints differ even for ten fingers of the same person.[1]Some of the advantages of fingerprint identification are : high distinctiveness , high permanence, low potential for fraud and high performance with medium collectivity and acceptability. It also has certain drawbacks like need for training, finger and hand impairment, worn ridges etc acting as a barrier to universality. The method of identification is suitable for workstation access control, physical access control, Information system control etc.

.

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.

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 template 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

4.4. 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.

4.5. 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

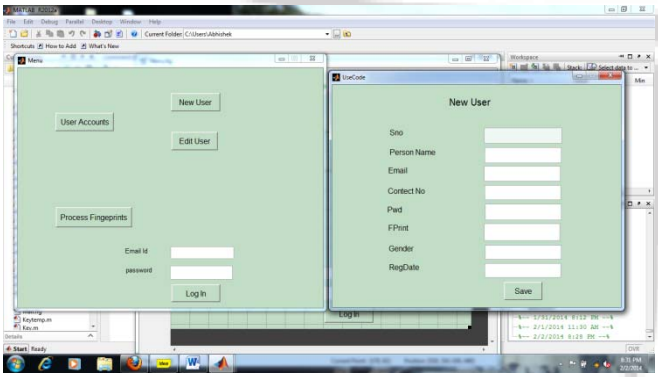
Where P9= P1. It is defined as the half the sum of the differences between pairs of adjacent pixels in the eight neighborhood. Using the properties of CN as mentioned below, ridge pixel can be classified as ridge ending, bifurcation or non-minutiae point.

Table 2: Properties of Crossing Number

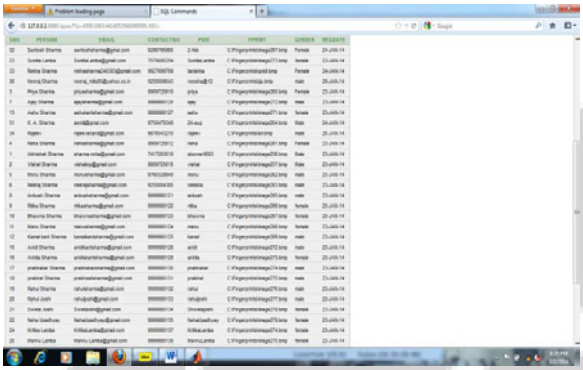
CN	*Property*
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

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.

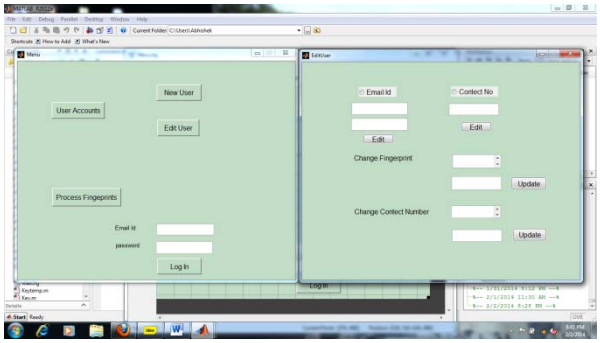


5.1. Create an account [9]

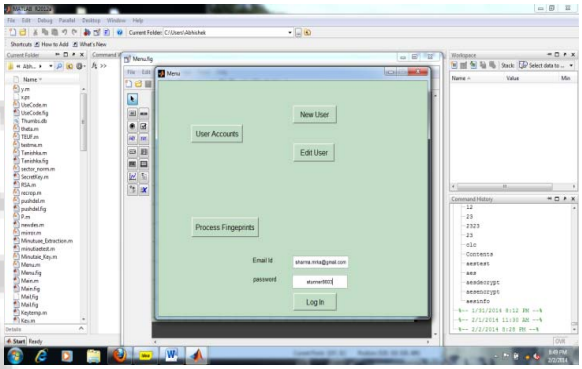


In case, if we want any change in the fingerprint template stored or contact number, we can edit the user information and update the particular record.

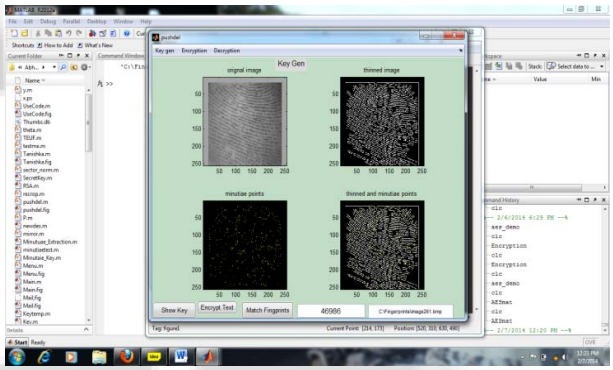
5.2. Edit Contact Number or Fingerprint



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



5.3. Log in

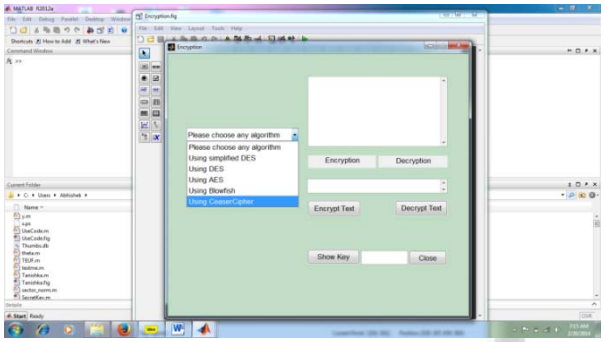


5.4. Algorithm to generate key using fingerprint:

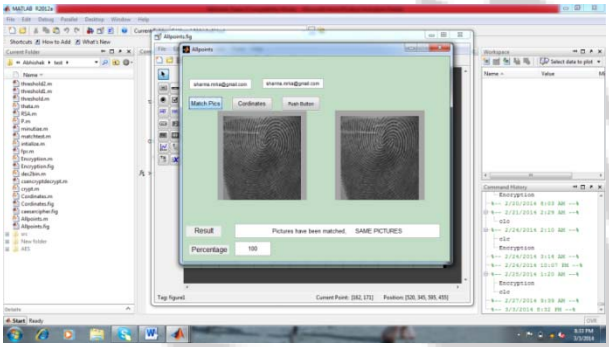
Step 1: Read the image into the memory.
Step 2: Covert to gray scale and thin image using canny edge detection.
Step 3: Minutiae Count.
Step 4: Loop through image and find minutiae, ignore 10 pixels for border.
Step 5: Make Minutiae image and create key
Step 6: Merge Thin image and minutia image together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



Matching of fingerprint



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.