A Comparative Study on Fingerprint Matching Algorithms for EVM

D. Ashok Kumar, T. Ummal Sariba Begum[*]

Department of Computer Science, Government Arts College, Trichy, India
*Corresponding author: tummalsariba@gmail.com

Abstract In biometric system, the fingerprint recognition has been researched for the long period of time and it has shown the most promising future in the real world application. However, because of the complex distortions among the different impression of the same finger in real life, fingerprint recognition is still a challenging problem. Matching two fingerprints can be unsuccessful due to various reasons and also depends upon the method that is being used for matching. Electronic Voting Machine (EVM) is a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system. Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token or knowledge based methods. In this paper, the authors are interested to compare three fingerprint matching algorithms by conducting the election using novel EVM. Based on the election result in terms of matching accuracy, time taken for matching, the best algorithm is found for novel EVM. The three matching techniques are direct matching, minutiae matching and matching based on Ratios of distance. We conducted the evaluation on the FVC-2000 datasets and the results were observed by conducting election with the help of these matching techniques and the best matching technique is found for novel EVM.

1. Introduction

Fingerprint recognition has been widely used in both forensic and civilian applications. Compared with other biometrics features, fingerprint-based biometrics is the most proven technique and has the largest market shares. In terms of applications, there are two kinds of fingerprint recognition systems: verification and identification.

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. The endpoints and crossing points of ridges are called minutiae. The minutiae ending and bifurcation are shown in the Figure 1. A ridge ending is defined as the ridge point where a ridge ends abruptly. A bifurcation is defined as the ridge point where a ridge bifurcates into two ridges. It is a widely accepted assumption that the minutiae pattern of each finger is unique and does not change during one's life. When human fingerprint experts determine if two fingerprints are from the same finger, the matching degree between two minutiae pattern is one of the most important factors. Thanks to the similarity to the way of human fingerprint experts and compactness of templates, the minutiae-based matching method is the most widely studied matching method. The algorithms which are compared in this paper belong to the minutiae-based matching method.

A fingerprint recognition system operates either in verification mode or in identification mode. In verification, the input is a query fingerprint and an identity (ID). The system verifies whether the ID is consistent with the fingerprint. The output is an answer of yes or no. In identification, the input is only a query fingerprint and the system tries to answer the question: Are there any fingerprints in the database that resemble the query fingerprint? The output is a short list of fingerprints. In this paper, we are dealing with the verification problem. Although fingerprint recognition has been studied for many years and much progress has been made, the performance of even state-of-the-art matchers is still much lower than the expectations of people and theory estimation [1]. Therefore, much effort is still needed to improve both the performance and the speed of fingerprint recognition systems. The matching algorithm plays a key role in a fingerprint recognition system.
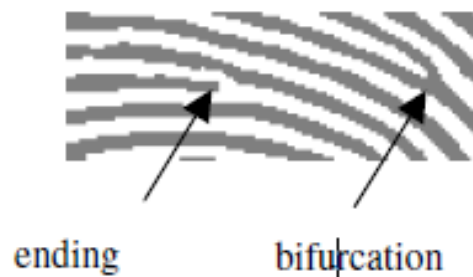

Figure 1. Minutiae Ending and Bifurcation

Voting is a method for a group such as a meeting or an electorate to make a decision or express an opinion—often following discussions, debates, or election campaigns. It is often found in democracies and republics. Electronic

voting (also known as e-voting) is a term encompassing several different types of voting, embracing both electronic means of casting a vote and electronic means of counting votes. A Study on enhanced fingerprint based electronic voting using minutiae is creates a user interface that use as a new alternative for paper-based ballot. Enhanced fingerprint also use to provide secure environment during election process as only authorized users with fingerprint recognition are available to vote. So, the purpose of this study is to improve the existing campus election process.

This paper is organized as follows: The next section II describes the Related Work and Contribution, Section III states the Fingerprint Matching Algorithm, Section IV describes the Electronic Voting Systems based on best fingerprint matching, Section V describes the Experimental Results and discussions and Section VI concludes the Present work and states the future work.

Generally, fingerprint-matching algorithms have two steps: (1) align the fingerprints and (2) find the correspondences between two fingerprints. The approach proposed by Jain et al. [2] is capable of compensating for some of the nonlinear deformations and finding the correspondences. However, since the ridges associated with the minutiae are used to estimate the alignment parameters, the size of the templates has to be large, which takes much memory and computation, otherwise, the alignment will be inaccurate. Jiang and Yau [3] use the local and global structures of minutiae in their approach. The local structure of a minutia describes a rotation and translation invariant feature of the minutia in its neighborhood, and the global structure tries to determine the uniqueness of a fingerprint. The problem with this technique is that it cannot compensate for real world distortions of a 3D elastic finger. These distortions can be considered equivalent to a space variant scale distortion. Furthermore, the weight vector that is associated with each component of the feature vector, such as distances, directions, relative local orientations, etc., has to be empirically determined. Another prominent matching algorithm, which is proposed by Kovacs-Vajna [4], uses triangular matching to deal with the deformations of fingerprints. However, the final results of matching have to be validated by a dynamic time warping (DTW) algorithm. Without DTW for further verification, the results are not acceptable.

Besides minutiae, researchers have also used other features for fingerprint matching. Saleh and Adhami [5] proposed an approach which transforms fingerprint images into a sequence of points in the angle-curvature domain. The matching between a query fingerprint and a template fingerprint is based on the least-squares error of the Euclidean distance between corresponding points in the angle-curve domain. Jain et al. [6] presented a filter-based algorithm, which uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length FingerCode. The authors reported that the FingerCode-based system performs better than a state-of-the-art minutiae-based system when the performance requirement of the application system does not demand a very low false acceptance rate.

The combinations of different kinds of features have also been used in fingerprint matching. Jain et al. [7] presented a hybrid-matching algorithm that uses both minutiae and texture information. Ceguerra and Koprinska [8] proposed an approach that uses matched minutiae as the reference axis to generate a shape signature for each fingerprint. The shape signature is then used to form a feature vector describing the fingerprint. A linear vector quantizer (LVQ) neural network is trained using the feature vectors to match fingerprints. Both approaches reported improvements in the matching results. Xuejun et al [9] propose a fingerprint-matching approach based on genetic algorithms (GA), which tries to find the optimal transformation between two different fingerprints. In order to deal with low-quality fingerprint images, which introduce significant occlusion and clutter of minutiae features, we design a fitness function based on the local properties of each triplet of minutiae. Germain et.al.,[10] propose the Flash algorithm uses a higher dimensional indexing scheme than geometric hashing by adding invariant properties of the feature subset to the index. Scalar properties such as color might be appropriate in some vision applications, while in fingerprint recognition the relationship of the chosen subset of features to the local ridge pattern provides additional distinguishing power. The second stage of the Flash algorithm uses transformation parameter clustering to accumulate evidence.

A few graph based algorithms [11,12,13] do matching by performing operations based on graph principles. The algorithm [14] proposed by Nalini K Ratha et all creates two Minutiae Adjacency Graphs, one each for the base and the input image, in which the vertices of the graph represent minutiae from the matched minutiae set. Point Pattern Matching problems [15,16] are also used in fingerprint matching though they are computationally expensive. [17] proposes a solution to fingerprint matching by incorporating ideas associated with point pattern matching problem. Werner Olz and Walter Kropatsch proposed an algorithm [18] that brings the entire ridge topology into consideration. Each ridge is assigned a symbol based on their kind, which includes a ridge ending, ridge bifurcation etc… These symbols are considered to be nodes/vertices of a graph, and two such graphs that are drawn from the entire ridge topology of the base and the input image is compared to arrive at a result. In [19], a new term called K-plet is introduced, which may either refer to 'K' nearest neighbors of a minutia or all neighbors within a circular radius etc… An adjacency graph is drawn for each of the K-plets and then the CBFS(Coupled Breadth First Search) algorithm is used to traverse through the nodes of the graphs to produce a matching score.

Sanjay kumar et al., [20] analyze the various electronic voting used across the country.There has been several studies on using computer technologies to improve elections [11,21,22,23,24]. These studies caution against the risks of moving too quickly to adopt electronic voting system, because of the software engineering challenges, insider threats, network vulnerabilities, and the challenges of auditing.

In this paper we compare three matching algorithm in order to use that for EVM. The matching algorithms are, Minutiae based matching, Direct matching, and Ratio of relational distance matching. In the direct matching technique the two fingerprints like template and query fingerprints are directly compared and the matching

results are observed. In minutiae based matching [25] the features called ridge ending and ridge bifurcation are extracted and stored along with the x axis, y axis and orientation. The same procedure is done for query image and the matching is done with the help of the features stored. Chandrasekaran et al., [26] present a fingerprint matching algorithm that initially identifies the candidate common unique (minutiae) points in both the base and the input images using ratios of relative distances as the comparing function. A tree like structure is then drawn connecting the common minutiae points from bottom up in both the base and the input images. Matching score is obtained by comparing the similarity of the two tree structures based on a threshold value. The proposed algorithm requires no explicit alignment of the two to-be compared fingerprint images and also tolerates distortions caused by spurious minutiae points. These three algorithms are compared and the best algorithms is found in terms of matching accuracy and time. This best algorithm is used for novel EVM.

2. Algorithms

In this paper, the authors are compared three fingerprint matching techniques which are discussed in this section.

2.1. Direct Matching

In this matching, the input and template images are read, the matching is performed by comparing the two images pixel wise.

2.2. Minutiae Based Matching

Let T and Q be the feature vectors, representing minutiae points, form the template and query fingerprint, respectively. Each element of these feature vectors is a minutiae point, which may be described by different attributes such as location, orientation, type, quality of the neighbourhood region, etc. The most common representation of a minutiae is the triplet x, y, θ where x, y is the minutiae location and θ is the minutiae angle. Let the number of minutiae in T and Q is m and n, respectively.

$$T = m_1, m_2, ..., m_m, \quad m_i = x_i, y_i, \theta_i, \ i = 1...m$$
$$Q = m'_1, m'_2, ..., m'_{ni} \quad m'_j = x'_j, y'_j, \theta'_j, \ j = 1...n \quad (1)$$

A minutiae m_i in T and m'_j in Q are considered matching, if following conditions are satisfied:

$$sd(m'_j, m_i) = \sqrt{\left(x'_j - x_i\right)^2 + \left(y'_j - y_i\right)^2} \le r_o$$
$$dd\left(m'_j, m_i\right) = \min\left(\left|\theta'_j - \theta_i\right|, 360 - \left|\theta'_j - \theta_i\right|\right) \le \theta_o \quad (2)$$

Here, r_0 and θ_0 are the parameters of the tolerance window which is required to compensate for errors in feature extraction and distortions caused due to skin plasticity. The number of "matching" minutiae points can be maximized, if a proper alignment (registration parameters) between query and template fingerprints can be found. Correctly aligning two fingerprints requires finding a complex geometrical transformation function (map ()), that maps the two minutiae set (Q and T) the

desirable characteristics of map () functions are: it should be tolerant distortion; it should recover rotation, translation and scale parameters correctly.

2.3. Ratio of Relational Distance Matching

The methodology is to obtain the common minutiae point set (minutiae points present in both the base and the input image). The prime purpose of this phase is to find the number of common minutiae points available in a pair of fingerprint images. Given two fingerprint images with 'N1' and 'N2' identified minutiae points respectively (where N1 need not be equal to N2), this phase outputs the 'M' common minutiae points, which would be available in both the images. Effectively, if N1 represents the set of minutiae points in image 1 and N2 represents the set of minutiae points in image 2, M would be the intersection of N1 and N2 (M = N1 ∩ N2). There is a new term called the 'M (i) – tuple' to represent information about a minutiae that would identify it uniquely among the set of all minutiae. The M (i) – tuples of a pair of minutiae can be compared/matched to find if they both are the same or not. When two images with identified minutiae points are given as input, the algorithm considers one image to be the base image (BM) and the other image to be the input image (IM). Either of them can be BM or IM and vice versa [26].

M(I) – Tuples in base image (BM):

For each minutiae i = 1 to N1, the 5 nearest minutiae points are found. This is done by calculating the Euclidean Distances from the 'i'th minutiae point to all the other minutiae points in the set N (BM) and noting down the 5 nearest minutiae points with respect to Euclidean Distances. If i1, i2, i3, i4 and i5 are the 5 nearest minutiae points of i, then we calculate M (i) – tuple in the following way: (a) Calculate distances i – i1, i – i2, i – i3, i – i4, and i – i5. Note that distance 'i – iN' means the Euclidean Distance between the points i and iN. So here, distance i – i1 means the Euclidean distance between minutiae point i and i1 and so on. (b) Find the following 10 ratios (i - i1): (i - i2), (i - i1): (i – i3), (i - i1): (i – i4), (i - i1): (i – i5) , (i – i2) : (i – i3), (i – i2) : (i –i4), (i – i2) : (i – i5), (i – i3) : (i – i4), (i – i3) : (i – i5), (i – i4) : (i – i5). Based on this procedure the algorithm finds the match between two fingerprint images.

3. Electronic Voting System

The main core of this section is to design a novel EVM based on the fingerprint minutiae feature and the best matching technique which found in the Section III.

3.1. Biometric Based Electronic Voting

Because biometric identifiers cannot be easily misplaced, forged, or shared, they are considered more reliable for person recognition than traditional token or knowledge based methods. The objectives of biometric recognition are user convenience (e.g., money withdrawal without ATM card or PIN), better security (e.g., difficult to forge access), and higher efficiency (e.g., lower overhead for computer password maintenance). The tremendous success of fingerprint based recognition technology in law enforcement applications, decreasing

cost of fingerprint sensing devices, increasing availability of inexpensive computing power, and growing identity fraud/theft have all ushered in an era of fingerprint-based person recognition applications in commercial, civilian, and financial domains. So the Electronic voting system has to be improved based on the current technologies viz, biometric system.

The Novel EVM is designed by two phases [25]. Enrollment and Voting. In the Enrollment Process, the fingerprint is captured with the help of the fingerprint scanner, and the captured image is enhanced with the techniques used in paper, once the image is enhanced the feature called minutiae (ending, bifurcation) are extracted with the help of the minutiae feature extraction technique and the extracted features are stored in the database for verification.

In the Verification process, the person who comes to cast a vote is registered his/her thumb impression in the controlling phase, once the image is captured it is enhanced and the feature is stored for future comparison. To check whether the voter is an authenticated voter, the input image is compared to the database. It is called authentication process. In case the print is not stored in the database, a single beep is given, so the person cannot vote or if the same person votes again, the system should give a double beep, so that the security can be alerted. If the image is found in the database then the person is allowed to vote in the balloting phase. In the balloting phase there is the number of fingerprint scanner with the symbols equallent to the number of nominees. The person allowed in the controlling phase may depict his/ her thumb impression in the corresponding scanner for whom they like to vote. Once it is captured, the identification process is carried between the controlling and balloting phase in order to identify that the person who crossed the verification process is the person who cast the vote. If there is no deadlock condition occur (i.e) Both the captured and query image is matched then their vote is recorded for a corresponding nominee.

4. Experimental Analysis

For our analysis, in the enrollment process, we stored 80 images with their minutiae features. A Pilot election is conducted with the help of the novel EVM. Each person is asked to vote for the candidates they wish by checking their identity through fingerprint and allowing them to vote by giving thumb impression against the fingerprint scanner of candidate. The Table 1 shows the analysis of the election for 80 voters in terms of time for all the three methods. The equalent chart is shown in the Figure 2.

Table 1. Analysis of the election for 80 voters

Methods	Time taken for casting a vote (Seconds)		Total Time Taken for Voting (Hr)	Local Movement Time Per Voter (sec)	Total Election Time (Hr)	Memory Required
	Identification (Control Unit)	Verification (Ballot Unit)				
Actual Image Matching	3.64054	4.120543	0.17246	30	0.8393	7.21 MB
Minutiae Feature matching	2.7815	3.5876	0.1415	30	0.8082	584 KB
Distance based Ratio Matching	3.1831	4.067	0.16112	30	0.8278	1.6 MB
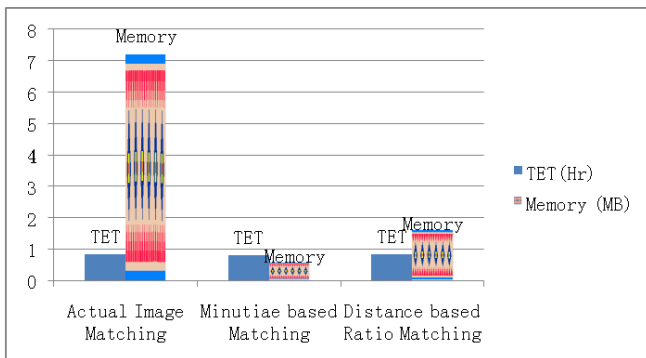
Figure 2. Analysis of the Election for 80 voters

The Figure 2 shows that the time taken for voting and memory required to store the features for control and ballot unit. That is the identification and the verification process. Compared to the all three methods the minutiae based matching has the lowest time with accuracy and less memory. Total election time by using the actual image matching is 83 mins, minutiae feature matching is 80 mins and distance based ratio matching is 82 mins. The memory needed to store the fingerprint features for actual image and raito matching is in MB various the memory required to store the minutiae feature is in KB.

From the results the minutiae based matching is best suited for voting in terms of time and memory. The next priority for matching is ratio matching. The FVC 2000 database is simulated into 500 images and with the help of this database the voting is conducted. That simulated database voting is analyzed in the Table 2. The Equivalent Chart is shown in the Figure 3.

Table 2. Analysis of the election for 500 voters

| Methods	Time taken for casting a vote (Seconds)		Total Time Taken for Voting (Hr)	Local Movement Time Per Voter (sec)	Total Election Time (Hr)	Memory Required
	Identification (Control Unit)	Verification (Ballot Unit)				
Actual Image Matching	51.453	54.568	14.725	30	18.892	45.06 MB
Minutiae Feature matching	22.753	25.753	6.737	30	10.904	3650 KB
Distance based Ratio Matching	24.135	27.812	7.213	30	11.38	10MB
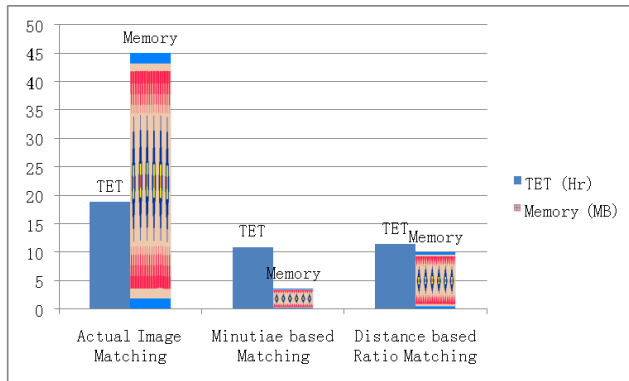
Figure 3. Analysis of the election for 500 voters

From the Figure 3, we conclude that the minutiae based matching is best to compare the other 2 methods in terms of memory and time. The Total election time (TET) is calculated with the help of the following formula,

$$TET = \big((N * MT)/3600 + TTV\big) \quad (3)$$

Where N is the Number of Voters, MT is the Movement Time per voter and TTV is the Total time taken for voting.

In actual image matching the total election time to complete the election for 500 voters is 18 hours, In minutiae based matching the total election time is 10 hours and in distance based matching the total election time for 500 voters is 11 hours. Hence, the minutiae based matching may improve the time as well as it is a secure one. If we reduce the movement time and apply some clustering techniques then we could conduct the election within a day for more than 1000 voters.

5. Conclusion

For over a decade, fingerprints have been one of the most highly used methods for person recognition. Automated biometric systems have only been available in recent years. This work is successfully implemented a PC based electronic voting system under Matlab 7.5. They arrived results were significant and more comparable. It proves the fact that the fingerprint image enhancement step will certainly improves the verification performance of the fingerprint based recognition system. The report of the pilot study for an election showed better accuracy. In this PC based voting verification, the best matching algorithm is found in a secure way in terms of time and memory. Since the fingerprints have broad acceptance with the general public, law enforcement and the forensic science community, they will continue to be used with many governments legacy systems and will be utilized in new systems for evolving applications that require a reliable biometric. So, in short future, we will design a device with Biometric Technology which can be used as if Indian Electronic Voting Machine.

Acknowledgment

References

[1] Pankanti S., Prabhakar S., Jain A.K., On the individuality of fingerprints, IEEE Trans. Patter Anal. Mach. Intell. 24 (8) pp: 1010-1025, 2002.

[2] Jain A.K., Hong L., Pankanti S., Bolle R., An identity-authentication system using fingerprints, Proc. IEEE 85 (9) pp: 1364-1388, 1997.

[3] Jiang X., Yau W.Y., Fingerprint minutiae matching based on the local and global structures, Proceedings of the International Conference on Pattern Recognition, pp. 1038-1041, 2000.

[4] Kovacs-Vajna Z.M., A fingerprint verification system based on triangular matching and dynamic time warping, IEEE Trans. Pattern Anal. Mach. Intel. 22 (11):1266-1276, 2000.

[5] Saleh A.A., Adhami R.R., Curvature-based matching approach for automatic fingerprint identification, Proceedings of the Southeastern Symposium on System Theory, pp. 171-175, 2001.

[6] Jain A.K., Prabhakar S., Hong L., Pankanti S., Filterbank-based fingerprint matching, IEEE Trans. Image Process. 9 (5): 846-859, 2000.

[7] Jain A.K., Ross A., Prabhakar S., Fingerprint matching using minutiae and texture features, Proceedings of the International Conference on Image Processing, vol. 3, pp. 282-285, 2001.

[8] Ceguerra A.V., Koprinska I., Integrating local and global features in automatic fingerprint verification, Proceedings of the International Conference on Pattern Recognition, vol. 3, pp. 347-350, 2002.

[9] Xuejun Tan, Bir Bhanu, "Fingerprint matching by genetic, algorithms, Pattern Recognition Society. Published by Elsevier Ltd, 39 pp: 465-477, 2006.

[10] Robert S. Germain, Andrea Califano, And Scott Colville, "Fingerprint Matching Using Transformation Parameter Clustering", theme article, IEEE Computational Science & Engineering, 1997.

[11] Gold S. and Rangarajan A., "A graduated assignment algorithm for graph matching," IEEE Transactions on Pattern Analysis and Machine Intelligence., vol. 18, no.4, pp.377-388, 1996.

[12] Hrechak A.K. and Mchugh J.A., "Automated Fingerprint Recognition using Structural Matching," Pattern Recognition, vol. 23, pp. 893-904, 1990.

[13] Eshera M. and Fu K.S., "A Similarity Measure between Attributed Relational Graphs for Image Analysis," in Proceedings of the 7th International Conference on PatternRecognition, Montreal, P.Q., Canada, July 30-Aug 3 1984.

[14] Ratha N.K, Pundit V.D, Bolle R.M, Vaish V., "Robust Fingerprint Authentication Using Local Structural Similarity," Workshop on Applications of Computer Vision, pp: 29-34, 2000.

[15] Ranade A. and Rosenfeld A., "Point Pattern Matching byRelaxation," Pattern Recog., vol, no: 12, 2; pp: 269-275, 1993.

[16] Ton J. and Jain A.K., "Registering landsat images bypoint matching," IEEE Transactions on GeoSci. RemoteSensing, vol.27, pp. 642-651, May 1989.

[17] Jain A.K., Hong L., Pankanti S. and Bolle R., "An identity authentication system using fingerprints," Proc. IEEE,vol.85, pp. 1365-1388, Sept.1997.

[18] Ölz W. and Kropatsch W.G., "Graph Representation of Fingerprint Topology," Computer Vision - CVWW'04, Slovenien Pattern Recognition Society, pp. 51-58, 2004.

[19] Chikkerur S., Cartwright A. N. and Govindaraju V., "Kplet and CBFS: A Graph based Fingerprint Representation and Matching Algorithm," ICB 2006.

[20] Sanjay Kumar, Ekta Waliam., "Analysis of Electronic Voting System in Various Countries", International Journal on Computer Science and Engineering (IJCSE)", ISSN: 0975-3397 Vol. 3 No. 5 May 2011.

[21] Meltemp Ballan, Ayhan Sakarya F. and Brian L. Evans, "A Fingerprint Classification Technique Using Directional Images", 1997..

[22] Mercuri R.. "Electronic Vote Tabulation Checks and balances", PhD thesis, University of Pennsylvania, Philadelphia, PA, Oct.2000.

[23] "Ridges and Furrows-history and science of fingerprint identification technology and legal issues". http://ridgeand.furrows.homestead.com/fingerprint.html

[24] "Voting: What Is; What Could Be", MIT Voting Technology Project, July 2001.

[25] Ashok Kumar D., Ummal Sariba Begum T., "A Novel design of Electronic Voting System Using Fingerprint", International Journal Of Innovative Technology & Creative Ngineering Vol.1 No.1, pp:12-19, January 2011.

[26] Abinandhan Chandrasekaran, 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.