ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Internet Security Based on Image Processing

Prathvi[1], Roshan Suvaris[2]

Dept. of MSc (Software Technology), AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India

Asst. Professor, Dept. of MCA, AIMIT, St. Aloysius College (Autonomous), Mangalore, Karnataka, India

ABSTRACT: From security point of view, human fingerprints can be used as identification marks for fingerprint verification. The aim of this is to develop a system for fingerprint verification through extracting and matching minutiae. To get good quality of fingerprint it under go preprocessing in form of binarization and image enhancement is first applied. Many method have been combined to build minutia matching and minutia extractor. To secure the internet verification over internet we use computational geometry algorithms which extracted feature of the fingerprint segmentation. Biometrics technology allows verification of ones identity through physical characteristics.

KEYWORDS: Computational Geometry, Security, Fingerprint, Verification, Image Segmentation

I. INTRODUCTION

Biometric is methods of recognizing a person's physiological or behavioral characteristic. Biometric technologies are extensively used for identification and personal verification solutions. We have used traditional finger scanning technique, which involves the analysis of small unique marks of the finger image which is known as minutiae. Minutiae points are the ridge ends of the finger image. When image is captured using the fingerprint scanner device there is possible that dirt, condition of the skin, force on the scanner device and alignment or rotation of the finger these all affect the quality of the fingerprint. These kind of methods may give chance for hackers to attack when biometric feature are transferred in internet. There are some problems like rotation and alignment of the finger position which is developed in this paper. This method is based on computational geometry algorithms. This features are depended on pixel brightness degree of fingerprint image, which is extracted using techniques like edge, minutiae points and ridge detection. No person can have same fingerprint, it differs from each person.

Principles of Fingerprint Analysis

Fingerprints are distinctive patterns, made by friction ridges and wrinkle, which appear on the pad of finger and thumbs. The various type of biometric category like palms, toe and feet are also unique, but these are used less often for verification and identification, so in this we focus on prints from fingers and thumbs. Friction ridge pattern are distinct into three types that is loop, whorls, and arches- each has a unique variation, relationship of the ridges depends on the shape.

Loop, whorl & arch pattern examples

Loops: account for approximately 60 percent of pattern types. It must have a one or more ridges which enters from one side, curve and exit from same side. Its Divided into ulnar loops (pointing toward the ulna bone, or pinky) and radial loops (pointing toward the radius bone, or thumb).

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

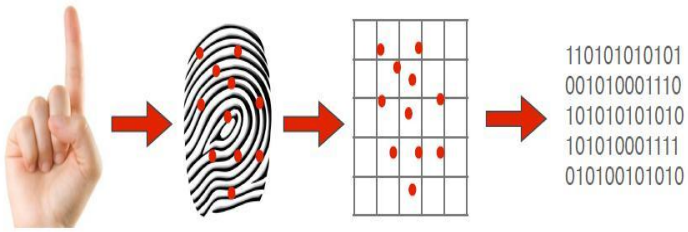
Vol. 3, Special Issue 7, October 2015

Whorls: has about 35 percent of pattern types. All whorls form circular or spiral patterns, like tiny whirlpools. There are four major types of whorls i.e. plain (concentric circles), central pocket loop (a loop with a whorl at the end), double loop (two loops that create an S---like pattern) and accidental loop (irregular shaped).

Arches: Arches has about five percent of all pattern types. Create a wave---like pattern and include plain arches and tented arches. Tented arches rise to a sharper point than plain arches. [6]

II. HOW DOES A FINGERPRINT OPTICAL SCANNER WORK?

A fingerprint scanner system has two basic jobs- it has to get image of your finger, and it needs to check whether the pattern of ridges in this image matches the pattern of ridges in pre-scanned images. Fingerprint are unique to every person, and it is saved as encrypted biometric key. Fingerprint images are not saved, only series of number which is used for verification. The algorithm cannot be converted back to an image, so no one can duplicate your fingerprints. [5]



III. METHOD

Pre-processing stage

In this stage a fingerprint image can have any formats like *tif, bmp, jpg,* etc, which is transformed into a two-dimensional array of pixels. The value of pixel is proportional to brightness of its each point. This gives the image of dark background on bright square image. This fingerprint image, is usually square and described as N x N m-bit, where m controls the number of brightness values and N is the number of points along the axes. M bits gives the range about 2_m values, ranging 0 to 2_m-1. Thus, digital image is denoted as the compact matrix form:

1.

$$f(x,y) = \begin{matrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,N-1) \end{matrix} \quad (1)$$

The coordinate vector of the above matrix is:

$$S = f(x,y) \quad (2)$$

Thus a vector S of $1 \times N^2$ dimension is constructed, which is then used in the next stage.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

Processing stage
Proposition:

It is considered that the *set of brightness values* for each fingerprint image contains a *convex subset*, which has a *specific position* in relation to the original set. This position may be determined by using a combination of computational geometry algorithms, which is known as *Onion Peeling* Algorithms.

Implementation:

A gray level fingerprint image g(i, j), i, j ∈ I, it is consists of align narrow ridges which is separated by narrow valleys. Ridge frequency and ridge orientation are two inherent characteristics of the fingerprint image, which define never changing coordinates for ridges and valleys in a local neighborhood. Consider the *set of brightness values* of a fingerprint image to be the vector **S.**

Onion Peeling algorithm start with a limited set of point $_0$ S in the plane, and the iterative process is considered.

Let $_1$ S be the set S $H(S)$: S $_{00}$ | | | | it minus every points on boundary of the hull of S. Similarly, it defines () S | S | H | S This process is continued till the set becomes 3. The hulls ( ) $_{i\,I}$ H H S | are called the layers of the

set, and process is peeling away the layers is known as onion peeling for obvious reason. Any point on $_i$ H is said to have just depth, *i.*

Meta-processing

It consider that the smallest convex layer has a depth 3 which carries particular information, this position give the explanation of average of the fingerprint brightness. In other words, the smallest convex layer depicts a specific geometrical area in which this average ranges. This feature has unique characteristics to each fingerprint, because the 2 following condition are ensured

1. The selected area layer is not intersected with another layer.

2. The particular depth of the smallest layer is from the proposed fingerprint method 2 variable are extracted: depth of this layer and the area of the smallest onion layer *xy S*, which is a subset of the original fingerprint set **S** values. Taking into account the specific feature of the aforementioned variables it is easy to make sure that these may be used for accurate fingerprint verification.

Verification stage
In this there is processing of other set N, the new subset *xy N is* tested and against this there is a subset tested *xy S.*
The following 3 levels takes place the testing.
i. Subset *xy N* is the cross-correlation of subset *xy S*..
ii. The extracted subsets are compared with the depths of iterative. The intersection between subset *xy N* convex layer

and one of set **S** onion layers is controlled. Furthermore, it is considered that subset *xy N* identifies set **S** as the parent onion layers when:
i. The cross-correlation number of subset *xy S* and subset *xy N* is *approximately 1*

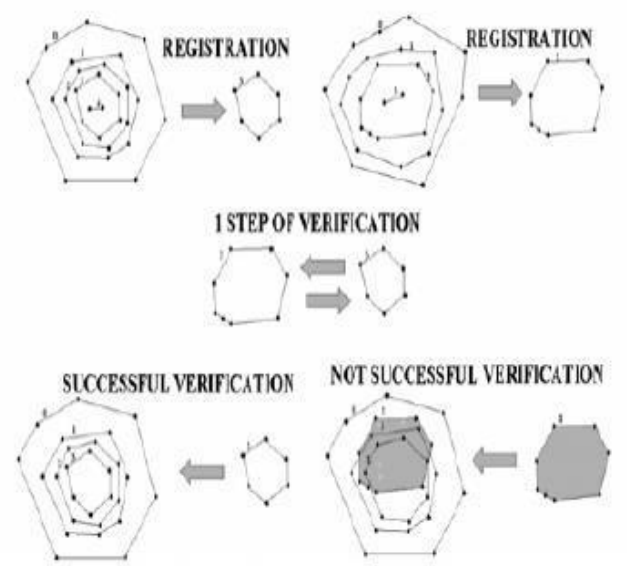
ii. The intersection between the convex layer of subset *xy N* and one of the onion layers of set **S** is *0*. Otherwise, subset *xy N* does not identify set **S** as the parent onion layers[1].

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015



III. WORK ON IMAGE PROCESSING

Every system has its own limitation. Therefore, verification is based on multiple biometrics is an emerging trend Multimodel biometric can impart a more balanced solution to the security Multimodel systems require more than one biometrics system. For offering to the above subject an algorithm is developed on banking system. Online banking is unsafe considering that bank is using biometric technology for its security purpose. The security is assured by using voice scan, finger scan, and by requesting password given by the bank. The following are the algorithm. [3]

3. Algorithm:

3.1 Algorithm 1:

a) STEP 1: A person has to enter the bank that uses biometric technology (finger scan and voice scan) for greater degree of security.

b) STEP 2: The person is requested to give his or her fingerprint (as input) on the finger scan pad.

c) STEP 3: The fingerprint which we have taken from above step is compared with all the fingerprints images which is available in the database.

If user fingerprint image is matches the stored fingerprint image
THEN …
Person can access his/her account.

ELSE
It throws an ERROR

Conclusion

As we all know biometrics is which the characteristics related to the humans. It is being used in many ways in the form of identification. In the digital technology, biometrics will gain acceptance from the universe. Biometrics is used for

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 7, October 2015

security purposes. In this paper I have done finger print verification and future I will be working on rotation and alignment of finger print which will be easy for the finger print verification method.

REFERENCES

[1] Shiv Kumar Tripathi, Anshul Maheshwari, SECURE INTERNET VERIFICATION BASED ON IMAGE PROCESSING SEGMENTATION, International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue 5 pp 091-095 August 2012
[2] A. K. Jain, A. Ross, & S. Pankanti, Fingerprint matching using minutiae and texture features, *Proc. International Conference on Image Processing (ICIP)*, Thessalonica, GR, 2001, 282-285.
[3] D. Maio & Maltoni, Direct gray-scale minutiae detection in fingerprints, *IEEE Transactions on PAMI*, *19*(1), 1997, 27-40.
[4] L. O¨Gorman, *Fingerprint verification, in Biometrics* (Jain, A, K. Bolle, R. & Pantanti, S.: Kluwer Academic Publishers, 1999).
[5] http://www.bioelectronix.com/what_is_biometrics.html
[6]A Simplified Guide To Fingerprint Analysis