Correlation Based Method for Identification of Fingerprint- A Biometric Approach

Prateek Verma, Maheedhar Dubey, Praveen Verma

Abstract: with identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometrics-based verification, especially fingerprint-based identification, is receiving a lot of attention Biometrics deals with identifying individuals with help of their biological data. Fingerprint scanning is the most common method of the biometric methods available today. The security of fingerprint scanners has however been questioned and previous studies have shown that fingerprint scanners can be fooled with artificial fingerprints, i.e. copies of real fingerprints. The fingerprint recognition systems are evolving and this paper will discuss the situation of today. We match the finger prints, one that is already in the database of the sensor and second the fingerprint that we enrolled in the sensor currently by using the Boolean function X-ORING. We get the matching score and decide the result on the matching score basis, whether the fingerprint is matched or not.

Index Terms: Fingerprint, Biometrics, Artificial Intelligence, Sensors.

I. INTRODUCTION

The use of biometric systems is growing every day. Fingerprint scanning is the one biometric identification method available today that is mostly used. The security of fingerprint scanners has however been questioned and previous studies have shown that fingerprint scanners can be fooled with artificial fingerprints, i.e. copies of real fingerprints. Since the fingerprint scanner market is growing and the technology is evolving, new products that can withstand attacks with artificial fingerprints might have seen the light today. This report will give a further examination of the fingerprint scanner area to clarify whether or not fingerprint systems can be trusted or if they are too insecure to be used today.

A. Need for Secured Identification System

In order to protect users of computer systems and to secure network-based transactions, demand is increasing for improved user authentication process. The hacking of passwords and personal information is increasing day by day. Identification is used to establish the identity of an actual user and to bar access to a terminal to anyone who is unauthorized.

B. Existing Methods

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers), or identification cards and PINS (personal identification numbers), suffer from several limitations. Passwords and PINS can be illicitly acquired by direct covert observation. Once an intruder acquires the user ID and the password, the intruder has total access to the user's resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner.

II. FINGERPRINT

A. *What is a fingerprint?*

Finger skin is made of friction ridges, with pores (sweat glands). Friction ridges are created during fetal live and only the general.Shape is genetically defined. Friction ridges remain the same all life long, only growing up to adult size. They reconductible the same if not too sévère injury.

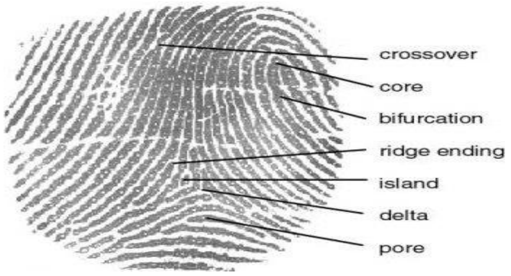

Figure 2.1 Fingerprint Details

- Minutie are the discontinuités of the ridges.

Manuscript published on 30 April 2012.
* Correspondence Author (s)

Prateek Verma*, Electronics & Telecommunication Engg., Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh India, 9907415003, (e-mail: prateekverma@csitdurg.in).

Maheedhar Dubey, Electronics & Telecommunication Engg., Chhatrapati Shivaji Institute of Technology, Durg, India, 9926170687,(e-mail:maheedhardubey@csitdurg.in).

Praveen Verma, Electronics & Telecommunication Engg., National Thermal Power Corporation Limited, Sipat Bilaspur,Chhattisgarh,India,9827158575,
(e-mail: contactpraveen001@gmail.com).

- Endings, the points at which a ridge stops.
- Bifurcations, the point at which one ridge divides into two.
- Dots, very small ridges.
- Islands, ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges.
- Ponds or lakes, empty spaces between two ridges.

B. *Types of Fingerprint*

Large volumes of fingerprints are collected and stored everyday in a wide range of applications including forensics, access control, and driver license registration. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large number of fingerprints in a database to reduce the search time and computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint.

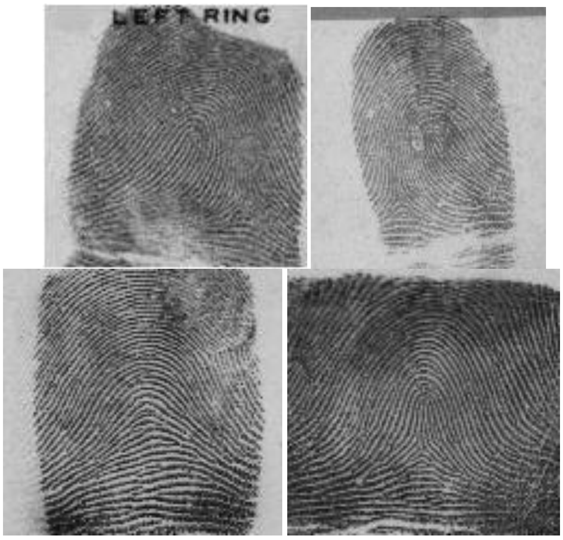

Figure 2.2 Types of Fingerprint

Fingerprint classification is a technique to assign a fingerprint into one of the several pre-specified types already established in the literature which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. We have developed an algorithm to classify fingerprints into five classes, namely, whorl, right loop, left loop, arch, and tented arch. The algorithm separates the number of ridges present in four directions (0 degree, 45 degree, 90 degree, and 135 degree) by filtering the central part of a fingerprint with a bank of Gabor filters. This information is quantized to generate a finger code which is used for classification. Our classification is based on a two-stage classifier which uses a k-nearest neighbor classifier in the first stage and a set of neural networks in the second stage. The classifier is tested on 4,000 images in the nist-4 database. For the five-class problem, classification accuracy of 90% is achieved. For the four-class problem (arch and tented arch combined into one class), we are able to achieve a classification accuracy of 94.8%. By incorporating a reject option, the classification accuracy can be increased to 96% for the five-class classification and to 97.8% for the four-class classification when 30.8% of the images are rejected.

Characteristic of Fingerprint

Personal characteristics often involved with horoscopes and similar non-scientifically proven prophesies. The two first are by far the greatest areas. Fingerprint-based systems, used for security reasons, are so popular today that they have almost become the synonym for biometric systems. Fingerprint-based systems will be further discussed. Enormous amounts of information are stored in a fingerprint database. For example, the total number of fingerprint cards (each card contains one impression each of the 10 fingers of a person) in the FBI fingerprint database has now exceeded 200 million, and is growing continuously. Most law enforcement agencies in the world use an AFIS (Automatic Fingerprint Identification System) today. These systems have increased the productivity and greatly reduced the cost of hiring and training human fingerprint experts. Since the discovery of the DNA structure in 1953, DNA has become more and more important in the society as a whole, as well as in forensics. With the science of cloning though, it can be questioned whether or not DNA can actually be used for identification purposes. If individuals can be cloned, DNA typing is as much help as it is in distinguishing identical twins. By definition, identical twins cannot be distinguished by DNA. The same problem does not occur with fingerprints. Even though the fingerprints of identical twins are very similar, automatic fingerprint system can successfully distinguish identical twins though with a slightly lower accuracy than no twins. It should however be noted that the algorithms in some fingerprint systems may not be robust enough to detect these divergences.

C.1 Other Characteristics

You have probably looked at your own fingerprint at some point in your life and noticed the papillary lines on it. In fingerprint literature, the terms ridges and valleys are used to describe the higher and lower parts of the papillary lines. The reason we have ridges and valleys on our fingers, is the frictional ability of the skin. The formation of the ridges and valleys is a combination of genetic and environmental factors.

III. DESCRIPTION OF PAPER

In this paper we are just making a comparison between two of the image using X-oring of the pixels. first of all we saves a image in any memory location then the person whose fingerprint is to be

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

matched is asked to place his finger in any of the sensor used, then the software using Matlab matches the image as follows:-

If the image is the RGB image then convert it into the gray scale image using the instruction rgb2gray.

Resize the image in the scale 512*512.

Enhance the image using histogram equalization for greater clarity and brightness.

Convert the image into the binary image using instruction im2bw in the matrix of 0s and 1s.

Start the matching process using instruction X-or and the corresponding pixels are compared.

If the two corresponding pixels are same then the score is incremented by one if not then compare the next pixel.

After comparing all the pixels the image is said to be matched if 90% of the pixels are matched.

A. Algorithm Level Design

Level 1:- If the image is the RGB image then convert it into the gray scale image using the instruction rgb2gray.
Level 2:- Resize the image in the scale 512*512.
Level 3:- Enhance the image using histogram equalization for greater clarity and brightness.
Level 4:- Convert the image into the binary image using instruction im2bw in the matrix of 0s and 1s.
Level 5:- Start the matching process using instruction X-OR and the corresponding pixels are compared.
Level 6:- If the two corresponding pixels are same then the score is incremented by one if not then compare the next pixel.
Level 7:- After comparing all the pixels the image is said to be matched if 92% of the pixels are matched.

IV. SENSOR USED

A. Optical Sensor

The advantages with optical sensors include withstanding temperature fluctuations (to some degree), a fairly low cost, and resolutions up to 500 dpi, better image quality and the possibility of larger sensing areas. The drawbacks of optical sensors are size and problems with latent prints. Cuts, abrasions, calluses, and other damage, as well as dirt, grease and other contamination, can also be a problem with optical scanners. Frustrated total internal reflection (FTIR) .When you place your finger on an FTIR -based optical sensor (see figure 9.1), the ridges will be in contact with the prism surface, while the valleys will remain at a distance. One side of the prism is illuminated through a diffuse light (a bank of light-emitting diodes (led) or a film planar light). The light is reflected at the valleys and randomly scattered (absorbed) at the ridges. The lack of reflection from the ridges makes it possible to acquire an image of the fingerprint. in the early days' ftir sensors, a CCD camera was used to acquire the fingerprint image. Today, the FTIR sensors have shrunk considerably in size and cost with help of the new CMOS technology. Since FTIR devices sense a three-dimensional surface, it is difficult to fool them with a photograph or image of a fingerprint. Latent prints are however still a problem. Furthermore, it is difficult to make a small enough FTIR device suitable to embed into a PDA or a mobile phone, even though they can be used in mousse and k/b.

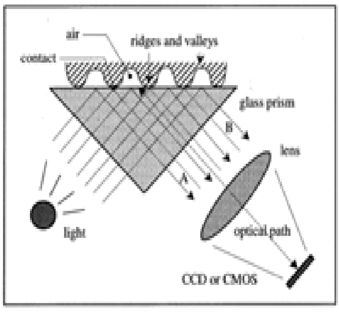

Figure 4.1 An FTIR-based Fingerprint Sensor

B. Fingerprint Image Preprocessing

B.1 Fingerprint Image Enhancement

Fingerprint Image enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a higher accuracy to fingerprint recognition.

Two Methods are adopted in fingerprint recognition system: the first one is Histogram Equalization; the next one is Fourier Transform.

B.2 Histogram Equalization:

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type [Figure 4.2.2(a)], the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced [Figure 4.2.2(a)].

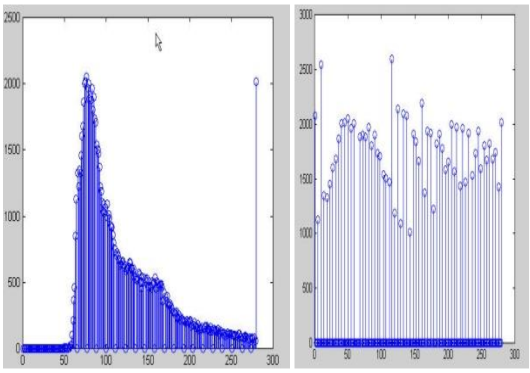

Fig. 4.2.2(a) the Original histogram of a fingerprint image (Left) Histogram after the Histogram Equalization (Right)

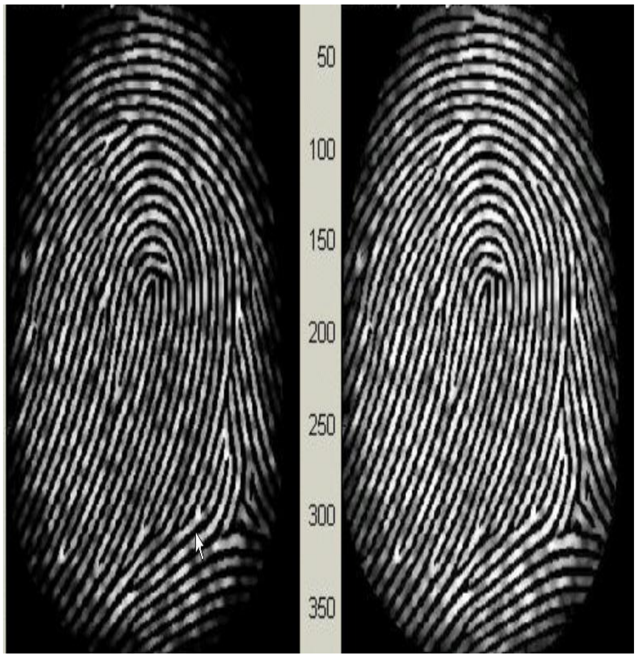

Fig. 4.2.2(b) Histogram Enhancement. Original Image (Left). Enhanced image (Right)

B.3 Fingerprint Enhancement by Fourier Transform

Divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

For u = 0, 1, 2... 31 and v = 0, 1, 2... 31.

In order to enhance a specific block by its dominant frequencies, multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.

Get the enhanced block according to

$$g(x,y) = F^{-1}\{F(u,v) \times |F(u,v)\,|^{k}\} \ldots (2)$$

Where F^{-1}(F(u,v)) is done by

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v) \times exp\left\{j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \ldots\ldots\ldots\ldots\ldots (3)$$

for x = 0, 1, 2... 31 and y = 0, 1, 2... 31.

The k in formula (2) is an experimentally determined constant, which choose k=0.45 to e having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation. Fig. 4.2.3 presents the image after FFT enhancement.

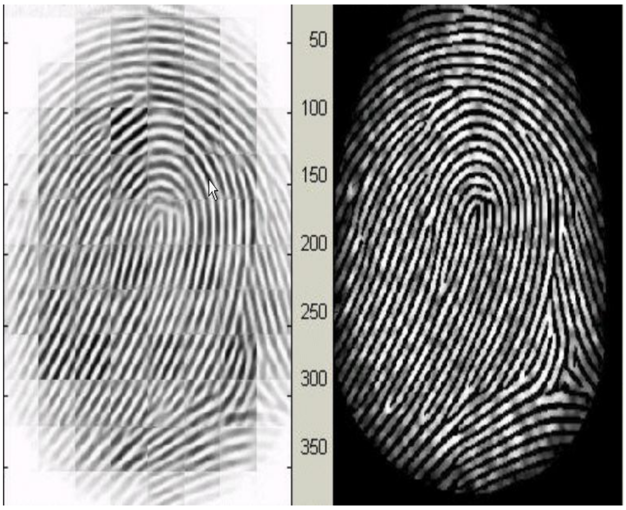

Fig 4.2.3 Fingerprint enhancement by FFT Enhanced image (left), Original image (right)

V. RESULT

The method is showing the correct result if we are taking the 92% threshold value. There is scope for future betterment of the algorithm by using Neural Network technique that can give better results as compared to this approach. With the help of neural network technique accuracy can be improved. Instead of having a constant threshold, it could be made adaptive, depending upon the conditions and the database available, so as to maximize the accuracy.

VI. FUTURE SCOPE

A. *Full system on a chip*

Imagine having the sensor, processor, associated Memory, and reference storage all together on the same chip. It would be practically impossible to crack the system by listening to transmission lines or PC connection, and breaking the security by mimicking the data traveling back and forth. This is the solution for most applications. Then, the only output is then a yes or no, ciphered with a proper code.

B. *In FpUI System (Fingerprint User Interfacing)*

The use of biometric systems is growing every day. Fingerprint scanning is the one biometric identification method available today that is mostly used. Since the fingerprint scanner market is growing and the technology is evolving, new products that can withstand attacks with artificial fingerprints might have seen the light today. This report will give a further examination of the fingerprint scanner area to clarify whether or not) fingerprint systems can be trusted or if they are too insecure to be used today. i.e. when a user touches the sensor with a certain finger, the sensor obtains an image of the fingerprint.

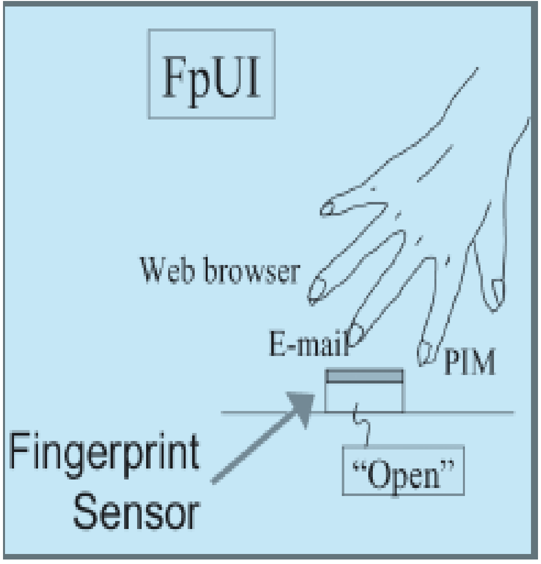

Figure 6.2 Fingerprint User Interfacing Systems

VII. CONCLUSIONS

Biometrics-based authentication has many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forge. We have shown that the intrinsic bit strength of a biometric signal can be quite good, especially for fingerprints, when compared to conventional passwords. Yet, any system, including a biometric system, is vulnerable when attacked by determined hackers. We have highlighted eight points of vulnerability in a generic biometric system and have discussed possible attacks. We suggested several ways to alleviate some of these security threats. Replay attacks have been addressed using data-hiding techniques to secretly embed a telltale mark directly in the compressed fingerprint image. A challenge/response method has been proposed to check the liveliness of the signal acquired from an intelligent sensor. Finally, we have touched on the often-neglected problems of privacy and revocation of biometrics. It is somewhat ironic that the greatest strength of biometrics, the fact that the biometrics does not change over time, is at the same time its greatest liability. Once a set of biometric data has been compromised, it is compromised forever.

REFERENCES

[1] B. Miller, "Vital Signs of Identity," *IEEE Spectrum* **31**, No. 2, 22–30 (1994).

[2] L. O'Gorman, "Practical Systems for Personal Fingerprint Authentication," *IEEE Computer* **33**, No. 2, 58–60 (2000).

[3] R. Germain, A. Califano, and S. Colville, "Fingerprint Matching Using Transformation Parameter Clustering," *IEEE Computational Science and Engineering* **4**, No. 4, 42–49 (1997).

[4] A. Jain, L. Hong, and S. Pankanti, "Biometrics Identification," *Communications of the ACM* **43**, No. 2, 91–98 (2000).

[5] B. Schneier, "The Uses and Abuses of Biometrics," *Communications of the ACM* **42**, No. 8, 136 (1999).

[6] B. Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., New York (1996).

[7] N. Memon and P. W. Wong, "Protecting Digital Media Content," *Communications of the ACM* **41**, No. 7, 35–43 (1998).

AUTHOR PROFILE

Prateek Verma, completed Bachelor of Engineering in Electronics & Telecommunication Engineering, currently working as a Lecturer in Electronics & Telecommunication Department in Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India. He has presented different research papers in conferences of different organizations & attended various workshops also. He has guided many UG students for their projects. Previous work experience of 1.5 Years in TATA Consultancy Services, Kolkata.

Maheedhar Dubey, completed Master of Engineering in VLSI Design, currently working as an Assistant Professor in Electronics & Telecommunication Department in Chhatrapati Shivaji Institute of Technology, Durg, Chhattisgarh, India. He has presented different research papers in conferences in different organizations & attended various workshops also. He is the member of five professional societies like IEI, ISTE, IETE, ISCA, IEEE. He has published 3 books in Jainam Publication, Bhilai, Chhattisgarh, India. He has guided many UG & PG students for their projects.

Praveen Verma, completed Bachelor of Engineering in Electronics & Telecommunication Engineering, currently working as an Engineer in National Thermal Power Corporation Limited, Sipat, Bilaspur, Chhattisgarh, India,. He has Completed his MBA from Sikkim Manipal University. He has presented different research papers in conferences in different organizations & attended various workshops also. He has guided many UG students for their projects, while working as a lecturer in Disha Institute of Management & Technology, Raipur, Chhattisgarh, India. Previous Work Experience of 1.5 Years in Disha Institute of Management & Technology, Raipur, Chhattisgarh, India.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)