Journal of Applied Information Science
7 (1), June 2019, 16-20
http://www.publishingindia.com/jais

Biometric System Based Election Procedure Using Pattern Based and Minutiae Based Method

Vaibhav Nagveker[1*], Sanket Patil[2], Nandakumar Gauns[2], Kalpesh Sawant[2], Joshua D'Souza[2], Kedar Sawant[3] and Pooja Dalvi[3]
[1]Student, Department of Computer Engineering, Agnel Institute of Technology and Design Assagao, Bardez, Goa, India. Email: danzo.ftw15@gmail.com
[2]Student, Department of Computer Engineering, Agnel Institute of Technology and Design Assagao, Bardez, Goa, India.
[3]Assistant Professor, Department of Computer Engineering, Agnel Institute of Technology and Design Assagao, Bardez, Goa, India.
*Corresponding Author

Abstract: No traditional election procedure present today is ideal. All of the current procedures have some major flaws to them. These flaws can lead to undemocratic election procedure, where people can manipulate the system using loopholes present in them. This tends to increase the risk of monopoly (i.e. a dominant leader keeps taking control of the post by manipulating the elections). Current traditional systems include technologies like ballot paper and EVM's. When people think about election based on ballot papers, they imagine that they are thinking of ancient technology, and in a way, this is true. Manipulations are possible by discarding many votes with even minute discrepancies and adding votes to the favored party. Although EVM's have taken great steps in improving the election procedure by making it safe, fast, efficient it still has its flaws and can be manipulated.

Proposed System uses fingerprint identification to verify a voter, only then he/she will be allowed to cast a vote. There are two major algorithms for fingerprint identification, the pattern based and the minutiae based algorithm. In the pattern based algorithm, the image of the scanned fingerprint is directly compared with the stored samples of the fingerprint. This method is useful when the scanned image is not very clear and minutiae details cannot be extracted. The disadvantages of this method are that it consumes a lot of memory as the entire fingerprint is stored. The minutiae-based algorithm is the fastest and most reliable method for fingerprint identification. In the minutiae based algorithm, the minutiae details of the finger are stored and not the original image. This is useful since it requires much less memory, and is required only when there are multiple fingerprints to be stored. The minutiae-based method is precise and much more efficient than the pattern based algorithm.

Keywords: Algorithm, Bifurcation, Enclosure, Minutiae, Pattern, Ridge, Voting.

I. Introduction

Elections are a shaping feature of democratic government, however, all too often; we have a tendency to take the particular mechanics of the election with no consideration. Before recent allegations of election fraud in many states of India and around the world, many people thought that voting was just one thing: "You visit the voting Booths and cast your vote, then the votes are calculated and the victor is announced." Recently due to many allegations, this has started changing and people now question the election process while casting the votes and after the votes have been cast. A more efficient and secure system then ballot papers and the EVM's are to add a security process before actually casting a vote. The best and the safest way of doing this would be by taking a biometric scan of the people before he/she casts a vote.

The different kinds of biometrics include fingerprint detection, face detection, iris detection, palm detection and matching of DNA. The practice of biometrics method has many merits. The most important one is high security level and accuracy that it ensures. In contrast to passwords, cards, or any other form of identification, biometric based information cannot be forgotten, stolen, replaced or forged. The ratio of finding two similar fingerprints is 1 in 64 billion even with identical twins. This is the reason why biometrics is linked or connected to the question of identity of every person. Fingerprints are the minute ridges, loops and more on each finger. They form from pressure on a fetus's tiny, growing fingers when it is in the womb. Although identical twins can have the same Deoxyribonucleic acid (DNA) but not the same fingerprint pattern. They're also easily accessible and do not need much effort. You leave fingerprints on just about anything else touch because of this sweat. Different features of the fingerprint are used to identify different fingerprints; all these features are different in different people.

II. Literature Survey

A thorough study on the Minutiae based method was done. Fingerprint image preprocessing techniques like, Image enhancement, Binarization and Image segmentation is discussed in the paper. The Minutiae based extraction involves the fingerprint image going through Thinning, False minutiae removal and Minutiae extraction. This paper focuses more on the thinning process by implementing an algorithm called Enhanced thinning [1].

Sangeeta Narwal and Daljit Kaur compared the two prime algorithms used in fingerprint identification technology namely, Minutiae based method and Pattern based method. The merits and demerits of both the methods are discussed and experimentally proven. It is found that the Minutiae based method has a less rate false match as compared to the Pattern based method. Comparing the efficiencies of the algorithms, it is determined that the Pattern based method is faster than Minutiae based method [2].

Muhammad Umer Munir *et al.* uses Gabor filtering to implement the algorithms. It first extracts the core point of fingerprint image using Poincare and slope method. Then, the spherical region is divided around the core point into total 128 sectors after which the pixel intensities are normalized to a constant variance and mean. The spherical region is filtered using sixteen Gabor filters and vectors are generated using Gabor filters. And at last calculation is done between two vectors to find the Euclidean distance. Genuine Accept Rate (GAR) and the False Accept Rate (FAR) are the two parameters which are used to find the efficiency of the system [3].

Instead of using the traditional Crossing Number (CN) method in which a 3x3 window is used, a 4x4 window is used to eliminate duplicate minutiae points. Binarization, Thinning and other preprocessing methods are applied on the fingerprint image before Minutiae can be successfully extracted. After applying the 4x4 window, 55% more valid bifurcation points were extracted [4].

III. Pattern Based Algorithm

They are also called as image based algorithm. Pattern based method algorithm compares some features of the fingerprint like the arch, whorl, and loop between a previously stored template which is present in its dataset and a candidate fingerprint. Image based approach may be the best choice to match fingerprints, which have a very low image quality to allow a reliable and efficient Minutiae extraction [5].

TIFF images are captured and stored in the database using a fingerprint scanner device. To distinguish the graphical image obtained from the capture device from a template or print stored in a database, it is commonly referred to as a live scan. The fingerprint image is examined by the processing software and the center of the image is located, which may be off-center from the fingerprint core. The captured image is then cropped from a fixed distance around this graphical center. The rectangle in the Fig. 1 details this particular cropped region. The obtained cropped region of the image is then compressed and stored for subsequent match.

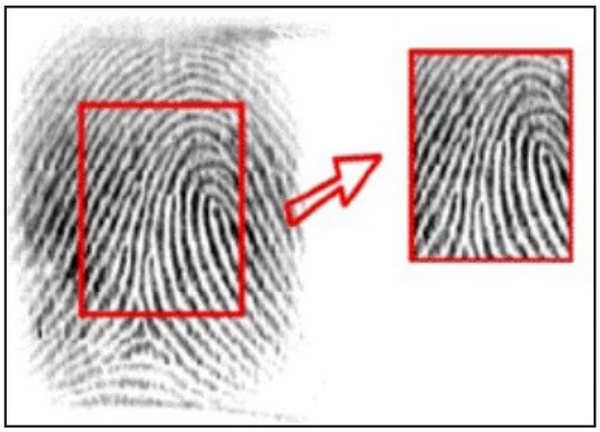

Fig. 1: Cropped TIFF Image

IV. Minutiae Based Algorithm

In the minutiae based approach, instead of storing and comparing the whole image we only keep track of the minutiae points. Minutiae points are categorized into ridge points, ridge ending, bifurcation, crossing points etc. In Minutiae based algorithm, a lot of pre-processing is required like binarization, thinning, and only then the minutiae features can be extracted and stored. Since this method is very memory efficient and highly accurate, it is generally more preferred than any other. Here TIFF images are captured and stored in the database using a fingerprint scanner device. Later on the stored images can be retrieved from the database whose minutiae points will be extracted/identified and compared with the minutiae points of the image of the users fingerprint to compute Similarity scores which will be used for authentication purpose.

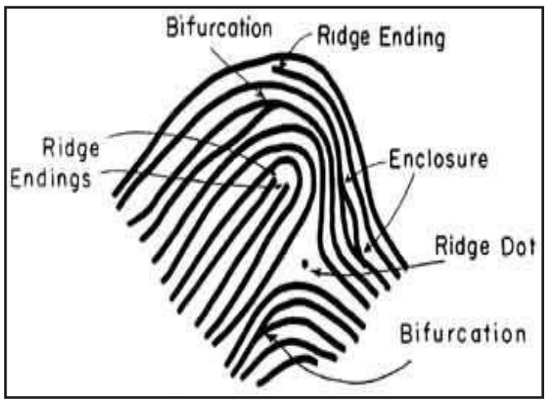

Fig. 2: Features of Minutiae Based Algorithm

The following is the block diagram of the minutiae based algorithm:

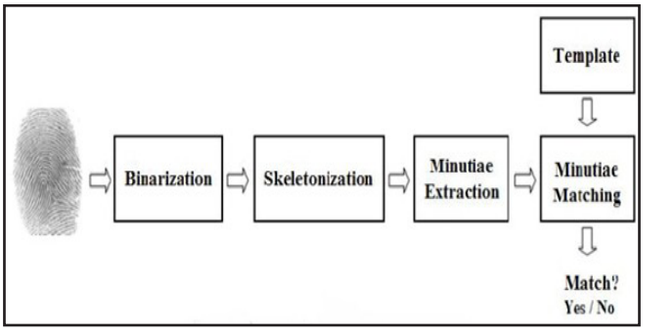

Fig. 3: Working of Minutiae Based Algorithm

A. Binarization

Binarization is the process of converting a pixel image to a binary image i.e. an image with only two colors black and white. These days it's still important for things like text digitization or segmentation process and for other image processing applications. The simplest and the best way to do this are to choose a threshold value, and classify all pixels above these values are as white, else black.

B. Skeletonization

After binarization is completed, next we need to thin the image. The process of thinning the image is called skeletonization. The binary picture obtained has to be thinned until its size is just 1 pixel wide. The way to do this is to consider all pixels on the boundaries of foreground regions (i.e. foreground points that have one or more background neighbor). Points having more than one foreground neighbours are deleted, as long as it does not locally disconnect (i.e. split into two) the region containing that pixel.

C. Minutiae Extraction

CN method is being employed here since it's the most common method of Minutiae.

This method is favored over other methods for its computational efficiency and inherent simplicity. Later the skeletonization process is applied on the binarized image which deletes all the pixels from ridges until one pixel wide image is obtained.

Next we use the CN AKA crossing number method to find the minutiae points.

The minutiae features are then extracted by identifying the local neighbours of each ridge pixel in the image using a 3x3 window (Fig. 4). The CN value is then computed as follows:

P4	P3	P2
P5	P	P1
P6	P7	P8

Fig. 4: CN Computation Table

$$CN = 0.5\sum_{i=1}^{8} |P_i - P_{i+1}| \quad \text{Where } P(9) = P(1)$$

TABLE I: CN TABLE

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

After substituting all the values in the CN formula, we check the value we get, and then compare the value to the values in Table I. In this way we get all the different points. Each fingerprint has around 40 such points. All such points are extracted using the CN Method on each and every pixel on the thinned image. The final result obtained is either one of the CN values that is 0, 1, 2, 3, and 4. The isolated point is always ignored or not taken into consideration. Ridge ending point, continuing ridge point and Bifurcation are considered because these are the most common features in a finger. The Crossing points are not taken into consideration because this point is extremely rare point in a finger.

D. Matching Algorithm

In a good quality scanned fingerprint image, there are about 70 to 80 minutiae points but in a general fingerprint scan the number of minutiae points are much lower (approximately 20 to 30). This system finds out the minutiae points from the images retrieved from the database and also the image taken from the user as input. These matched minutiae points are used for calculating similarity scores which can be used for authentication purpose.

When there is a match of a required amount of minutiae's, the fingerprints are said to be of the same finger.

Matching algorithm compares two minutiae sets:

Template T = $\{m_1, m_2, \ldots, m_j\}$ from stored fingerprint;

Input I = $\{m_1, m_2, \ldots, m_i\}$ of the input fingerprint.

And it returns a similarity score S.

$$sd(m_i, m_j) = 1 \Leftrightarrow \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \leq r_0$$

$$dd(m_i, m_j) = 1 \Leftrightarrow \min(|\theta_i - \theta_j|, 360 - |\theta_i - \theta_j|) < \theta_0$$

If the score is above 0.5, it is considered to be a match, else not a match.

V. Time Complexity

Total time is taken to process the inputs and produce the final result.

A. Time Complexity of Minutiae Based Algorithm

i) Time complexity of Minutiae algorithm depends on the time taken to retrieve the images from the database, then extracting all the features of the retrieved images and the input/user fingerprint captured using the Fingerprint Scanner device and comparing features of all 5 images with the input/user fingerprint. The total amount of time taken for executing this process and producing the final result is the Time Complexity.

ii) Minutiae based algorithm is much slower as compared to Pattern based algorithm but it's much more accurate.

B. Time Complexity of Pattern Based Algorithm

i) The Pattern based algorithm is much faster compared to Minutiae based algorithm.

ii) Time Complexity of Pattern Based algorithm depends on the time taken to retrieve the images from the database, identifying all the pixels from the retrieved images and the input/user fingerprint captured using the fingerprint scanner device and then comparing pixels of all five images with the input/user fingerprint. The total amount of time taken for executing this process and producing the final result is the time complexity of Pattern based algorithm.

iii) This algorithm counts total number of pixels in an image that is retrieved from the database (DB) and pixels of all five images are compared with the fingerprint taken from the user during authentication.

VI. Performance of Minutiae Algorithm Compared with Pattern Based Algorithm

Table II: Time Complexity Table

Algorithms	Time
Minutiae based algorithm	>3000 ms
Pattern based algorithm	<1000 ms

A. Performance of Minutiae Based Algorithm

i) Performance of Minutiae based algorithm is computed on the total amount of time taken by the algorithm to execute and produce the final result.

ii) During the execution of Minutiae based algorithm, it can take "n" number of fingerprint images from the database where value of "n" is defined by the user. After the retrieval of the images from the database, processes it and the final result that is either the fingerprints match or not will determine its performance.

iii) The performance of Minutiae Based algorithm will always have a Good performance because it compares similar Minutiae points of the all the images which most of the times produce accurate result. Total time taken by the Minutiae Based Algorithm in greater than 3000 ms.

B. Performance of Pattern Based Algorithm

i) The performance of Pattern Based Algorithm is computed on the total amount of time taken by the algorithm to execute and produce the final result.

ii) The performance of pattern based in case of Pattern based algorithm, the pixels are compared of all the stored images with the image taken from the user using the fingerprint scanner device. In Pattern based algorithm the result will not always be accurate. Total time taken by the Pattern based algorithm in less than 1000 ms.

iii) Pattern based algorithm is much faster as compared to Minutiae based algorithm because it doesn't extract all the features of a fingerprint but rather counts total number of pixels present in a fingerprint image. This algorithm is not recommended as it's not accurate and might produce false match resulting in user authentication.

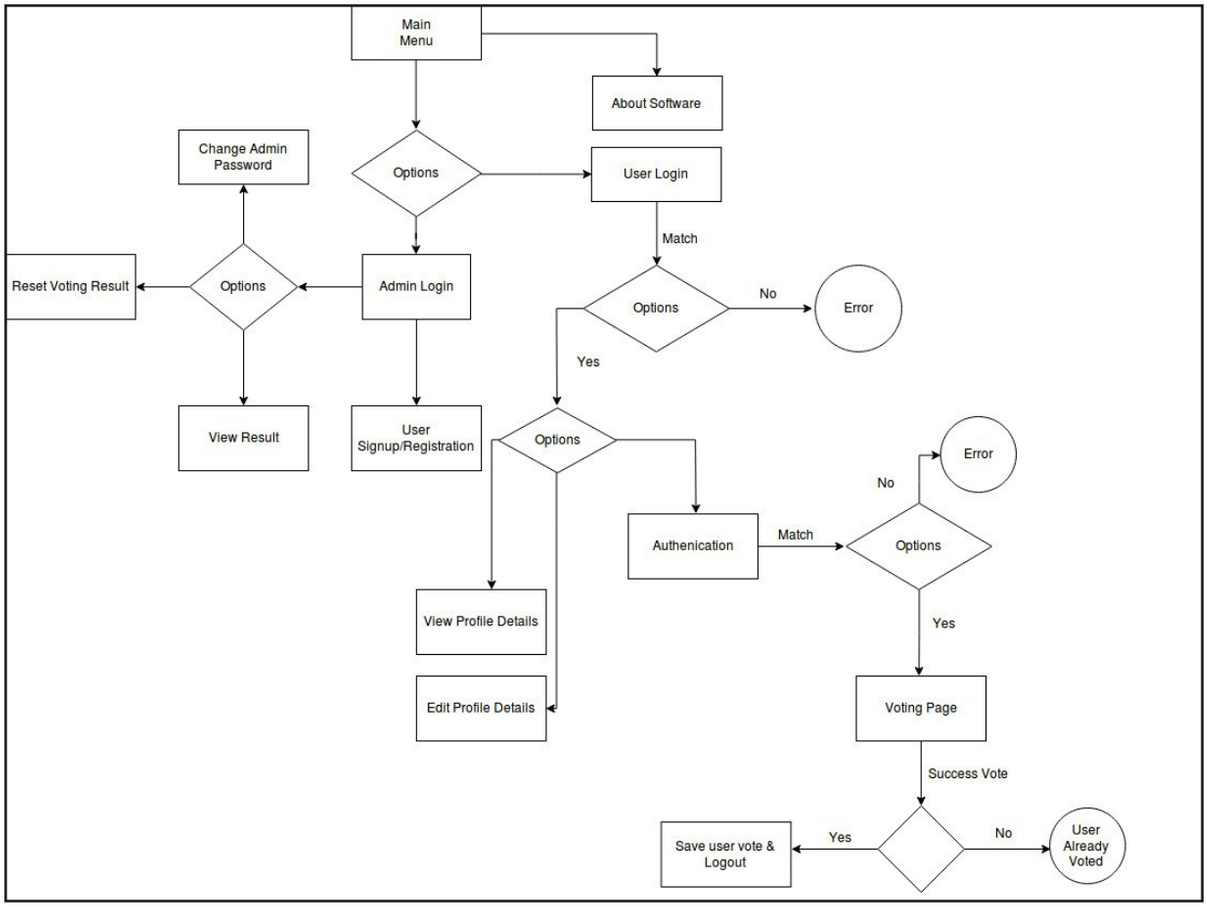

Fig. 5: Flowchart

VII. Conclusion

The biometric based election procedure looks promising and will ensure that there will be efficient, secure, and fast election procedure. The pattern based algorithm is useful when the quality of the scanner or the quality of fingerprint is low, but it is also seen that this method is generally flawed as it accepts even a photocopy of fingerprint and gives a match. It is also noted that pattern based requires more memory as it has to store the entire fingerprint [6]. The minutiae based approach ensures high security, and also is seen to be memory efficient. Although it requires quite an amount of preprocessing, it is very secure and cannot be faked or duplicated.

References

[1] M. Kaur, M. Singh, A. Girdhar, and P. S. Sandhu, "Fingerprint verification system using minutiae extraction technique," *World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering*, vol. 2, no. 10, pp. 3405-3410, 2008.

[2] S. Narwal, and D. Kaur, "Comparison between minutiae based and pattern based algorithm of fingerprint image," *International Journal of Information Engineering and Electronic Business*, vol. 8, no. 2, pp. 23-29, 2016.

[3] M. U. Munir, and M. Y. Javed, "Fingerprint matching using gabor filters," *National Conferences on Emerging Technologies*, pp. 147-151, 2014.

[4] A. K. Jain, Y. Chen, and M. Demirkus, "Pores and ridges: High-resolution fingerprint matching using level 3 features," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 29, pp. 15-27, 2007.

[5] K. Mali, S. Bhattacharya, and S. Chakraborti, "Revolutionary Extended Spatial Point Extraction Using Circular Technique (RESPECT)," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 5, no. 7, pp. 672-677, 2013.

[6] A. Ackerman, and R. Ostrovsky, "Fingerprint recognition," UCLA Computer Science Department, 2012.