ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 4, April 2013

A SURVEY ON BIOMETRIC RECOGNITION TECHNIQUES AND ALGORITHMS

K.Rajasri, S.Sathiyadevi, S.Tamilarasi

Abstract— A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of establishing the identity is to ensure that only a legitimate user, and not anyone else, accesses the rendered services. Examples of such applications include secure access to buildings, airports, computer systems, cellular phones and ATM machines. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Biometrics allows us to confirm or establish an individual's identity based on who she is, rather than by what she possesses (e.g., an ID card) or what she knows (e.g., a password). Current biometric systems make use of identifiers such as fingerprints, hand geometry, iris, face and voice to establish an identity. Biometric systems also introduce an aspect of user convenience. For example, they alleviate the need for a user to remember multiple passwords associated with different applications. A biometric system that uses a single biometric trait for recognition has to contend with problems related to non-universality of the trait, spoof attacks, limited degrees of freedom, large intra-class variability, and noisy data. Some of these problems can be addressed by integrating the evidence presented by multiple biometric traits of a user (e.g., face and iris). Such systems, known as multimodal biometric systems, demonstrate substantial improvement in recognition performance. In this manuscript, the presentation on various applications of biometrics, challenges associated in designing biometric systems, individuality of biometric identifiers, and fusion strategies available to implement a biometric system.

***Index Terms*—Biometrics, Biometric Recognition, Methods, Techniques.**

I. INTRODUCTION

Biometric recognition, or biometrics, refers to the automatic identification of a person based on his/her anatomical (e.g., fingerprint, iris) or behavioral (e.g., signature) characteristics or traits. This method of identification offers several advantages over traditional methods involving ID cards (tokens) or PIN numbers (passwords) for various reasons: (i) the person to be identified is required to be physically present at the point-of-identification; (ii) identification based on biometric techniques obviates the need to remember a password or carry a token. With the increased integration of computers and Internet into our everyday lives, it is necessary to protect sensitive and personal data. By replacing PINs (or using biometrics in addition to PINs), biometric techniques can potentially prevent unauthorized access to ATMs, cellular phones, laptops, and computer networks. Unlike biometric traits, PINs or passwords may be forgotten, and credentials like passports and driver's licenses may be forged, stolen, or lost. As a result, biometric systems are being deployed to enhance security and reduce financial fraud. Various biometric traits are being used for real-time recognition, the most popular being face, iris and fingerprint. However, there are biometric systems that are based on retinal scan, voice, signature and hand geometry. In some applications, more than one biometric trait is used to attain higher security and to handle failure to enroll situations for some users. Such systems are called multimodal biometric systems.

A biometric system is essentially a pattern recognition system which recognizes a user by determining the authenticity of a specific anatomical or behavioral characteristic possessed by the user. Several important issues must be considered in designing a practical biometric system. First, a user must be enrolled in the system so that his biometric template or reference can be captured. This template is securely stored in a central database or a smart card issued to the user. The template is used for matching when an individual needs to be identified. Depending on the context, a biometric system can operate either in verification (authentication) or an identification mode.

A. Verification vs. Identification:

There are two different ways to recognize a person: verification and identification. Verification (*Am I who I claim I am?*) involves confirming or denying a person's *claimed identity*. On the other hand, in identification, the system has to recognize a person (*Who am I?*) from a list of N users in the template database. Identification is a more challenging problem because it involves 1:N matching compared to 1:1 matching for verification.

B. Applications:

While biometric systems, particularly automatic fingerprint identification systems (AFIS), has been widely used in forensics for criminal identification, progress in biometric sensors and matching algorithms have led to the

***Mrs. K. Rajasri**, Assistant Professor, Department of Computer Science, Christ College of Engineering and Technology, Pondicherry University Pondicherry, India,*

***S. Sathiyadevi**, Department of Computer Science, Christ College of Engineering and Technology, Pondicherry University, Pondicherry, India,*

***Mrs. S. Tamilarasi**, Department of Computer Science, Christ College of Engineering and Technology, Pondicherry University, Pondicherry, India,*

deployment of biometric authentication in a large number of civilian and government applications. Biometrics is being used for physical access control, computer log-in, welfare disbursement, international border crossing and national ID cards. It can be used to verify a customer during transactions conducted via telephone and Internet (electronic commerce and electronic banking). In automobiles, biometrics is being adopted to replace keys for keyless entry and keyless ignition. Due to increased security threats, the ICAO (International Civil Aviation Organization) has approved the use of e-passports (passports with an embedded chip containing the holder's facial image and other traits) [1].

II. A Survey of various biometric recognition

A number of biometric characteristics exist and are in use in various applications (see Figure 3). Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is "optimal". The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction of the commonly used biometrics is given below:

A. *Fingerprint Recognition*

Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high [25]. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about US $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

B. *Iris Recognition*

The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective[3].

C. *Face Recognition*

Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled "mug-shot" verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either (i) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or (ii) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable [34], they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence [29]. In order that a facial recognition system works well in practice, it should automatically (i) detect whether a face is present in the acquired image; (ii) locate the face if there is one; and (iii) recognize the face from a general viewpoint (i.e., from any pose). • Facial, hand, and hand vein infrared thermogram: The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infrared camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is non-invasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infrared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms [2].

D. *DNA Recognition*

Deoxyribo Nucleic Acid (DNA) is the one-dimensional ultimate unique code for one's individuality - except for the fact that identical twins have identical DNA patterns. It is,

however, currently used mostly in the context of forensic applications for person recognition. Three issues limit the utility of this biometrics for other applications:

1 Contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose;

2 Automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involving an expert's skills and is not geared for on-line non-invasive recognition;

Privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may result in discrimination, e.g., in hiring practices.

E. Hand and finger geometry

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).

F. Palm print Recognition

The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and as a result, palm prints are expected to be even more distinctive than the fingerprints. Since palm print scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper [32]. Finally, when using a high resolution palm print scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system[2].

G. Retinal scan Recognition

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these factors adversely affect the public acceptability of retinal biometric. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan based biometrics.

H. Signature Recognition

The way a person signs her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.

I. Voice Recognition

Voice is a combination of physiological and behavioral biometrics. The features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioral part of the speech of a person changes over time due to age, medical conditions (such as common cold), emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel [1].

III. ALGORITHMS FOR SOME BIOMETRIC RECOGNITIONS

A. Face Recognition

Some approaches define a face recognition system as a three step process. They are:

- Face Detection
- Feature Extraction
- Feature Recognition

From this point of view, the Face Detection and Feature Extraction phases could run simultaneously. Face detection is defined as the process of extracting faces from scenes. So, the system positively identifies a certain image region as a face. This procedure has many applications like face tracking, pose estimation or compression. The next step -feature extraction- involves obtaining relevant facial features from the data. These features could be certain face regions, variations, angles or measures, which can be human relevant (e.g. eyes spacing) or not. This phase has other applications like facial feature tracking or emotion recognition. Finally, the system does recognize the face. In an identification task, the system would report an identity from a database. This phase involves a comparison method, a classification algorithm and an accuracy measure. This phase uses methods common to many other areas which also do some classification process -sound engineering. These phases can be merged, or new ones could be added. Therefore, we could find many different engineering approaches to face recognition problem. Face detection and recognition could be performed in tandem, or proceed to an expression analysis before normalizing the face.

B. Algorithm for Finger print recognition

A fingerprint is made of a series of ridges and furrows on the surface of the finger. Everyone have unique, immutable fingerprints [3]. Pattern of ridges and furrows as well as minutiae can be used to determine the uniqueness of fingerprint. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint is preprocessed to remove the noise and irrelevant information. Pre-processing consist of the following steps.

- Image Normalization is a process to improve the quality of image by eliminating noisy and correcting it by changes the range of pixel intensity values. Here it is performed to remove the gray-level background and effect of sensor noise.

- Binarization is to convert the gray scale image in binary image, so that the intensity of the image has only two values: black, representing the ridges are highlighted with black color and furrows are highlighted with white color. This method transforms a pixel value to 1 if value is larger than intensity value otherwise to 0.

- Marking of minutiae is done by following procedure. For each 3x3 window, if the central is 1 and has only 1 one-value neighbor, then the central pixel is a termination (figure-3), it is marked. At this point the average inter-ridge width D is estimated.

- Spurious minutiae is removed if the distance between a termination and a bifurcation is smaller than D, remove this minutiae. If the distance between two bifurcations is smaller than D, remove this minutia process. If the distance between two terminations is smaller than D, remove this minutiae. Region of Interest (ROI) is used to remove the image area without effective ridges and furrows.

- Once ROI is defined extrema minutiae are suppressed. Finally marked x, y position of minutiae are stored in the file which is further used to transform into cancelable fingerprint.

- Then the method of transformation of extracted minutiae points into transformed points and generation of cancelable fingerprint will be occurred.

- After the above process matching of fingerprint from cancellable template with fingerprint in database will occurred.

- If the matching is true, authentication passed, otherwise failed.

C. Iris Recognition

Iris recognition is one of the biometric systems for gathering unique details of the individual. In most trustworthy biometrics Iris recognition is considered to be a reliable technique with low false rejection and false acceptance rates. Four modules of iris recognition involved are:

1. Morphological Operators

The morphological operators are used to extract the pupil region apart from the other regions of the eye.

The different morphological operators used are:

Morphological Edge Edges are detected by convolving the image with a simple convolution kernel devised by Sobel and Feldman.

Morphological Dilate The morphological dilate applies the dilate operation rule to expand the boundary of the image.

Morphological Erosion The morphological erosion contracts the boundary.

Morphological Fill Since non-default connectivity is specified, the morphological fill, fills hole pixels on the outer edge of an image that are not connected to the background

Morphological Clear Border The pixels that are lighter than the surroundings and are connected to the image border are suppressed by using morphological clear border. It uses the morphological reconstruction. In reconstruction the input is mask image.

2. Centre and Inner Boundary Localization

The gray point histogram is analyzed and designed.

3. Outer Boundary Localization

It is applied for detecting the iris outer boundary later than the pupil‘s inner boundary is predicted.

4. Sectoring

After the iris boundaries are segmented using the three

stages (Morphological operations, Inner boundary and Outer boundary detection), the iris regions are sectored before normalization.

5. Normalization

Iris Normalization is the conversion from polar to rectangular co-ordinates.

6. Iris code Generation and Indexing

The normalized iris images are evenly cropped into blocks, and count the number of corners in each block. Then, also crop the mask off code into blocks, and if there exist masked regions in the block, a flag will record this block as 0, and other blocks are marked as 1 [3].

IV. CONCLUSION

The Biometric recognition Systems are the automatic recognition systems which uses the physical characteristics of a person like finger print, hand geometry, face , voice and iris. These systems overcomes the drawbacks of the traditional computer based security systems which are used at the places like ATM, passport, payroll, drivers' licenses, credit cards, access control, smart cards, PIN, government offices and network security. The biometric recognition systems have been proved to be accurate and very effective in various applications. The biometric features can be easily acquired and measured for the processing only in the presence of a person. Hence these systems are proved highly confidential computer based security systems.

REFERENCES

[1] Kresimir Delac, Mislav Grgic "A Survey on Biometric methods," *IEEE Conf. on Electronics in marine*, June 2004.

[2] Sulochana sonkamble, dr. ravindra thool, balwant sonkamble "survey of biometric recognition systems and their applications" *Journal of Theoretical and Applied Information Technology*, 2005-2010.

[3] K.Rajasri, S.Sathiyadevi, S.Tamilarasi " new algorithm and indexing to improve the accuracy and speed in iris recognition", International Journal of Engineering Research and Development, 2012.

Mrs. K. Rajasri received the B.Tech (Information Technology) and M.Tech (Information Security) degrees in computer science and Engineering from Pondicherry Engineering College affiliated to Pondicherry University, Pondicherry. She is Assistant Professor at the Christ College of Engineering And Technology Affiliated To Pondicherry University, Pondicherry She published her manuscript in reputed journals and her research towards on Network security.

Ms. S. Sathiyadevi Received Post Graduation MCA in Computer Science And Applications From Rajiv Gandhi College Of Engineering And Technology Affiliated To Pondicherry University, Pondicherry and She is Currently Pursuing M.Tech In Computer Science And Engineering From Christ College Of Engineering And Technology Affiliated To Pondicherry University,Pondicherry. She published her manuscript in reputed journals and interested in Web Security and Network Security.

Mrs. S. Tamilarasi received B.E in computer science and Engineering From Priyadharshini Engineering College affiliated to Anna University,Vellore and She is currently pursuing Masters in Computer science and Engineering from Christ College Of Engineering And Technology Affiliated To Pondicherry University,Pondicherry. She published her manuscript in reputed journals and interested in Web Security and Network Security and pervasive computing.