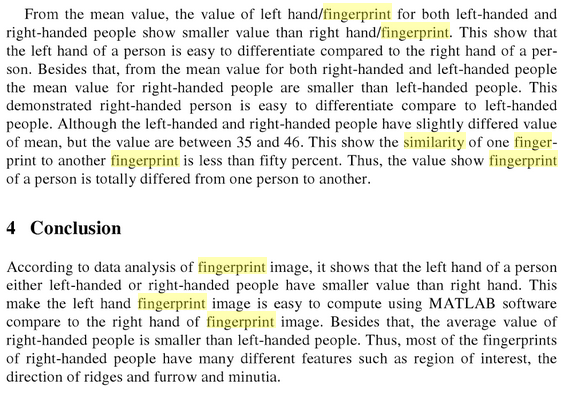
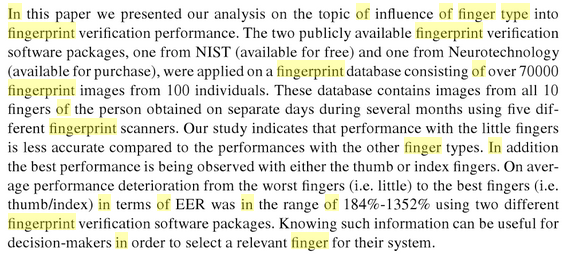
**PENGENALAN SIDIK JARI**



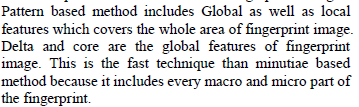


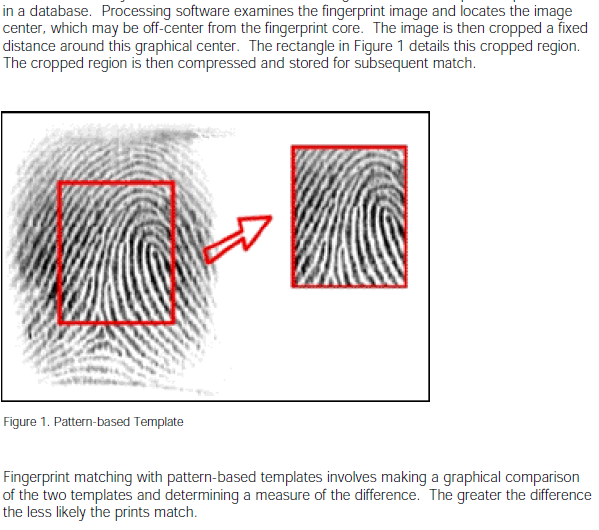
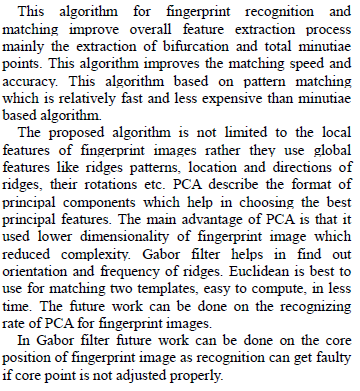
<https://books.google.co.id/books?id=ykG7BQAAQBAJ&pg=PA1&lpg=PA1&dq=Impact+of+Finger+Type+in+Fingerprint+Authentication&source=bl&ots=knUDH_96KF&sig=82vF_DNDEyGlugBBbNB6UEPA9fs&hl=en&sa=X&redir_esc=y#v=onepage&q=Impact%20of%20Finger%20Type%20in%20Fingerprint%20Authentication&f=false>

Pattern based

Pattern based technique compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images be aligned in the same orientation. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which they match

Fingerprint patterns are divided into three main groups consisting of Arches, Loops and Whorls. Approximately 5% of all fingerprints are Arches, 30% are Whorls and 65% are Loops.







*Template Size vs. Search and Match Speed*

On average, minutia-based templates are significantly smaller than pattern-based templates

on a byte count basis. The size of a minutia template is directly related to the number of

minutia extracted. Identix minutia templates typically average about 350 bytes, or

approximately 35 minutia, but can be as small as 125 bytes. The minutia extraction software

is easily able to affect the size of the template by controlling the number of final minutia

based on their strength.

Pattern-based templates average about 300-400 bytes when compressed, and about 1024

bytes when uncompressed. Matching and other related functions can only operate on the

uncompressed version. However, the size of the template is directly related to the image

and cannot easily be controlled without sacrificing detail (and thus usefulness) in the image.

Template size and storage capacity are directly related, with minutia templates requiring

about half the storage of pattern template. This impacts storage media costs, network

bandwidths, etc., and has a direct effect on the time required to retrieve a template for

searching and matching.

Template size also directly relates to the search and match speeds. Although search and

match speeds are also dependant on the efficiencies of the algorithms involved, smaller

templates will usually result in shorter match time.

*Sensitivity to Physical Changes*

Physical changes to the finger include such things as scars, cuts, folds, various blemishes,

etc. Physical changes can occur through accident or as a normal course of work, such as

cement workers, bricklayers, etc., whose fingerprint ridges are usually severely worn.

When a minutia based system processes a fingerprint, a scar, fold or other blemish may

result in a few minutia, but these typically represents a small percentage of the total minutia

extracted. For example, if 20% of the extracted minutia is disrupted due to physiological

changes to the fingerprint since the template was first taken, then there are still 80% of the

minutia available for matching. Since a good match can be made with as few as 30% of the

minutia, 80% availability provides for a wide safety margin.

Minutia templates are therefore very forgiving of physical changes to the fingerprint without

having to resort to re-extracting a new template from a new image of the finger.

On the other hand, pattern-based templates are more sensitive to physical changes in the

fingerprint because the match is done using a cropped fingerprint image. Physical changes can obscure critical elements of the image and significantly increase differences between two

images of the same finger, thus reducing the likelihood of obtaining an accurate match. In a

pattern-based system, new scars or other blemishes typically require a new image of the

fingerprint be obtained, converted to a template and stored in the system. This presupposes

the person is readily available for this activity, which may not be the case if, for example, the

original print was a latent print taken from a crime scene.

*Security and Playback*

When a minutia-based template is extracted from a fingerprint, subtle variations in the

orientation and centering of the finger on the capture device have subtle affects on the

minutia generated. This means that the same finger placed on a capture device multipletimes will produce slightly different minutia templates each time. This has no effect

whatsoever on the accuracy of the matching algorithms (as previously discussed, minor

variations in the minutia do not affect the match outcome). Consequently, the same finger

presented multiple times will match, but not perfectly in the sense that the extracted

templates will never be absolutely identical. This directly leads to a method for detecting the

presentation of a stolen template: if the match is exact, the template must be an identical

match, minutia for minutia, with the template in the database. The template must therefore

be a duplicate of the one in the database and could not have come from a live scan.

With a pattern-based template, obtaining the template, since it is a cropped graphical image

of the fingerprint, gives you the actual fingerprint. Adding logic in the authentication system

to detect that the exact same fingerprint image is being presented increases the False Reject

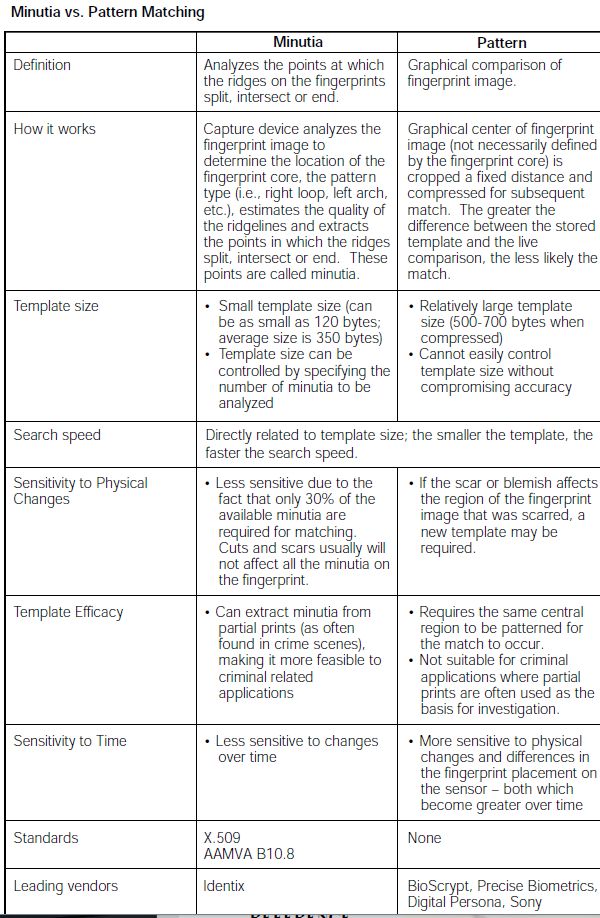
Rate, that is, the number of valid users being rejected. Further, the stolen print from the

template can be subtly altered so as to prevent a duplication detection, but still result in a

positive match.

With a minutia template, the fingerprint cannot be reconstructed, and thus the fingerprint

itself cannot be subtly altered and then replayed to the authentication system.



Correlation based

In correlation based matching the two fingerprint images are matched through corresponding pixels which is computed for different alignments and rotations. The main disadvantage of correlation based matching is its computational complexity.

**A Correlation-Based Fingerprint Verification System**

**Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez,**

**Leo P.J. Veelenturf and Berend Jan van der Zwaag**

*University of Twente, Department of Electrical Engineering,*

**The correlation-based \_ngerprint verification system \_rst selects appropriate**

**templates in the primary \_ngerprint, uses template matching to locate them in the secondary print, and compares the template positions of both fingerprints. Unlike**

**the traditional minutiae-based systems, this system**

**directly uses the richer gray-scale information**

**of the \_ngerprints.**

It \_rst selects characteristictemplates in the primary \_ngerprint. Then, templatematching is used to \_nd the positions in the secondary\_ngerprint at which the templates match best. Finally,the template positions in both \_ngerprints arecompared in order to make the decision whether theprints match.

1. Correlation-Based Template Selection

templates are selected by checking how well they \_t at other locations in the same fingerprint. if a template \_ts much worse at all other locations in thefingerprint, it is a template that o\_ers alot of distinction.Therefore, the ratio of git at a template's

original location to the fit at the next best locationSince the correlation-based checking is carried out by means of template matching, this method consumes

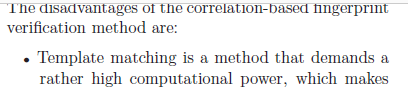
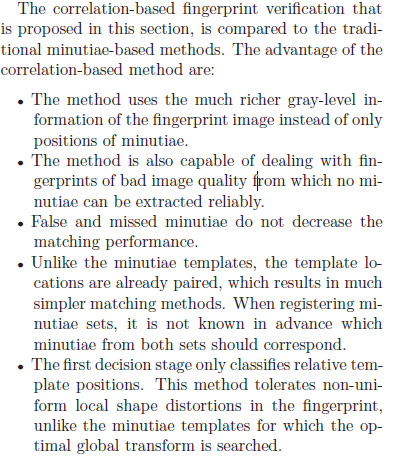
a lot of computational powercan be used as a template selection criterion.

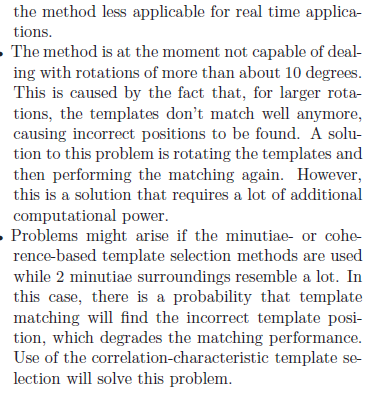
1. Template Matching

The template is shifted pixelwise over the secondaryprint. At each position, the gray-level distance betweenthe template and the corresponding area inthe secondary print is determined by summing thesquared gray-level di\_erences for each pixel in thetemplate. After having shifted the template over theentire \_nger, the location where the distance is minimalis chosen as the corresponding position of the template in the second \_ngerprint.

1. Classification of template position

The \_ngerprint matching algorithm, based on twosets of template positions, uses two decision stages.First, elementary decisions are made by classifying theindividual template position pairs to be matching ornot. Then, the information of all template pairs ismerged in order to make a \_nal decision whether theprimary and secondary \_ngerprint match or not.



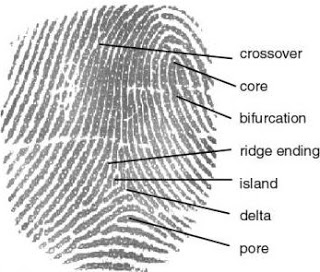


Minutiae based

This is the most popular and widely used technique, for fingerprint comparison. In minutiae-based techniques first of all we find minutiae points on which we have to do mapping. However, there are some difficulties when using this approach. It is difficult to identify the minutiae points accurately when the fingerprint is of low quality.

Untuk lebih jelasnya, *minutiae* pada sidik jari adalah titik-titik yang mengacu pada:

* *crossover* (persilangan dua garis)
* *core* (putar-balikan sebuah garis)
* *bifurcation* (percabangan sebuah garis)
* *ridge ending* (berhentinya sebuah garis)
* *island* (sebuah garis yang sangat pendek)
* *delta* (pertemuan dari tiga buah garis yang membentuk sudut, dan
* *pore* (percabangan sebuah garis yang langsung diikuti dengan menyatunya kembali percabangan tersebut sehingga membentuk sebuah lingkaran kecil).

[](http://2.bp.blogspot.com/-EkpCuwckzpU/T2K7DjMK87I/AAAAAAAAACA/zR7TLse96YQ/s1600/minutiae.jpg)

Mesin pemindai sidik jari akan mencari titik-titik ini dan membuat pola dengan menghubung-hubungkan titik-titik tersebut. Pola yang didapat dari menghubungkan titik-titik inilah yang nantinya akan digunakan untuk melakukan pencocokan bila ada jari yang dipindai. Jadi, sebenarnya mesin sidik jari tidak mencocokkan gambar, tapi mencocokkan pola yang didapat dari *minutiae-minutiae* ini.

**Sensor Optikal**

Inti dari sensor optikal adalah adanya CCD (*Charge Couple Device*) yang cara kerjanya sama seperti sistem sensor yang terdapat pada kamera digital atau *camcorder*. CCD merupakan chip silikon yang terbentuk dari ribuan bahkan jutaan dioda fotosensitif yang disebut *photosites*, *photodelements*, atau disebut juga piksel. Tiap *photosite* menangkap satu titik objek, kemudian dirangkai dengan hasil tangkapan *photosite* lain menjadi satu gambar.

[](http://4.bp.blogspot.com/-qJv7m7uH5x8/T2K7UpnsTaI/AAAAAAAAACI/HLAjGh0jQFw/s1600/fingerprint.jpg)

Bila mengambil contoh pada kamera, saat menekan tombol ‘*capture*’ pada kamera digital, sel pengukur intensitas cahaya akan menerima dan merekam setiap cahaya yang masuk menurut intensitasnya. Dalam waktu yang sangat singkat, tiap titik photosite akan merekam cahaya yang diterima dan diakumulasikan dalam sinyal elektronis.

Gambar yang sudah dikalkulasikan dalam gambar yang sudah direkam dalam bentuk sinyal elektronis akan dikalkulasi untuk kemudian disimpan dalam bentuk angka-angka digital. Angka tersebut akan digunakan untuk menyusun ulang gambar untuk ditampilkan kembali. Perekaman gambar yang dilakukan oleh CCD sebenarnya dalam format *grayscale* atau *monochrome* dengan 256 macam intensitas warna dari putih sampai hitam.

Kelemahan metode ini adalah hasil scanning sangat tergantung dari kualitas sidik jari. Jika kualitas sidik jari miskin (poor) atau luka, maka kualitas hasil pembacaan akan tidak bagus. Kelemahan lain adalah tehnik ini bisa diakali dengan jari palsu. Tapi tehnik ini mempunyai keuntungan mudah dilakukan dan tidak membutuhkan biaya yang mahal.

**Sensor Kapasitif**

Sensor kapasitif bekerja berdasarkan prinsip pengukuran kapasitansi dari material yang dipindai. Material tersebut bisa saja besi, baja, alumunium, tembaga, kuningan, bahkan hingga air. Berbeda dengan pemindai optikal yang menggunakan cahaya, pemindai kapasitif menggunakan arus listrik untuk mengukur besarnya kapasitas.

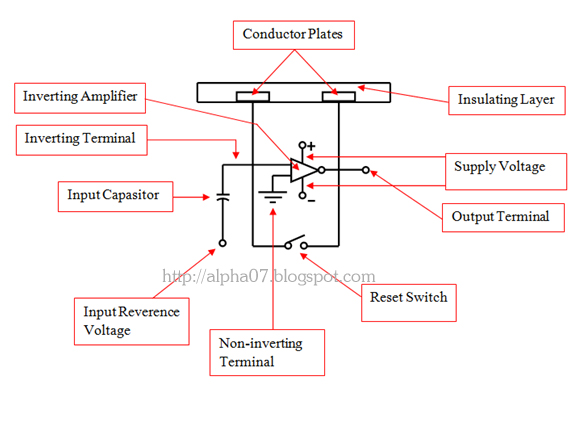
[](http://1.bp.blogspot.com/-mS8LhcOV2Wc/T2K8XExvzJI/AAAAAAAAACQ/_Yu4O8VoFpk/s1600/sensor-kapasitif.jpg)

Diagram diatas menunjukkan sebuah sensor kapasitif sederhana. Dimana sensornya dibuat dari beberapa chip semikonduktor pada sebuah sel yang tipis. Setiap sel memiliki tempat konduktor yang ditutupi dengan lapisan isolasi.

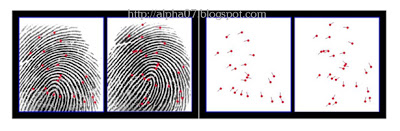
Sensor tersebut terhubung dengan sebuah integrator yang dilengkapi dengan inverter penguat yang dapat menerjemahkan, sehingga pada akhirnya akan membentuk sidik jari yang sedang dipindai

.

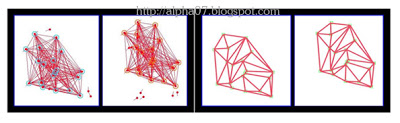
adanya ridge (gundukan) dan valley (lembah) pada sidik jari, maka kapasitas dari kapasitor masing-masing orang akan berbeda

**Ilustrasi Minutiae**

Setelah mesin pemindai menyimpan image atau gambar yang diambil, mesin lalu melakukan ‘*searching minutiae*’ atau mencari titik-titik minutiae. Lalu mesin pemindai akan mencari kecocokan pola pada minutiae-minutiae yang telah terkumpul tersebut.

[](http://3.bp.blogspot.com/-x54iBxoKZCk/T2K9tqC0byI/AAAAAAAAACY/tNQFif9mUhs/s1600/searching-minutiae.jpg)

Jika mesin pemindai sidik jari mendapatkan pola sidik jari yang sama, maka proses identifikasi sudah berhasil. Tidak semua minutiae harus digunakan, dan pola yang ditemukan tidak harus sama. Maka dapat disimpulkan bahwa posisi jari kita pada saat identifikasi tidak harus sama persis dengan pada saat pertama kali menyimpan data sidik jari pada mesin tersebut.

[](http://3.bp.blogspot.com/-e1XEbmB9cYE/T2K-kZbsOsI/AAAAAAAAACg/m0Z5EuSgTDw/s1600/matching-minutiae.jpg)

Pemindai sidik jari optikal dan kapasitif dianggap menghasilkan tingkat keamanan yang tinggi, karena tidak bisa dipalsukan dengan fotocopy sidik jari, sidik jari tiruan, atau bahkan dengan cetak lilin yang mendetil dengan guratan-guratan kontur sidik jari sekalipun.

<http://alpha07.blogspot.co.id/2012/03/cara-kerja-fingerprint-scanner.html>

**Teknik penyimpanan pada sidik jari**

1. Data sidik jari disimpan di dalam perangkat alat absensi sidik jari.

Cara ini disebut sabagai pendapat desentralisasi. Biasanya terjadi pada mesin sidik jari tipe standalone, yakni mesin sidik jari yang dalam pengoperasiannya bisa berjalan tanpa harus terhubung dengan komputer. Data akan tersimpan pada memori yang ada pada mesin.

Keuntungan metode ini adalah adanya kecepatan dalam proses pencocokan serta mesin absensi sidik jari bisa diletakan di tempat yang jauh dari computer. Kelemahannya dalah kapasitas yang terbatas sesuai dengan besar memori yang disediakan oleh mesin.

Saat ini sudah tersedia mesin absensi sidik jari yang mampu menampung sampai 5000 sidik jari atau lebih.

1. Data sidik jari disimpan pada database di computer.

Cara ini disebut sebagai cara sentrilisasi. Biasanya digunakan pada alat sidik jari tipe online atau yang harus terhubung dengan computer. Data sidik jari yang harus diregistrasi akan langsung disimpan pada database yang ada pada harddisk computer.

Keuntungan cara ini adalah kapasitas penyimpanan yang sangat besar, sesuai dengan kapasitas harddisk komputer. Kelemahannya adalah proses identifikasi yang agak lambat dan wajib adanya computer dalam pengoperasiannya.

**Teknik pencarian**

1. Menggunakan metode one to one

Metode ini mengharuskan si pemilik atau karyawan mengetikan no.id terlebih dahulu baru kemudian meletakan sidik jarinya di alat absen sidik jari. Dengan cara ini, mesin absensi sidik jari akan hanya mengecek citra sidik jari milik no.id tersebut

1. Mengelompokannya ke dalam grup.

Pengguna atau karyawan yang terdaftar pada alat atau mesin sidik jari dikelompokan berdasarkan kelompok-kelompok dengan cara ini mesin absensi sidik jari hanya akan mencari sidik jari yang ada dalm kelompok karyawan yang bersangkutan.

1. Sidik jari dikelompokan ke dalam tipe sidik jari.

Dalam hal ini mesin absensi sidik jari akan mengelompokan sidik jari ke dalam kelompok menurut tipenya, yaitu whorl, right loop, arch, tented arch dll. Selain itu juga berdasarkan banyaknya ridge yang muncul dalam empat arah dari nol derajat, 45 derajat, 90 derajat dan 135 derajat

<https://masthink.wordpress.com/2012/11/13/teknis-dan-cara-kerja-mesin-sidik-jari-finger-print/>

**Algoritma**

ALGORITHM:

Input : Gray-scale Fingerprint image.

Output : Verified fingerprint image with matching score.

1. Step 1. Initialized fingerprint in a binary form.
2. Step 2. Thinning on image from step 1
3. Step 3. Minutiae points are extracted from image. Data

matrix is generated to get the position, orientation

and type of minutiae.

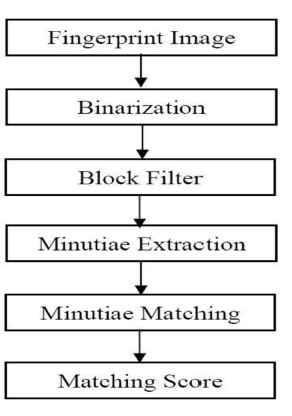
1. Step 4. Comparison & Matching of test fingerprint with

template.

1. Step 5. Match the score of two images is computed, if

matching score is 1 images are matched and if it is 0

then they are mismatched

 **ATM Transaction Using Biometric Fingerprint Technology**

**Mr. Mahesh A. Patil Mr.Sachin P.Wanere Mr.Rupesh P.Maighane Mr.Aashay R.Tiwari**

A.Binarization: The pre-processing of FRMSM uses

Binarization to convert gray scale image into binary image

by fixing the threshold value. The pixel values above and

below the threshold are set to ‘1’ and ‘0’ respectively. An

original image and the image after Binarization are shown

in the Figure 5.



B.Block Filter: The binarized image is thinned using Block

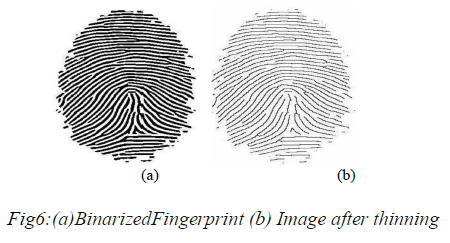
Filter to reduce the thickness of all ridge lines to a single

pixel width to extract minutiae points effectively. Thinning

does not change the location and orientation of minutiae

points compared to original fingerprint which ensures

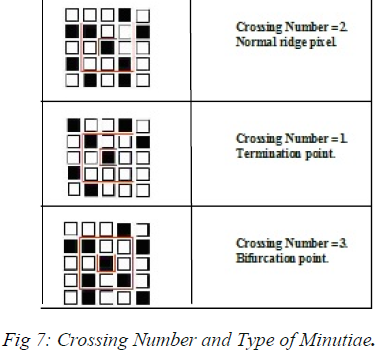
accurate estimation of minutiae points. Thinning preserves

outermost pixels by placing white pixels at the boundary of

the image, as a result first five and last five rows, first five

and last five columns are assigned value of one. Dilation

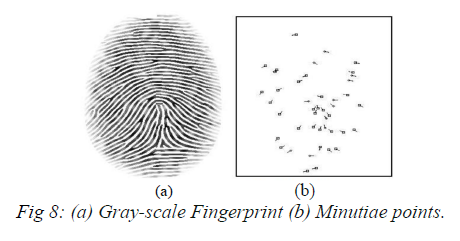
and erosion are used to thin the ridges.

*C.Minutiae Extraction****:*** The minutiae location derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the minutiae points in fingerprint image. Crossing Number is defined as half of the sum of greater than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively, is shown in figure7

Square shape shows the position of

termination and diamond shape shows the position of

bifurcation as in figure.8



D.Minutiae Matching: To compare the input fingerprint data

with the template data Minutiae matching is used. For efficient

matching process, the extracted data is stored in the matrix format.

The data matrix is as follows.

Number of rows: Number of minutiae points.

Number of columns: 4

Column 1: Row index of each minutia point.

Column 2: Column index of each minutia point.

Column 3: Orientation angle of each minutia point.

Column 4: Type of minutia. (A value of ‘1’ is assigned for

termination, and ‘3’ is assigned for bifurcation).

E.Matching Score: it is used to calculate the matching score

between the input and template data is given in an equation

(3)

Matching score = Matching Minutiae / Max(NT,NI ) -------

(3)

International Journal of Electronics, Communication & Soft Computing Science and Engineering

ISSN: 2277-9477, Volume

2, Issue 6

26

Where, NT and NI represent the total number of minutiae in

the template and input matrices respectively. By this

definition, the matching score takes on a value between 0

and 1. Matching score of 1 and 0 indicates that data matches

perfectly and data is completely mismatched

respectively.[12][15][18][21][22][23]

*\_* directional \_eld estimation,

*\_* adaptive \_ltering for noise reduction,

*\_* thresholding to obtain a binary \_ngerprint image,

*\_* morphological operations like thinning to obtain

ridges that are only one pixel wide,

*\_* minutiae extraction from the thinned image,

*\_* application of heuristics to reduce the number of

false minutiae,

*\_* registration of minutiae templates by Hough transform,

*\_* matching score computation.

A good fingerprint contains 25 to 80 minutiae points. Minutiaebased fingerprint recognition consists of Thinning, Minutiae extraction, Minutiae matching and Computing matching score. Verification specify an individual fingerprint by comparing only one fingerprint template stored in the database, while identification specify comparing all the fingerprints stored in the database. (Fingerprint Recognition Using Minutia Matching-Dr. Neeraj Bhargava#1,Dr. Ritu Bhargava\*2,Prafull Narooka#3,Minaxi Cotia\*4)

<https://subs.emis.de/LNI/Proceedings/Proceedings31/GI-Proceedings.31-3.pdf>

<https://sourceafis.machinezoo.com/>

<https://github.com/rtshadow/biometrics> (Phyton)

<https://www.codeproject.com/Articles/19323/Image-Recognition-with-Neural-Networks> (neural network)

**Modul Fingerprint**

**Fingerprint Sensor:** This is a finger print sensor module with TTL UART interface for direct relationship with microcontroller UART or to PC through MAX232/USB-Serial connector. The customer can store the exceptional imprint data in the module and can plan it in 1:1 or 1: N mode for recognizing the person. The FP module can particularly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port. Optical biometric one of a kind imprint for each client with remarkable components and can be embedded into a variety of completed things, for instance, access control, cooperation, prosperity store box, auto door locks. **Advantages:**

 Low Power Consumption

 Easy To Use

 Simple Construction

 Which Will Ensure Safety For Human

 Simple Connections

 Purely Wireless

 High Reliable

 Early notification

 Rugged In Construction

 Supports Remote Monitoring Feature

**ARM Mikrokontroler**

“ARM” is the abbreviation of “Advanced RISC Machines”. It is a widespread processor cores in the world. It is especially used in portable devices due to reasonable performance and low power consumption. ARM is a family of RISC architectures. **LPC2148 Chip Features:**

 ARM7 is a 32 bit microcontroller in a small LQFP64 bundle.

 It has 32kb on chip SRAM and 512kb on chip Flash memory.

 It has two IO ports each of 32 bit wide gave by 64 pins .

 It has single 10 bit ADC which gives variable simple yield.

 It has two 32 –bit Timer/outside occasion counters, PWM unit and watch dog.

 It underpins different serial interfaces including two UARTs and two quick I2C transport.

**Peralatan**

**ATM Client Authentication System Using**

**Biometric Identifier & OTP**

Jaydeep Shamdasani#1, Prof. Pravin Matte\*2

The system consist of following modules :-

1. LCD module: The OMAP5910 is used as LCD module in LCD controller, it supported 1024\*1024 images of 15 grayscale or 3375 colours.

2. Keyboard/Touch-Screen module: It is used for inputting passwords.

3. Fingerprint recognition module: FIM3030 fingerprint module is used for recognition of is used for recognition of fingerprints. This module uses optical sensor for capturing and detecting of fingerprint images.

4.GSM Modem: A GSM modem(SIM 300) provides an interface that allows sending and receiving messages over the modem interfaces.



Neural Network based