ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

An Approach to Demonstrate the Fallacies of Current Fingerprint Technology

Pinaki Satpathy [1], Banibrata Bag [1], Akinchan Das [1], Raj Kumar Maity [1], Moumita Jana [1]

Assistant Professor in Electronics & Comm. Engineering, Haldia Institute of Technology, Haldia, India[1]

ABSTRACT: Fingerprint technology is no more safer in today's world. Fingerprints are unique for everyone but it is also easily reproducible, without the use of complicated technologies. In this paper we demonstrate the matching of an ink stamped fingerprint of an individual with a picture of his thumb. The matching process involves few MATLAB programming and Photoshop. For clear, noise free samples the match percentage can be anywhere between 65-100%. Usually a value above 70% is considered a perfect match.

KEYWORDS : Morphological Method, Minutiae Marking, Minutiae Extraction, Minutiae Match

I INTRODUCTION

Fingerprint technology is believed to be one of the safest and most accurate forms of security tools available to us. No two people can have the same fingerprint, even twins and they are easy to decipher, which makes them so unique and convenient for security purposes. This technology is used widely all across the planet in all sectors from educational institutes to government facilities to lock up sensitive areas. But a major fallacy of this technology lies in one of its key strength- easy to decipher. We propose a simple mechanism via which a picture of a thumb can be used to match with actual fingerprints of an individual. The picture requires a little modification (cropping, transforming to binary scale etc) which can be done via photoshop. For matching with an actual fingerprint (ink stamp on paper) we used Matlab programs which match both sets with respect to the minutiae of fingerprint on each set. A pair is said to be a match if the matching percentage is more than 70%.

Fingerprint recognition technology extracts features from impressions made by the distinct ridges on the fingertips. The fingerprints can be either flat or rolled. A flat print captures only an impression of the central area between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger.

II RELATED WORK

Our main objective is to demonstrate that fingerprints can be reproduced with the help of a camera and photoshop software. The large number of approaches to fingerprint matching can be coarsely classified into three families.

• **Correlation-based matching**: Two fingerprint images are superimposed and the correlation between corresponding pixels is computed for different alignments (e.g. various displacements and rotations).

• **Minutiae-based matching**: This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that result in the maximum number of minutiae pairings

• **Pattern-based (or image-based) matching**: Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match.

We have implemented a minutiae based matching technique. This approach has been intensively studied, also is the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

backbone of the current available fingerprint recognition products.

III. SYSTEM LEVEL DESIGN

A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutia matcher. The system takes in 2 input fingerprints to be matched and gives a percentage score of the extent of match between the two. Based on the score and threshold match value it can distinguish whether the two fingerprints match or not. To implement a minutia extractor, a three-stage approach is widely used by researchers. They are preprocessing, minutia extraction and post-processing stage. For the fingerprint image preprocessing stage, Histogram Equalization and Fourier Transform are used to do image enhancement. And then the fingerprint image is binarized using the locally adaptive threshold method. The image segmentation task is fulfilled by a three-step approach: block direction estimation, segmentation by direction intensity and Region of Interest extraction by Morphological operations.

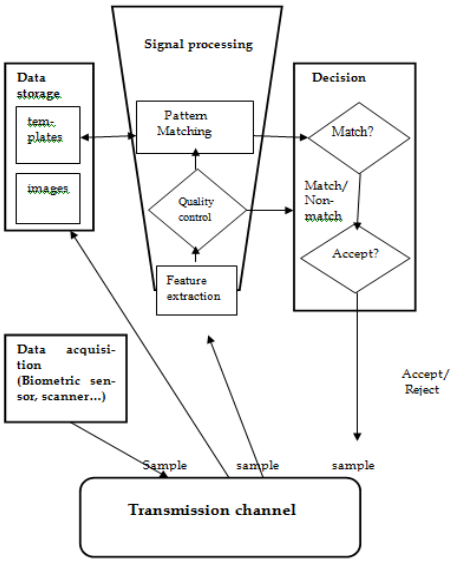


Figure – 2.1

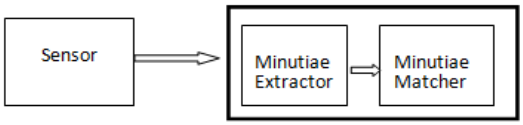


Figure 2.2 - Simplified Fingerprint Recognition System

For minutia extraction stage, iterative parallel thinning algorithm is used. The minutia marking is a relatively simple task. For the post-processing stage, a more rigorous algorithm is developed to remove false minutia.
The minutia matcher chooses any two minutiae as a reference minutia pair and then matches their associated ridges first. If the ridges match well, the two fingerprint images are aligned and matching is conducted for all the remaining minutiae.

IV. FINGERPRINT ENHANCEMENT BY FOURIER TRANSFROM

In this method the image is divided into small processing blocks (32 x 32 pixels) and perform the Fourier transform according to equation:

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

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.
In order to enhance a specific block by its dominant frequencies, we 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)|
We get enhanced block according to:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

$$g(x,y) = F^{-1}\left\{F(u,v)\times\left|F(u,v)\right|^{K}\right\}$$

Where F-1(F (u, v)) is done by:

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

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

The k in the 2nd formula is an experimentally determined constant, which we choose k=0.45 to calculate. While 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.

V. MINUTIAE EXTRACTION

Now that we have enhanced the image and segmented the required area, the job of minutiae extraction closes down to four operations: Ridge Thinning, Minutiae Marking, False Minutiae Removal and Minutiae Representation.

VI. MINUTIAE MARKING

After the fingerprint ridge thinning, marking minutia points is relatively easy. The concept of Crossing Number (CN) is widely used for extracting the minutiae.
In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch . If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending , i.e., for a pixel P, if Cn(P) = = 1 it's a ridge end and if Cn(P) = 3 it's a ridge bifurcation point.

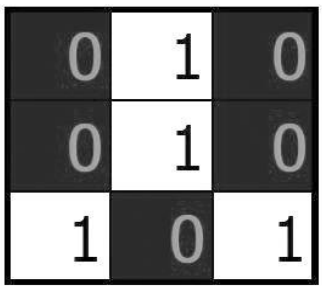


Fig. 3.1. Bifurcatio

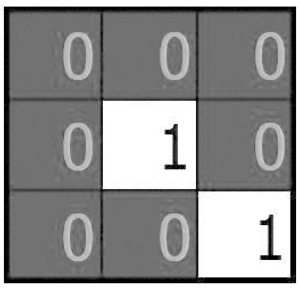


Fig. 3.2. Termination

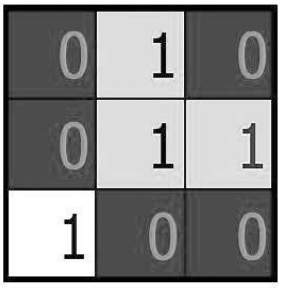


Fig. 3.3. Triple counting branch

There is one case where a general branch may be triple counted in Figure 3.4. Suppose both the uppermost pixel with value 1 and the rightmost pixel with value 1 have another neighbor outside the 3x3 window due to some left over spikes, so the two pixels will be marked as branches too, but actually only one branch is located in the small region. Thus this is taken care of.
The average inter-ridge width D is estimated at this stage. The average inter-ridge width refers to the average distance

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

between two neighboring ridges. The way to approximate the D value is simple. Scan a row of the thinned ridge image and sum up all pixels in the row whose values are one. Then divide the row length by the above summation to get an inter-ridge width. For more accuracy, such kind of row scan is performed upon several other rows and column scans are also conducted, finally all the inter-ridge widths are averaged to get the D. Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation.

VII. FALSE MINUTIAE REMOVAL

At this stage false ridge breaks due to insufficient amount of ink & ridge cross connections due to over inking are not totally eliminated. Also some of the earlier methods introduce some spurious minutia points in the image. So to keep the recognition system consistent these false minutiae need to be removed.
Seven types of false minutia are specified in following diagrams:

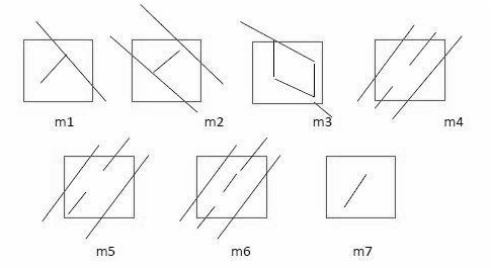


Fig. 3.4. False Minutia Structures.

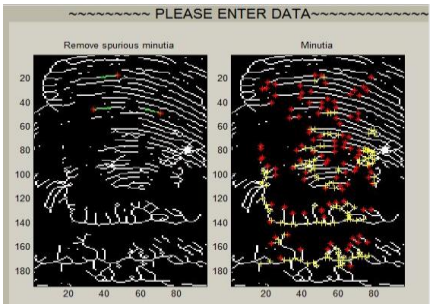


Fig. 3.5. Image (left) after false minutiae removal

m1 is a spike piercing into a valley. In the m2 case a spike falsely connects two ridges. m3 has two near bifurcations located in the same ridge. The two ridge broken points in the m4 case have nearly the same orientation and a short distance. m5 is alike the m4 case with the exception that one part of the broken ridge is so short that another termination is generated. m6 extends the m4 case but with the extra property that a third ridge is found in the middle of the two parts of the broken ridge. m7 has only one short ridge found in the threshold window.
The procedure for the removal of false minutia consists of the following steps:
1. If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge (m1 case). Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.
2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations. (m2, m3 cases).
3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutiae derived from a broken ridge and are removed. (Cases m4,m5 & m6).
4. If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).
This procedure in removing false minutia has two advantages. One is that the ridge ID is used to distinguish minutia and the seven types of false minutia are strictly defined. The second advantage is that the order of removal procedures is well considered to reduce the computation complexity because it utilizes the relations among the false minutia types. For example, the procedure3 solves the m4, m5 and m6 cases in a single check routine. And after procedure 3, the number of false minutia satisfying the m7 case is significantly reduced.
2. Match stage: The matching algorithm for the aligned minutia patterns needs to be adaptive since the strict match requires that all parameters (x, y, θ) are the same for two identical minutiae which is impossible to get when using biometric-based matching.This is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangle box and the direction difference between them is very small, then the two minutiae are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia. The final match ratio for two fingerprints is the number of total matched pairs divided by the number of minutia of the template fingerprint. The score is 100*ratio and ranges from 0 to 100. If the score is larger

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

than a pre-specified threshold (typically 80%), the two fingerprints are from the same finger.

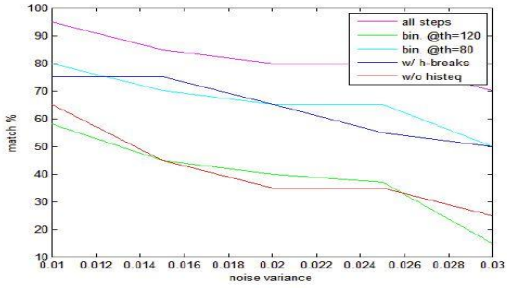


Fig. 3.6. Match percentage vs. noise variance

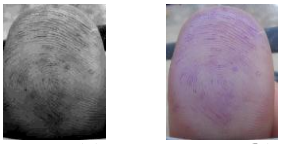
VIII. RESULTS

Depending on the clarity of the fingerprint impressions, the result varied quite significantly. We have taken three impressions of the right thumb and matched them with the digital image of the individual's thumb.

Sample 1 Sample 2 Sample 3

Fig. 4.1. Three different samples of the right thumb impressions.

We have used a Nikon L180 to capture the image of the thumb. Then we have used photoshop to make suitable adjustment to the image so that the Matlab programs can capture it efficiently. Photoshop is a raster grahics editor developed and published by Adobe system. We have used the Adobe Photoshop CS version 8.



(a) (b)

Fig. 4.2 (a). Original captured image (b) Image after contrast/brightness adjustment

For sample 1 in Figure. 4.1 we get a 100% match as the impression is clear and noise free and the ridges are clearly demarcated, which can be seen in Figure 4.3.

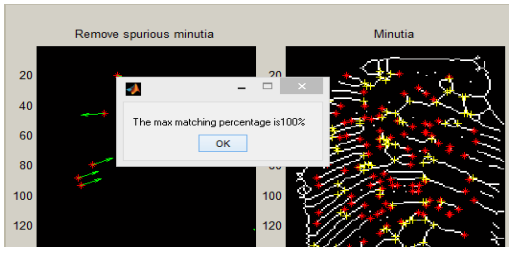


Fig. 4.3. Impression matching percentage with sample 3 thumbnel expression

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

For sample 2 in Fig. 4.1. we get a matching percent of 66.66%, as the sample has considerable noise, but the ridges are quite demarcated, which can be seen in figure 4.4.

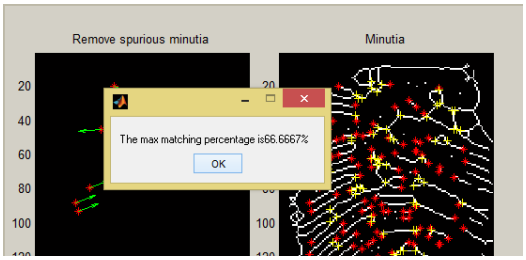


Fig. 4.4. Impression matching percentage with sample 2 thumbnel expression.

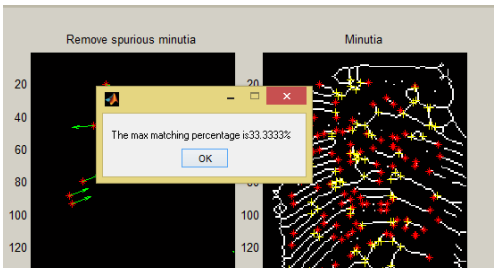


Fig. 4.5. percentage when matching with sample 3 thumbnel expression.

In Figure 4.5 it shows that the sample 3 in Fig. 4.1, the matching percentage is only 33.33%, as the ridges are highly smudged by noises and therefore the Matlab program cannot detect it.

IX. CONCLUSION

As demonstrated, the fingerprint technology is no longer a very safe option for day to day usage. It will require further modification to make it safer in today's tech savy world.

ACKNOWLEDGMENT

The work is carried out through the research facility at the Department of Electronics and Communication Engineering, Haldia Institute of Technology, Haldia, West Bengal. The authors would like to thank to the authorities of HIT for encouraging us for doing this research work. We would like to thank to all those experts who have contributed their efforts, knowledge towards the development of our research work.

REFERENCES

1. Ahmed and I.Traore. "Anomaly intrusion detection based on biometrics". In 6th IEEE Information Assurance Workshop, 2005.
2. Jain, A.Lin, Hong and Sharath Pankanti, 9th September 1997, "An Identity Authentication System Using Fingerprints", Proceeding of the IEEE, Vol 85, No. 9
3. A. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. In Transactions onDependable and Secure Computing, pages 165–179, 2007.
4. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics: a grand challenge. In Proceedings of the 17th International Conference on Pattern recoginition, pages 935–942, 2004.
5. D. Gunetti and C. Picardi. Keystroke analysis of free text. ACM transactions on information and System Security, 8(3), 2005.
6. E. Lau, X. LI, C. Xiao, and X. Yu. Enhanced user authentication through keystroke biometrics. In Computer and Network Security, Massachusetts Institute of technology, 2004.
7. J. McHugh. Intrusion and intrusion detection. International Journal of Information Security, 1:14–135, 2001.
8. Khalil Challita, Hikmat Farhat, Khaldoun Khaldi. Biometric Authentication for Intrusion Detection Systems. First International Conference on Integrated Intelligent Computing, 2010