Securing smart cities by fingerprint matching

Karan Sharma
Department of Computer Science
Poornima Institute of Engineering and Technology
Jaipur, India

***Abstract*— Smart cities are the need of developing India. One of the main concerns of smart cities is security of its people and safeguarding them from human threats. This concern can be solved to a great extent by using fingerprint recognition & matching techniques in smart cities. Also, fingerprint matching can be used to have public records, smart attendance system and can be used at many more places. So this paper deals with using fingerprint matching and recognition to make cities smarter.**

Keywords—Image processing, Fingerprint, Smart Cities, Minutiae points.

I. INTRODUCTION

Fingerprint matching technique is an emerging field in identification and security. It is a form of biometric recognition technique. Biometric techniques consider certain human physical and behavioural characteristics to have a unique identity of them. It includes fingerprints, face, iris, hand geometry, signature, etc. Traditional approach of having password is not much efficient as it can easily be hacked. They are still prevalent in areas where fingerprint technique is not applicable. So biometric methods provide a secured way of authentication and access control. They are popular due to the fact that every human being can be uniquely identified by his biometric characteristics.

Fingerprint matching technique is one of the most reliable biometric ways of identity management and access control. It has been into use from a long time. Fingerprint recognition is an automated method to verify and match two human fingerprints. It is easy to use. It has been suggested that no two individuals in the world have same pattern of fingerprints. Also, fingerprints of an individual do not change throughout his life unless there is a physical injury to the finger which leaves a scar. So it makes the fingerprint matching approach very robust.

Our approach deals with the use of fingerprint matching and detection to make smart cities safer. A smart city uses technically advanced features for the betterment of its people. It gives better quality of life to its people. It provides smart solutions to the day-to-day need of people. A city with such level of technical advancement needs a robust security system. The security needs of a smart city can be solved to a great extent by using fingerprint matching techniques wherever there is a need for authentication and access control. It is easy to use and provides high level of security. So our main focus will be implementation of this approach in smart cities.

A. Fingerprints

A fingerprint is an impression made by ridges of a human finger. Fingerprint impressions can be easily left on a surface making their detection easier. Every human being has a pattern of ridges and valleys on his finger which differ from individual to individual. It is believed that every individual on the earth has a different pattern of fingerprints. There are various patterns of a fingerprint. Fingerprints are mainly used in forensic tests to determine a criminal at a crime scene. Figure 1 shows a fingerprint image.

Fig. 1. Fingerprint Image

Fingerprint features can be generally characterized into three levels. The first level is pattern based, second level is minutiae points based and the third level is based on pores and ridge contours.

The first level considers macro details of a fingerprint such as an arch, loops or whorl. These are the basic patterns of fingerprints. Further, each pattern can be subdivided, like tented arch, radial loop, etc. These basic pattern form the first level of matching [4].

The second level considers more minute details of the fingerprints. There are certain minutiae points in a fingerprint. These points can be ridge ending or ridge bifurcation. A ridge ending is the point where a ridge ends and a ridge bifurcation is the point where a ridge divides in two. See figure 2 to get more details about minutiae characteristics [4].

The third level considers the micro details of a fingerprint. Usually it is an effective way of fingerprint matching, but its cost of operation is more. It takes into consideration the pores between ridges, line shapes, etc. [4] Figure 2 shows all the three levels which we just discussed.

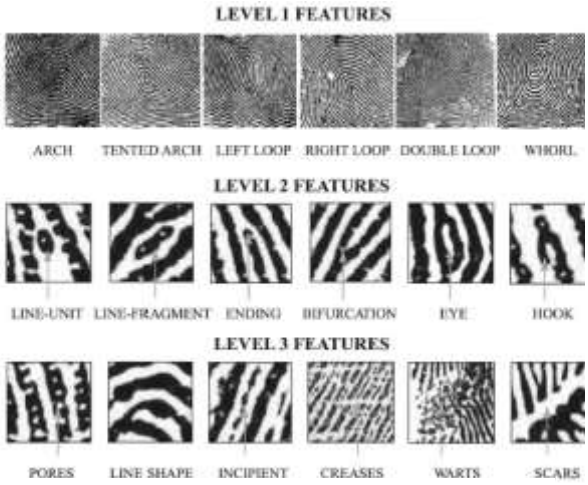


Fig. 2. Levels of Fingerprints

II. USING FINGERPRINT MATCHING IN SMART CITIES

A. Flaws in traditional approaches

Traditional method for authentication and access control is using passwords. It is not so secured method of protection as passwords are easily traceable. Passwords does not uniquely identify an individual. There are various methods of breaching the password security. As the password technology is improving, hacking techniques are also improving. So it is necessary to have a precise system of identification and access control.

Traditional approach of keeping entries of people for a particular work is neither reliable nor hassle-free. It requires a lot of paperwork and does not guarantee correctness of the information for identification. The security of that information is quiet difficult as it is present physically on papers.

B. How can fingerprint technology be a smart solution?

A smart city uses information and communication technology to apply smart solutions to enhance quality of life, performance and interactivity of urban services and to reduce cost and resource consumption to reduce the gap between citizens and the government. The security needs of a smart city are large and smart cities need a precise security system to safeguard its people and their property. Also it needs smart solutions to day to day activities. So fingerprint matching technique maybe used in a smart city in order to have authentication and access control.

Consider a society where manual entries of incoming people are kept. It is not a smart way of keeping the entries as it is time consuming and can be highly inaccurate. Such places need a precise and smart system in order to make it more secured.

Smart cities are in a growing need of applying new technologies in order to make life of its people easier. An easy way to identify individuals uniquely in smart cities is using the information of that person's fingerprints. This system can be used in most of the aspects.

C. Applications in smart cities

The most difficult thing about fingerprint technique is its implementation. In this section, we will have a look on the various places where this approach can be implemented.

1) Having public records:

One of the best applications of fingerprint technique is having records of people that can uniquely identify each individual. There can be a central database which would contain information of all the people. Each person would be needed to register first. In this way, each person will have his own identity with the government.

2) Having smart gate-entry keeping systems:

Traditional system of gate-entry keeping is having entries on paper. This is not a reliable system as there is no authenticity of the identity of the user. A more smart solution for it can be using fingerprint technique. A fingerprint recognition system can be installed on gates so that each incoming person just has to keep his finger on the screen. Each person's fingerprint sample would be stored in the database.

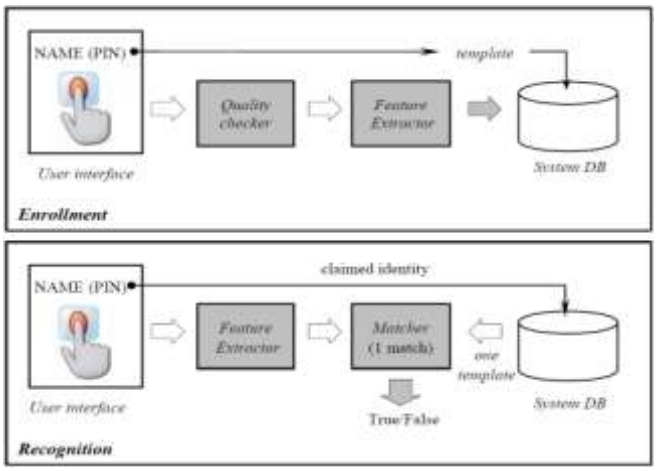


Fig. 3. System

This technology can even be used in colleges and institutions for verifying the identity of students. A database would contain information of fingerprints of all the students. So a student entering the college should verify his/her fingerprint. This will not only ensure security but also help to count the number of students and also their attendance.

It can even be used on toll points on the road so that a city can register the incoming and outgoing citizens. There can be numerous more applications of this technique in cities to make them smarter.

Further we will see how fingerprint matching technique is implemented, i.e. what is the procedure to identify and match two fingerprints.

III. IMPLEMENTING FINGERPRINT TECHNIQUE

Practically, Fingerprint Matching technique can be implemented by using Image Processing technique. Image Processing is the technique which involves performing various operations on an image in order to get useful information from the image. Image Processing is an emerging field. Everyday new technologies are emerging for processing images. One of the applications of Image Processing is Fingerprint Matching technique.

A. *Fingerprint Matching Techniques*

Based on the type of matching, fingerprint matching technique can be broadly classified into three categories:

1) Co-relation based matching:

In this approach, two fingerprint sample images are superimposed on each other and then relation between corresponding pixels is computed at different alignments.

2) Minutiae based matching:

This is the most popular approach followed at most of the places. In this approach, minutiae points are extracted from the fingerprint sample image. Then the position of those points are matched with the already existing points in the database. It is said to be matched if number of matching points exceed a particular threshold.

3) Pattern based matching:

There can be different patterns of a fingerprint like arch, whorl or loop. Pattern based approach compares these patterns with the samples already stored in the database. Then the degree up to which they match is computed [1].

We will be studying minutiae based approach in this paper as it is less complex procedure which yields better results.

B. *Minutiae based approach*

Minutiae based approach is the most widely used fingerprint matching technique. During scanning, it stores the locations of minutiae points in a database for later matching. Minutiae points mostly are ridge endings and ridge bifurcations. A ridge ending is a point where a ridge ends and a ridge bifurcation is a point where a ridge divides into two. Every fingerprint contain about 20-70 minutiae points. Refer Figure 4 for details.

Fig. 4. Minnutiae Points

Minutiae based approach is a two-step process, minutiae extraction and minutiae matching. Minutiae Extraction contains Image Enhancement, Image Segmentation and Final Extraction. Minutiae matching has Minutiae Alignment and Final Matching.

1) Minutiae Extraction

It has the following processes:

a) Image Enhancement

The first step in fingerprint matching technique is image enhancement. Image enhancement refers to improving the quality of an image so that we can get more visual information from it. This step is required as the fingerprint samples are of very low quality. It has the following methods:

i) Histogram Equalization

This method is used to improve the global contrast of an image by adjusting its total distribution on a histogram. It is a method of enhancing the image by adjusting its intensity. The intensity values on a histogram are spread so that it is not concentrated at a place. The MATLAB function for histogram equalization is 'histeq'. Figure 5 shows a histogram and a corresponding equalized histogram.

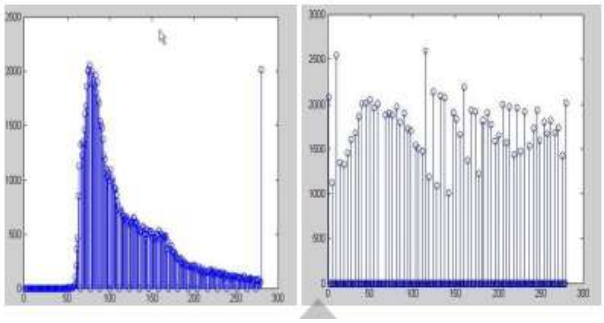


Fig. 5. Histogram and its equalization.

(a) (b)

Fig. 6. Original Image (a), Enhanced Image after histogram equalization (b)

ii) Fast Fourier Transformation

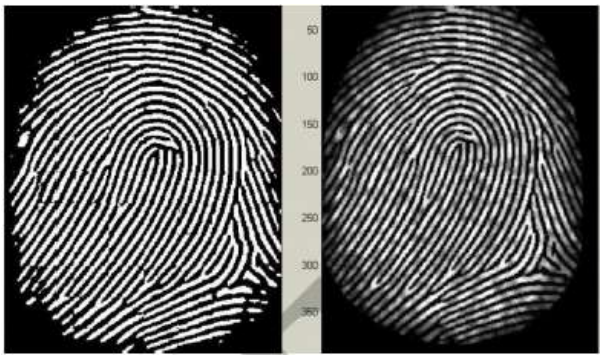
The image is divided into small blocks and Fourier Transform is applied on it according to this equation:

$$F(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j)\, e^{-\iota 2\pi \left(\frac{ki}{N} + \frac{lj}{N}\right)}$$

Fourier transformation fills the broken ridges in the sample. Its MATLAB function is 'fft2'.

iii) Image Binarization

This process converts an 8-bit gray image into a 1-bit image with 0-values for ridges and 1-value for furrows. This creates a black and white image which is simple for computation. The MATLAB function for binarization is 'im2bw'.



(a) (b)

Fig. 7. Binarized Image (a), Image before binarization (b)

b) Image Segmentation

Image segmentation deals with getting a specific region of the image so as to make the complexity less. It selects a particular Region of Interest (ROI).

c) Final Minutiae Extraction

After enhancing the image, final minutiae points are extracted from the fingerprint image. It follows the following steps:

i) Ridge Thinning

This method eliminates the redundant pixels from the image. Each ridge is many pixels wide. So thinning makes the ridge a single pixel wide. MATLAB's function 'bwmorph' is used for thinning. A parameter 'thin' is passed in the function for thinning.

ii) Minutiae Marking

As now we have each ridge of a single pixel, it is easier for us to mark the minutiae points. It is done for each 3x3 pixel window. If the center pixel is 1 and it has exactly 3 1-value neighbors, then the center pixel is a point of minutiae bifurcation (Figure 8) [1].

0	1	0
0	1	0
1	0	1

Fig. 8. Ridge bifurcation

If the center pixel is 1 and it has only 1 1-value pixel as its neighbor, then the center pixel is a ridge ending (Figure 9) [1].

0	1	0
0	1	0
0	0	0

Fig. 9. Ridge ending

iii) False Minutiae removal

At this stage, there can be ridge cross connections due to over inking and false ridge may break due to insufficient amount of ink. Also extra minutiae points can be introduced in the sample by some earlier methods. So to keep the recognition system consistent, these false minutiae need to be removed.

iv) Minutiae Representation

Finally the minutiae points thus detected are stored in the database. They are stored with the 'x' and 'y' coordinate to the pixel where they are detected. Along with them, the orientation and associated ridge is also used for representation. The process of storing only these minutiae is less complex as the entire fingerprint is not stored and scanned.

2) Minutiae Matching

After minutiae points are detected from the fingerprint sample, they are matched with the existing present samples in the database. It involves

a) Minutiae alignment

Firstly, the minutiae points from the two samples are aligned so as to match them. Correlation factor is calculated between 2 minutiae points from each set. So a similarity score is calculated by the formula

$$S = \sqrt{\frac{\sum_{i=0}^{m} xiXi}{\sum_{i=0}^{m} xi^2 Xi^2}}$$

Where (xi…xn) and (Xi...Xn) are the set of x-coordinates for each of the 2 minutia chosen. 'm' is minimal one of the 'n' and N value. If the similarity score is larger than 0.8, then go to next step, otherwise continue to match the next pair of ridges [1].

Let M (x, y, θ) be reference minutia found from step 1(say from I1). For each fingerprint, translate and rotate all other minutiae (xi, yi, θi) with respect to the M according to the following formula:

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta i\_new \end{pmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} xi - x \\ yi - y \\ \theta i - \theta \end{bmatrix}$$

The new x-axis is coincident with the direction of minutiae and the coordinate system is originated at reference minutia M. We get transformed sets of minutiae I1' and I2' [1].

b) Minutiae Matching

This is the final step in fingerprint matching technique. An elastic string match algorithm is used to find the number of matched minutiae pairs among I1' and I2'. Two fingerprint samples are said to be matched if minutiae points more than a particular threshold are matched, or else they are said to be unmatched. Threshold is the minimum number of points that must be matched to term both the samples as matched.

IV. RESULTS AND CONCLUSION

Minutiae based approach is preferred over other approaches as it has comparatively less computation work. It computes only over the minutiae points and not the entire fingerprint. This approach can be used in smart cities as there is a need of faster processing.

In this technique, there can be two types of errors. First error can be a False Match Error. It occurs when two fingerprint samples of different people are said to be matched by the system. This error may occur when the threshold value is too less.

Another error which can occur is a False Non-match Error. This error occurs when two fingerprint samples of same person are said to be non-matched by the system. This may happen when the threshold value is too high. So we cannot eliminate both the errors simultaneously as the value of threshold can either be high or low and not both at the same time. The value of threshold depends on the place where it is being used.

There are two indexes to evaluate the performance of the system, False Acceptance Rate and False Rejection Rate. False Rejection rate is calculated by matching each sample with the remaining sample of the same fingerprint. False Acceptance Rate can be computed by matching first sample of each finger in the database with the first sample of the remaining fingers [1].

V. FUTURE SCOPE

People may alter their fingerprints in order to act as a different person. Such fake fingerprints can be used by a person to imitate legitimate user's fingerprints for getting access to information he is not authorized to access. So such practices can be reduced by using 'liveness detection' of fingers. It is done by checking whether the finger is 'live' by measuring pulse, perspiration, and deformation of the finger.

Criminals may mutilate their fingers to avoid being caught. So mutilation detectors may be installed in the fingerprint system [2].

VI. REFERENCES

[1] Sangram Bana and Dr. Davinder Kaur, "Fingerprint Recognition using Image Segmentation", International Journal of Advanced Engineering Sciences and Technologies (IJAEST) , Vol No. 5, Issue No. 1, 012 – 023.

[2] Anil K Jain, Jianjiang Feng and Karthik Nandakumar, "Fingerprint Matching".

[3] Naresh Kumar and Parag Verma, "Fingerprint Image Enhancement and Minutiae Matching", International Journal of Engineering Sciences & Emerging Technologies, Volume 2, Issue 2, pp: 37-42.

[4] Anil K Jain, Yi Chen, Meltem Demirkus, "Pores and Ridges: High Resoluton Fingerprint Matching Using Level 3 Features", IEEE Transactions on Pattern Analysis and Machine Intelligence, VOL. 29, NO. 1.

[5] Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain & Salil Prabhakar.

[6] A. K. Jain, F. Patrick, A. Arun, "Handbook of Biometrics", Springer science + Business Media, LLC, 1st edition, pp. 1-42, 2008.

[7] S. Pankanti, S. Prabhakar, and A.K. Jain, "On the Individuality of Fingerprints," IEEE Trans. Pattern Analysis and Machine Intelligence,vol. 24, no. 8, pp. 1010-1025, Aug. 2002.

[8] J.D. Stosz and L.A. Alyea, "Automated System for FingerprintAuthentication Using Pores and Ridge Structure," Proc. SPIE Conf. Automatic Systems for the Identification and Inspection of Humans,vol. 2277, pp. 210-223, 1994.

[9] D.R. Ashbaugh, Quantitative-Qualitative Friction Ridge Analysis: An Introduction to Basic and Advanced Ridgeology. CRC Press, 1999.

[10] J. Thornton, "Latent Fingerprints, Setting Standards in the Comparison and Identification," Proc. 84th Ann. Training Conf. Calif. State Division of IAI, May 2000.