

An Observed Voting System Based On Biometric Technique

B. Devikiruba

ABSTRACT: This article describes a computational framework, which can run almost on every computer connected to an IP based network, to study biometric techniques. This paper discusses with a system protecting confidential information, puts strong security demands on the identification. Biometry provides us with a user-friendly method for this identification and is becoming a competitor for current identification mechanisms. The experimentation section focuses on biometric verification, specifically based on fingerprints. This article should be read as a warning to those thinking of using methods of identification without first examine the technical opportunities for compromising mechanisms and the associated legal consequences. The development is based on the java language that easily improves software packages that is useful to test new control techniques.

INDEX TERMS: Fingerprint sequence, auto-confirm algorithms, mifaun techniques, Kerberos technique and probabilistic match

I-INTRODUCTION

This article turned their attention to the development of voting system due to several reasons. Currently, there are over 10 different techniques to identify a person based on biometric: Identification system based on biometric[15] are capable of identifying persons on the basis of either physical or behavioral characteristics.

BEHAVIORAL CHARACTERISTICS:

Keystrokes dynamics, voice recognition, and signature dynamics.

PHYSICAL CHARACTERISTICS:

Iris recognition, retina recognition, vein pattern recognition, recognition of hand or finger geometry, finger recognition. Main draws of the fingerprint recognition[11] while identifying the particular persons is by means of counterfeiting fingerprints. They are as follows: duplication with co-operation, duplication without co-operation. The resolution for this problem is that before a system is able to verify the specific biometric of a person, it requires something to compare with it. Therefore a profile containing the biometric properties is stored in the system recording the characteristics of a person is called enrollment. Storing profiles in tokens requires a combination of tokens and biometric for verification and therefore gives a higher level of security. However, we need something more formal to analyze the voting system so modeled. Our work demonstrated that how well the citizen can be made the vote as easy as possible. Environmental modeling, perception and mapping are all needed for a successful approach. In this paper, we use java as user friendly as it's a web enabled language.

II-SERVER SIDE

The election offices have to prepare the voter id for all the citizens. For this procedure, the citizen have to show their name and address identity proof. According to the proof given by the citizen, the voter id is to be prepared. Here

we use the Kerberos technique[1] for creating voter id card is as follows,

- a) Request for getting voter ID card from election office.
- b) Request to store signature as he/she is the citizen for the particular voter ID.
- c) Request to store the symbol that would be proceeded by the right candidate.

- a) Request for getting voter ID card from election office.
 - I. $C \in AS : Name \parallel Address \text{ proof}C \parallel TS1$
 - II. $AS \in C : EKC[KC, TgsVoterID \parallel IDC \parallel TS2 \parallel Lifetime1 \parallel VoterIDTicket]$

TS1- allows AS to verify that client's clock is synchronized with AS. TS2- inform client of time this ticket was issued. Lifetime1- inform client of the lifetime of the ticket. Voter ID- ticket to be used by client to access Tgs. EKC- The encryption key is based on user's password enabling AS and client to verify password and protecting content of message.

- b) Request to store signature as he/she is the citizen for the particular voter ID.

- I. $Tgs \in AS : EKC[Name \parallel Address \text{ Proof}C \parallel Voter \text{ ID}]$
- II. $AS \in DB : Match \parallel TgsC$ III. $AS \in Tgs : DBAS \parallel TgsC \parallel fingerprint \text{ sensor}$
- IV. $Tgs \in AS : EKC[fingerprint \text{ sensor} \parallel fingerprint \parallel KC, TgsC \parallel DB]$

These are all the procedures, to be followed before the election is to be conducted.

- c) Request to store the symbol that would be preceded by the right candidate.

- I. $C \in Voter \text{ Machine} : Voter \text{ ID} \parallel fingerprint \parallel Lifetime2$
- II. $Voter \text{ Machine} \in C : Match[Voter-IDC \parallel fingerprint]db \parallel [Voter_IDC \parallel fingerprint] \parallel Lifetime2$
- III. $C \in Voter_Machinedb : press \text{ symbol} \parallel Lifetime2$

• B.Devikiruba,
E mail ID: dkiruba3@gmail.com

IV. Voter_Machine € C : ACK || Lifetime2 || ACH//ACH – Automatic Clearing House

If there are N more systems, then there must be N(N-1)/2 secure key exchanges so that each Kerberos realm can interoperate with all other Kerberos realms[1]. This is the procedure, to be followed at the time of the election. There is no need for the election officers to know the voter ID/Name of the citizen at the time of election. At the time, the server show only the symbol and T/D voted by the citizen from anywhere in the country. The voter ID is encrypted by using hill cipher technique. In this technique, the encryption algorithm [1, 7] takes m successive plaintext letters and substitutes m cipher text. The substitution is determined by m linear equation in each character is assigned a numerical value(a=0,b=1..., z=25). For example, consider m=3, expressed in row and column matrices

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$\begin{pmatrix} C1 \\ C2 \\ C3 \end{pmatrix} = \begin{pmatrix} K11 & K12 & K13 \\ K21 & K22 & K23 \\ K31 & K32 & K33 \end{pmatrix} \begin{pmatrix} P1 \\ P2 \\ P3 \end{pmatrix} \pmod{26}$$

$$C = EK(P) = KP \pmod{26}$$

The voter ID for the citizen is given as TNDEV1122. The first two letters will determine the “state” to which he/she belong. The next four letters will determine the “1st four letters of the person” and then the next three letters will be the “ID” given to the person by the election officers. For getting the cipher text, we will take 1st three letters as such

$$\begin{aligned} C &= \langle 19 \ 13 \ 3 \rangle \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \pmod{26} \\ &= \langle 559 \ 696 \ 121 \rangle \pmod{26} \\ &= 13 \ 20 \ 17 \\ &= \text{NUR} \end{aligned}$$

As like as when we proceeded, the cipher text for the next three letters will be YFD. For getting the cipher text[1], we use the Key, K and K⁻¹ as

The numeric identifier is also be converted to cipher text as C E E.

$$P = DK(C) = K^{-1}(C) \pmod{26} \quad K^{-1}KP = P$$

None will be able to determine the voter ID of the citizen at the time of election. None will be able to change the vote ID, when the citizen gets the voter ID and sensor reads the signature(fingerprint) both would be locked. Any malicious attacker made any change it will automatically gets destroyed. Algorithm sample for the procedure as,C as citizen, E as election office;

```

if(Name & Address proof in db == Match)
    Send("voter IDTgs")

do read("fingerprint of C")
save("fingerprint")

lock("voter IDC & fingerprintdb)
while(voter ID == (Name &
Addressproof)db)

if((fingerprint | voter IDTgsdb)=
=(rewrite)voter ID)

destroy("voter ID && fingerprint of CTgs
in db")
    
```

Only the pattern matching is proceeded for the voterID and fingerprint at the time of election.

III-DATABASE

The hash keeper database is used for maintaining and updating the data. It is maintained by US National AFIS system[14], as for the purpose of fingerprint identification. The identification of fingerprint from the database is a repository of fingerprint of “known to be good” and “known to be bad” computer files for use in law enforcement applications. Here we use the Rabin’s fingerprint scheme [8] is a method for implementing public key as fingerprint

using polynomials over a finite fields. The sample database for the relation1, 2 and 3 are as shown:

Relation1:

RELATION1		
Voter ID	NAME	ADDRESS
TNDEVI122	DEVIKIRUBA	DPM
TNPRAB012	PRABHURAJ	DPM
JKSACH111	SACHIN	KASHMIR
APGANG011	GANGULY	HYDERABAD

Table 1: Shows the relation of voter ID, name and address

Name, Address and voter ID of the citizen are intersected by the relation1, it can be defined in terms of the probability as such

$$P(\text{voter ID} \cup \text{Address} \cup \text{Name}) \in P(\text{KEY})$$

Relation2:





RELATION2	
voter ID	FINGERPRINT
TNDEVI122	
TNPRAB012	
JKSACH111	
APGANG011	

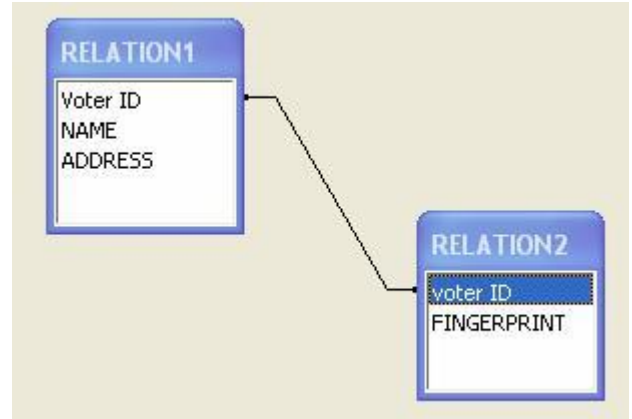
Table2: Shows the relation of voterID and fingerprint

Here fingerprint is the primary key in relation2. It can be determined in probabilistic manner[4] as

$$P(\text{Fingerprint}) \in P(\text{KEY})$$

$$P(\text{voter ID} \cup \text{Fingerprint}) \in P(\text{KEY})$$

The relation1 & relation2 can be intersected by the join operation. The election offices can check the database at some other time, but not to be allowed to change the details.



At the time of election, the voting machine performs the checking whether the candidate is right one. The time and date [T/D] is also one of the component of voting machine. It can only perform checking, when it will be connected to the relation3.

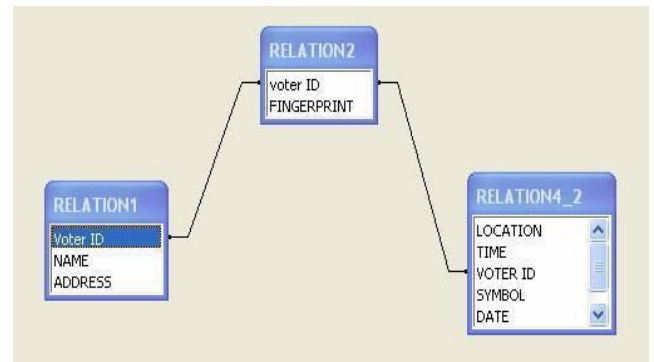


Fig2: Shows the relation between relation1, relation2 and relation3

The time and date [T/D] can be updated automatically when the symbol is pressed by each candidate. The place where the citizen puts the vote can also be stored in the database. When the different symbol is entered by each candidate, the total for each symbol is automatically get incremented in the database[6]. It would be an easy job for the election offices to calculate the total ratio of the symbol for those holding parties. These are the details to known only to the election officers at the time of election.

Fig1: Shows the relation between relation1 and relation2

RELATION3					
LOCATI	VOTER	SYMBO	DATE	TIM	TOT




ON	ID	L	E	AL
MUMBAI	TNDEV1122		20/10/10 10.3 5	120
HYDERABAD	TNPRAB012		20/10/10 3.45	36
KASHMIR	APGANG011		20/10/10 2.00	150

Table3: Shows the total, location and the symbol voted.

The fingerprint can be only identified in a secure when we use Rabin's fingerprint algorithms, and so it is stored in hash keeper database. For any event, P (voter_ID>0) according to probabilistic approach. (i.e.) the probability of every event is non-negative. Proof: according to axiomatic approach of probability.

Axiom I:

We have given the idea that the chance of event A occurring should be at least zero, so that negative probability are not allowed. The information available here is to establish the primary key that would satisfy both the relations 1& 2.

$$P(\text{fingerprint U voter ID}) \in P(\text{key matching})$$

When we obtain this probability, matching can be successfully verified and so the intersecting the fingerprint and voter ID would be perfect key pair for identifying the candidate.

IV- STRING MATCHING

To introduce the problem of string matching[7], let us consider that the first string has been extended from current location. When the candidate shows his/her finger toward the sensor, the second string has been extracted from the database. According to the Merkle-Damgard Construction, the whole data(string) is to break the input into sequence of small units(bits, bytes, words etc) and combine all the units b[1],b[2]...b[m] of the sequential manner. As like as creating the cipher text for each of voter ID. Now we get confused in determining what type of sequence to be used to determine the perfect match with high confidence? Some more time we attain the level of k-mismatches. In such a cases, matching[9] can be obtained by calculating length of the string and then comparing the string in the database. String1: TNDEV1122 String2 from db: TNDEV1122. While performing the computations mathematically,

String1: $a(t)=x1+....+xn$ **String2:** $a1(t)=y1+....+yi+n-1$
where $xi, yi=\{0,1\}$

Let us do the string length calculation as, $S \in S0$ //Initializing the string

For[S in 0....n] **do** $S \in F[S, b[k]]$ **return**[S, n]

```
while[F[S, b[k]] = F[S, b[k]]db] //comparing the string
in bit by bit manner if[b[k] = '\0' && b[k]db = '\0']
equal else not equal
```

Furthermore the standard algorithms[7] are quite sensitive to calculate the length and comparing the string, which cause to reduce the problem of mis-matching. The algorithm is relatively fast that works in O(n) times on average. When step1 of the process is not succeeded, it stops the procedure further goes to the next step.

For example:

```
String2db:TNDEV1122234
String1sensor:TNDEV1122 //Null characters
```

We describe our sequence matching algorithm considering the length as String2db=12 and String1sensor=9, in the step1 of the process. We obtain the mis-match and so no need for the process to move to the next step of the process.

V -FINGERPRINT RECOGNITION:

Fingerprint is a two-dimensional pattern ridges[10] on a human fingerprint. Such a ridges are believed to form in the embryo and to persist unchanged through life. Fingerprint technologies are based upon the characteristics of an individual's fingerprint which is considered highly distinctive and unique. Matching can be proceeded in two ways as such,

IDENTIFICATION:

(1: n, 1: many matching) of an individual using fingerprints is usually done by matching with database. AFIS is the most mature of all biometric systems with the most implemented use and has through its own major advancements in terms of reliability and integrity.

VERIFICATION:

(1:1matching)is accomplished using system which are referred to as fingerprint recognition systems. This technology is widely used for access control applications.

FINGERPRINT PROPERTIES:

VIRTUAL UNIQUENESS - The probability of collision-two files yields the same fingerprint –must be too small, when compared to the probability of other unavoidable causes of fatal errors: say 10-2 or less. This requirement is somewhat similar to that of a checksum function, but is much more strict. To detect accidenta data corruption or transmission errors, if is sufficient that the checksums of the original file and any corrupted version will differ with near certainty, given some statical model for the errors. Fingerprint need to be at least 64-bit[11] long to generate virtual uniqueness in large file systems.

COMPOUNDING - A fingerprint algorithm allows the fingerprint of a composite file to be computed from the fingerprints of its constituent parts. This “compounding” property may be useful in some applications such as detecting when a program is to be recompiled.

VI -AUTO-CONFIRM ALGORITHM

Fingerprint matching algorithms vary in forms of false positive and false negative error rates. The accuracy of the algorithms, print matching speed, and robustness to poor images are the critical elements of the system performance, while software are used to attain matching speed and throughput. Here we use light-out/auto-confirm algorithms that produce identified or non-identified responses. In any case, the search systems return results with some numerical measure of the probability[3] of a match (a “score”). This type of techniques is most widely used in forensic systems.

VII -FINGERPRINT PATTERN MATCHING

Pattern based algorithms compare fingerprint pattern between previously stored template and candidate fingerprint. Image is aligned in same orientation. The template of the fingerprint contains type, size and orientation. Those three features are compared with original fingerprint to determine at which degree of polynomial they match. The template of fingerprint[15] contains arch, loop and whorl. Line scan is digitally processed to create a biometric template which is stored and used for matching. Most of the fingerprint algorithms avoid the comparisons and transmission of bulky data. When the fingerprint is captured by the sensors, pattern matching is to be performed with the fingerprint in database. Assume captured fingerprint is taken to be f1 and it is in the orientation of 45. this fingerprint has some features as that of the already stored fingerprint as ridge, core and delta. The fingerprint in database is at the orientation of 60.The orientation itself is not a problem. It will compare both the fingerprint without considering the orientation. In fingerprint, it first comes ridge, next core and then the delta. The length and size of the ridge, core and delta only be changed. So there is need to compare the length and size.

S€ridge, t€core, d€delta //declaration S€S0, C€Cn, d€dn //initializing For[t in C0....Cn] then do

S€F[S,t] Return G[S,n]

For[d in d0....dn] then do S€F[[S,t],d]

Return G[[S,n],N]

VIII -PARAMETER ESTIMATION

The fingerprints stored in the database[6] are estimated as length in terms of arcs, loop, whorl and tented arch. Examining thumbprint by width and height. All length are in mm,

For example,

The estimated length in parameter range

ARCH	RANGE
x _y	4,2,2,8
h	4,0,5
b	2,5
LOOP	RANGE
x _y	2,7,2,8
r	4,5,8
TENTED ARCH	RANGE
x _y	5,4,2,8
h	4,0,5
WHORL	RANGE
x _L ,y _L	2,7,4,1
x _C ,y _C	5,4,1,2,2

The mean of the whole fingerprint (i.e.) mean number of minutiae is to be taken as =50±10.

IX- MODEL ANALYSES AND TESTING

The fingerprint patterns are distributed independently, the probability that two points match[5] is $P_c^2(x)$. Let the probability that a print has a configuration x be $PC(x)$. We restrict each parameter to a region of parameter space in which we expect to find it and assume it is uniformly distributed there. This approximation is enough to estimate order of magnitude[3], which suffices for our analysis. The study of tests of significance which enables us to decide on the basis of sample results if

- i) The deviation between the observed sample statistic and the hypothetical parameter value is significant.
- ii) The deviation between samples statistics is insignificant.

The study is to draw the valid inferences about the population parameters on the basis of the samples results. We decide to accept or to reject the after examine a sample from it.

I)Accept II)Reject

a and b are sizes of type I and type II. a

=P(Reject)

$p=P(\text{Accept})$

Here by we use the probabilistic[5] T test to test the significance between two means of the statistic.

$$t = \frac{x_1 - x_2}{\sqrt{s^2 \left(\frac{1}{n_1} + \frac{1}{n_2} \right)}}$$

The value of S can be estimated as $s^2 = \frac{\sum(x_1 - \bar{x}_1)^2 + \sum(x_2 - \bar{x}_2)^2}{[n_1 + n_2 - 2]}$ Where s_1, s_2 are sample standard deviation. Degree of freedom = $n_1 + n_2 - 2$. Let us consider sample I as fingerprint of the user view and sample II as fingerprint db.

For example,

While estimating these samples, we get

NULL HYPOTHESIS H0 :

Both have the same mean.

ALTERNATIVE HYPOTHESIS H1 :

$$\mu_1 > \mu_2 \quad (\mu_1 \neq \mu_2)$$

We get the tabulated value t for 14d.f at 5% level = 1.76

Here we obtain calculated $t <$ tabulated t. Therefore we accept the null hypothesis (i.e) both are come from same fingerprint.

X -HISTORICAL UNIQUENESS OF FINGERPRINTS

Here we denote the probability[5] of a match of any two left thumbprints w_n , the history of the human race by P and the database contains whole countries fingerprint db as by N. the probability of atleast

one match among $\binom{N}{2}$ thumbprints is

$$P = 1 - (1 - P)^{\binom{N}{2}}$$

The probability that two thumbprints have the same overall ridge structure and so that the range we obtained through the probability as

$$P_1 = \frac{1}{\binom{100000000}{2}} = 0.00044$$

XI-SECURE TRANSMISSION

For secure transmission. We use technology called mifan. As mifaun[16] is the web-enabled biometric authenticator with complete control techniques that are built into the system that provides high level of security. In case of multiple units applications, we use master/client concepts. Master provides the web interfaces and manages all the client on the network. The web-enabled feature provides

facility to every citizen to vote at any location wherever he/she is. The master system are kept in all the election offices and so all these systems are connected to all the maters. The voter ID and the fingerprint data can be transferred through internet to the host processor for verification. This technology provides security while transferring. The data are already stored in host in the election office and so the process is made easy. This technology has some of the built in features as such: webserver, database server, iGuard.

VOTING MACHINE INTERFACING

An interface connects the voting machine and the election office. The interface taps the data from voting machine going to modem which in turn connects to the central network. The interface extracts the symbol from the other details going to the database. None of the person is able to know who vote the symbol at the time.

DATA CONNECTIONS

MODEM TAPS:

Usually one modem for each voting machine but sometimes there are modem sharing devices for multiple voting machine on one high speed modem line. Voting machine interfaces[2] are passive devices and do not interface with the data communications. When installing a tap on a modem, the machine must not be disconnected for too long.

TCP/IP LAN TAPS:

The popular method of connecting voting machine to the election office is via Ethernet LAN via TCP/IP. Election office has the high security and use VPN routers which communicate via one port only to the voting machine. Tapping such a type of connection is simplest.

DVRS

TIME DATE SEARCH:

Most DVRS used for voting machine surveillance. This will be beneficial when election officers needs to find the database. The alarming function is used in this type of DVRS to change record speed. Remote [2] or local election officials can search the DVR database and can recomputed the total symbols when question arises at the some other times.

VOTING MACHINE NETWORK

COMMUNICATION:

Voting machine communicates with the modem via RS232 type or Ethernet LAN connections. Modems are usually connected to dedicated leased telephones lines back to the network hub. Most of the voting machine and network communicate using a poll selection technique[2]. The host polls or asks each voter machine in sequence if it has any data to send or tells a certain machine the host has data to send. If the voter machine selects the host in response to a poll then the machine transmits the data to the host. This is continuously repeated allowing multiple voting machine to share the same network.

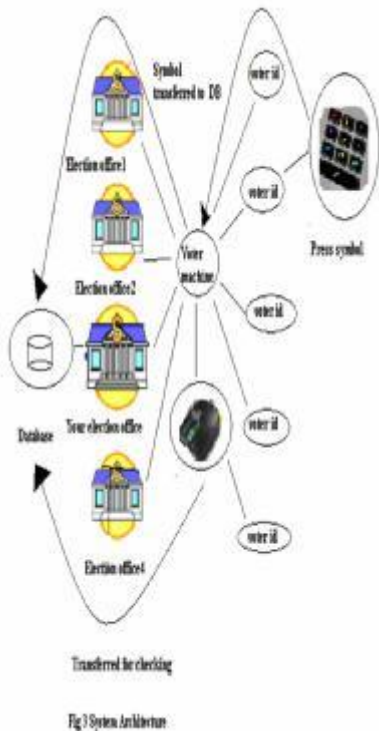
LAN NETWORKS:

The trend in communication is Local Area Network (LAN). These communications are usually high speed serial communications. Some of the data may vary radically and so the radiations are reduced by using the technique HDLC. We use three frames of the HDLC[2], for the transferring data, securing and controlling the data in the timely manner.

Ethernet – 10Mbps/100Mbps and 1000Mbps Gigabit.

PC Baseband LAN 1Mb.

XII-SYSTEM ARCHITECTURE



When a citizen has voter ID, wants to vote. Then the particular person has to provide the necessary information by means of voter ID and fingerprint for verification. The voter machine forwards this information to the host processor, which routes the transaction request for verification to the election offices or the office that issued the voter ID. If the verification is positive then the signal alert will be passed as he/she is the right candidate. Then the citizen is allowed to press the button for whom he/she wants to vote. It allows to press the button only once. When is pressed many more times it would become an invalid vote. The selected symbol is stored in database. Each time the each citizen presses the different symbol the vote the different symbols gets incremented. The election offices are allowed to read only the symbol, place from which the citizen votes, T/D, total number voter for the symbol, but not the details of citizen. None of the information (i.e.) voter ID/fingerprint is get by the election offices, it will be given security in hash code. ACH (Automatic Clearing House) facility is provided, and so it will be in ready manner to allow the next citizen to vote.

XIII- CONCLUSION AND FUTURE WORK

We have proposed a new way of looking at analysis of voting system. Modeling of voting systems should be done in a language which is easy and more intuitive to work. This demonstration will provide more efficiency and reliability. We demonstrated this model by giving a tool which can model voting system using mifaun technique and then providing the security using hash code and biometric techniques. In future, we will develop the system that will be useful for the physically challenged persons. We use the biometric techniques as such face recognition, voice recognition, iris recognition and heart beat recognition techniques. The application can be developed with all possible techniques to be useful for the human society.

XIV -REFERENCES

- [1] Cryptography and network security, "principles and practices" William Stallings 3rd edition.
- [2] "Data communication and networking", Behrouz A Forouzan 4TH.
- [3] "Numerical methods", G.Balaji
- [4] Osterburg, James W, T.Parthasarathy, T.E.S.Ragavahan and Stanley L.Sclove. "Development of a mathematical formula for the calculation of fingerprint probability based on individual characteristics".
- [5] "Probability and Statistics" Prof A.Singaravelu, Prof V.Sundarsan, Prof S.Sivasubramanian.
- [6] Watson, C.T and C.L.Wilson 1992 NIST special database for fingerprint. U.S. National Institute of Standard and Technology.
- [7] Alfred V.Aho, "Algorithms for finding patterns in string". In J.Van leewen editor.
- [8] Michael O.Rabin (PDF) "fingerprint by random polynomials", center for research in computing technology, Harvard University.
- [9] Baeza-Yades, R. Navarro, G. "Faster approximate string matching", department of computer science, university of Chile Santiago.
- [10] "The myth of fingerprint" Steven G.Amery, Eric Thomas Harley, Eric J.Malm., Harvey Mudd college Claremont, CA
- [11] Biometric recognition system system at
- [12] CARDIS conference [online] <http://www.fingerpint.org/standard>
- [13] Haugty P.V.C "methods and means of recognizing complex patterns" US patent 1962
- [14] Fingerprint as table primary key Burseson consulting [online] www.oracletips.org

[15] [online] www.afissystem.org

[16] Biometric fingerprint recognition system,
department of computer science.

[17] [online] www.mifaun.com