Fingerprint Validation and Outlier Detection using Minutiae Approach in Network Security

Prathima Devi Sirivella[#1], Mrs D.Raaga Vamsi[#2]

[1] M.Tech (CSE),Gudlavalleru Engineering College, Gudlavalleru

[2] Assistant professor, Gudlavalleru Engineering College, Gudlavalleru.

ABSTRACT:

In this recent information technology biometric techniques are being used increasingly against identity theft. The basic need of biometric applications provides a measurable physical characterstics is a more reliable indicator of identity than legacy systems such as PASSWORDS and PINS.The necessity for security in fields such as improving airport security,strengthening the national borders, in travel documents,in preventing ID theft has brought the need to develop an able and efficient method for correct classification of personal authentication ,many countries begin to issue Edriving License and Epassports containing biometric data for their citizens. Biometric template recognition is the challenging problem in the real world applications.This project deals with the fingerprint classification and recognition systems. which consists of extracting and matching of minutiae from the input image.

In this project a new statistical ecc method is provided for finger print biometric applications. User authentication is verified based on the elliptical curve that is generated for each finger print image that are stored in the database. This approach gives better results in realtime applications from database type of attacks.

1. INTRODUCTION

Fingerprints have actually been utilized for over a century and therefore are the most often kind of biometric identification. Fingerprint identification is usually employed in forensic science to compliment criminal investigations, and then in biometric systems such as civilian and commercial identification devices. Regardless of this widespread utilization of fingerprints, there has been little statistical jobs done on the uniqueness of fingerprint minutiae. Specially, the issue of how many minutiae points should be utilized for matching a fingerprint is unresolved.

Biometrics refers to the automatic identification of the living person based upon physiological or behavioural characteristics. There are quite a few different kinds of biometric technologies that you can purchase: face-recognition, fingerprint recognition, finger-geometry, hand geometry, iris recognition, vein recognition, voice and signature recognition.

The procedure of biometric identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

The partner that should be identified is essential to remain physically present along at the point-of-identification. The identification based upon biometric techniques obviates the need to remember a password or carry a token or maybe a smartcard.

When using the rapid increase in use of PINs and passwords occurring having been a result of information technology revolution, it can be necessary to restrict use of sensitive/personal data. By replacing PINs and passwords, biometric techniques are definitely more convenient relative to the user which can potentially prevent unauthorised access to or fraudulent using ATMs, Time & Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, and computer networks. PINs and passwords may be forgotten, and token based ways of identification, like passports, driver's licenses and insurance cards, can be forgotten, stolen, or lost.

The fingerprint associated with an individual is unique and remains unchanged over the lifetime. A fingerprint is formed from an impression on your pattern of ridges throughout the finger. A ridge is defined as one curved segment, and a valley is the region between two adjacent ridges. The minutiae, being aware of the local discontinuities within the ridge flow pattern, provide the features that are used for identification. Details typically the type, orientation, and location of minutiae

are taken into account when performing minutiae extraction [9].

Galton [5] defined documented features for fingerprint identification, which since that very day, has also been refined to include additional types of fingerprint features. However, a large number of features are not widely used in fingerprint identification systems. Instead the set of minutiae types are restricted into just two types, ridge endings and bifurcations, as other types of minutiae can be expressed concerning the above feature types. Ridge endings are classified as the points in which the ridge curve terminates, and bifurcations are locations where a ridge splits a single path to two paths with a Y-junction. Figure 1.1 illustrates a good example of a ridge ending and a bifurcation. In this example, the black pixels correspond to the ridges, and the white pixels embody the valleys.

(a) Ridge ending (b) Bifurcation

Fingerprint images are rarely of perfect quality. Numerous could be degraded and harmful which have elements of noise because many aspects which includes combinations in skin and notion stipulations. This disrespect may end up in an indispensable multitude of spurious minutiae being produced and genuine trivia being ignored. A major improvement studying the the statistics of fingerprint sophisticated regularly often to continually extract sophisticated from fingerprint image files. And hence, it is had the need to take on picture improvement practices earlier than minutiae installation enroll in a more respectable presume of workings spots. The chief aim in this undertaking typically apply documented styles for finger-print picture progression and trivia removal. Examination utilizing both lab created experiment graphics and beneficial fingerprint graphics pre owned out to assess performance the applied styles. These techniques are then designed to extract minutiae issued from a sample definitive set of fingerprint images. By using the extracted minutiae data, preliminary experiments inside the statistics of fingerprints can then be conducted.

2 RELATED WORK

One of the most widely cited fingerprint enhancement techniques will be the method employed by Hong et al. [8], that's dictated by convolution of one's image with Gabor filters tuned onto the local ridge orientation and ridge frequency. The best stages of this algorithm include normalisation, ridge orientation estimation, ridge frequency estimation and filtering.

Your first step within this approach involves the normalisation of one's fingerprint image ensuring it features a prespecified mean and variance. From imperfections in the fingerprint image capture process an example would be non-uniform ink intensity or non-uniform contact with the fingerprint capture device, a finger-print image may reveal distorted rates of variation in grey-level values along side ridges and valleys. And thus, normalisation is made to decrease the result of such combinations, which often allows the subsequent image development methods.

An angle image is then smart, that's a matrix of path vectors

representing the ridge orientation at each position in the whole image. The extensively employed gradient-based approach is made to actually compute the gradient [18, 15, 22], which makes consumption of the undeniable fact that the orientation vector is orthogonal towards the gradient. Firstly, the image is partitioned into square blocks to discover that the gradient is determined for each pixel, within the x and y directions. The orientation vector for one obstruct can in that case be resulting by performing an averaging procedure on many the vectors orthogonal onto the gradient pixels supplied in the prevent. As a result of the profile of clatter and damaged factors in the image, the crease angle will possibly not you must be perfectly determined. Given that this pleat angle varies little by little utilizing a regional neighbourhood, the orientation image is then smoothed making use of a low-pass filter to decrease the result of outliers.

Finger-print improvement methods driven by Gabor filter are now widely used out to permit many finger-print applications inclusive of fingerprint matching [17, 19] and fingerprint classification [12]. Gabor filters are bandpass filters which may have both frequency-selective and angle-selective locations [4], which implies the filters can be successfully tuned to actually specific frequency and angle values. One beneficial element of finger prints is the fact that they are known to have clearly particular local ridge angle and ridge frequency. Thus, the improvement algorithm takes advantage of this persistence of spatial constitution by applying Gabor filters which are tuned to complement the neighborhood ridge angle and frequency.

FVMRSF

The Fingerprint is verified using Fingerprint Verification based on fusion of Minutiae and Ridges using Strength Factors. Objectives of the algorithm are:

(i) The Minutiae Extraction using thinned image by Block Filter.

(ii) The true ridge information is extracted by Hough Transform.

(iii) The true minutiae and ridges information are combined to get matching score

3 PROPOSED ARCHITECTURE

Modules present in this project are:
1)Image Storage
2)Feature Extraction
3)Minutia Approach.
4)Classification and Identification.

Image Storage:

This module helps to storing the image in database. It gets the image name from where it should be retrieved and encodes the image in database. The value of image will be stored image in database like arrays.

Feature Extraction:

The human fingerprint is comprised of various types of ridge patterns, traditionally classified according to the decades-old Henry system: left loop, right loop, arch, whorl, and tented arch. Loops comprise nearly 2/3 of most fingerprints, whorls are nearly 1/3, and maybe 5-10% are arches. These classifications are relevant in many large-scale forensic applications, but they are rarely employed in biometric authentication. Many types of minutiae exist, including dots (very small ridges), islands (ridges lightly about dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross one other)

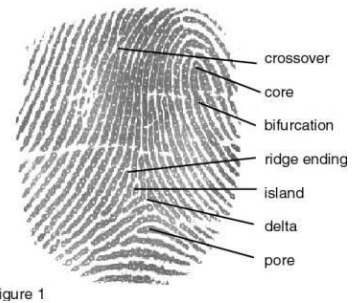


Figure 1

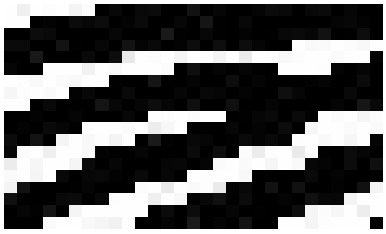
First the fingerprint is filtered to remove background noise, secondly the reputation is “binnarized”; the third sub module extract the minutiae. A minutia is ready of coordinates and parameters. If (m) is a minutia as to the fingerprint (F), (m) is represented by its coordinates, its orientation vector along with its constellation affiliation

$$m = (x, y, \Theta, T)$$

where (x, y) are classified as the coordinates of one's minutia as documented in the coordinate, Θ is naturally a vector consists of two relative angles, and T its constellation affiliation.

$$\Theta = (\Theta 1, \Theta 2)$$

The process to compute the relative orientation as to the minutia is dependent upon the minutia type. Whether it is a bifurcation ridge minutia, the ridges close to the minutiae are approximated with three fixed size segments, notice the end of each segment becomes a summit of a triangle.



A constellation is defined by its centre, its orientation, and its size. The constellation center is the virtual minutia Cc(i),

$$Cc(i)=1/n\sum m(x,y,\Theta)=M(x,y,Oci)$$

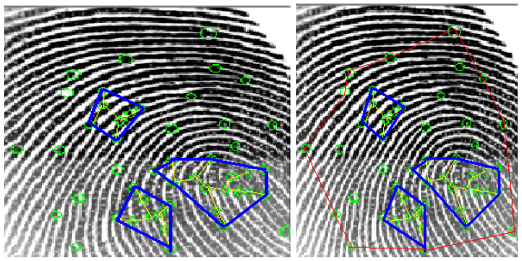
where *n* is the number of minutiae that composes the constellation C(i), *n* is always called size of the constellation. Note that the Orientation, Oc(i), takes the nearest value of the following list, {0, pi/4, pi/2,3pi/4, pi}.

The global fingerprint border is defined as the line joining the external minutiae composing the pattern.

If Ci, j is the constellation (j) of the fingerprint F (i) is can described by the following parameters:

$$Ci,j = (Cc(i,j), n(i,j))$$

Where n(i, j) is the number of minutiae including in the Ci,j Constellation.



Minutiae Approach:

Fingerprint matching techniques can possibly be placed into two categories: minutiae-based and correlation based. Nonetheless the frequently used technique with minimum FAR and FRR is Minutiae-based techniques. In this process we, first find minutiae points and after that map their relative placement on the finger. However, that there have been so many difficulties while i was using this approach. It truly is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method will not check the worldwide pattern of ridges and furrows [5]. Fingerprint Verification Structure is a system that determines the correspondence in an input fingerprint by having template fingerprint kept in data base.

Minutiae extraction is only a trivial task of extracting singular points because we are part of a thinned ridge map. Overall performance currently available minutiae matching algorithms depends heavily by the quality of input fingerprint images. It is were required to verify one who you must be registered before. So the steps are: 1.Registration, 2.Verification.

Registration: In this process, the actual procedure takes the one's fingerprint as a possible image format and processed that image as few steps such as filtering, enhancing, lining and shaping. In that acse requires selection of minutiae points as feature then generates a template and stores it. The authenticate template contains the total number of minutiae points selected by proposed feature selection technique. How many minutiae points limited using a bindings named limited region to improve the flexibility of verification, then find out the co-relation among the many features bounded by limited region.

Verification: To verify one, the process takes one's fingerprint since a image format through fingerprint acquisition hardware and processed that. Then it requires technique to detect minutiae points and selects features, then to verify, load the templates and compare with the information gathered from verifying one. When it obtains any template matched with that of verifying one, it really makes a decision that you was authenticated, or otherwise.

Classification and Identification:

Fingerprint classification was carried out by the extraction of the singular points from the fingerprint image. The extraction images are stored in different arrays. This module matching the input image arrays and existing image arrays.

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 is required to be matched only with a subset of the fingerprints in the database.

3.2 MINUTIA MATCHING ALGORITHM

Step 1. Take X and Y as two co-ordinates.

Step 2. Take a minutiae point (I th), where 1<=I<=total minutiae points.

Step 3. Now, take another minutiae point J th,

Where 1<=J<=total minutiae points

and I!=J.

Step 4. if Y_I=Y_J then DISTANCE : = X_J-X_I

if DISTANCE <0 then

DISTANCE := DISTANCE × (-1);

else if (Y_I>Y_J) then

if (Y_I-Y_J:=1) or (Y_I-Y_J:=-1)

then DISTANCE := 0

else if (Y_I-Y_J:=2) or (Y_I-Y_J:=-2) then

DISTANCE := Y_I-Y_J

else DISTANCE:=(Y_I-Y_J)-2

DISTANCE := (DISTANCE * WIDTH) + (WIDTH - X_J) + X_I

else if (Y_I-Y_J):=1 or(Y_I-Y_J):=-1

then DISTANCE := 0

else if (Y_I-Y_J:=2) or (Y_I-Y_J:=-2)

then DISTANCE := Y_J-Y_I

else DISTANCE := (Y_J-Y_I)-2

DISTANCE := (DISTANCE * WIDTH) + (WIDTH - X_I)+X_J

Step 5. Repeat step 1, 2 & 3 for the verified image also.

Step 6. Find the equality of minutia points (M1 & M2),

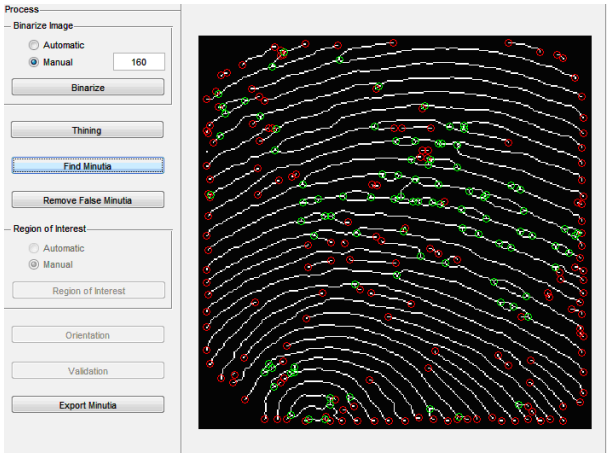
as EQ: = matched (M1, M2)/greater (M1, M2);

Step 7. Calculate total number of correlated distances DISTANCE-of-both.

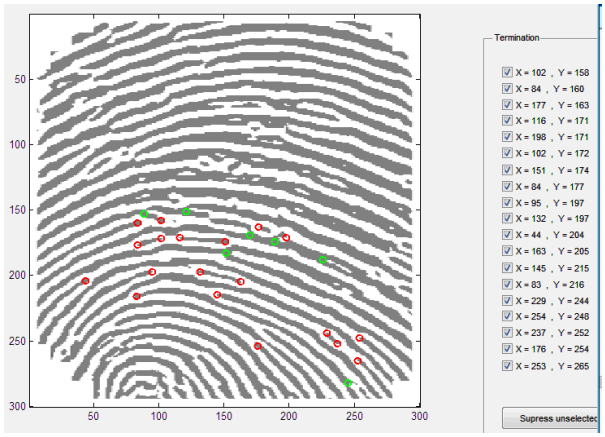
Steps Description:

(1). In Image fingerprint consider the X and Y of two coordinates that represent to by its coordinates, its orientation vector and its constellation affiliation m = (x, y, Θ, T). The coordinates of one's minutia per the coordinate, Θ serves as a vector consists of two relative angles, and T its constellation affiliation. Θ= (Θ1, Θ2)
(2).Within this step determining the minutia points with denoting as I. After selecting the Minutia Points, The minutia point of I must be select between 1 and total minutia points.
(3).In this step use the another minutia point with represent to denoted as J. The Jth point should be between 1 and total minutia points, where the Jth and Ith point is not recommended to be equal and near (step2).
(4).When the Yth coordinate of Ith and Jth minutia reality is equal, then the distance ought to be subtracted from Xth coordinate of Ith and Jth minutia point. When the distance truth is lower than 0 then distance value is multiplied by -1, else when the Yth coordinate of Ith truth is bigger than Jth point then the condition of Yth coordinate of Ith and Jth point ought to subtracted that value ought to be equal to 1 or -1 this process will carry on to the minutia truth is add up to 2 or -2. After calculating the minutia points the distance value ought to be calculated by distance value is multiplied by width and that's included in width subtracted by Xth coordinate of Ith and Jth minutia points.
(5). Within this step repeat the steps 1, 2, and 3 verifying the fingerprint image.
(6).Within this step find the equality of minutia points is matched with M1 and M2 and greater of M1 and M2.
(7).In this particular step calculate the full no of correlated distances of both.

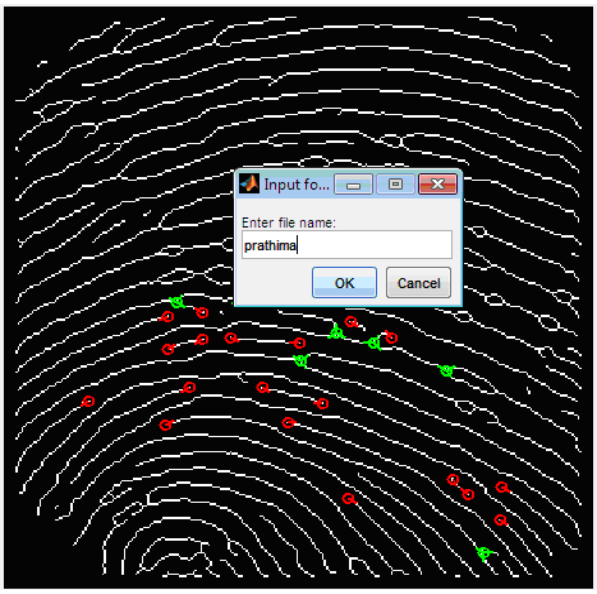
4. EXPERIMENTAL RESULTS



Selecting orientation button to finding minutia points



Select the validation button to validate the Image by bifurcation values



Select the Export minutia button to save the minutia points in text format by giving the file name

Conclusion and Future scope:

The main advantage of this algorithm is its fast running speed. It greatly improves verification performance too. The algorithm identifies the unrecoverable corrupted areas supplied in the fingerprint and drives out them from further processing. Now you have an important aspect of the algorithm like the presence of those areas would turn out to be extremely harmful for our extraction of minutiae points. It aids in removing the spurious minutiae too which may also turn out being harmful in matching fingerprints correctly.

The further improvement in terms of efficiency and accuracy, which can be achieved by improving the image enhancement techniques or by improving the hardware to capture the image. So that the input image to the thinning stage could be made, better this could improve the future stages and the outcome.

REFERENCES

1) Fingerprint Identification: An Aid to the Authentication Process: By Rodger Jamieson, Ph.D., CA, Greg Stephens and Santhosh Kumar:
2) http://fingerprints/What_are_the_advantages_of_fingerprint_recognition_files.html
3) Fingerprint Identification and Verification System using Minutiae Matching: F.A. Afsar, M. Arif and M. Hussain.
4) Technology Review:Image Enhancement, Feature Extraction and Template Protection of a Fingerprint Authentication System: Md Rajibul Islam , Md. Shohel Sayeed and Andrews Samraj.
5) Automated Fingerprint Recognition : Using Minutiae Matching Technique For The Large Fingerprint Database: S M Mohsen, S M Zamshed Farhan and M M A Hashem
6) Reducing Process-Time for Fingerprint Identification System: Chander Kant Lecturer, Department of Computer Science andapplications K.U.Kurukshetra, Haryana (INDIA), Rajender Nath Reader, Department of Computer Science andapplications K.U.Kurukshetra, Haryana (INDIA).
7) A Matching Algorithm of Minutiae for RealTime Fingerprint Identification System: Shahram Mohammadi, Ali Frajzadeh.