International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 11 | Nov -2017 www.irjet.net p-ISSN: 2395-0072

A Comparative Study of Fingerprint Matching Algorithms

Neelima Kanjan [1], Kajal Patil [2] ,Sonal Ranaware [3], Pratiksha Sarokte[4]

[1,2,3,4] *Department of Computer Engineering ,Pimpri Chinchwad College of Engineering Pune,India.*

Abstract - *In today's computerized world, it has become more important to authenticate people in a secure way. Therefore biometric authentication methods provides a unique way to authenticate people. A secure and confidential biometric authentication technique is the utilization of fingerprints .In recent years, fingerprint recognition technique is the dominant technology in the biometric sector. A number of fingerprint recognition methods have been used to perform fingerprint matching. This paper discusses the existing algorithms, limitations, and future research directions in each of the recognition phase. The main objective of this paper is to review the extensive research work that has been done over the past few years and discuss the various techniques proposed for fingerprint matching.*

Key Words: **Fingerprint matching, Minutiae, Gabor , clustering, cryptography.**

1. INTRODUCTION

Fingerprint-based identification is one of the most important biometric technologies which have drawn a substantial amount of attention recently. Fingerprints are believed to be unique across individuals and across fingers of same individual. Even identical twins having similar DNA, are believed to have different fingerprints. Conventional security systems used either knowledge based methods (passwords or PIN), and token-based methods (passport, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and fool-proof personal identification, authentication systems will necessarily require a biometric component. The word "biometrics" comes from the Greek language and is derived from the words bio (life) and metric (to measure). Biometric systems use a person's physical characteristics (like fingerprints, irises or veins),or behavioural characteristics (like voice, handwriting or typing rhythm) to determine their identity or to confirm that they are who they claim to be. The most widely used biometric technology is the fingerprint system. In fact, fingerprint can be used to replace the PIN or passwords in most security aspect. Fingerprints can be used instead of PIN in the smart card applications, passwords on workstations, etc. Many researches about fingerprint technology are undergoing all around the world. There are two types of fingerprint systems [9]: fingerprint verification and identification.

The verification system is a one-to-one matching and is based on the comparison of two groups of minutiae, respectively corresponding to two fingers to be compared. It is basically identity verification since you have to first input some information about yourself then the information is verified using your fingerprint. A fingerprint the pattern of ridges and valleys on the surface of fingertip .Fingerprint recognition can be categorized into identification and verification. Fingerprint identification is the process of determining which registered individual provides a given fingerprint. Fingerprint verification, on the other hand, is the process of accepting and rejecting the identity claim of a person using his fingerprint.

Fingerprint matching using a Gabor filter [6] is another technique which uses fingerprint matching using a 16 Gabor filter from the template which results in designing a new method for comparing two ridge patterns map of image using adaptive filter method. Minutiae based fingerprint matching algorithm [3] is useful in certain application for privacy protection. Previously, some work has been carried out to reduce the FRR (False Rejection Rate) by using certain techniques. Some of the techniques use the minutiae position of fingerprint images like Gabor filter technique [6] in which core & ridge pattern is used. All technologies of fingerprint recognition, identification and verification, minutiae extraction based and spectral features based, each has its own advantages and disadvantages and it may requires different treatments and techniques. The choice of which technologies to use is application specific.

2. FINGERPRINT MATCHING

The existing fingerprint recognition systems uses the approaches based on the local and global feature representations of the fingerprint images such as minutiae, ridge shape, texture information etc.

2.1 Ratio of Relational Distance Matching [1]

This algorithm works in two phases 1. Finding common unique points , 2. Matching phase .

In first phase , two images with N1 and N2 identified minutiae points respectively, this phase output is M which is a common minutiae points from N1 and N2 , M is N1 intersection N2 i.e M= ($N1 \cap N2$) where N1 is minutiae points of image1 and N2 is minutiae point of image2. After this new term called M(i)-tuples is introduced which represents information about a minutiae that can be identified uniquely among the set of all minutiae . There are 2 images are consider as a base image (BM) and input image (IM). Either of them can be BM or IM and vice versa. Step 1 to find M(i)-tuples is for each i = 1 to N1 , 5 nearest minutiae points are found . This is calculated by finding euclidean

distance from 'i'th minutiae point to all the other minutiae points in set N1 (BM) and noting down 5 euclidean distance with respect to euclidean distance. Step 2 if there are 5 points then calculate euclidean distance by subtracting the iN from i . then calculate ratio between them according to the formula (a – b): (a – c) = Max {(a-b), (a-c)} / Min {(a-b), (a-c)}. same way calculate M(i)-tuples for input image (IM). All this ratios are compared to get an candidate common list which is done in phase 2 matching phase confirmed common points are identified by drawing tree like structure and listed them , this algorithm results a tree whose vertices features are in Confirmed Common Points List which contains common minutiae points in image 1 and image 2 . Now final results is given if C(N) is the number of points in Confirmed Common Points List and N is maximum (Number of points in base and input images) , then C(N)>= (N/2) if this is true then positive score of both images are same is given else negative score is displayed.

2.2 K-Nearest Neighbor Minutiae Clustering [2]

Mainly two considerations are lie in this algorithm which are as follows :

1.It uses graph as fingerprint data structure.
2. Fingerprint search is optimized by clustering fingerprint graph feature.

As graph is set of edges and vertices here vertices represents feature of fingerprint and edges represents minutiae so clustering of graph data is done by K-NN clustering algorithm based on Euclidean distance between the vertices of the graph .It is the simplest clustering algorithm.

The nodes are classified by votes of its neighbors , each node is assigned to the class that is closest among its K nearest neighbor's , where K is integer value. If K=1 then node is assigned to the class of its nearest neighbor.

Following steps are involved for K-NN clustering :

1. Each node of the graph which is in the feature set has a class label , Class = c1,c2,...cn.
2. Calculating the Euclidean distance matrix for finding K-nearest neighbor's where K is the number of neighbors.
3. Most common class labels within the set are determine by analyzing K-closest nodes.
4. The most common class label is assigned to the node being analyzed.

After this clustering of graph nodes the fingerprint matching is performed. To identify the fingerprint it reads each fingerprint clustered graph templates from database and compares it with clustered input fingerprint graph templates. If graph templates are matched then the total graph isomorphism is applied. This continues till the input fingerprint is matched with fingerprint stored in database otherwise no match found returns.

2.3 Minutiae Extraction And Matching Algorithm

The basic method of minutiae extraction is divided in to three part Pre-processing, Minutiae Extraction, Post processing .Fig. 1. shows the Fingerprint recognition process using minutiae based algorithm .

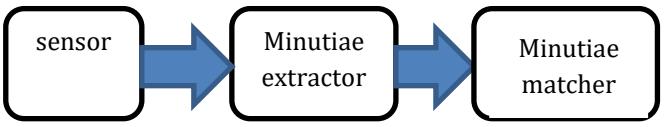

Fig.1.Fingerprint recognition process

This method divides three basic steps in to 7 modules which are given below [10].

Step 1: Input-

In this step we take five fingerprints of personas input and process them.

Step 2: Binarization:

This transform the 8-bit Gray fingerprint image to a 1-bit image with 0- value for ridges and 1-value for furrows.

Step 3: Thinning:

Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. [7] Uses an iterative, parallel thinning algorithm.

1) To get a thinned image we find the location of middle black pixel at each stage of continuation of the curve.
2) In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3).
3) And finally removes all those marked pixels after several scans.

Step 4: Minutiae Connect:

This operation takes thinned image as input and produces refined skeleton image by converting small straight lines to curve to maximum possible extant.

Step 5: Minutiae Margin:
This increases the margin of endpoints by one pixel of curves of length at least three pixels.

Step 6: Minutiae point Extraction:

For extracting minutiae point we compute the number of one- value of every 3x3 window:

- If the centroid is 1 and has only 1 one valued neighbor, then the central pixel is a termination.
- If the central is 1 and has 3 one-value neighbours, then the central pixel is a bifurcation.

- If the central is 1 and has 2 one-value neighbours, then the central pixel is a usual pixel.

Step 7: False Minutiae Removal

Procedure for removing false minutiae is given below [12]:

- If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge. Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.

- If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations.

- If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that now any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed.

- If two terminations are located in a short ridge with length less than D, remove the two terminations.

- If a branch point has at least two neighboring branch points, which are each no further away than maximum distance threshold value and these branch points are closely connected on common line segment than remove the branch points. And last we do the minutiae matching. Two fingerprint images to be matched, any one minutia is chosen from each image, and then the similarity of the two ridges associated with the two referenced minutia points is calculated. If the similarity is larger than a threshold, each set of minutiae to a new coordination system is transformed, whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point. After we get two sets of transformed minutia points, we use the elastic match algorithm to count the matched minutia pairs by assuming two minutiae having nearly the same position and direction are identical.

2.4 Threshold Cryptography Technique [5]

In Threshold cryptographic technique, fingerprint image is divided into two or more shares using visual cryptographic technique followed by compression. Also one share of fingerprint is stored in server & remaining shares given to user. The template can only be reconstructed by super-imposing shares. During the authentication phase the T share are superimposed with the ID card shares available with the user & it gets authenticated. The major concern of this technique is reducing the error rate. The advantage of the technique is the system is secured from the attack from server side. The disadvantage of this technique is there is no privacy Combined minutiae template for enrolment of database. The server side attacks are removed by using this techniques.

2.5 Fingerprint Matching using Gabor Filter[11]

The different processing steps from pre-processing to matching as the final step of the fingerprint authentication are

- Quantized co-sinusoidal triplets
- Discrete Fourier transform
- Gabor filters

The first step is the normalization, which results in a better contrast of the fingerprint image. After that, the fingerprint is segmented, which crops areas of the recorded image, which do not contain any relevant information. This is the end of the pre-processing. The last pre-processing step usually consists of a fingerprint enhancement as described in [7]. However, tests have shown that the subsequent reference point detection works on non-enhanced fingerprint images as well as on enhanced. Therefore, any further enhancement is not required for the subsequent processing steps. After that, the fingerprint image is filtered using a Gabor filter. Now, it is possible to create the feature map, which is used as the template. This template is matched in the subsequent matching step with templates of other fingerprints.

The result of the matching is the matching score, which represents how good two fingerprints resemble each other. Most methods for fingerprint identification use minutiae as the fingerprint features. For small scale fingerprint recognition system, it would not be efficient to undergo all the pre-processing steps (edge detection, smoothing, thinning), instead Gabor filters will be used to extract features directly from the gray level fingerprint. No pre-processing stage is needed before extracting the features [7].

1) Image Acquisition

A number of methods are used to acquire fingerprints. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also present eliminating the intermediate digitization process [11]. Fingerprint quality is very important since it affects directly the minutiae extraction algorithm. Two types of degradation usually affect fingerprint images: 1) the ridge lines are not strictly continuous since they sometimes include small breaks (gaps); 2) parallel ridgelines are not always well separated due to the presence of cluttering noise. The resolution of the scanned fingerprints must be 500 dpi while the size is 300 x 300.

2) Feature Extractor

Gabor filter based features have been successfully and widely applied to face recognition, pattern recognition and fingerprint enhancement. The family of 2-D Gabor filters was originally presented by Daugman (1980) as a framework for understanding the orientation and spatial frequency selectivity properties of the filter. The fingerprint print image will be scanned by a 8x8 window; for each block the magnitude of the Gabor filter is extracted with different values of m (m = 4 and m = 8). The features extracted (new reduced size image) will be used as the input to the classifier.

3) Classifier

The classifier is based on the k-nearest neighborhood algorithm KNN. "Training" of the KNN consists simply of collecting k images per individual as the training set. The remaining images consists the testing set. The classifier finds the k points in the training set that are the closest to x (relative to the Euclidean distance) and assigns x the label shared by the majority of these k nearest neighbors. Note that k is a parameter of the classifier; it is typically set to an odd value in order to prevent ties. The last phase is the verification phase where the testing fingerprint image [10]:

1) Is inputted to the system
2) Magnitude features are extracted
3) Perform the KNN algorithm
4) Identify the person

3. COMPARATIVE ANALYSIS

Table 1 shows the comparative analysis of various matching techniques**.**

Table -1: Comparative Analysis of Techniques.

Techniques	Objective	Limitations
Minutiae Based Algorithm[3]	To design an algorithm with privacy & security purpose.	Not suitable for low quality template .
Threshold Cryptography Technique [5]	To develop a technique by dividing it into small shares	Compression is required for reconstruction of fingerprint image
Fingerprint Matching using Gabor Filter[6]	To develop technique to increase genuine acceptance rate.	More number gabor filter used.
K-Nearest Neighbour Minutiae Clustering [2]	To identify the fingerprint it reads each fingerprint clustered graph templates from database	This technique increase the processing time .

4. CONCLUSIONS

A large number of fingerprint matching techniques for the purpose of authentication proposed in the literature have been reviewed. This paper provides a broad study of the various algorithms used in fingerprint matching process based on the various fingerprint representations and features extracted from the fingerprints images. A performance comparison table of various techniques proposed earlier for fingerprint matching, evaluated on the various parameters explained in paper is also presented. The benefits and limitations of these approaches have been highlighted. Mostly accepted finger scan technology is based on minutiae. Minutiae based techniques produce the fingerprint by its local features, like termination and bifurcation when minutiae points match between two fingerprints, so fingerprints are match .Most of techniques has high FRR rate which is not suitable for development of secure application. Hence, secured application with fingerprint authentication using a minutiae based algorithm will create a impact on other techniques with its security, privacy & low FRR rate.

ACKNOWLEDGEMENT

We would like to show our gratitude to Mr. Atul Pawar , Professor PCCOE who guided us throughout the preparation of the paper and gave us relevant concept to materialize the paper.

REFERENCES

[1] AbinandhanChandrasekaran, Dr.Bhavani Thuraisingham, "Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances"Second International Conference on Availability, Reliability and Security (ARES'07), IEEE Computer society 2007.

[2] Vaishali Pawar ,Mukesh Zaveri "Graph Based K-Nearest Neighbor Minutiae Clustering for Fingerprint Recognition" 10th International Conference on Natural Computation , IEEE 2014.

[3] Sheng Li and Alex C. Kot "Fingerprint Combination for Privacy Protection," IEEE Transactions on Information Forensics and Security, February 2013.

[4] Chandra Prakash Singh, Susheel Jain, Anurag Jain "

Literature Survey On Fingerprint Recognition Using Level 3 Feature Extraction Method " IJECE, Volume 3 Issue 1 January, 2014.

[5] Rajeswari Mukeshi & V.J.Subashini, "Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique," IEEE-International Conference On Advances In Engineering, Science And Management, March 2012 .

[6] Muhammad Umer Munir and Dr. Muhammad Younas Javed, "Fingerprint Matching using Gabor Filters," National Conference on Emerging Technologies, 2004.

[7] Munir, M. U., Javed, M. Y., ''Fingerprint Matching using Gabor Filters,'' 2005.

[8] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique", World Academy of Science, Engineering and Technology 46 2008.

[9] NTSC Subcommittee on Biometrics, ''Fingerprint Recognition'', 2000.

[10] Roli Bansal, Priti Sehgal and Punam Bedi "Minutiae Extraction from Fingerprint Images - a Review" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[11] Lin Hong, Yifei Wang, and Anil Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation" IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(8), August 1998.

[12] Maltoni D., Maio D., Jain A.K. and prabhakar S., "Handbook of Fingerprint Recognition," Second Edition, Springer , 2009.

[13] Sun Bei, Luo Wusheng, Du Liebo, Lu Qin , "A fingerprint identification algorithm based on local minutiae topological property" , IEEE First International Conference on Data Science in Cyberspace , 2016 .

[14] Gianmarco Baldini , Gary Steri , "A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components", IEEE Communications Surveys Tutorials , 2017

[15] Renuka Hawanna , Urmila Pawar , Pooja Sashte , "Android based application for an attendance monitoring" , International Engineering Research Journal (IERJ) Volume 1 Issue 11 Page 1649-1652, 2016 .

[16] Hariyanto , Sunny Arief Sudiro , Saepul Lukman , "Minutiae Matching Algorithm using Arti_cial Neural Network for Fingerprint Recognition",3rd International Conference on Arti_cial Intelligence, Modelling and Simulation , 2015