Minutiae vs. Correlation: Analysis of Fingerprint Recognition Methods in Biometric Security System

Bharti Nagpal, Manoj Kumar, Priyank Pandey, Sonakshi Vij, Vaishali

Abstract— Identification and verification of a user's identity in an organization is a big challenge. Earlier, it was done through passwords that had various limitations for example it could be cracked or stolen. Biometric technology has replaced all the existing technologies with greater advantage. Fingerprint technique, so far, is recognised as a better technique than others and is widely used. It provides accurate results and has less false rate as compared to other techniques. This paper aims to analyse the two main methods of fingerprint recognition in biometric security systems which are minutiae based and correlation based methods. An analysis of these two has been summarized and it shows the pros and cons of both the methods, with respect to factors such as computational power, poor quality image evaluation etc. The paper concludes all the features of both these methods and explains the process followed by them.

Keywords- biometric system, correlation based fingerprint, minutiae based.

I. INTRODUCTION

Authentication and Verification of a user's identity is a huge and challenging task, in the current scenario in order to achieve authenticated access in any validation based system. Traditionally, it was done using two methods: -

a. Method based on Possession: The one that requires Hardware components like smartcards and supports identity card etc.
b. Method Based on Knowledge: The one that requires a piece of information for instance, passwords etc.

Password is the gateway to bypass the authentication login process. The problem that arises with the usage of passwords is that it can be guessed or cracked very easily by professional hackers and crackers for their malicious intentions. Valid user's password can be misused by some other person being personified as the original user. To overcome these limitations of traditional methods, biometric security systems come into play.

The word biometric is the combination of two words, "bio" and "metrics", in which the first half indicates the unique features of a human body and the second half refers to the unit of measurement. Biometrics is the method that has overcome previous methods and has been the latest method of authentication and verification. It is a science/ art/ process of matching the special or unique characteristics of an individual. It is further classified into Physiological and Behavioural biometrics [1] as described in figure 1. Physiological biometrics includes detection of face, iris, fingerprints, retina, hand geometry, DNA, ear shape, skin reflectance etc. whereas, Behavioural biometrics includes voice, speech, action, signature, gait, key stroke, lip motion etc. In order to understand successful orientation of Biometric system the classification of biometrics is important for better utilization of both techniques namely minutiae and correlation which is explained with details in next sections.

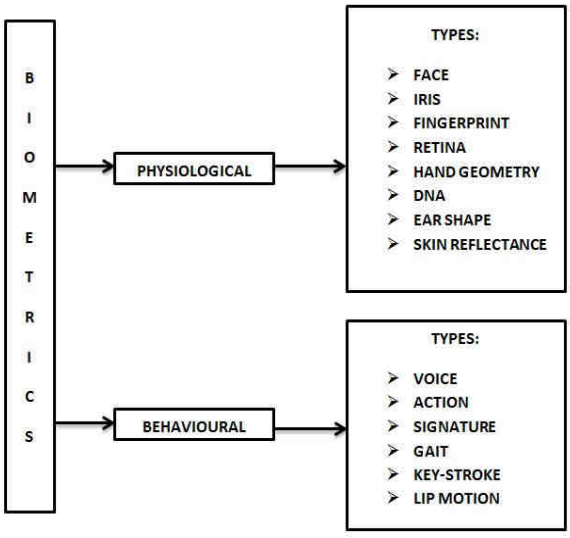

Figure 1:- Biometric Classification

Among these detection methods, Fingerprint Recognition technique is widely used in biometric security systems. This paper will be focusing on the two major methods of fingerprint recognition:

a. Minutiae based fingerprint recognition
b. Correlation based fingerprint recognition

Revised Version Manuscript Received on October 24, 2015.

Bharti Nagpal, Computer science & engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Guru Gobind Singh Indraprastha University, Delhi, India.

Manoj Kumar, Computer science & engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Guru Gobind Singh Indraprastha University, Delhi, India.

Priyank Pandey, Computer science & engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Guru Gobind Singh Indraprastha University, Delhi, India.

Sonakshi Vij, Computer science & engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Guru Gobind Singh Indraprastha University, Delhi, India.

Vaishali, Computer science & engineering, Ambedkar Institute of Advanced Communication Technologies and Research, Guru Gobind Singh Indraprastha University, Delhi, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Fingerprint based biometrics is the most commonly used biometrics technique where impressions of the fingerprint are taken as an input and matched with the impressions already stored in the template database. Fingerprinting technique is relatively better than other techniques due to the following factors: permanency, feasibility, accuracy, reliability and acceptability. Fingerprint contains the pattern of ridges, valleys, furrows / minutia. Ridges are the dark lines that are present in the fingerprint arena. Valleys are the light area between two ridges. Minutiae are also sometimes referred to as furrows. The overall working process of fingerprint recognition is shown in figure 2. The process starts with an input of the user's fingerprint which is initially pre-processed. The biometric system will read the pixels and will convert those pixels into digital format that can be easily interpreted by the machine [2]. Necessary features are then mined from the fingerprint which is then matched with the fingerprint that is already stored in the template/pre-stored fingerprint database to give the final output.

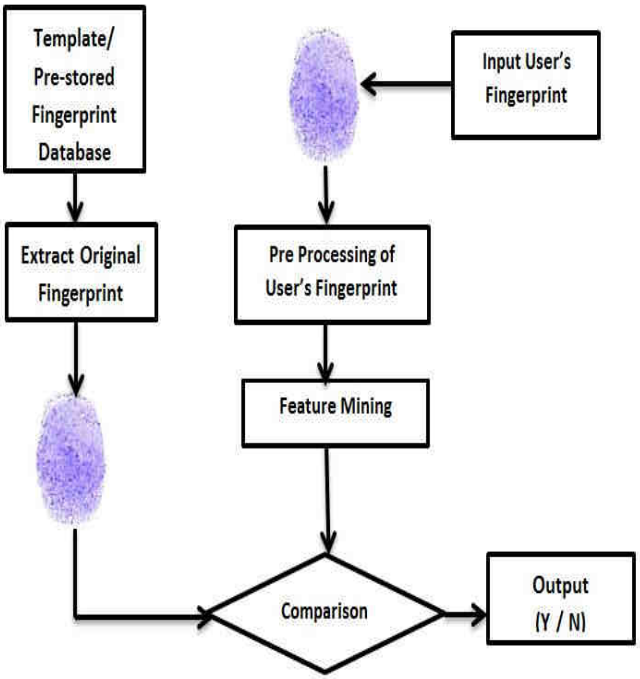

Figure 2:- finger print recognition process

II. MINUTIAE BASED FINGERPRINT RECOGNITION METHOD

Minutiae based fingerprint recognition method is one of the most widely used methods for biometric verification system. It works on the concept of "minutiae" i.e. the basic minute details of the fingerprints. This method extracts the minutiae details as shown in figure 3, from the images of the fingerprints and makes its decisions on the basis of location of these minutiae details.

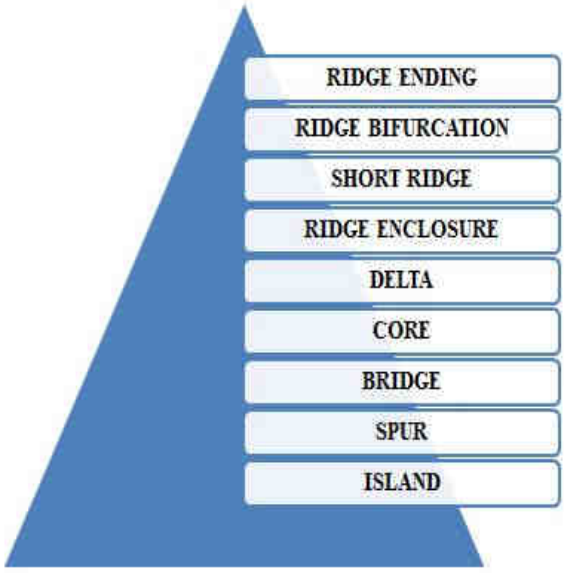

Figure 3: - Information Extracted from Minutiae

The basic pocess of Minutiae based finger print recognition is shown in figure 4, the generalised minutiae process. The initial steps consist of taking the users finger print and generating corresponding image maps from it. The details of minutiae details of the finger print are detected such as the ridge ending, delta, core, bridge, spur, island, ridge bifurcation etc. and the false minutiae is eliminated. This step is followed by the calculation of neighbour ridges [2]. Finally the minutiae quality is allocated. For the successful implementation of the above explained process we need to use certain smoothing filters in the initial stage [3]. Various types of smoothing filters are available but we need to choose the one that meets the requirements of the system under concern.

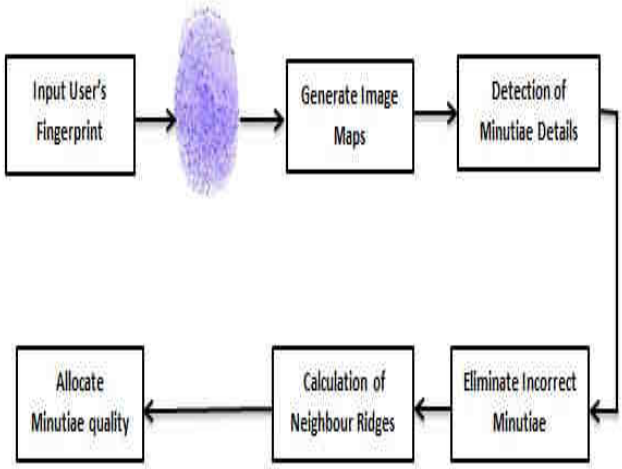

Figure 4:- Generalized Minutiae Process

This process can be implemented by following a sequence of steps listed below in table I.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Table I Steps to be implemented in minutiae based system

I. Estimating the directional field
II. Perform necessary noise reduction steps such as adaptive filtering
III. Calculating the threshold value
IV. Thinning operations
V. Extracting the minutiae from the obtained thinned image
VI. Applying the heuristics
VII. Performing Hough transform which implements the Brute force search on the various pairing options that are possible
VIII. Calculating the "matching score"

1) Template selection for minutiae based method:

It can be easily observed that when a template has more minutiae details then it will be easier to find the correct minutiae matching score. But this is not always true. Hence in practical scenarios we can say that minutiae based template selection is not of much real time significance as it does not consider the poor quality fingerprint images [4]. Also this method does not incorporate the necessary steps that are to be taken in the case of distorted fingerprints.

2) Major advantages of minutiae based fingerprint recognition:

a. It requires less computational power and cost.
b. It is also capable of handling rotations greater than ten degree. Hence the user does not suffer from the "orientation problem" regarding his fingerprints.

3) Major disadvantages of minutiae based fingerprint recognition:

a. Distorted fingerprints are not taken into account
b. Poor quality fingerprint images are not considered for recognition and verification

III. CORRELATION BASED FINGERPRINT RECOGNITION METHOD

The Correlation based fingerprinting algorithm is the one that is based on the pixel values of the images. It uses gray scale information of the user's fingerprints. This algorithm selects the template and the pixel values of those template is then correlated with the pixel values of all the images in existing template database and then looks for the maximum value in the so called obtained correlated data which is greater than our selected threshold score. Maximum score of all the correlated data gives us the correct match of the template from all the images existing in the database.

This technique is under the category of "area based matching algorithms" in which the segment of image pixels (from a pair of M X N images) are compared and then matched. This method is less time consuming and needs less pre-processing of data as compared to the Pattern based and Minutiae based methods but it is observed that it is somewhere less accurate than those methods [5].

We also need to calculate the sum of squared differences between the pixel values of the two images that are used for matching purposes. Our aim is to maximize the correlation value. Figure 5 shows the correlation based process in detail. The process begins with the pixel evaluation of the two images. The values so obtained are then correlated.

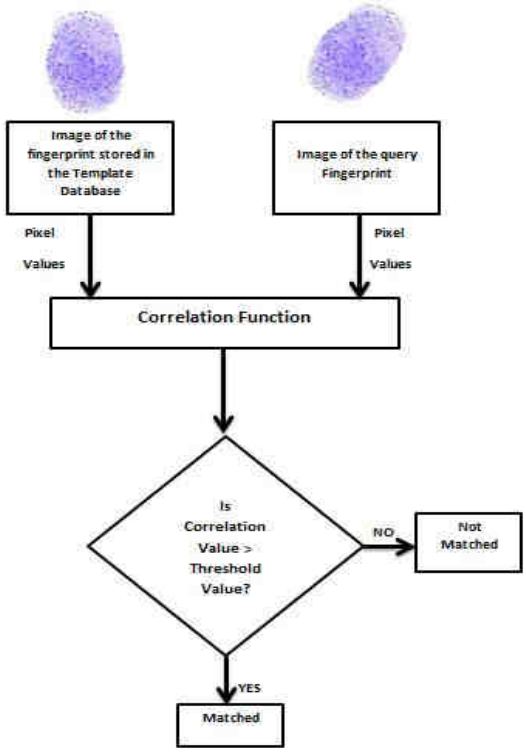

Figure 5:- Correlation Based Fingerprint Recognition

The correlation value is compared arithmetically with the threshold value that we have calculated in figure 6 below that is calculation of threshold value for correlation method.

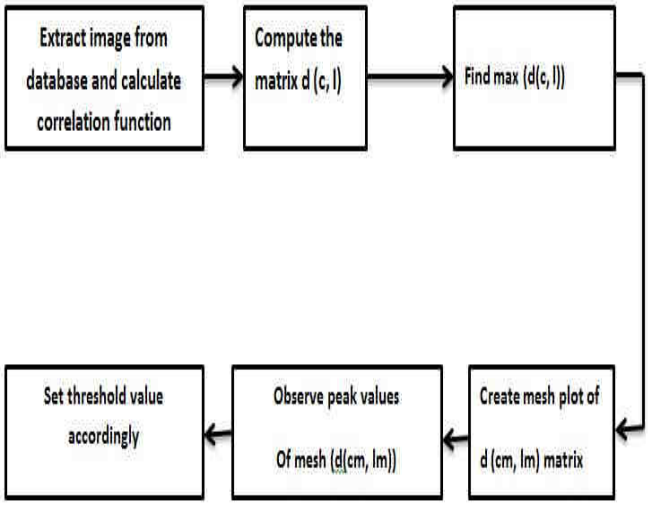

Figure: - 6 Calculation of Threshold value for Correlation method

The process of generating the threshold value for correlation based system under consideration can be implemented by executing the following sequence of steps as listed below in table II. The threshold score plays an important role in determining the output of our system because that value is used for comparison with the correlation value which was calculated previously [6].

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Table II Steps to be followed to generate the threshold score

i. Extract all of the images from the database.
ii. Compare each database image with the images using cross correlation function
iii. d (c, l) : compute this matrix
iv. Find max (d(c, l)) after every calculation of the value of the cross-correlation value and d (cm, lm).
v. Creation of mesh plot of d (cm, lm) matrix by executing the command : mesh (d(cm, lm))
vi. Observation of the peak values of mesh (d(cm, lm))and then set threshold score accordingly

Unlike the minutiae based technique, it uses the rich gray scale information directly, of the fingerprints.
It first chooses the appropriate Templates in the elemental fingerprint and then uses template Matching algorithm to find them in the secondary print. It then compares the template positions of both the elementary and the secondary print. Unlike minutiae based techniques, it is capable of handling the bad quality images i.e. the one from which no relevant minutiae details can be acquired. It also helps to handle the case of the fingerprints that are non-uniform in shape or have some distortions.

1) Template Selection based on correlation based fingerprint recognition method by using this algorithm; the templates are selected by verifying one simple rule:

"How the templates fit at other physical locations in that fingerprint".

If it fits well at some other location as it does at its prime location, then that template is not very useful but if it doesn't fit well then it is the one that offers contrast. Hence the ratio of "fit at a template's prime location" to the "fit at the second option location" is used as criteria for template selection .as we know the correlation based verification is done by template matching method hence this method needs large amount lot of computational power.

2) The advantages of the correlation based fingerprint recognition algorithm include:

a. Usage of Rich gray scale information and not just the Minutiae details.
b. Capability to handle the fingerprint images which are of poor quality
c. Inability of false/incorrect minutiae to affect its performance.
d. The template locations are pre-paired, hence, it is simpler to implement
e. Tolerant to non-uniform and distorted fingerprints

3) Major disadvantages of the correlation based fingerprint recognition algorithm are as listed below:

a. Template matching needs high computational power hence it is not of much use for real time applications as it is computationally expensive. This factor can be covered up by applying the spatial correlation theorem.
b. Not capable of handling rotations greater than 10 degree.

IV. COMPARISON OF MINUTIAE AND CORRELATION BASED APPROACH

Both these techniques are used for fingerprint recognition in a verification system and both have their share of advantages and disadvantages. While the minutiae based approach is computationally inexpensive, it also has a setback that it cannot be used in case the fingerprints of the user are distorted or the image quality of the fingerprint is poor. Correlation based approach is more flexible in this respect as it uses gray scale information of the image of the fingerprint. Hence it can be used to recognize and uniquely identify the fingerprints of an individual even if the image sample is of low quality.
Table III shows the comparison between minutiae and correlation based methods on the basis of some parameters such as cost, computational power, ability to handle poor as well as distorted or non-uniform fingerprint images, usage, templates etc. These parameters play an important role in deciding which type of method should be adopted for our system under consideration.

Table III Comparison of minutiae and correlation based approach

Parameters	**Minutiae based approach**	**Correlation based approach**
Basic concept	Minutiae i.e. Small physical details of our fingerprints	Calculation of correlation values
Gray scale information	Gray scale information is not utilized	Rich Gray scale information is used
Poor quality images	Can't handle poor quality images	Can handle poor quality images
Computational power	Less computational power is needed	More computational power is needed
Usage	Most widely used	Not used in real time applications due to more computational power
Cost	Less costly	More costly due to greater power consumption
Rotations	Capable of handling rotations greater than 10 degree	Not capable of handling rotations greater than 10 degree

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

False minutiae	False minutiae leads to incorrect template matching	False minutiae can't affect its performance
Templates	Template locations are not pre paired	Pre pairing of template locations is there
Non uniform fingerprints	Intolerant to non-uniform/distorted fingerprints	Tolerant to non-uniform/distorted fingerprints

This table tells us about the fact that in those systems in which we have less financial budget allocated for biometric purposes, we can use minutiae based method. Also it can be used in the systems which do not allow poor quality of fingerprint images. In other cases we can use correlation based method as it can deal with poor quality images as well as non-uniform/distorted fingerprints where minutiae cannot be well extracted.

V. CONCLUSION

The correlation based fingerprint recognition method is one of the most widely used methods in biometrics due to its simplicity in application and its performance regarding poor quality images. This method does not need much of pre-processing. Hence the errors generated at this step are also avoided. It uses richer gray scale information of the image and is capable of handling false /incorrect minutiae as well. As the templates are paired, hence it is simpler to implement. The correlation based method has comparable performance with the other methods but in future its performance can be upgraded if more number of rotations is taken care of. Also it is possible to upgrade the performance of the correlation based method in the near future, if we use the spatial correlation theorem.

REFERENCES

1. K. Mali and S. Bhattacharya, "Comparative study of different biometric features", international journal of advanced research in computer and communication engineering (IJARCCE) Vol. 2, Issue 7, 2013.
2. M Kaur, M Singh, A Girdhar and P.S sandhu, "Fingerprint verification system using minutiae extraction technique", published at world academy of science engineering and technology, issue 46, 2008.
3. T.Y Jea and V Govndaraaju, "A minutia-based partial fingerprint recognition system", published at Elsevier in pattern recognition issue, 2005.
4. J Ravi, K Raja and K. R venugopal, "fingerprint recognition using minutia score matching", international journal of engineering science and technology, vol. 1,issue 2, 2009.
5. P Verma, M dubey and P verma, "Correlation based method for identification of fingerprint- A biometric approach" international journal of engineering and advanced technology (IJEAT), vol. 1, issue 4, 2012.
6. A.M. Bazen, G. T. B Verwaaijen and S.H Gerez et al, "A correlation based fingerprint verification system", published at Proceedings of the ProRIsc, IEEE workshop, 2000.

AUTHORS PROFILES

Bharti Nagpal is currently a faculty member in AIACTR having post of Assistant Professor and pursuing PHD. She has completed her M.Tech in Information System from NSIT Dwarka.

Manoj Kumar is currently pursuing M.Tech (Information Security) from AIACTR, GGSIPU. He has completed B.Tech in Computer Science and Engineering from DGIGN, UPTU.

Priyank Pandey is currently pursuing M.Tech (Information Security) from AIACTR, GGSIPU. He has completed B.Tech in Computer Science and Engineering from AMITY UNIVERSITY, LUCKNOW.

Sonakshi Vij is currently pursuing M.Tech (Information Security) from AIACTR, GGSIPU. She has completed B.Tech in Computer Science and Engineering from BPIT, GGSIPU.

Vaishali is currently pursuing M.Tech (Information Security) from AIACTR, GGSIPU. She completed B.Tech in Computer Science and Engineering from NIEC, GGSIPU.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.