THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

Biometric Authentication System by Various Techniques

Dr. Manju Mandot
Associate Professor, Department of Computer Science & IT, J.R.N. Rajasthan Vidyapeeth, Udaipur, Rajasthan, India
Sharad Verma
Research Scholar, Department of Computer Science & IT, J.R.N. Rajasthan Vidyapeeth, Udaipur, Rajasthan, India

Abstract:
Biometrics is an evolving technology which is used in various fields like forensics, secured area and security system. Biometric system takes the base for the pattern recognition system that recognize a person with authentication by using different features such as Fingerprint, Retinal Scan, Iris scan, Hand geometry and Face recognition. These are the major biometrics systems. These are used in various applications like ATM, cellular phones, secure access to a building. Biometrics are designed to enhance the security and reduce vulnerability. In this paper different biometrics techniques such as Fingerprint, Iris Scan, Retinal Scan, Face Recognition, Hand Geometry, Voice and Signature are available to implement a biometric system.

Keywords: *Biometrics, biometric recognition, fingerprint, retinal scan, iris scan, hand geometry and face recognition techniques*

1. Introduction to Biometric

Biometrics has been widely used in forensics applications such as criminal identification and prison security. The biometric technology is rapidly evolving and has a very strong potential to be widely adopted in civilian applications such as electronic banking, e-commerce, and access control. Due to a rapid increase in the number and use of electronic transactions, electronic banking and electronic commerce are becoming one of the most important emerging applications of biometrics. These applications include credit card and smart card security, ATM security, cheque cashing and fund transfers, online transactions and web access. The physical access control applications have traditionally used token-based authentication. With the progress in biometric technology, these applications will increasingly use biometrics for authentication. Remote login and data access applications have traditionally used knowledge-based authentication. These applications have already started using biometrics for person 4 authentication. The use of biometrics will become more widespread in coming years as the technology matures and becomes more trust worthy. Other biometric applications include welfare disbursement, immigration checkpoints, national ID, voter and driver registration, and time and attendance.

A biometric system can be operated in two modes:

1. Verification mode
2. Identification mode.

In the verification mode, a biometric system either accepts or rejects a user's claimed identity while a biometric system operating in the identification mode establishes the identity of the user without a claimed identity. Fingerprint identification is a more difficult problem than fingerprint verification because a huge number of comparisons need to be performed in identification. We have focused on a biometric system operating in a verification mode and an indexing scheme (fingerprint classification) that can be used in an identification system. A number of civilian applications operate in verification mode on a regular basis and perform identification only at the time of the user registration to check the integrity of the database (e.g., finding duplicates). For example, in an ATM application, after a user has been registered and issued an ATM card, the acquired fingerprint needs to be matched only with a single template fingerprint stored on the ATM card on each transaction. A typical verification system can be divided into two modules: (*i*) enrollment and (*ii*) verification. The enrollment module scans the fingerprint of a person through a sensing device and then stores a representation (called template) of the fingerprint in the database. The verification module is invoked during the operation phase. The same representation which was used in enrollment phase is extracted from the input fingerprint and matched against the template of the claimed identity to give a "yes/no" answer. On the other hand, an identification system matches the input fingerprint with a large number of fingerprints in the database and as a result, fingerprint classification is effective only in an identification system and is not an issue in a verification system.

A biometric is any unique biological characteristic that can be used to identify a person."Bio" in the name refers to the an account of the series of events making up a person's life physiologically that are measured, while "metrics" refers to the system of measurement related to the quantitative analysis that provides a positive identification of a unique individual. During registration, physical and behavioral samples are captured by either fingerprint scanner or video camera. Biometric authentication requires comparing registered biometric sample against a newly captured biometric sample.

This process generally consists of four-step process: Capture, extraction, Comparison, Match/non-match followed by a Verification and identification. In the 21st century, it seems almost intuitive to think of our bodies as natural identification systems for our unique selves. Biometrics involves using the different parts of the body, such as the fingerprint or the eye, as a password or form of identification. Currently, Federal Bureau of Investigation uses the fingerprints from a crime scene to find a criminal. Biometric authentication or, simply biometrics refers to establishing identity based on the physical and behavioral characteristics (also known as traits or identifiers) of an individual such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. Biometric systems offer several advantages over traditional authentication schemes. They are inherently more reliable than password-based authentication as biometric traits cannot be lost or forgotten (passwords can be lost or forgotten); biometric traits are difficult to copy, share, and distribute (passwords can be announced in hacker websites); and they require the person being authenticated to be present at the time and point of authentication (conniving users can deny that they have shared the password). It is difficult to forge biometrics (it requires more time, money, experience, access privileges) and it is unlikely for a user to repudiate having accessed the digital content using biometrics. Thus, a biometrics-based authentication scheme is a powerful alternative to traditional authentication schemes.

In some instances, biometrics can be used in conjunction with passwords (or tokens) to enhance the security offered by the authentication system. In the context of a DRM system, biometrics can be used 1) to facilitate the entire authentication mechanism, or 2) secure the cryptographic keys that protect a specific multimedia file.

2. Biometric Variance

Password-based authentication systems do not involve any complex pattern recognition techniques (passwords have to match exactly) and, hence, they almost always perform accurately as intended by their system designers. On the otherhand, biometric signals and their representations (e.g., facial image and eigen-coefficients of facial image) of a person vary dramatically depending on the acquisition method, acquisition environment, user's interaction with the acquisition device, and (in some cases) variation in the traits due to various patho-physiological phenomena. Below, we present some of the common reasons for biometric signal/representation variations.

2.1. Inconsistent Presentation

The signal captured by the sensor from a biometric identifier depends upon both the intrinsic biometric identifier characteristic as well as the way the biometric identifier was presented. Thus, an acquired biometric signal is a nondeterministic composition of a physical biometric trait, the user characteristic behavior, and the user interaction facilitated by the acquisition interface. For example, the three-dimensional (3-D) shape of the finger gets mapped onto the two-dimensional (2-D) surface of the sensor surface.

As the finger is not a rigid object and since the process of projecting the finger surface onto the sensor surface is not precisely controlled, different impressions of a finger are related to each other by various transformations. Further, each impression of a finger may possibly depict a different portion of its surface. In case of face acquisition, different acquisitions may represent different poses of the face [Fig. 2(a)]. Hand geometry measurements may be based on different projections of hand on a planar surface. Different iris/retina acquisitions may correspond to different no frontal projections of iris/retina on to the image planes.

2.2. Irreproducible Presentation

Unlike the synthetic identifiers [e.g., radio-frequency identification (RFID)], biometric identifiers represent measurements of a biological trait or behavior. These identifiers are prone to wear-and-tear, accidental injuries, malfunctions, and pathophysiological development. Manual work, accidents, etc., inflict injuries to the finger, there by changing the ridge structure of the finger either permanently or semi permanently [Fig. 2(b)]. Wearing different kinds of jewelry (e.g., rings) may affect hand geometry measurements in an irreproducible way. Facial hair growth (e.g., sideburns and mustache), accidents (e.g., broken nose), attachments (e.g., eyeglasses and jewelry), makeup, swellings, cyst growth, and different hairstyles may all correspond to irreproducible face depictions. Retinal measurements can change in some pathological developments (e.g., diabetic retinopathy). Inebriation results in erratic signatures. The common cold changes a person's voice. All of these phenomena contribute to dramatic variations in the biometric identifier signal captured at different acquisitions.

2.3. Imperfect Signal/Representational Acquisition

The signal acquisition conditions in practical situations are not perfect and cause extraneous variations in the acquired biometric signal. For example, non uniform contact results in poor quality fingerprint acquisition. That is, the ridge structure of a finger would be completely captured only if ridges belonging to the part of the finger being imaged are in complete physical/optical contact with the image acquisition surface and the valleys do not make any contact with the image acquisition surface. However, the dryness of the skin, shallow/worn-out ridges (due to aging/genetics), skin disease, sweat, dirt, and humidity in the air all confound the situation resulting in a nonideal contact situation (Fig. 3). In the case of inked fingerprints, inappropriate inking of the finger often results in

"noisy" low contrast (poor quality) images, which lead to either spurious or missing fingerprint features (i.e., minutiae). Different illuminations cause conspicuous differences in the facial appearance. Backlit illumination may render image acquisition virtually useless in many applications. Depending upon ergonomic conditions, the signature may vary significantly. The channel bandwidth characteristics affect the voice signal. Further, the feature extraction algorithm is imperfect and introduces measurement errors. Various image processing operations might introduce inconsistent biases to perturb feature localization. A particular biometric identifier of two different people can be very similar because of the inherent lack of distinctive information in it or because of the inadequate representation used for the identifier. As a result of these complex variations in the biometric signal/representations, determining whether two presentations of a biometric identifier are the same typically involves complex pattern recognition and decision making.

3. Biometric Techniques

Many biometric system are available in various applications. Biometric means "life measurement". Each human acquire some sole physiological characters to identify a person. There is no biometric is optimal; depending upon the application they were used. A brief introduction of commonly used biometric techniques is given below:

3.1. Fingerprint Recognition

Fingerprint biometric is widely used in various fields for security. Fingerprint identification are used for past many year by matching. A Fingerprint contains patterns of valley and ridges on the surface of finger lips. Even for twins the Fingerprint won't be same. It is probable that two individual having same fingerprint less than one in billion. The cost of this biometric is low and they were embedded in laptops also. The accuracy of current biometric system is adequate for verification. Only one problem in current biometric that it requires large amount of computational resource, when using in identification mode. Finally the fingerprint biometric is not suitable for some factors like aging, environmental or occupation reason (e.g.: manual workers who use had frequently for their work). The main advantages of fingerprint biometrics are easy to use, economy, very high accuracy and small size for template. The disadvantages are change quickly for children, compose mistake with dryness or dirty in fingers and a cut or scar on finger.

3.2. Iris recognition

Iris recognition is an automated method of biometrics identification that uses mathematical path recognition technique. The visual texture of iris is formed during fetal development and becomes stable in first two years itself. Iris recognition is also widely used, it is feasible in large scale. Each iris are different for twins like finger print. It is extremely difficult to change iris pattern and it's easy to detect the artificial iris. For iris scan a specialized camera is required. The complete process will take few seconds only. The main advantages of iris recognition are very high accuracy and verification times takes less than five seconds. The disadvantage of this recognition are cost is high, too much movement of head and use of colour contact lens.

3.3. Face Recognition

A facial recognition is computer application for automatically identify or verify a person from a digital images or a video frame from a video source. One method to proceed by comparing selected facial features from the image and a facial database. Face recognition records the spatial geometry of unique features of the face. This technique is used to identify terrorist and criminal and etc. This is a non-intrusive, cheap technology. Face recognition is a challenging task for the researchers, on one side its applications is used for verification and recognition on other side it is complicated to implement due to all different situation that a human face can be found. Face recognition is including five stages such as extracting the image of individual face, locate image of face, analysis of facial image, comparison and match or no match. Facial recognition ranges from single to multiple background (e.g.: airport). The most common approach for face recognition is based on either the location, shape of facial attributes such as eyebrows, eyes, nose, lips, and their spatial relationships or the overall analysis of face image that represents a face as a weighted combination of number of canonical faces. For best work of facial recognition system in practise, it should automatically

(i) Detect whether face is available in the acquired image.
(ii) Locate the face if there is only one face and,
(iii) Recognize the face.

Facial, hand and hand vein infrared thermogram: the pattern of heat radiation from human body is a characteristic of an individual and can be capture by infrared cameras. But it is difficult to implement in heat emanating environment like room heater and etc. It is expensive and used with thermograms.

3.4. DNA recognition

Deoxyribo nucleic acid (DNA) is the one dimensional unique pattern for one's individuality but in case of identical twins have identical DNA patterns. This technology is mostly used in forensics application for person recognition. DNA recognition has three main issues to limit the utilization of this biometrics for other application.

i. Contamination process and Sensitivity module: Easy to take a portion of DNA.
ii. Automatic recognition issues in real time: The current technology for DNA pattern matching requires cumbersome chemical method involving an expert's skill.
iii. Privacy issues: With the DNA pattern of a person certain diseases can be gained.

3.5. Hand and Finger Geometry

Hand geometry recognition system is based on a measurements taken from the human hand, which includes shape, size and length and widths of fingers. Commercial hand geometry based verification system were used in various places around the world. This technique is very simple, easy to use and also inexpensive. Environmental factors such as dry weather won't affect the verification accuracy of hand geometry based system. Hand geometry information may not be invariant during growth period of children. In addition, an individual jewellery (e.g.: ring) or limitations in dexterity may leads to further challenges in extracting correct informations. The size of this device is larger and it can't be embedded in certain devices like laptop or mobiles devices. Instead of using entire hand, there are some verification systems that based on measurement of few fingers.

3.6. Palm Print Recognition

Palm print recognition is more or like finger print recognition both contains pattern of ridges and valleys. The size of the palm is larger comparing to the Finger, as a result palm print scanner needs to capture larger area and also they are more expensive. Human palm contains some additional distinctive features such as principal lines and wrinkles that can be captured with low resolution scanner, which would be cheap. So with the help of high resolutions scanners all features of palm such as hand geometry, ridges and valleys features, principal lines and wrinkles can be extracted to build highly accurate biometric system

.

3.7. Retinal Scan Recognition

Then retinal vasculature is highly rich in structure. It is said to be most secure biometric since it is difficult to change or duplicate the retinal vasculature. The image acquisition done by a person to peep into an eye- piece and focus to find specific spot in visual field. The image acquisition involves co-operation from the opposite side also. Retinal vasculature can reveal some medical conditions like hypertensions.

3.8. Signature Recognition

Signature verification method in various fields like government, legal and commercial transactions. Signature is a behavioural biometric that change over a period of time. Signature of some people vary substantially: even successive impressions of their signature looks different. Further professional forgers may able to reproduce signature that freaks the system.

3.9. Voice Recognition

Voice is the combination of physiological and behavioural biometrics. The physiological characteristic of human voice may be unique but the behavioural characteristic of human may change over a period of time due to illness, age, emotional state, etc. Voice is also not very distinctive and may not be suitable for large scale identifications. Text dependent voice recognition system is based on the pitch of a predetermined phrase. It is more difficult to design a text independent system than a text dependent systems but offers high secure against Fraud. The main disadvantages of voice based recognition is that speech features may be affected by some factors like background noise. Speakers recognition is most appropriate in phone based applications but the voice signal overall phone is typically degraded in quality due to low quality microphones and the communication channels.

4. Biometric Recognition Algorithms

4.1. Fingerprint Recognition Algorithm

A series of ridges and furrows makes the fingerprint on the surface of the finger. Every human possess unique, immutable fingerprint. With the help of furrows and ridges as well as minutiae can be used to determine the inimitability patterns of the fingerprint. Minutiae points are local ridges characteristics that occur at either a ridge ending or ridge bifurcation. To remove noise and irrelevant information fingerprint pre-processing is done. The steps of Pre-processing are Image Normalization, binarization, making of minutiae and etc.

Two algorithms for fingerprint are

1. Pattern segmentation.
2. Minutiae local mapping.

The main factors of fingerprint algorithm are

1. Normalisation.
2. Segmentation.
3. Filtering.

4.2. Face Detection Algorithm

There are three steps of process for face recognition process. They are:

1. Face detection.
2. Feature extraction.
3. Feature recognition.

The main approaches for face detection algorithms is

1. Texture of unique mapping detection.

4.3. Iris Recognition Algorithm

The unique details of the individual were collected in Iris Recognition system. There are four modules of Iris Recognition methods.

1. The pupil region was extracted with the help of Morphological Operator.
2. Localization of centre and inner boundary.
3. Localization of outer boundary.
4. Sectoring.
5. Normalization.
6. Iris code Generation and Indexing.

4.4. Retina Recognition Algorithm

The Algorithm for Retina Recognition is

4.4.1. Orientation of Special Swing

A biometric system may be viewed as a signal detection system with a pattern recognition architecture that senses a raw biometric signal, processes this signal to extract a salient set of features, compares these features against the feature sets residing in the database, and either validates a claimed identity or determines the identity associated with the signal. Biometric systems attempt to elicit repeatable and distinctive human presentations, and consist (in theory, if not in actual practice) of user-friendly, intuitive interfaces for guiding the user in presenting the necessary traits. In the context of biometric systems, sensing consists of a biometric sensor (e.g., fingerprint sensor or charge-coupled device (CCD) camera), which scans the biometric characteristic of an individual to produce a digital representation of the characteristic. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input digital representation is usually further processed by a feature extractor to generate a compact but expressive representation called a feature set which can be stored as a template for future comparison. The feature extraction stage discards the unnecessary and extraneous information from the sensed measurements and gleans useful information necessary for matching

5. Conclusion

Biometrics presents important technical, policy, and system challenges that must be solved because there is no substitute for this technology for addressing many critical information security problems. Considering the recent government mandates for national and international use of biometrics in delivering crucial societal functions, there is urgency to further develop basic biometric capabilities, and to integrate them into practical applications. Because biometrics cannot be easily shared, misplaced, or forged, the resultant security is more reliable than current password systems and does not encumber the end user with remembering long cryptographically strong passwords. Biometric-based system administrator access to sensitive user information affords effective accountability. While biometric technology appears to be well suited to provide a user-convenient component of secure person-identity linkage, there may be cultural, societal, and religious resistance toward acceptance of this technology.

6. References

i. K P Tripathi, International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011
ii. Iridian Technologies, http://www.iriscan.com
iii. EyeDentify, http://www.eyedentify.com/
iv. Zdeněk Říha Václav Matyáš "Biometric Authentication Systems", FIMU Report Series, November 2000.
v. Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.
vi. Yongsheng Gao; Leung, M.K.H., "Face recognition using line edge map", Pattern Analysis and Machine Intelligence, IEEE Transactions on, Volume: 24 Issue: 6, June 2002, Page(s): 764 -779.
vii. Pentland, A.; Choudhury, T. "Face recognition for smart environments ", Computer, Volume: 33 Issue: 2, Feb. 2000, Page(s): 50 -55.
viii. KresimirDelac, MislavGrgic "A Survey on Biometric methods," IEEE Conf. on Electronics in marine, June 2004.
ix. Sulochanasonkamble, dr. ravindrathool, balwantsonkamble "survey of biometric recognition systems and their applications" Journal of Theoretical and Applied Information Technology, 2005-2010.
x. R.Wildes, "Iris recognition: an emerging biometric technology," Proc. IEEE, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.
xi. International Biometric Group, "Independent Testing of Iris Recognition Technology May 2005 [Online]. Available: http://www.biometricgroup. com/reports/public/reports/ITIRT_report.htm.
xii. JAIN et al.: BIOMETRICS: A TOOL FOR INFORMATION SECURITY 143
xiii. J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., Biometric Systems: Technology, Design and Performance Evaluation. New delhi