IJSTA
International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

Analyzing 2D & 3D Fingerprint Recognition Techniques as Secure Biometric

Gagandeep Jagdev[1], Ashok Kumar[2]
[1]Dept. of Computer Science, Punjabi University Guru Kashi College, Damdama Sahib, Bathinda (PB).
[2]Research Scholar (M.Tech CE), Yadavindra College of Engineering, Punjabi University Campus, Talwandi Sabo (PB).
Email SAddress: [1]drgagan137@pbi.ac.in

Abstract**—**Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes. In addition to security, the driving force behind biometric verification has been convenience. Among different available biometric techniques, fingerprint recognition is the most prominent one. Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify an individual and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration. In this research paper, we have studied about the different modules involved in fingerprint recognition system and discussed the steps involved in the process with algorithm analysis. In addition to this we studied about 3D fingerprint recognition technology and compared it with 2D fingerprint recognition system.

Keywords**—** 2D fingerprint recognition; Biometrics; Contactless 3D fingerprint recognition; minutiae.

I. Introduction

As the necessity for higher levels of security rises, technology is bound to swell to fulfill these needs. Any new creation, enterprise, or development should be uncomplicated and acceptable for end users in order to spread worldwide. This strong demand for user-friendly systems which can secure our assets and protect our privacy without losing our identity in a sea of numbers, grabbed the attention and studies of scientists toward what's called biometrics. Since, after 9/11 biometrics is getting a titanic attention all over the world by scientist, researchers and engineers. Now days everywhere in the world security is given the top priority to counter the possible treats from terrorists and hence biometrics and security are the synonyms. Biometric systems are spreading rapidly at all security prone areas such as airports, banks, offices also with documentation like passport, identity card, driving license, etc. Reliable user identification is increasingly becoming important in the Web enabled world today and there has been a significant surge in the use of biometrics for user identification. Many corporate heads use laptops and personal digital assistants (PDAs) loaded with sensitive business and personal information. According to the Gartner group, over 250,000 mobile gadgets are lost or stolen every year, and only 25-30 per cent of these ever make it back to their rightful owners. Such mishaps have created a dire need to ensure denial of access to classified data by unauthorized persons. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. Biometrics technology is based on identification of individuals by a physical or behavioral characteristic. Examples of recognition of physical characteristics are fingerprints, iris, and face or even hand geometry. Behavioral characteristic can be the voice, signature or other keystroke dynamics. Biometrics is the budding area of bioengineering. It is the automated method on basis of which one can identify a person based on his/her physiology. Biometrics modes of identification have been found to be the most compelling and intriguing authentication technique. Tokens can be lost, stolen or duplicated and passwords can be forgotten or shared. Forgotten passwords and lost smart cards are a nuisance for users and waste the expensive time of system administrators. However, biometrics can authenticate you as you. Biometrics is a means of using parts of the human body as a kind of permanent password. Using biometrics for identifying and authenticating human beings offers unique advantages over traditional methods. Biometrically secured resources effectively eliminate risks, while at the same time offering a high level of security and convenience to both the users and the administrators. The table 1 below illustrates different biometric parameters [1, 2, 3, 9].

TABLE I. Biometric Parameters

Universality	Signifies that each person should have the biometric characteristic
Uniqueness	Signifies that biometric adopted should be such that it separates individuals from another
Permanence	Signifies that biometric should be such that it should resist factors like aging and other variance over time
Collectability	Signifies that biometric should be easily acquirable for measurement
Performance	Signifies that accuracy, speed, and robustness of biometric should be dependable
Acceptability	Signifies degree of approval of technology
Circumvention	Signifies ease of use of a substitute

Among these systems, fingerprint recognition appears to be the most universal, collectable, and accessible system. One of the main goals of this system is to use the knowledge of distinguishing one person's fingerprint from other's and how humans represent faces in order to discriminate different identities with high accuracy with the use of the two most universally accepted biometric mechanisms. Table II below shows finger prints compared to other biometric technologies in terms of accuracy, convenience, cost and size (1 being worst and 5 being the best) [9].

TABLE II. Biometric Technologies

Technology	Accuracy	Convenience	Cost	Size
Fingerprint	5	5	4	4
Voice	1	5	5	5
Face	2	3	4	3
Hand	3	3	2	2
Iris	5	2	3	3

Among the most remarkable strengths of fingerprint recognition, we can mention the following:

- Its maturity, providing a high level of recognition accuracy.
- The growing market of low-cost small-size acquisition devices, allowing its use in a broad range of applications, e.g., electronic commerce, physical access, PC logon, etc.
- The use of easy-to-use, ergonomic devices, not requiring complex user-system interaction.

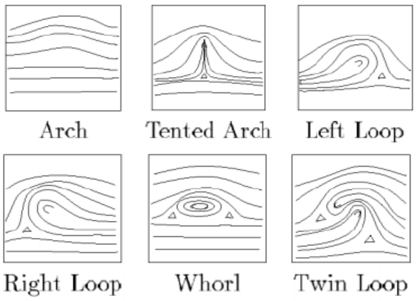

Fig. 1. Different patterns of fingerprints.

II. Finger Prints Identification Systems And Its Modules

It is the oldest scientific method of personal identity verification. Fingerprint Scanner authenticates the fingerprint applying digital technology. The basic principle of fingerprint identification is based on the following features:

- ➢ The fingerprints of any two people cannot be identical.
- ➢ The fingerprint of a person remains the same throughout his life.
- ➢ The pattern of the fingerprints can be expressed by algorithms.

The main modules of a fingerprint verification system (Fig. 2) are:

- Fingerprint sensing – Firstly, fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation.
- Preprocessing - In this the input fingerprint is enhanced and adapted to simplify the task of feature extraction.
- Feature extraction - In this step the fingerprint is further processed to generate discriminative properties, also called feature vectors.

Matching - In this step the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints

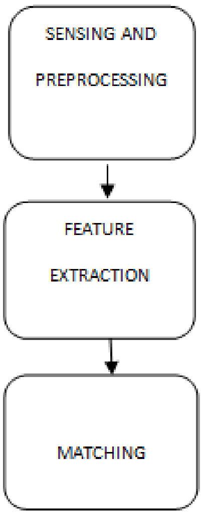

Fig. 2. Steps involved in fingerprint recognition system

The finger print verification system receives two inputs: the identity of the person requesting authentication (usually a PIN or smart card) and the scanned fingerprint (Fig. 3). The PIN is used as a key to retrieve a fingerprint template stored in a database and is compared against the currently offered fingerprint. The verification decision is based on the outcome of the search. Identification systems identify a person based on a currently scanned fingerprint. A database is searched for a matching fingerprint, if a matching fingerprint is found in the database, the search returns a positive outcome otherwise access is denied [4, 5, 9].

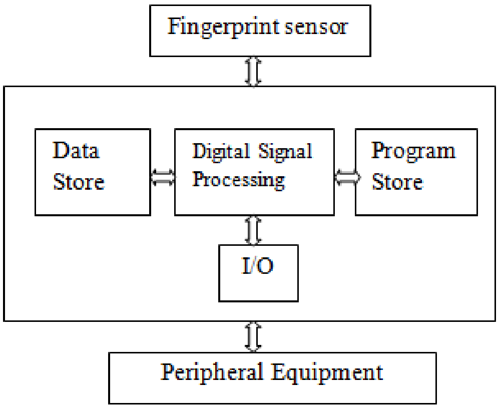

Fig. 3. A typical fingerprint identification system

III. Algorithm Analysis

The algorithm is a hierarchical based matching system that uses Level 1, Level 2 and Level 3 features to determine whether a set of fingerprints match. Various algorithms and transforms are used at each step. The key differentiator which determines distinctiveness is based on comparing Level 3 features. Analysis of the other levels on high resolution scans is performed to reduce complexity and running time and allow for an early termination of the algorithm [9].

Level 1 Feature Extraction

Level 1 feature includes orientation field which is responsible for measuring the directions of whorls, loops and arcs in fingerprint. This is done in addition to Level 2 features and string distance based matching algorithm is used to calculate the alignment of two images.

- The minutia and orientation fields are converted to polar coordinates w.r.t. and anchor point
- The features from 2D are reduced to strings.
- The edit distance is than normalized and converted to a matching score.

These matching scores than are compared and then based on this result we either exit indicating a mismatch or proceed further to next step.

Level 2 Feature Extraction

It is often known as minutia points. Rectangular form also known as bounding boxes are used around the minutia. Thereafter the score is computed to determine the level of matching.

The expression for evaluation is as follows

$$P2=V1*P1+V2*1/2*\frac{R_2^{TQ}-0.20*(R_2^{T}-R_2^{TQ})}{R_2^{T}+1}+\frac{R_2^{TQ}-0.20*(R_2^{Q}-R_2^{TQ})}{R_2^{Q}+1}$$

Here

V1- weight for combining information at Level 1

V2- (1-V1) weight for combining information at Level 2

R_2^{TQ}= number of matched minutiae

R_2^{T}=number of minutiae within the overlapping region of template(T)

R_2^{Q}=number of minutiae within the overlapping region of query(Q)

A 12-point threshold is set. If $R_2^{TQ}>12$ then the algorithm terminates else proceed to next step.

Level 3 Feature Extraction

Level 3 features include detecting pores and ridge contours.

Pores are of two types – open pores and closed pores. A closed pore is entirely enclosed by a ridge, while an open pore intersects with the valley lying between the two ridges. Figure 4 shows open pores in white and closed pores in black.

The ridge contour is defined as edges of a ridge. Ridge contour is used directly as a spatial attribute and the matching is based on the spatial distance between points on the ridge contours.

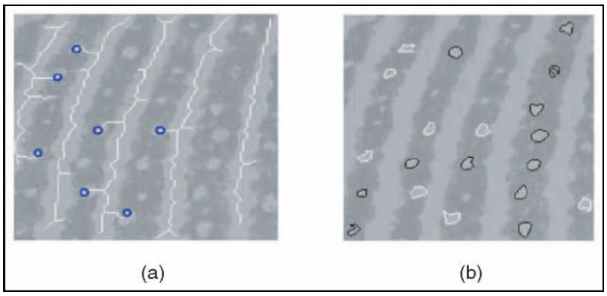

Fig. 4. Open pores (white) and closed pores (black)

IV. Working Of Touchless 3D Fingerprints Technology

Touchless 3D fingerprint technology was founded in 2003 and was based on focusing development of new and unique fingerprint sensor. In this technology finger imaging is used instead of finger printing. It makes use of complex illumination process. Touchless fingerprinting is essentially a remote sensing technique used to capture the ridge-valley pattern. While it is not a completely new approach to acquire fingerprints, it did not generate a sufficient interest in the market, in spite of its advantages with respect to the contact-based technology. The main reason is the cost of this technology. In fact, in order to keep the production costs of these devices low, their manufacturers often use only one camera. This result in fingerprint images with less usable area, due to the curvature of the finger, compared to the contact-based approach. In a touchless fingerprint image, the apparent frequency of the ridge-valley pattern increases from the center towards the side until ridges and valleys become undistinguishable. Hence, multiple cameras must be used as shown in the figure 5.

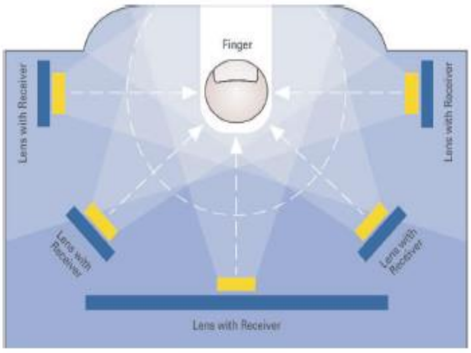

Fig. 5. Fingerprint acquisition using a set of cameras surrounding a finger

It offers superior image quality. There is no chance of failure to enroll. It is quite capable to handle critical fingers. It is least affected by finger condition. Full-3D provides almost nail-to-nail images. It covers larger areas than touch sensors. More indications are available than just fingerprints. It is based on build-in guidance and self-learning experience. Moreover, sensor misuse is avoided [9].

V. 2D Vs 3D Fingerprints Recognition Technology

Traditional fingerprint acquisition is performed in 2D using contact methods which have evolved over the last century. In order to avail the benefits of higher user convenience, hygiene, and improved accuracy, contactless 3D fingerprint recognition techniques have recently been introduced. Multiple cameras are applied to systematically acquire multiple views of the presented finger. Major obstacle in the path of emerging 3D fingerprint technologies to replace the conventional 2D fingerprint system is their immensity and high cost, which mainly results from the nature of imaging technologies employed for the 3D fingerprint reconstruction.

2D synthetic fingerprint generators make use of mathematical or statistical models to output fingerprints. There is a need to conduct evaluation on millions of known fingerprint images to test the performance of a finger scan system. But because of limited test data availability, these performance estimates are also limited. In addition, the 2D synthetic fingerprint generators are not enough for testing touch less fingerprint sensing technologies, which has been used more and more as alternatives to the traditional touch based fingerprint capture systems [9].

In many applications that require high precision fingerprints, limitations are imposed upon the current fingerprint capture technologies, including:

- mandatory maintenance of a clean sensor or prism surface;
- uncontrollable and non-uniform pressure of the finger on the device;
- change in the finger ridge structure which may be permanent or semi-permanent due to injuries or heavy manual labors;
- left over’s from the previous fingerprint capture;
- data distortion under different illumination, environmental, and finger skin conditions; and
- Additional scanning time and motion artifacts involved in technologies that require finger rolling.

The majority of these limitations arise due to the physical contact of the finger surface with the sensor plate, or the nonlinear distortion introduced by the 3D-to-2D mapping during image acquisition

To overcome the problems of 2D technology, a team of computer scientists from Michigan State University (MSU) led by Anil Jain, an alumnus from Indian Institute of Technology (IIT) Kanpur have developed the world's first 3D-printed fingerprint. Such 3D fingerprints could help both sensor manufacturers and algorithm developers improve the hardware and software of fingerprint matching systems. All this could ultimately lead to improvements in security. A technique was developed that takes a two-dimensional image of a fingerprint and maps it to a 3D finger surface. The 3D finger surface, complete with all the ridges and valleys that make up the human fingerprint, is made using a 3D printer. It creates a fingerprint phantom [9].

VI. Biometrics In India

In our country India, even today old fashioned system is used for security purposes by different security agencies like CBI (Central Bureau of Investigation), RAW (Research and Analysis Wing). Our country is continuously facing threats from terrorist organizations like cross border terrorism, drug trafficking, illegal immigrants entering into our country especially from neighboring countries. But now Indian security agencies have realized that adapting to modern biometric systems is a compulsion today. As the biometric technology advances, the acceptance rate of biometric recognition technologies will also grow with time.

There are some latest examples in this field. Indian government has planned to install such ATM machines in the rural areas where user can perform a transaction by pressing his/her thumb on a sensor and pressing appropriate color-coded button for desired denominations to get the cash. Another example is of the car seat which is developed by AIIT (Advanced Institute of Industrial Technology” which can identify the person sitting on it. The success rate achieved is 98 percent.

Social sector schemes in India are also planning to use biometric devices for ensuring proper identification of those who are entitled to their payments. Government MNREGA scheme suffered a serious setback because of the problem of ghost workers and of local leaderships appropriating the job cards. But with the use of biometric and GPS enabled ICT devices on work sites, it will become possible to conduct biometric attendance of the workers.

Billions of people in India have been provided unique digital identity using biometric systems via UIDAI initiative of Indian government. Often it is noticed that just because of failure to provide appropriate documents, poor people are forced to pay bribe for obtaining benefits. The foolproof biometric systems like retina scan, face scan and fingerprinting that are being used for creation of unique UID Cards will make it possible for many more Indians to gain easy access to all kinds of benefits. The UID could eventually turn into the world’s largest biometric database [9].

VII. Vulnerability To Attacks

In some biometrics based authentication system, there are five points vulnerable to attacks [8, 9] (Fig. 5).

- 1st attack point – Fake biometric sensor can be used like fake finger or mask.
- 2nd attack point – Resubmitting previously stored digitized biometric signals.
- 3rd attack point – Overriding the feature extractor.
- 4th attack point – Corrupting the matcher so that it produces preselected matched scores.
- 5th attack point – Overriding the final match decision.

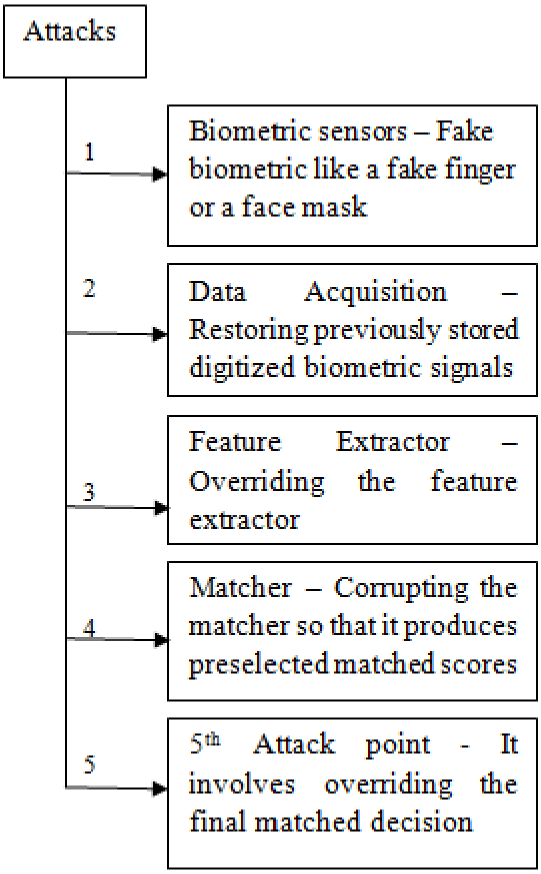
Attacks
1
Biometric sensors – Fake biometric like a fake finger or a face mask
2
Data Acquisition – Restoring previously stored digitized biometric signals
3
Feature Extractor – Overriding the feature extractor
4
Matcher – Corrupting the matcher so that it produces preselected matched scores
5
5th Attack point - It involves overriding the final matched decision

Fig. 6 Attacks involved in biometric systems

VIII. 3D Fingerprint Recognition Techniques

Identifying humans automatically is a vital part of infrastructure required to identify humans for different commercial and law enforcement applications. Out of many biometric features available today, fingerprints are most accepted one because of its properties and requirements. Working of traditional fingerprint scans involved placing and pressing of fingers against a hard surface which may be glass or silicon, and often results in partial or degraded quality images. There are several reasons like moisture, finger dirt, finger sweat, finger slips and smear or sensor noise which may result in poor capturing. The alternative to all these problems is contactless fingerprint systems which provide hygienic solutions to such problems and can cope-up with the residue of previous fingerprint impressions which can also be a potential security threat.

Contactless fingerprint identification is primarily based on acquiring fingerprints without any physical contact between the finger and sensor surface. The image quality from such contactless 2D fingerprint sensors does not match the quality of most popular FTIR (frustrated total internal reflection) sensors and its physical size is larger than that of solid-state sensors. Lack of popularity of such contactless 2D fingerprint systems is because of their high cost as compared to the low-cost touch-based fingerprint devices commonly available today.

High user convenience, hygiene, and improved accuracy can be obtained by contactless 3D fingerprint recognition techniques which have recently been introduced. The technique uses multiple cameras to systematically acquire multiple views of the presented finger. [6, 7, 9].

IX. Advantages Of 3D Fingerprint Recognition

The advantages of 3D fingerprint recognition are summarized in the table below.

Feature	Benefit
3-D data	Better image quality result in better matching rates. The potential exists to identify new matching features based on the 3D data.
Non-contact	As there is no contact of the print with the scanner, better image quality can be achieved. Provides extremely consistent prints. More hygienic. No cleaning between uses.
Speed of capture	Superior throughput. Allows for use in high volume environments.
Lower failure to acquire rates	3D imaging technique is not affected by dry skin, sweat, oil or skin color.
Better treatment of damaged or worn prints	3D techniques have the advantage of capturing the surface independent of how smooth it is leading to better image quality for fine or worn prints.
Anti-spoofing	System is harder to fool by common misleading means including latex overlays.
Automated	The device can function independently of an operator. Quality of the print no longer tied to the skill of operator manipulating the subject's hand.
Backwards compatible	3D prints are flattened to produce 2D fingerprints consistent and compatible with existing databases and matching programs.
Segmentation	Enhanced segmentation for multi-finger capture.

X. CONCLUSION

Each biometric has its own pros and cons. Biometric authentication systems have become the standard for access control because of their security, speed competence and ease of use. To judge the acceptance and rejection rates of a biometric in any particular application, one has to consider factors like scalability, user privacy and system security. Unlike 2D image, a 3D model can identify a person much more easily and effectively irrespective of position of his/her head or even if camera is not perfectly aligned with the subject. It can be concluded that 3D fingerprint recognition technology will prove as a major boon in the field of biometrics [9].

REFERENCES

[1] www.cse.iitk.ac.in/users/biometrics/pages/what_is_biom_more.htm

[2] www.biometricidentitycards.info/articles/biometric_identity_cards.html

[3] M. D'Acuntoa , G. Pierib, M. Righib, and O. Salvettib, A Methodological Approach for Combining Super Resolution and Pattern Recognition to Image Identification1, Springer, Pattern Recognition and Image Analysis, Vol. 24, No. 2, pp. 209-217, 2014.

[4] Ravi Subban and Dattatreya P. Mankame, A Study of Biometric Approach Using Fingerprint Recognition, Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.

[5] Neeraj Bhargava, Ritu Bhargava, Manish Mathuria, Minaxi Cotia, Fingerprint Matching using Ridge-End and Bifurcation Points, International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012).

[6] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490310/

[7] www.iaeng.org/publication/WCECS2012/WCECS2012_pp908-913.pdf

[8] danishbiometrics.files.wordpress.com/2009/08/biometric.pdf

[9] Gagandeep Jagdev et. al., "A Study on working of 2D fingerprint recognition system and how contactless 3D Fingerprint recognition systems assures greater perfection in human identification", ICACCT-2014,ISBN-978-93-84935-00-9