

BIOMETRIC USING FINGERPRINT AND ITS APPLICATIONS

Project report submitted in fulfilment of the requirement for the degree of
Bachelor of Technology

in

Computer Science and Engineering

by

Jyotir Aditya Sharma (161452)

Manu (161380)

Under the supervision of

Dr.Ekta Gandotra

to



Department of Computer Science & Engineering and Information
Technology

Jaypee University of Information Technology Wanknaghat, Solan-173234,

Himachal Pradesh, India

May 2020

Certificate

Candidate's Declaration

We hereby declare that the work presented in this report entitled **BIOMETRIC USING FINGERPRINTING AND ITS APPLICATIONS** in fulfillment of the requirement for the award of the degree of Bachelor of Technology in Computer Science and Engineering submitted in the department of Computer Science & Engineering and Information Technology, Wagnaghat is an authentic record of our own work carried out over a period from August 2019 to May 2020 under the supervision of Dr. Ekta Gandotra, Associate Professor, Computer Science and Engineering.

The matter embodied in the report has not submitted for the award of any other degree or diploma.



Jyotir Aditya Sharma (161452)



Manu (161380)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.



Dr. Ekta Gandotra

Computer Science and Engineering

Dated:

Acknowledgement

We have taken endeavors in this undertaking. In any case, it would not have been conceivable without the caring help and help of numerous people and associations. I might want to stretch out our genuine gratitude to every one of them. Principal, We might want thank our boss for the undertaking, Dr.EktaGandotra , Department of Computer Science and Engineering, Jaypee University of Information Technology,Waknaghat for his limitless commitment to the task. He invigorated us to take a shot at the point and gave significant data which helped in the fruition of the task.

We might likewise want to recognize her praiseworthy direction, checking and consistent consolation all through the writings on this venture. I am obligated to every one of the teachers of the Department of Computer Science and Building, JUIT Waknaghat for ingraining in me the essential information about the fields that incredibly profited me while taking a shot at the venture.

I likewise thank my companions and friends who broadened their assistance and backing at whatever point required. Their commitment has consistently been huge.

At last, I might want to accept this open door to thank my family, who have consistently been a wellspring of motivation and inspiration for me, and furthermore for the love they have given in distressing periods, which has been a managing power for the culmination of the undertaking.

Contents

I.	Declaration		
II.	Acknowledgement		
III.	List of Figures		
Chapter-1			7.
Introduction to Biometrics			
1.1	Introduction		8.
1.2	Biometric Identification System		9.
Chapter-2			10.
Biometric Databases			
2.1	Need for a DBMS in Biometrics	}	
2.2	Indexing Issues		10.
2.3	Binning		11.
2.4	Using the RDBMS	}	
2.5	Loose Integration		12.
2.6	Tight Integration		
2.7	Tight Integration – A basic approach	}	
2.8	Tight Integration – Indexing		13.
2.9	Fingerprint Indexing		
2.10	Basic Indexing approach		
2.11	Indexing Challenges	}	
2.12	Loose Vs. Tight Integration		14.
Chapter-3			15.

Biometric Encryption

3.1 Merger of biometrics with cryptography	15.
3.2. Biometric Encryption Algorithm	17.
3.2.1 Image Processing	17.
3.2.2 Correlation	18.
3.3 System requirements	18.
3.4 Enrolment / Verification	20.
3.4.1 Enrollment:	20.
3.4.2 Verification:	21.
3.5 Enrolment	22.
3.6 Verification	23.

Chapter-4 25.

How Fingerprinting works

4.1 How Fingerprints work	26.
4.2 Dactyloscopy	27.

Chapter-5

Fingerprint Scanning 29.

5.1 Fingerprinting scanning	29.
5.2 Digital scanning	29.

Chapter-6

Database Server 32.

6.1 Adding External Database Servers using Plesk	32.
6.2 Adding External Database Servers using MySQL	33.

Chapter -7

Adding Fingerprints to Database 35.

Chapter -8

Database Creation on Mysql **37.**

Conclusion **39.**

References **40.**

List of figures

Fig 1: Loose to Tight Integration	11.
Fig2: “Overview of the enrolment process for Biometric Encryption” ²⁰ .	
Fig 3: “Overview of the verification process for Biometric Encryption” ²¹ .	
Fig 4: Image processing used in enrolment	22.
Fig 5: Image processing used in verification	23.
Fig 6: Fingerprinting	25.
Fig 7: How fingerprints work	26.
Fig 8 : Ridges	27.
Fig 9: Optical Sensor	29.
Fig 10: A CMOS Sesnsor	30.
Fig 11: Sony CCD	30.
Fig 12: Server	26.
Fig 13: Captured Fingerprints stored as VarChar	35.
Fig 14: More Complete database storage of Fingerprints	35.
Fig 15: Screenshot of Table Students	36.
Fig 16: Users with different levels of access	36.
Fig 17: Privileges of user Registrar	37.
Fig 18: Privileges of Amit K Shrivastava	37.
Fig 19: Privileges of Software engineer	37.

Chapter - 1

Introduction to Biometrics

1.1 Introduction

The word Biometrics originates from the Greek words "Bio" (life) and "metrikos" (measure). What fingerprint does is rather simple, it does a mathematical, factual examination of our natural uniqueness. Be that as it may, we will utilize the present moment "biometrics" to allude to "biometric acknowledgment of individuals".

“Biometric acknowledgment offers a promising methodology for security applications, with certain favorable circumstances over the old style strategies, which rely upon something you have (key, card, etc.), or something you know (secret phrase, PIN, and so on.)” A pleasant property of biometric attributes is that it depends on something you are or something you do, so you don't have to recollect that anything neither to hold any token.

A solid blend of biometrics and cryptography will can possibly connect a client with an advanced mark she made with an elevated level of affirmation. For instance, it will get more diligently to utilize a taken token to create a mark or for a client to dishonestly renounce a mark by guaranteeing that the token was taken when it was most certainly not. Past endeavors toward this path incorporate a mark confirmation pen and related sign processor made accessible with the IBM Transaction Security System in 1989 . "One issue with this methodology is its finished dependence on equipment alter opposition:" If the token is broken, both the layout and the key are lost. As a rule, assailants have had the option to break tokens, regardless of whether by equipment assaults abusing chip-testing innovation or (similarly as with the IBM plan) by API assaults on the token's product . We in this manner set out to locate a superior method of joining biometrics, cryptography, and alter opposition.

"The primary hinderance to algorithmic mix is that biometric information is loud; just a surmised match can be required to a put away format. Cryptography, then again, necessitates that keys be spot on, or conventions will come up short. Consequently, past item contributions have been founded on explicit equipment gadgets. It will be greatly improved to have a progressively broad, convention level methodology, joining cryptography and biometrics. One more thought is protection." Many clients might be hesitant to have biometric information put away on focal databases; there might be less protection from biometric innovation if clients can be believably guaranteed that their layouts are not put away halfway (or, maybe, by any means).

1.2 Biometric Identification System :

Biometric frameworks are those which distinguish a client by putting away their natural data's and looking at them during that individual's accessor, at the end of the day biometric is a non-repeatable characteristic of us people that can consequently uncover one's personality and subtleties.

The principle three degrees of security, when actualized in the reality, are

The first level is utilized when you have your ownership, for example, ID.

The second level is utilized as a secret phrase for PC login or a PIN code in your bank ATM cards

Third level or the most elevated level of security is something that you are and something that you do. This is the fundamental things of biometric innovation.

"Biometrics frameworks have different capacity alternatives gave, for example, a database on a focal PC, plastic cards, (for example, strip, standardized tag, keen cards). The fundamental engineering of biometric recognizable proof contains 5 principle parts to be specific Data assortment, Signal preparing, Decision, Data stockpiling, and Transmission."

All the biometrics gadgets have similar standards of catch, correlation, extraction and coordinating in like manner. A portion of the biometrics procedures utilized in human organs for security objects is fundamentally Eye, in which it utilizes Iris and retina examining face

acknowledgment, unique finger impression filtering, hand geometry, finger geometry, palm, signature, voice acknowledgment.

These strategies are in this manner being quickly talked about here. A portion of things to come methods in biometrics are DNA examining, ear Shape, keystroke dynamic filtering, vein check and so forth.

Chapter -2

Biometric Databases

2.1 Need for a DBMS in Biometrics

- Each enormous scope Biometrics Solution uses a RDBMS for proficient capacity and to access the information .
- Examples are :
 - AIFS – contains 400 million fingerprints
 - Retail location Biometric recognizable proof framework (100 million sections)

2.2 Indexing Issues

- Factors which are utilized to figure out which ordering strategy ought to be based on a Column:

Characteristics of recorded section

- Cardinality Data
- Distribution
- Value go

Understanding the Data and the Usage

Developing another Indexing strategy for Data distribution center's Queries

- The file must be little and use space effectively.
- The Index must have the option to work with different lists.
- The Index must help AdHoc and complex Queries and accelerate join activities
- The Index must be anything but difficult to assemble actualize and keep up.

2.3 Binning

- Origin from arrange data hypothesis
- It is the division of set of code words (or formats) into subsets with the end goal that each canister fulfills a few properties relying upon the application
- It is an approach to fragment the biometric layouts, e.g.,
 - Male/Female
 - Particular Finger
 - Loop versus whorl versus curve versus circle curve
 - may be another biometric
 - Increases search execution, may diminish search accuracy(increases bogus non coordinate proportion)
- Search for a coordinating layout may bomb attributable to an off base container arrangement
- May need to remember a similar format for various containers
- Bin blunder rate is identified with trust in binning procedure

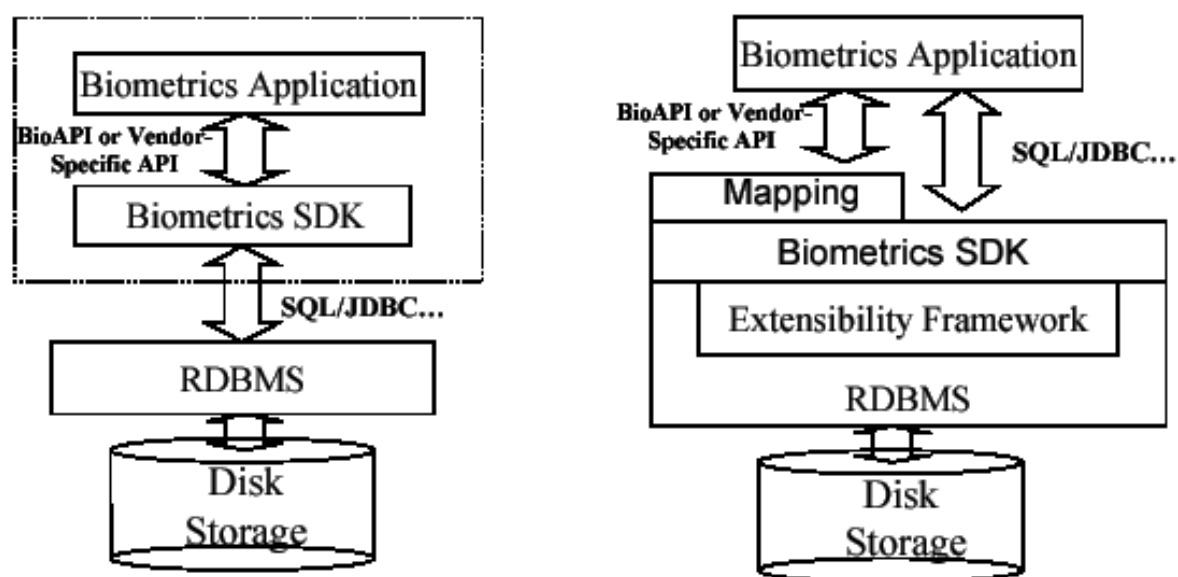


Fig1: Loose to Tight Integration

2.4 Type of “Tight Integration” – “The basic approach”

- The Biometric Vendors present the SQL administrators as
 - Identify_Match() Given an info layout, brings all back the formats which coordinate the contribution inside a certain edge (characterized as essential administrator)
 - Score() Returns the level of match of the info format with a put away layout (characterized as auxiliary to Identify_Match administrator)
- Biometric Vendors characterize usage for these administrators which are explicit to their biometric data.

2.5 Type of Tight Integration – Indexing

- Biometric Vendors propose an ordering plan (list type) for quick assessment of the Identify_Match() administrator
- Defining an ordering plan includes
 - Developing a filter(s) which will fastly erase an enormous number of non-coordinating formats
 - A careful match is performed against the coming about arrangement of formats

2.6 Fingerprint Indexing

- Possible ordering approach includes
 - “To order the fingerprints as (Left Loop, Right Loop, Whorl, and other) types”
- Query includes
 - “To order the info unique mark into one of these classes”
 - “To perform precise matches against fingerprints of the class”

2.7 “The Indexing Challenges”

- “may not generally be conceivable to create filter(s) to decrease the hunt space”
- “may be hard to beat in-memory coordinating calculation”

2.8 “The Loose Vs. Tight Integration”

“Loose Integration”

- “Memory-based” arrangement; can be genuinely proficient and utilize pointers
- “Memory bound”
- Customform highlights for enormous scope treatment of information.
- Does not have to think about extra DBMS highlights
- The Index structures may be
 - unadulterated “memorybased” structures
 - Not easy to join
 - The social predicates
 - Not easy to help multimodal apps

Chapter - 3

Biometric Encryption of Data

3.1 The Merger of biometrics with cryptography

Cryptography has become an undeniably significant element of PC security. Numerous cryptographic calculations are accessible for making sure about data, and a few have been examined beforehand in this book. When all is said in done, information will be made sure about utilizing a symmetric figure framework, while open key frameworks will be utilized for advanced marks and for secure key trade between clients. Be that as it may, whether or not a client conveys a open key framework, the security is subject to the mystery of the mystery or private key, individually. Due to the big size of the encrypted key, it would be uncomfortable for the client to enter the key each time. Therefore the client is simply required to remember a password that will evoke the encrypted key otherwise he/she will have to carry the key along with them whenever they need to access the database.

There are 2 reasons why the password headed security has its issues. Firstly anyone who gets the password will be able to access the database. That is a problem. Clearly these strategies present potential security dangers. The subsequent issue is the absence of direct association between the password and the client. Since a password isn't attached to the client, the framework running the cryptographic calculation can't separate between the genuine client and an aggressor who falsely gets the password of an authentic client.

As an alternative to secret key affirmation, biometric approval offers another framework for key security by using a biometric to ensure about the cryptographic key. As opposed to entering a secret word to get to the cryptographic key, the use of this key is checked by biometric affirmation. Exactly when a customer wishes to get to an ensured about key, the individual being referred to will be instigated to think about the catch of a biometric test. If this check test facilitates the selection regard design, by then the key is released and can be used to encode or unscramble the perfect data. As such, biometric affirmation can replace the use of passwords to ensure about a key. This gives both settlement, as the customer no longer needs to review a secret phrase, and secure character assertion, since simply the considerable customer can release the key.

In like manner these are the various procedures that may be used to ensure a key with a biometric. One procedure incorporates remote format planning and key accumulating. The biometric picture is gotten and the relating group is sent to a secured region for format assessment. If the customer is checked, by then the key is released from the secured zone. This gives a worthwhile instrument for the customer, as they no longer need to review a secret phrase. This technique would work outstandingly in a physical access application where the designs and keys may be taken care of in a shielded zone genuinely segregated from the image get device. In this situation, the correspondence line should likewise be made sure about to dodge busybody assaults. In any case, for PC use, the keys would almost certainly be put away free on a client's hard drive, which isn't secure and safe which is very terrible.

The subsequent technique includes concealing the cryptographic key inside the enrolment format itself by means of a trusted (mystery) bit-substitution calculation. Therefore, in the event that an assailant could decide the bit areas that indicate the key, at that point the aggressor could recreate the inserted key from any of the other clients' formats. On the off

chance that an assailant approached the enlistment program, at that point he could decide the areas of the key by, for instance, selecting a few people in the framework utilizing indistinguishable keys for every enlistment. The assailant then needs just to find those bit areas with normal data over the layouts and assault them which causes a serious ruin.

3.2. Biometric Encryption Algorithm

3.2.1 The Image Processing

A general diagram of connection, as it identifies with Biometric Encryption, is given in the accompanying segment. Progressively point by point conversations of relationship and its applications are given in the references by Goodman and Steward.

3.2.2 The Correlation

“The 2-dimensional information picture cluster is signified by $f(x)$ and its relating Fourier change (FT) mate by $F(u)$.” Here x means the space area and u signifies the spatial recurrence area.. A channel work, $H(u)$, is gotten from a picture, $f_0(x)$, where the addendum 0 signifies a picture got during an enrolment meeting. The relationship work, $c(x)$, between a resulting rendition of the information, $f_1(x)$, got during confirmation and $f_0(x)$ is officially characterized as
$$c(x) = \int_{-\infty}^{\infty} f_1(x) f_0^*(x) dx$$
, where $*$ means the intricate conjugate. In a handy connection framework, the framework yield is figured as the reverse Fourier change (FT-1) of the result of $F_1(u)$ and $F_0^*(u)$ where $F_0^*(u)$ is normally spoken to by the channel work, $H(u)$, that is gotten from $f_0(x)$. For relationship based biometric frameworks, the biometric format utilized for recognizable proof/confirmation is the channel work, $H(u)$. Typically in the relationship procedure the channel work $H(u)$ is intended to deliver an unmistakable connection top (which approximates a delta work) at the yield of the framework. Such a connection pinnacle can without much of a stretch be recognized in a correlator framework, and its position can be utilized to follow an object of intrigue, see Hahn and Bauchert. Moreover, a scalar worth can be gotten from the connection plane (Kumar and Hassebrook), and utilized as a proportion of the comparability somewhere in the

range of $f_1(x)$ and $f_0(x)$. The procedure of relationship gives a compelling component to deciding the comparability of items, and has been effectively utilized for unique finger impression confirmation (Stoianov et al). In the following segment, it will be shown that the procedure of connection can likewise be utilized as the reason for the Biometric Encryption calculation.

3.3 The System requirements

“Most Common goal of the Biometric Encryption calculation is to give a component to the connecting and ensuing recovery of an advanced key utilizing a biometric, for example, a unique mark. This advanced key would then be able to be utilized as a cryptographic key. The significant framework necessities that apply to a key recovery framework utilizing a unique mark are contortion resilience, separation and security.”

- Distortion resilience is the capacity of the framework to suit the everyday contortions of the unique mark picture. These contortions are a result of the social changes (situating, revolution, and distortion), just as ecological (encompassing temperature and moistness) and physiological (dampness content) conditions. A key recovery framework must have the option to reliably deliver the right key for the distinctive expected variants of a real client's unique mark.
- Discrimination is the capacity of a framework to recognize the entirety of the framework clients' fingerprints. An aggressor should create an erroneous key when the assailant's unique mark is joined with a genuine client's channel.
- Security of the framework implies that neither the advanced key, nor the real client's unique finger impression, can be freely separated from any put away data and source.

3.4 The Enrollment / Verification

The accompanying area gives subtleties of the usage of the Biometric Encryption calculation. A review of the procedures of enlistment and check is expressed beneath, concerning figure 22-1 and 22-2, separately and continuously.

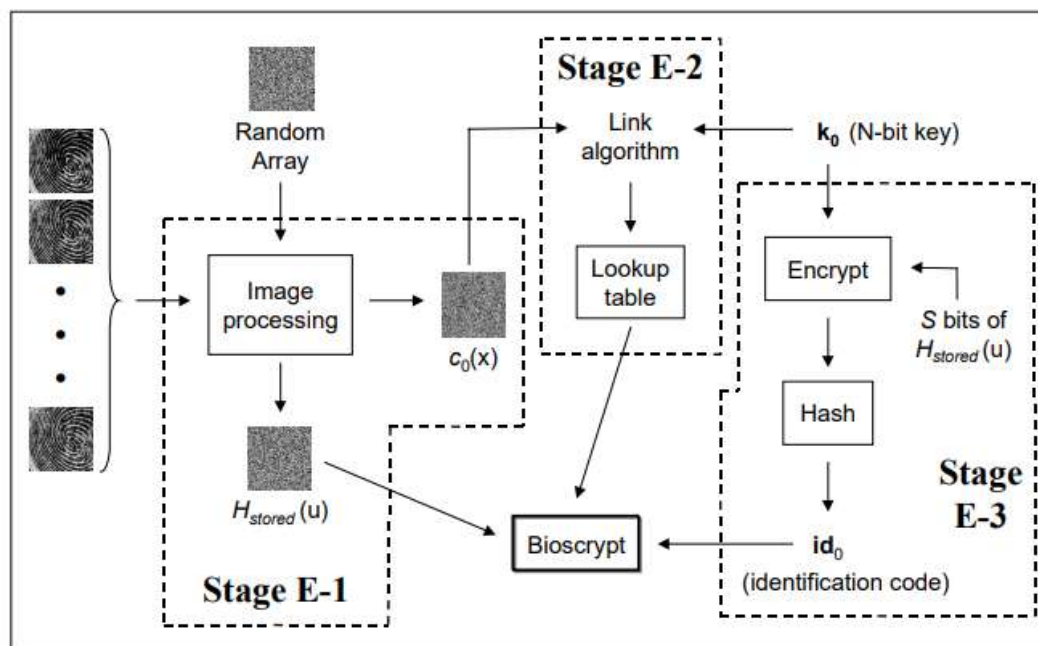


Fig2: Overview of the enrollment process for Biometric Encryption

3.4.1 The Enrollment:

E-1: Image Processing

The Combination of a progression of information unique mark pictures with an arbitrary (stage) exhibit to make two yield clusters: $H_{stored}(u)$ and $c_0(x)$.

E-2: Key connecting

Connecting of a cryptographic key, k_0 , to the example, $c_0(x)$, by means of the connection calculation.

E-3: Identification code creation

The Creation of a distinguishing proof code, id_0 , got from the key, k

The goal of the enlistment system is to connect a self-assertive N-bit key to the client's unique mark and make the client's Bioscrypt.

Regarding figure 22-1, the three sources of info required for the enlistment method are: a lot of the real client's unique mark pictures, a haphazardly produced stage just exhibit, $R(u)$, and

a N-bit cryptographic key, k_0 . $R(u)$ is created utilizing an arbitrary number generator (RNG). The key, k_0 , might be a current key that is contribution to the Biometric Encryption calculation, or it might be produced by the RNG. Note that both the key, k_0 , and the arbitrary stage exhibit, $R(u)$, are totally autonomous from the biometric pictures.

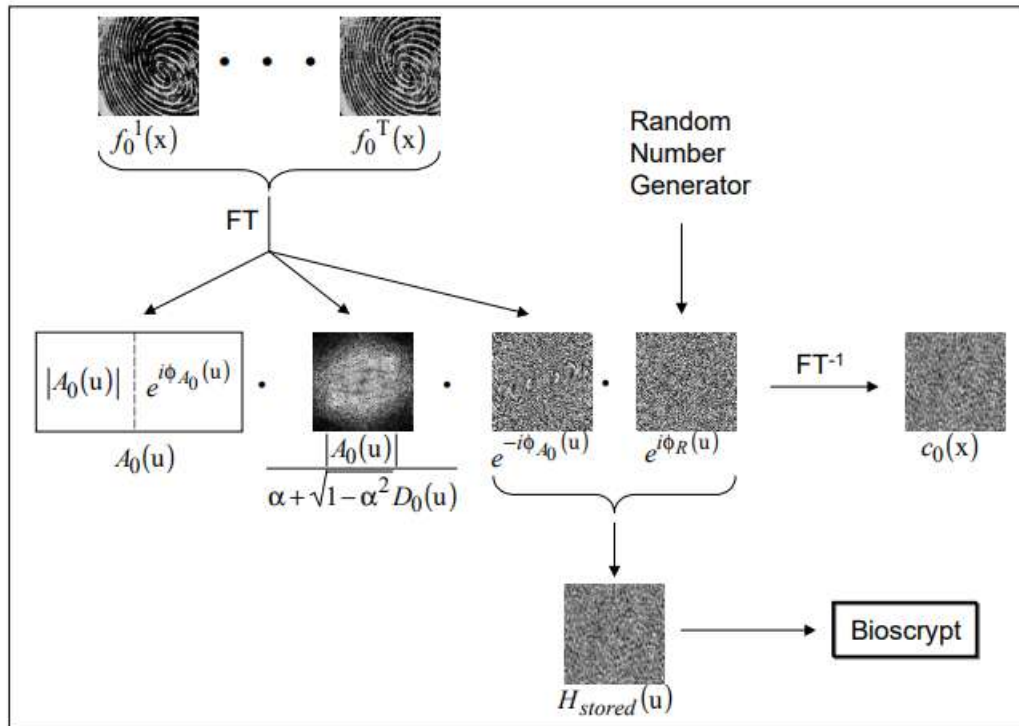


Fig 3: Image processing used in enrolment

Concerning figure 3, the goal of this phase of enlistment is to create a yield design, $c_0(x)$, to be passed to arrange E-2, just as to produce the put away channel work, $H_{stored}(u)$.

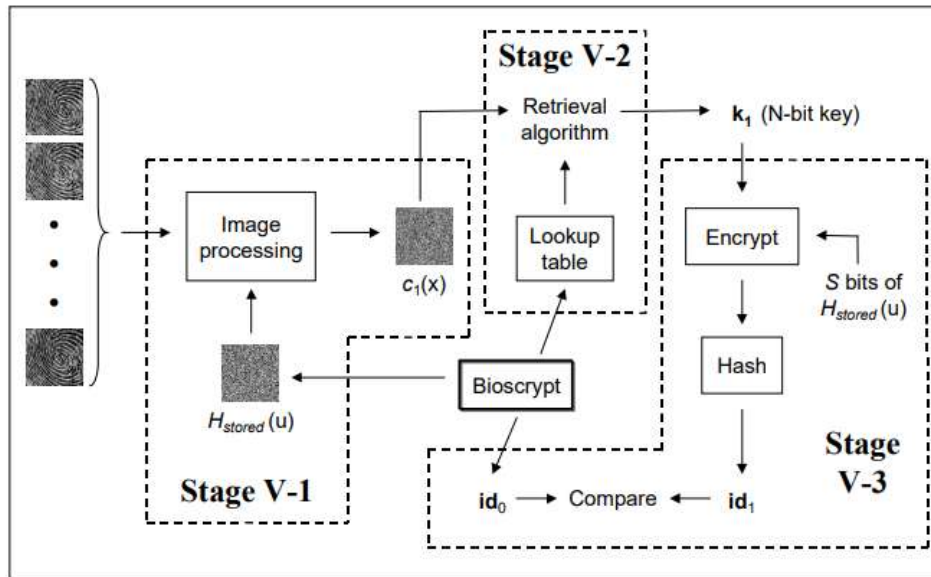


Fig 4: Overview of the verification process for Biometric Encryption

3.4.2 The Verification

V-1: Image Processing

Join $H_{stored}(u)$, from the Bioscrypt, with another arrangement of info unique mark pictures to make a yield design, $c_1(x)$.

The target of the check technique is the fruitful recovery of the N-bit key for a real client.

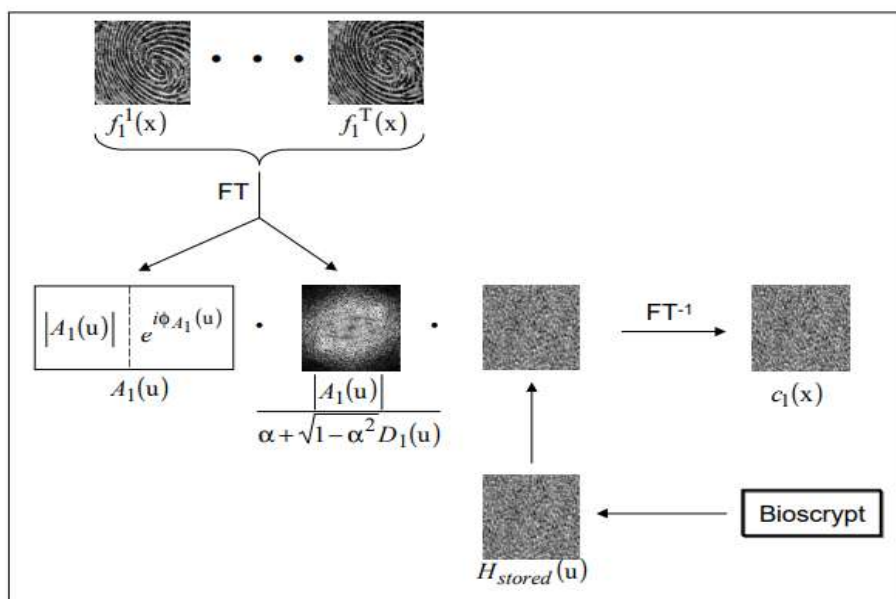


Fig 5 Image processing used in verification

Chapter – 4

How Fingerprinting works



Fig 6 Fingerprinting

- One's fingerprints can match up with someone else, that chance is a one in 64 billion.
- Different areas of human's hands and feet can be used for unique identification. But as the fingerprints are much easier to access by the person, although that can't be said. I think toe-prints are as much as accessible depending on how the scanning machine is built.
- There are older fingerprint records but it maybe due to wear and tear or available technologies, they were not recorded the way as today. The Babylonians used clay to record their fingerprints. The Chinese used a more simple way to record fingerprints and that was to store them using ink and paper. Well ofcourse then someone probably had to identify them using a magnifying glass probably by a fingerprint knowledgeable person.ss
- And then at the advent of 19th century fingerprints were used to identify law-offenders.

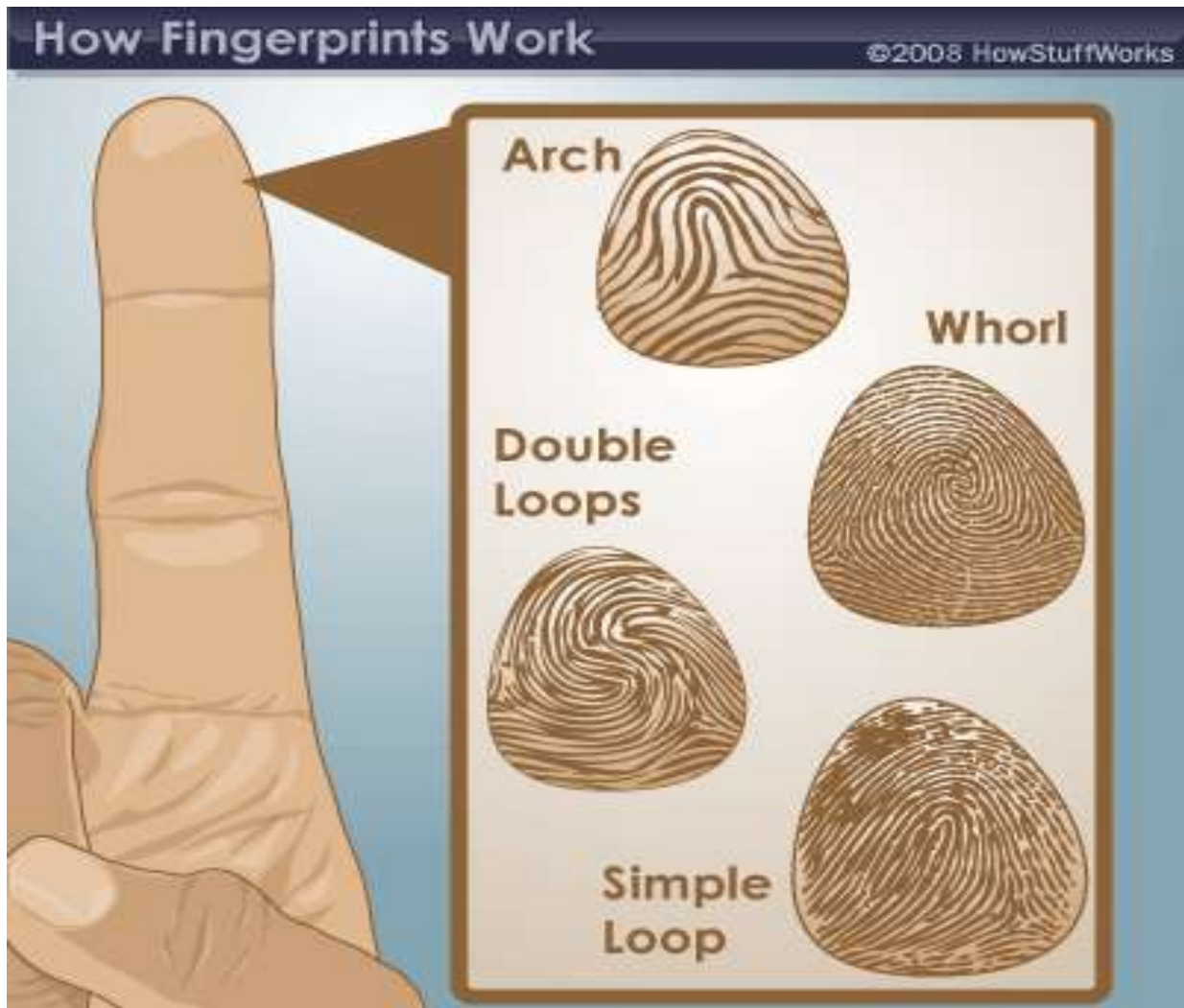


Fig 7: How fingerprints work

4.1 How Fingerprints work

- Fingerprints are more unique than the genetic material i.e. DNA. Twins can share same DNA but they don't share the same fingerprints.
1. "Fingerprints are made of an arrangement of ridges, called **friction ridges**"
 2. "All of the ridges of fingerprints form patterns called **Loops, Whorls or Arches**"
 3. "Each ridge contains pores, which are attached to sweat glands under the skin." One leaves fingerprints on any surface, in a general sense, because of sweat in our body.

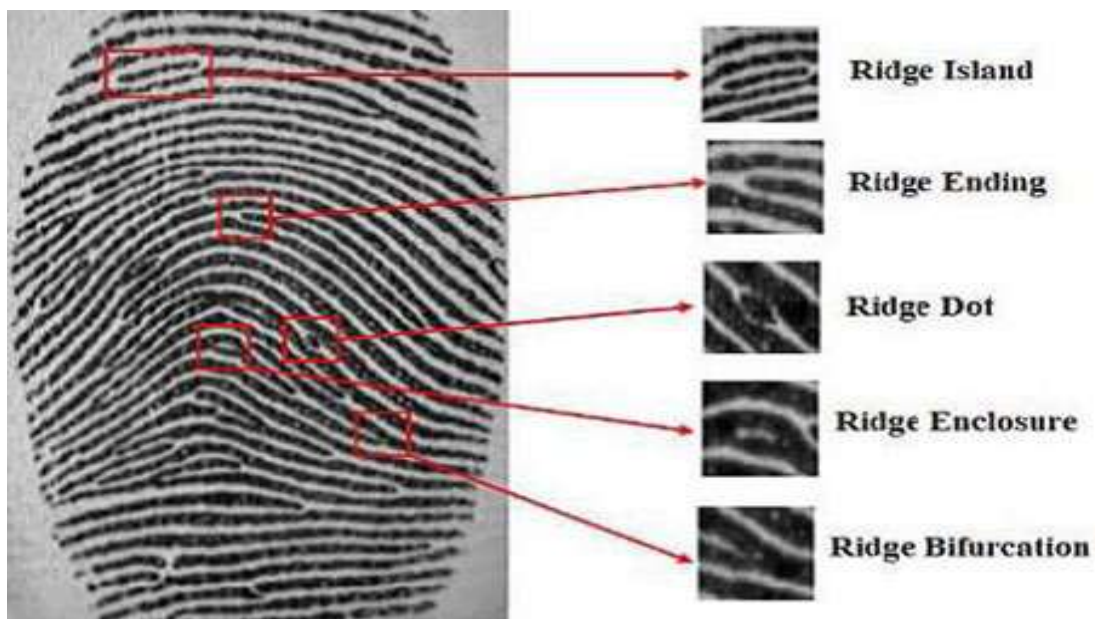


Fig 8 : Ridges

4.2 Dactyloscopy

- “**Ridge ending** is the point where the ridge ends suddenly.”
- “**Ridge bifurcation** is the point where a single ridge branches out into two or more ridges.”
- “**Ridge dots** are very small ridges.”
- “**Ridge islands** are slightly longer than dots and occupy a middle space between the two diverging ridges.”
- “**Ponds or Lakes** are the empty spaces between two diverging ridges.”
- “**Spurs** is a notch protruding from a ridge.”
- “**Bridges** are the small ridges which join two longer adjacent ridges.”
- “**Crossovers** are formed when two ridges cross each other.”

“The technique of fingerprinting is called **dactyloscopy**”

- Ink and card were used to scan fingerprints before any digital advancements.
- Scientists view the shape, size , arrangement, number of lines etc. to distinguish fingerprints from one another.
- Scientists also look for very minute fingerprint characteristics called **minutiae** that are invisible to the naked eye.

“Minutiae : Minutiae can be defined as the points where the ridge lines end or fork”

Chapter - 5

Fingerprint Scanning

5.1 Fingerprinting scanning

- A person's finger is cleaned thoroughly with alcohol and then dried well to get an ink fingerprint. The person rolls his or her fingertips in ink to cover the entire fingerprint area. Then the next step is to roll the finger over a card completely, called rolled fingerprints. "Finally, all fingers of each hand are placed down on the bottom of the card at a 45-degree angle to produce a set of **plain** (or **flat**) impressions." The above step is used to check the accuracy of the fingerprint impressions.

5.2 The Digital scanning

An optical sensor.

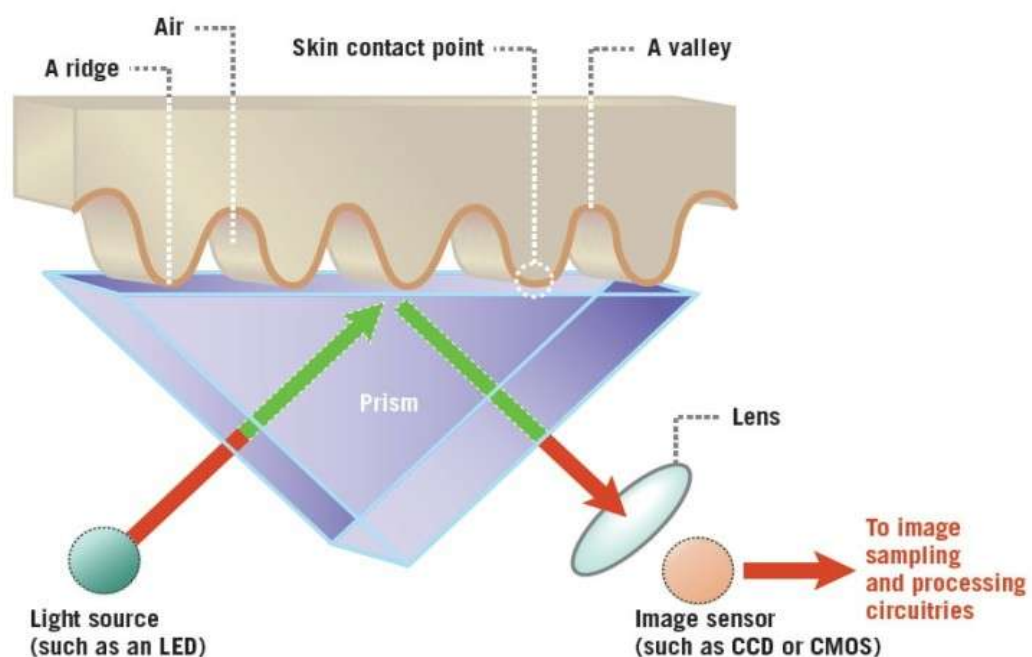


Figure 2

Fig 9 Optical Sensor

- Today, digital scanners capture an image of the fingerprint.
- The scanning process starts when one places his/her finger on a glass plate, and a CCD camera captures a picture.

- CCD : The heart of an optical scanner is the charge coupled device (CCD), the same light sensor system used in digital cameras and camcorders. A CCD is simply an array of light-sensitive diodes called photosites, which generate an electrical signal in response to light photons. Each photosite records a pixel
- The scanner uses light emitting diodes generally to illuminate the fingertips.
- CCD produces an inverted image with darker areas the ridges of fingers and lighter areas the valleys between ridges.

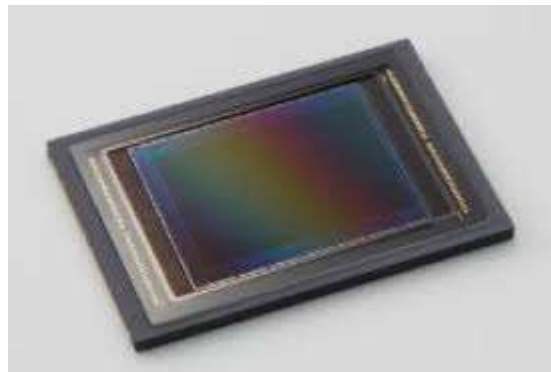


Fig 10 A CMOS Sesnsor

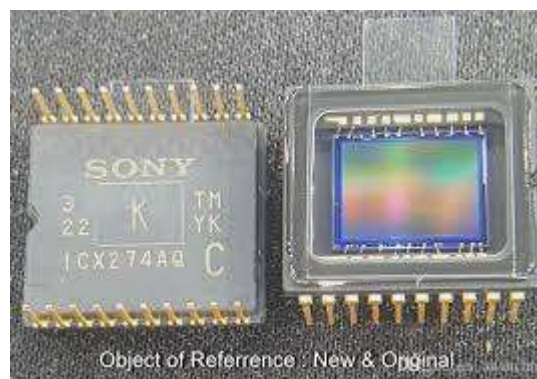


Fig 11 Sony CCD

- Both CCD and CMOS (complementary metal oxide semiconductor) covert light into electrons.

The reader (software) converts the data from the scan i.e. analog signal to digital signal image patterns.

- The scanner system programming utilizes outstandingly complex estimations to see and inspect these points of interest. The essential idea is to check the general spots of subtleties, in a comparable sort of way you may see a bit of the sky by the general spots of stars. A fundamental strategy to consider it is to consider the shapes that diverse minutia structure when you draw straight lines between them.
- If two prints have three edge endings and two bifurcations, encircling a comparable shape with comparative estimations, there's a high likelihood they're from a comparative print.
- To get a match, the scanner structure doesn't have to find the entire case of subtleties both in the model and in the print on record, it fundamentally needs to find a satisfactory number of points of interest plans that the two prints share for all goals and reason. The particular number contrasts as showed by the scanner programming.

Chapter- 6

Database Server



Fig 12 Server

6.1 The Addition of External Database Servers using Plesk database Systems

1. First Set up an external database server:
 1. Install MySQL.
 2. Set up the database administrator's account.
 3. Enable network access to the database server.
2. Log in to Plesk.
3. Then Go to Tools & Settings > Database Servers, and click Add Database Server.
 - 3.1. Specify the properties of the database server:
 - Then Specify the hostname or IP address of the database server.

- After that Specify the port number of the database server is listening on. This option is available only for MySQL software.

About Plesk

Plesk is designed to help IT specialists manage web, DNS, mail and other services through a comprehensive and user-friendly GUI. Plesk is a [hosting control panel](#), an intermediary between system services and users. For example, when a user creates a website through the Plesk GUI, Plesk propagates this request to a web server, either Apache or IIS, and the latter adds a new virtual host to the system. This method of administering all system services from a single web interface reduces maintenance costs and gives administrators more flexibility and control.

How Can I Use Plesk?

Plesk is an essential instrument for hosting service providers (HSPs) - companies that sell shared and dedicated hosting accounts. Being installed on a server, Plesk enables HSPs to organize server resources into packages and offer these packages to their customers. The customers are companies and individuals who need web presence but do not have the necessary IT infrastructure. Learn more about the Plesk's intended audience in the section **About Plesk Users**.

6.2 Adding External Database Servers using MySQL

- Open The board Studio and in the "Associate with Server" exchange box enter your association parameters
- Click the "Alternatives >>" fasten and explore to the "Associations Properties" page
- In the "Interface with database" discourse box type the word ace.
- Open up Another Question window and glue the accompanying T-SQL code into it:

```
USE [master]
GO

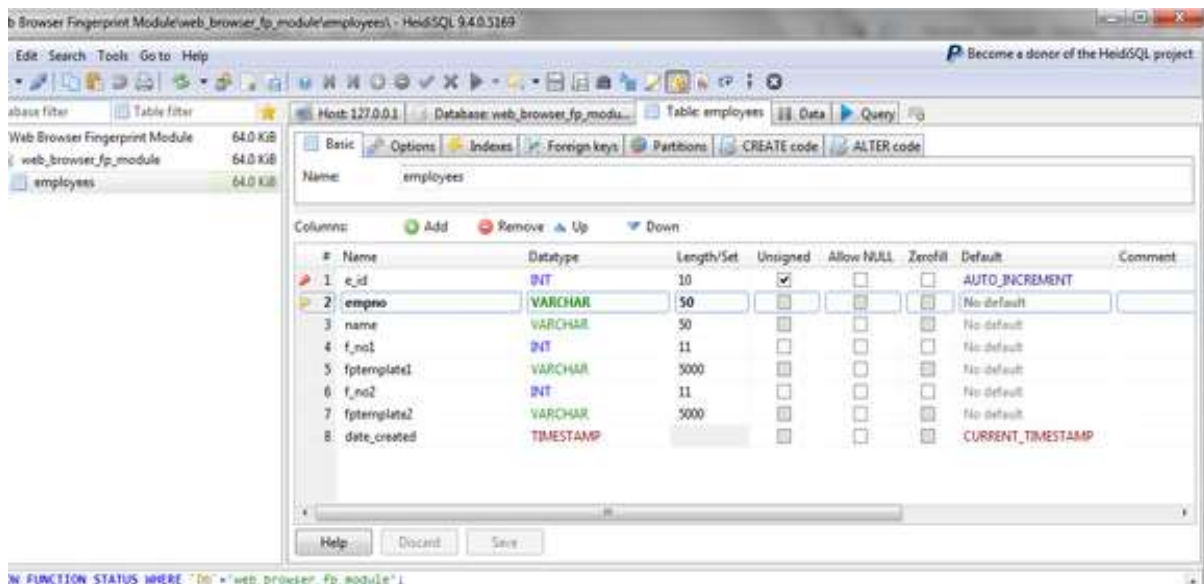
ALTER DATABASE [DB_123_database] SET ONLINE
GO
```

Supplant DB_123_database with your genuine database (the one you are attempting to bring on the web)

- Execute the code
- If the code executed effectively, however you don't see the adjustment in your database status, disengage from the server and associate once more. This time, you can interface with your default database rather than ace.

Chapter-7

Adding Fingerprints to Database



- **Fig 13. An Example..** Captured Fingerprint images stored as VarChar datatype in ftemplate1 & ftemplate2

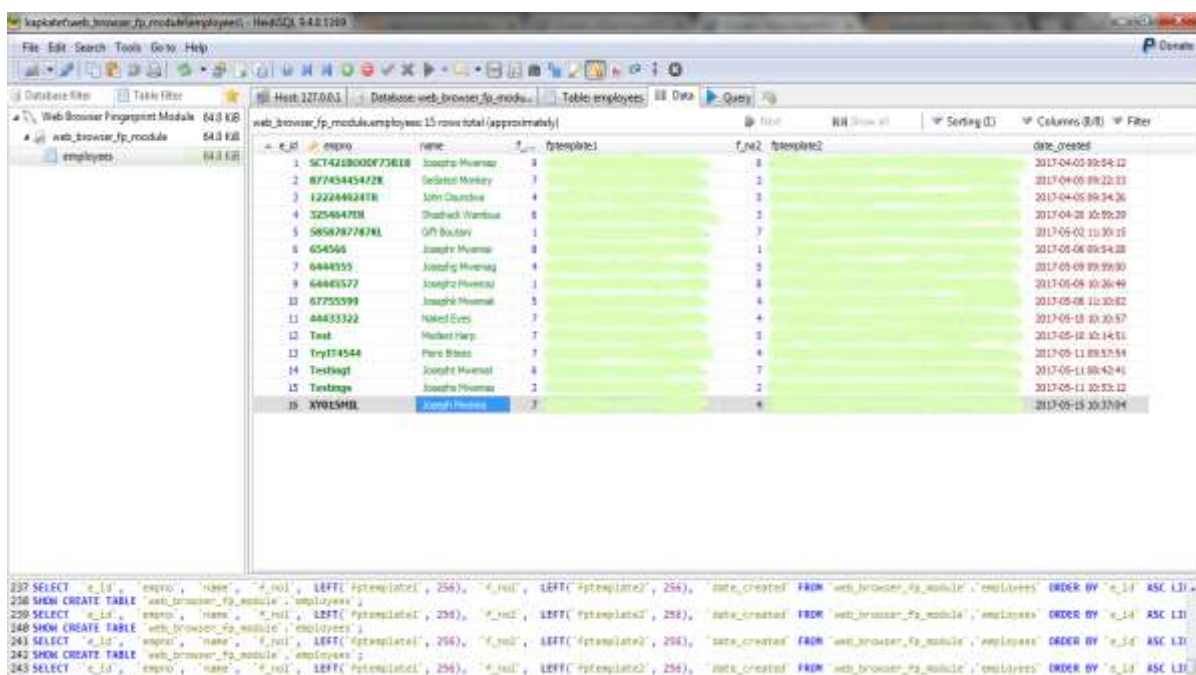


Fig 14. A more complete database of employee fingerprints stored in the database

Chapter-8

Database Creation on MySQL

Including the screenshots

```
mysql> SELECT* FROM Students;
```

Rollno	Name	Address	Year	CGPA
161001	Manu	38/6 Ropa Colony Sarkaghat 175024	4	6.5
161002	Rahil Patial	3/7 Aadarsh Colony Palampur 175343	4	6.5
161003	Muskan Kaushal	21/7 Vihar Colony Sundarnagar 175341	4	7
161004	Jyotir Aditya	74/8 New Colony Sanjauli	4	7
161005	Manish	45/3 Nehru Apartments NerChowk, Mandi 171742	4	7.2
161006	Simran	32/5 Teachers Colony Jogindarnagar, Mandi, 171456	4	7.5
161007	Angana	54/8 New Apartments Solan 173211	4	7.2
161008	Naveen	32/9 Near Jwalaji Temple, Kangra, 176001	4	8
161009	Yashwin	47/8 Ganj Market Solan, 173211	4	7.2
161010	Anshul Sharma	32/8 Sudarshan Market Jogindarnagar, 175015	4	6.8
161011	Shoryan	5/8 Near Himalyan School Sarkaghat 175024	4	7.4
161012	Vanshika	7/9 Near Lower Bazaar, Shimala 171001	4	7.5

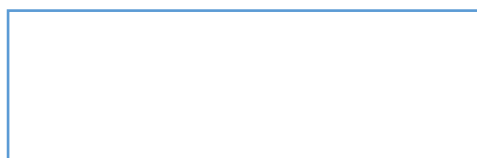
```
12 rows in set (0.36 sec)
```



```
mysql> SELECT USER FROM MYSQL.USER;
```

USER
AmitK
Registrar
mysql.session
mysql.sys
root

```
5 rows in set (0.00 sec)
```



1. Privileges for the Registrar of the University --All Access

```
mysql> SHOW GRANTS FOR "Registrar"@"localhost";
+-----+
| Grants for Registrar@localhost |
+-----+
| GRANT USAGE ON *.* TO 'Registrar'@'localhost' |
| GRANT ALL PRIVILEGES ON `biometric`.`students` TO 'Registrar'@'localhost' |
+-----+
2 rows in set (0.00 sec)
```

Fig 17.

2. Privileges for Amit K. Shrivastava (University Communications) – Can view every Student-data but cannot change it without permission.

```
mysql> SHOW GRANTS FOR "AmitK"@"localhost";
+-----+
| Grants for AmitK@localhost |
+-----+
| GRANT USAGE ON *.* TO 'AmitK'@'localhost' |
| GRANT SELECT ON `biometric`.`students` TO 'AmitK'@'localhost' |
+-----+
2 rows in set (0.03 sec)
```

Fig 18.

3. Privileges for The Software Engineer(**root**) – Absolutely Everything, Legal action if does-Somethingwrong.

```
mysql> SHOW GRANTS FOR "root"@"localhost";
+-----+
| Grants for root@localhost |
+-----+
| GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' WITH GRANT OPTION |
| GRANT PROXY ON ''@'' TO 'root'@'localhost' WITH GRANT OPTION |
+-----+
2 rows in set (0.20 sec)
```

Fig 19.

Conclusion

From the above report and the project that it includes we both have come to a better understanding of Fingerprinting and how it works. We have understood the applications that enable us to uniquely identify a human from one another. It has led to better security, better propagation of resources to the people and held employees accountable for their jobs.

We have come to better understand biometric encryption as well as inclusion of databases to the biometric world.

In the end we hope that this project and report increase the simplification of biometrics and its subsidiaries and help the future generation of JUIT students to better understand these subjects, hopefully.

References

1. <http://www.cse.lehigh.edu/prr/Biometrics/Archive/Papers/BiometricEncryption.pdf>
2. <https://pdfs.semanticscholar.org/e7e5/167704b82bd89e436c6c15accebf0c887db2.pdf>
3. <https://computer.howstuffworks.com/fingerprint-scanner.htm>
4. <https://www.bayometric.com/miutiae-based-extraction-fingerprint-recognition/>
5. Quora Article - How can I save a fingerprint in MySQL database with PHP. By JosepMaster of Science in Computer Systems and Biometrics.

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date:

Type of Document (Tick): PhD Thesis M.Tech Dissertation/ Report B.Tech Project Report Paper

Name: _____ Jyotir Aditya, Manu Gupta _____ Department: _____ Information Technology, Computer Science _____
Enrolment No _____161452, 161380_____

Contact No. _____9418236943, 8988264600_____ E-mail. _____akshujas@gmail.com, manugupta2598@gmail.com_____

Name of the Supervisor: _____Mrs. Ekta Gandotra_____

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): _____

_____ Biometrics using fingerprints and its applications _____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/ revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

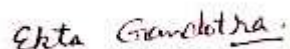
- Total No. of Pages = 36
- Total No. of Preliminary pages = 7
- Total No. of pages accommodate bibliography/references = 1



(Signature of Students)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at21.....(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.



(Signature of Guide/Supervisor)

Signature of HOD

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Abstract & Chapters Details	
	<ul style="list-style-type: none">• All Preliminary Pages• Bibliography/ Images/Quotes	21%	Word Counts	
Report Generated on			Character Counts	
		Submission ID	Page counts	

Please send your complete Thesis/Report in (PDF) & DOC (Word File) through your Supervisor/Guide at plagcheck.juit@gmail.com

	• 14 Words String		File Size	
--	-------------------	--	-----------	--

Checked by
Name & Signature

Librarian

.....

Please send your complete Thesis/Report in (PDF) & DOC (Word File) through your Supervisor/Guide at plagcheck.juit@gmail.com