© 2018 IJSRST | Volume 4 | Issue 3 | Print ISSN : 2395-6011 | Online ISSN: 2395-602X

National Conference on Advances in Engineering and Applied Science (NCAEAS)
29th January 2018
Organized by : Anjuman College of Engineering and Technology (ACET) Nagpur, Maharashtra, India, In association with
International Journal of Scientific Research in Science and Technology

Overview of Fingerprint Identification

Dr. LeenaGahane[1] , Rashida Ali[2], Aparna Sharma[2]

[1]Professor Department OF Physics ,Anjuman College Of Engineering and Technology , Sadar , Nagpur, Maharas htra, India

[2]BE.II Sem ,Anjuman College Of Engineering and Technology , Sadar , Nagpur, Maharashtra, India

ABSTRACT

This article is an overview of a current research Based on fingerprint recognition system. Here, we have highlighted on the previous studies of fingerprint recognition system and its review in the conceptual &Structur of fingerprint recognition .The basic fingerprint Recognition system consist of four stages: firstly ,the sensor Which is used for enrolment &recognition to capture the biometric data .Secondly ,the pre-processing stage which is used to remove unwanted data and increase the clarity of ridge structure by using enhancement technique. Thirdly, feature extraction stages which take the input from output of the pre-processing stage to extract the fingerprint feature. Fourthly,the matching stage is to compare the acquired feature with the template in the database.

Finally the data base which stores the feature for the matching stages .The current trend of fingerprint sensing and identification algorithms are presented in detail in order to show how fingerprint based system works .These include actual example of fingerprint based personal identification system ,large scale fingerprint identification system (AFIS) International activities on standardization and performance evaluation and a "Fingerprint User Interface(FPUI),which is a new type of application of this technology used to enhance human -machine interaction . Also we put in to few suggestions for the errors which occurs in some of the cases due to defects in finger ridges. Also suggesting a multi sensor device.

Keywords: Biometric, Fingerprint, Security, Identification.

I. INTRODUCTION

Along of various biometrics techniques, In the past few decades, human-beings have been addicted to various technologies such as captured photos, scanned signatures, bar code systems, verification Id & so on. Also, Biometrics is oneof the applications in Image processing which refers to technologies that used physiological or behavioural characteristics of human body for the user authentication. The biometric authentication system based on two modes:

II. ENROLMENT AND RECOGNITION

In the enrolment mode, the biometric data is acquired from the sensor and stored in a database along with the person's identity for the recognition. In the recognition mode, the biometric data is re-

acquired from the sensor and compared to the stored data to determine the user identity.

Biometric recognition based on uniqueness and permanence. The uniqueness means that there is no similarity of feature between two different biometrics data. For example, there are no two humans having the same fingerprint feature even if they are twins. And when the features of biometrics do not change over the lifetime or aging, it is called permanence. Biometrics can have physiological or behavioural characteristics. The physiological characteristics are included in the physical part of body such as (fingerprint, palm print, iris, face, DNA, hand geometry, retina... etc). The behavioural characteristics are based on transaction taken by a person such as (Voice recognition, keystroke-scan, and signature-scan). Any biometrics system including two phases first phase is enrolment phase and second is recognition phase. The recognition phase divided to two things which is verification and identification. During the enrolment phase the biometrics data are captured and generate digital image then Pre-processing apply to digital image for removing unwanted data and apply the post-processing than store this data in database. In the case of identification process the fingerprint acquired from one person is compared with all the fingerprints which store in database. Also it is known as (1:N) matching. it is used in the process of seeking the criminals. In the verification process the person's fingerprint is verified from the database by using matching algorithms. Also it is known as (1:1) Matching. It is the comparison of a claimant fingerprint against enroll fingerprint, initially the person enrolls his/her fingerprint into verification system, and the result show whether the fingerprint which take from the user is matching with the fingerprint store as a template in database or not match.

III. FINGERPRINT

A friction ridge is a raised portion of the epidermis on the palmar (palm and fingers) or plantar (sole and toes) skin, consisting of one or more connected ridge units of friction ridge skin.These ridges are sometimes known as "dermal ridges" or "dermal papillae".Fingerprint identification (sometimes referred to as (dactyloscopy) is the process of comparing questioned and known friction skin ridge impressions (see Minutiae) from fingers, palms,and toes to determine if the impressions are from the same finger (or palm, toe, etc.).The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike (never identical in every detail), even two impressions recorded immediately after each other.

Fingerprint identification (also referred to as individualization) occurs when an expert (or an expert computer system operating under threshold scoring rules) determines that two friction ridge impressions originated from the same finger or palm (or toe, sole) to the exclusion of all others.

IV. FUNDAMENTAL STEPS OF FINGERPRINT

INPUT FINGERPRINT

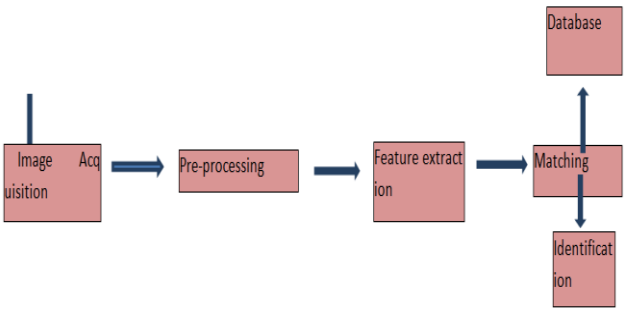

Figure 1

- **IMAGE ACQUISITION STAGE:**The Image Acquisition stage is the process to obtain images by different ways. There are two ways to capture fingerprint image; online and offline. In the online fingerprint identification the optical fingerprint reader is used to capture the image of fingerprint. The size of fingerprint image will be 260* 300 pixels. The offline fingerprint identification is obtained by ink in the area of finger and then put a sheet of white paper on the fingerprint and finally scans the paper to get a digital image.
- **IMAGE PRE-PROCESSING STAGE:**The pre-processing stage is the process of removing unwanted data in the fingerprint image such as noise, reflection .etc. The fingerprint image pre-processing is used to increase the clarity of ridge structure. There are many steps for doing this,such as Image Segmentation, Binarization, Elimination of noise, smoothing and thinning which are used to enhance the fingerprint image. In [3], theGaussian filter, Short Time Fourier Transform analysis are adopted to enhance fingerprint image quality. In some cases thebinarized of fingerprint image contains some of false minutiae .In [4] . A detailed pre-processing is mentioned to remove false minutiae.
- **FEATURE EXTRACTION STAGE:**The feature extraction process of fingerprint image applied on the output of pre-processing stage. The process of feature extraction depends on set of algorithms. A fingerprint feature extraction program is to locate, measure and encode ridge endings and bifurcations in the fingerprint. There are various methods for extracting the features from the fingerprint image. The famous methods is minutiae extraction algorithm which is find the minutiae points and map their relative placement on the fingerprint .There are two types of minutiae points; Ridge ending and Ridge bifurcation. Inthey are used an advanced method for extract feature from fingerprint whichdone by extract minutiae directly from original gray-level images without use binarization and thinning and they usegabor filter methods to extract features from fingerprint.
- **MATCHING STAGE**: The matching stage is the process to compare the acquired feature with the template in the database. In other words the process of matching stage is to calculate the degree of similarity between the input test image (for user when he wants to prove his/her identity) and a training image from database (the template which created at the time of enrolment). Matching can be done in three methods: hierarchical approach, classification approach and Coding approaches. The hierarchical approach is increases matching speed at the cost of accuracy.

V. TYPES OF FINGERPRINT SCANNER

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezoresistive, ultrasonic, piezoelectric, MEMS

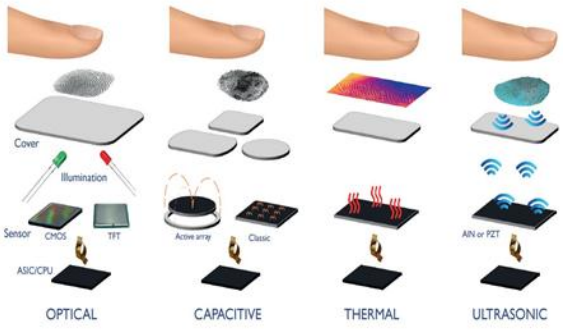

Figure 2

1. **Optical readers** are the most common type of fi

ngerprint readers. The type of sensor in an optical r eader is a digital camera that acquires a visual image of the fingerprint. Advantages are that optical read ers start at very cheap prices. Disadvantages are that readings are impacted by dirty or marked fingers, a nd this type of fingerprint reader is easier to fool th an others.

2. Capacitive readers, also referred to as CMOS rea ders, do not read the fingerprint using light. Instead a CMOS reader uses capacitors and thus electrical c urrent to form an image of the fingerprint. CMOS r eaders are more expensive than optical readers, alth ough they still come relatively cheap with prices sta rting well below 100 euro's. An important advantage of capacitive readers over optical readers is that a capacitive reader requires a real fingerprint shape rather than only a visual imag e. This makes CMOS readers harder to trick.

3. Ultrasound readers are the most recent type of f ingerprint readers, they use high frequency sound waves to penetrate the epidermal (outer) layer of th e skin. They read the fingerprint on the dermal skin layer, which eliminates the need for a clean, unscar red surface. All other types of fingerprint readers ac quire an image of the outer surface, thus requiring hands to be cleaned and free of scars before read-ou t. This type of fingerprint reader is far more expensi ve than the first two, however due to their accuracy and the fact that they are difficult to fool the ultras ound readers are already very popular.

4. Thermal readers sense, on a contact surface, the difference of temperature in between fingerprint ri dges and valleys. Thermal fingerprint readers have a number of disadvantages such as higher power co nsumption and a performance that depends on the environment temperature.

FINGERPRINT PATTERNS: Identifying the Differe nt Types Easily

Every person in the world possesses a unique set of fingerprints. However, the differences between som e can be very subtle. By studying the arrangement, shape, size, and number of lines in each fingerprint, experts have been able to classify them into unique patterns, which are used for identification. A person's weight, eye color, and hair color can cha nge or be changed, but his fingerprints cannot be al tered. They are unique to each individual, and can be differentiated and identified based on certain dis tinctive patterns made by the ridges. The following are some of the commonly used fingerprint patterns that have been identified and used in the process of fingerprinting.

There are basically three main forms of patterns tha t are made by the ridges of fingerprints.

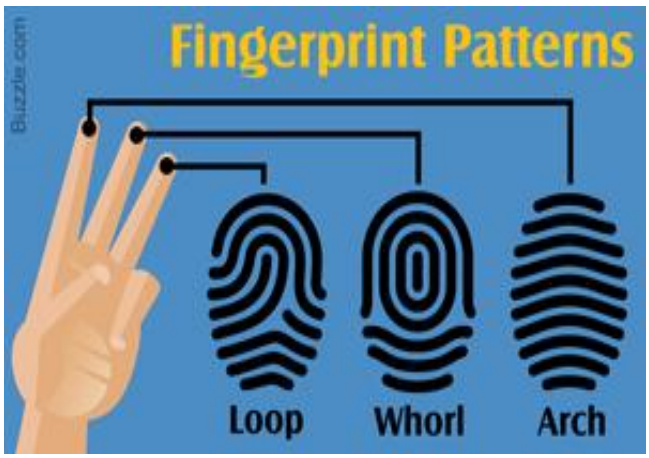

Figure 3

- **Loops**:
  Loops make up almost 70 percent of fingerprint patterns. They originate from one side of the fin ger, curve around or upward, before exiting out the other side. A loop pattern always comprises one delta, which is roughly a triangular formati on in the pattern.
- **Arches:**
  Arches are encountered in only 5 percent of the patterns, and comprise lines that slope upward

and then down, similar to the outline of a small hill. There is generally no delta.

- **Whorls:**
  Whorls constitute around 25% percent of all patterns. They are circular or spiral patterns, similar to eddies. A pattern that contains 2 or more deltas will always be a whorl pattern.

There are many subtypes of these three basic finger print patterns Applications of fingerprint recognition

- Forensic scientist have used fingerprints in criminal investigation as a means of identification for centuries to find the criminal.
- A FINGERPRINT USER INTERFACEis a user interface that employs fingerprint recognition. Using the FUI, a user can specify different tasks by using different fingers for operating an input device. Since all fingers of a single person have unique fingerprint patterns, the finger used for the operation can be identified through the matching of the fingerprint patterns.
- Fingerprint is also used to identify a person for their properties {legal house paper, identity paper,etc.}. It was the old style of using fingerprint stamp insist of signature the people who were illiterate used to give their fingerprint stamp. It was moresecure than the signature because signature can be copied but fingerprint identification is unique for single person
- Nowadays, fingerprint identification is mostly used in the android phones in the security password for screen look, application lock, etc.
- It can be also used in the home security system by putting fingerprint system on the main door.
- The is widely used for the identification of a person that he/she belongs to the nation (country, city ,town.) that is .we can sayadhaarcard.
- Voter registrations and identification
- Border control via passport verification by using biological parameters
- Population census by using biometric
- Drivers license and professional ID card verification with biometric identities

Advantages and Disadvantages

As with all biometric system there are a number of advantages and disadvantages associated with using fingerprintscanning to confirm an individual's identity. Often weighingthe various benefits and costs associated with particularbiometric methods greatly affects which systems areimplemented by an organisation and in some cases,whetherbiometric systems are adopted at all. In the case of fingerprint scanning,the relative advantages and disadvantages arereasonably straightforward.

The advantages include

Acceptance

As most people are familiar with the use of fingerprinting for identification purpose it is generallyaccepted as a technology. Most people understand itsapplicability to access control.

Accuracy

By and large fingerprint technology is accurate.There is a small chance of rejection of a legitimate print i.e. there is a chance of accepting a false print or a chance of rejecting a legitimate print. The chances of accepting a falseprint are very low.

Ease of use

Very little time is required for enrolment witha fingerprint scanning system. Unlike other biometric devices such as retina scanners,fingerprint scanners do notrequire concentrated effort on the part of the user. Accordingly one could consider fingerprint scanning to berelatively nonintrusive.

Installation

Changes in technology have made fingerprintscann ers relatively easy to install and inexpensive. Mostfi ngerprint scanners are now very small and portable. Plug-and-play technologies have made installation very easy.In many cases,the scanning device has be en incorporatedintokeyboards,mouse buttons and e ven notebook computers.

Training

Due to the intuitive nature of scanningfingerprints, such devices require no training to use and little tra ining to support.

Uniqueness

As noted previously,fingerprints are a unique identi fier specific to the individual.

Security

Fingerprints cannot be lost or stolen,andare difficul t to reproduce. Furthermore,storingfingerprinttemp lates as statistical algorithms rather than completec opies ensures that the ability to reproduce these uni queidentifiers is significantly reduced.

The disadvantages include:

Acceptance

Although also an advantage,user acceptance isnot g uaranteed. Fingerprint scanning crosses the fine lin ebetween the impersonal and nonintrusive nature o f passwordsand personal identification numbers (PI Ns),and utilising partof an individual's body to identify hi m/her. As will bed is cussed some people view this as a n invasion of privacyor worse.

Injury

Injury whether temporary or permanent,cani nterfere with the scanning process. In some casesre enrolment is required. For example,bandaging a fin ger fora short period of time can impact an individu al if fingerprintscanning is used in a wide variety of situations. Something assimple as a burn to the iden tifying finger could prevent use of an automatic teller machine (ATM).

Others

In 2002, a Japanese cryptographer demonstrated ho w fingerprint recognition devices can be fooled 4 o ut of 5 times using a combination of low cunning, c heap kitchen supplies and a digital camera.

Conclusion

Identification can be done via various types of Biom etric that are Fingerprint, iris, hand Geometry, Gest ures, Signature etc. Within biometric methods, auto matics Signature Recognition are an important rese arch area due to the social, legal and wider acceptan ce of handwritten signature as means of identificati on. Offline Signature recognition system is used in t he proposed model. Recognition decision is usually based on local or global features extracted from sign ature under processing. Excellent recognition result s can be achieved by comparing the robust model of the query signature with all the user models using appropriate classifier. After the authentication of th e signature, invisible watermark fingerprint recogni sation is proceed by going through enhancement te chniques which will improve the quality of the fing erprint, reduce the enhancement errors. Orientatio n point is extracted either by NLMS/INLMS which will help in matching accuracy by getting the optim al point.Then matching of both input image and out put image will be carried out if the images are matc hed. Then it is authenticated otherwise authenticati on cannot be done. Hence High Recognition rate is first requirement of an effective signature recogniti on system which depends upon the techniques adop ted in training and classification of signatures. It als o depends on the extracted features. Among various stochastic approaches, HMMs have proven very eff ective in modelling both dynamic and static signals.

VI. REFERENCES

[1]. Jyotika Chopra and 2 Dr. P.C. Upadhyay 1 Research Scholar, 2 Associate Professor SLIET, Longowal, Punjab, India

[2]. D.maltoni, et al "Handbook of fingerprint recognition" springer 2003

[3]. N.Ratha,etal."Automatic Fingerprint Recognition System'

[4]. NaliniRatha and Ruud Bolle, Automatic Fingerprint Recognition Systems (Springer: New York, 2004).

[5]. FBI IAFIS "Integrated Automated Fingerprint Identification System: What is it" 30 June 2005

[6]. A.monden and S. Yoshimoto,"Fingerprint identification for security application"oct 2003

[7]. K.uchid, Fingerprint identification for enchanced user interface "July 2011