ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 8, August 2015

Recognition and Authentication by Biometric Techniques

Deepali H. Shah[1], Tejas V. Shah[2], J. S. Shah[3]

Research Scholar, School of Engineering, R. K. University, Rajkot, Gujarat, India[1]

Associate Professor, Instrumentation & Control Department, L. D. College of Engineering, Ahmedabad, Gujarat, India[1]

Associate Professor, Instrumentation & Control Department, S. S. Engineering College, Bhavnagar, Gujarat, India[2]

Ex-Principal, Government Engineering College, Patan, Gujarat, India[3]

Abstract: Identifying attackers is a major apprehension to both organizations as well as governments. The most used applications for prevention or detection of intrusion are based on biometric systems. Biometrics is inherently most reliable and most capable than any other traditional knowledge-based and token-based techniques. The bio stands for life and metric stands for measurement, combined together make the term "biometrics". Biometric recognition refers to an automatic recognition of individuals by determining the authenticity of a specific physiological or behavioural characteristic based on feature vector possessed by the user. The biometric authentication provides the instances of authentication in such a quick and easy manner that individuals are not bothered by the additional requirements. It is a promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. This paper provides an overview of the different biometric techniques with their respective inherent features.

Keywords: Biometrics, eigenfaces, principal component analysis, signature dynamics.

I. INTRODUCTION

Reliable authorization and authentication has become an integral part of every man's life for a number of routine applications. Biometrics is automated method of recognizing a person based on a physiological or behavioural characteristic. Biometrics, though in its nascent form, has a number of tractable aspects like security, data integrity, fault tolerance and system recovery.It is considered a reliable solution for protecting the identity and the rights of individuals as it recognizes unique and immutable features.

Biometric system has been used for securing the system to allow the person access on the basis of their individual human body parts which is unique for any particular individual. Those human parts could be iris, retina, fingerprint, hand etc. All these parts are really rare parts of any human; it could not resemble any of other individual ever. It means that part must be recognized at the time of accessing system. Hence, we can define biometric system as the system which is essentially a pattern recognition system used to secure the system acquiring the individual human body parts' data by extracting a feature set from the acquired data and then matching these data sets against the predefined feature sets stored in the database. Depending on this methodology biometric system working can be segregated into two modes.

A. Verification Mode

In this mode, biometric system already has a database in which it stores the authorised individual feature set as a template. This database has legitimate details regarding the human parts. The system validate the persons by matching their extracted feature set against those feature set that has been stored as a template in a database. In such a case, an individual tries to recognize himself as an claimed identity usually via Personal Identification Number, smart card, user name etc and the system then performs one to one matching to determine whether the claim is true or not. This mode is typically used for positive recognition just to prevent the other people from using the same identity.[1]

B. Identification Mode

In this mode, the system already assumes to check if the claimed identity would be false. For this purpose, it checks all the stored templates in their database by matching the individual feature set one to one. This mode works on negative recognition nature. It simply signifies that the extracted biometric would be further tested by matching the entire template stored in database. It simply matches of the pattern extracted involving the human features. On the basis of this recognition the person or individual would be proven to access the system as being a claimed identity[1].

II. BIOMETRIC SYSTEM

Biometric system uses different human body parts for recognition or the authentication. Depending upon the characteristic, they are classified in physical andbehavioural. Physical characteristic may be face, iris, hand geometry, finger print, palm print and dental. Behavioural characteristic may be voice, signature and gesture. The complete classification is shown in Fig. 1.

The biometric characteristic data are captured and processed in specific manner. The feature is extracted from it and created template is stored in the database.The complete process has been depicted in Fig. 2. The stored data are used for authentication as well as verification purpose. The whole biometric application has been depicted in Fig. 3.

DOI 10.17148/IJIREEICE.2015.3826

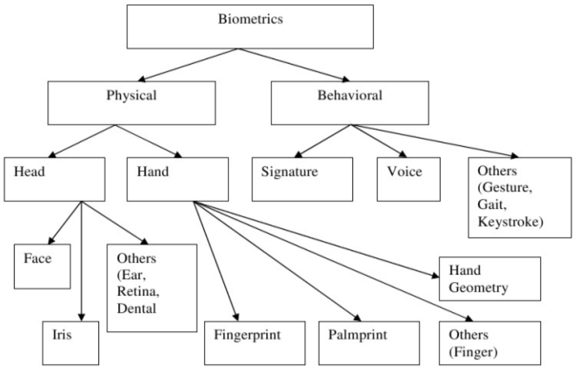

Fig. 1. Various Biometrics Approach [2]

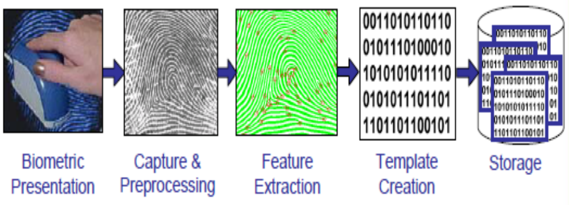

Fig. 2. Data Processing in Biometric

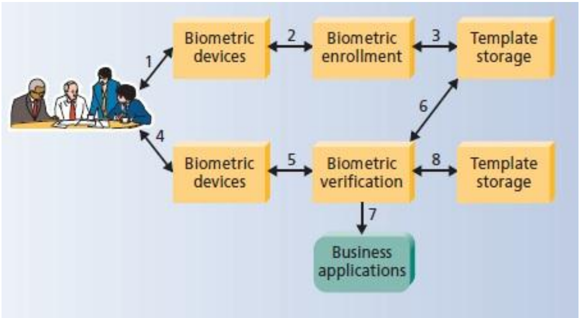

Fig. 3. Complete Biometric Process

A. Fingerprint

Our fingerprint is constructed of numerous ridges and valleys on the surface of finger which are unique to each and every human [3]. Ridges are the top skin layer portions of the finger and valleys are the lower portions. The particular individuality of a fingerprint could be determined by the several patterns of ridges and furrows plus the minutiae points. A fingerprint pattern has individually distinctive composition and characteristic remains the same with time [3], which provides high accuracy with ease of approach. Cuts, marks transform fingerprints which often has negative effect on performance [3].

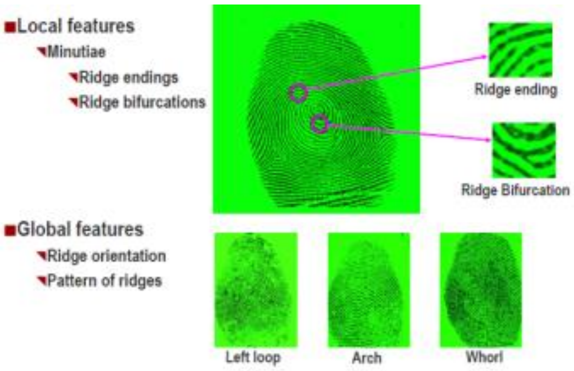

Fig 4 Biometric of Fingerprint

Fingerprint Recognition involves taking an image of a person's fingertips and records its characteristics like whorls, arches, and loops along with the patterns of ridges, furrows and minutiae as shown in Fig. 4.

Fingerprint matching can be achieved in three ways [4]:

Minutiae basedmatching stores minutiae as a set of points in a plane.These points are matched in the template and the input minutiae in respect of location and direction of minutiae as shown in Fig.5.

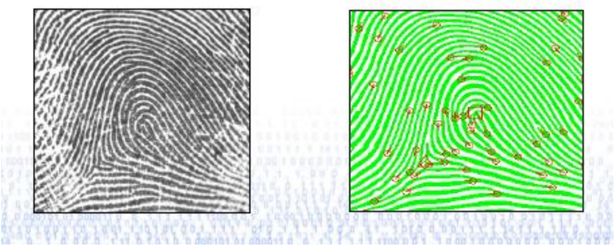

Fig. 5. Minutiae Points of Fingerprint

Correlation based matching superimposes two fingerprint images and correlation between corresponding pixels is computed.

Ridge feature basedmatching is an advanced method that captures ridges. This is useful where minutiae capturing are difficult in low quality fingerprint images.

CCD or CMOS image sensor, solid state sensors are used to capture the fingerprints. Capacitive, thermal, piezoelectric sensors or ultrasound sensors work on echography. They send acoustic signals through the transmitter towards the finger and capture the echo signals with the receiver. [4]

Fingerprint scanning is very stable and reliable. It secures entry devices for building door locks and computer network access.

Two twins do not share same fingerprints as the environment in the uterus affects the phenotypic development of all parts of the twin foetuses. This assures that despite an identical DNA structure of the two foetuses, fingerprints become different.

B. Iris Recognition

Iris recognition is the most secure strategies of authentication and recognition. This can be a combination of specific characteristics known as corona, crypts, filaments, freckles, pits, furrows, striations and rings [5]. The impression of an iris is taken using a standard digicam. The authentication process involves evaluating the present subject's iris with stored version.

The iris pattern is taken by gray scale camera in the distance of 10- 40 cm. Once the gray scale image of the eye is obtained then the software tries to locate the iris within the image.

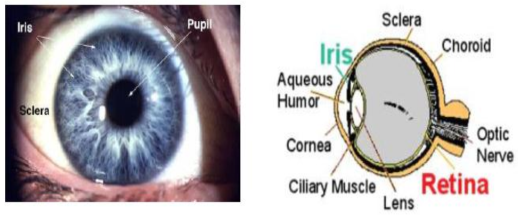

Fig. 6. Iris

DOI 10.17148/IJIREEICE.2015.3826

After finding the iris, the software creates a net of curves covering the iris. Depending on the darkness of the points along the lines the software creates the iris code. The overall darkness of image is influenced by the lighting condition. The darkness threshold, used to decide whether a given point is dark or bright, cannot be static; it must be dynamically computed according to the overall picture darkness. Moreover, the size of the iris changes as the size of the pupil changes. A proper transformation is to be done before computing the iris code. In decision process, the matching software takes two iris codes and computes the hamming distance based on the number of different bits. We can also implement the concept of template matching in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced one. Depending on theresult decision is taken [6,7,8].

Iris possesses unique structure shaped at the age of 10 months which is always stable throughout the life. It incorporates fine texture. Even genetically similar people have entirely independent iris textures [3]. This approach has high accuracy and high recognition process speed [3]. That is a reason for Iris recognition security systems to be a one of the most appropriate security system nowadays. It is truly a distinctive and easy way to identify a user. Iris scanning technology is not very intrusive as there is no direct contact between the subject and the camera technology. Moreover, it is non-invasive. It is one of the most accurate techniques with very low false acceptance as well as rejection rates.

C. Face Recognition

Face recognition provides us a convenient way to identify and recognize a person in a large database. With face recognition, we can recognize a person by just taking a photo of that person. In a face recognition system, cameras are installed at a surveillance place, so the system can capture all the objects in real time without being noticed.

Face recognition is used for two primary tasks[20,21]:

Verification (one-to-one matching): When presented with a face image of an unknown individual along with a claim of identity, ascertaining whether the individual is who he/she claims to be.

Identification (one-to-many matching): Given an image of an unknown individual, determining that person's identity by comparing(possibly after encoding) that image with a database of (possibly encoded) images of known individuals.

Automatic face recognition is all about extracting those meaningful features from an image, putting them into a useful representation and performing some kind of classification on them [9].

Face recognition based on the geometric features of a face is probably the most intuitive approach to face recognition. One of the first automated face recognition systems was described in[11]: marker points (position of eyes, ears, nose,...) were used to build a feature vector (distance between the points, angle between them,...). The recognition was performed by calculating the euclidean distance between feature vectors of a probe and reference image. Such a method is robust against changes in illumination by its nature, but has a huge drawback: the accurate registration of the marker points is complicated, even with state of the art algorithms. Some of the latest work on geometric face recognition was carried out in [12]. A 22-dimensional feature vector was used and experiments on large datasets have shown, that geometrical features alone my not carry enough information for face recognition [9].

The Eigenfaces method described in [13]took a holistic approach to face recognition: A facial image is a point from a high-dimensional image space and a lower-dimensional representation is found, where classification becomes easy. The lower-dimensional subspace is found with Principal Component Analysis, which identifies the axes with maximum variance [9].

There are two phases for face recognition using eigenfaces. The first phase is the training phase. In this phase, a large group of individual faces is acted as the training set. These training images should be a good representation of all the faces that one might encounter. The size, orientation and light intensity should be standardized. For example, all images are of size 128 x 128 pixels and all are frontal faces. Each of the images in the training set is represented by a vector of size N by N, with N representing the size of the image. With the training images, a set of eigen-vectors is found by using Principal Component Analysis (PCA) [21].

Second phase of this algorithm is recognition phase. In this phase, a new image is obtained. To recognize this image, we first subtract the image by the average face ψ. Then we calculate the dot product of the input vectors with the eigenfaces. This makes a projection of the input image onto the face space. Similarly, we make projections of the training image onto the face space. The euclidean distances of point of the input image with the points of training set are then computed. The training set image with minimum distance from the input image should be the best match [21].

D. Voice

Voice recognition attempts to identify individuals by how they sound when speaking [14]. The dynamics of vocal annunciation are partly a product of our vocal tract, mouth and nasal cavities, and general physiological "architecture".

Speaker identity is correlated with physiological and behavioural characteristics of the speech production system of an individual speaker. These characteristics derive from both the spectral envelope (vocal tract characteristics) and the supra-segmental features (voice source characteristics) of speech [17]. Speaker recognition can be classified into speaker identification and speaker verification.

Speaker authentication systems can be categorised depending on requirements for what is spoken.

- Fixed Text: The predetermined word or phrase is recorded at enrolment. This secret word acts as a password.
- Text-Dependent: The speaker is prompted by the authentication system to say a specific thing. The machine aligns the utterance with known text to determine the user.

DOI 10.17148/IJIREEICE.2015.3826

- Text Independent: The speaker authentication system processes any utterance of the speaker. There is continuous monitoring and the system's confidence in the identity of the user is greater. This system can even authenticate a person when they switch language.
- Conversational: In this type, the speech is recognised to verify identity by inquiring about knowledge that is secret, or at least is unlikely to be known or guessed by an impostor during authentication. It is very attractive for high-security applications [15], [16].

E. Signature

The signature dynamics recognition is based on the dynamics of making the signature instead of a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, number of strokes and their duration. Due to this it is not possible to get any information on how to write the signature by simply looking at one that has been previously written. There are various kinds of devices used to capture the signature dynamics such as tables which captures 2D coordinates with pressure [18], [19], special pens which captures 3D coordinates.

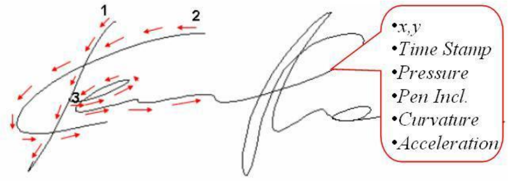

Fig. 7. Features of Signature

III. CONCLUSION

This paper presents a shorter introduction on numerous biometric techniques regarding widely used biometric identifiers and the identification strategies. Current electronic security systems rely primarily on personal identification to ensure an authorized user of a system which is common vulnerable. Their verification can be duplicated and it can be nearly eliminated using biometrics. Biometrics provides benefits that may improve our lives by increasing security and efficiency, decreasing scams and reducing password administrator cost. Despite, the biometrics security systems have many issues like data privacy, physical privacy, and spiritual arguments. Biometrics is used by various organizations to increase security levels and protect their data and patents. The merit of biometrics is proven by endeavours of the G8countries which prevent forgery of passports and other travel documents as part of their fight against terrorism and scams.

REFERENCES

[1] AkashShrivastavaand Vedpalsingh,"Biometrics Based Identification Techniques (BITS)", Journal of Global Research in Computer Science, Vol. 2, No. 11, pp. 11-15, Nov. 2011.

[2] Kalyani Mali and Samayita Bhattacharya, "Comparitive Study of Different Biometrics Features", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 7,pp. 2776 -2784, July 2013.

[3] RupinderSaini and NarinderRana, "Comparision of Various Biometric Methods", International Journal of Advances in Science and Technology, Vol. 2, Issue 1,pp. 25 -30, March 2014.

[4] DavideMaltoni, DurioMaio, Anil K. Jain, SalilPrabhakar, *Handbook of Fingerprint Recognition*, 2002

[5] Sanjay R. Ganorkar, Ashok A. Ghatol, "Iris Recognition: An Emerging Biometric Technology", In Proc. of the6th WSEAS International Conference on Signal Processing, Robotics and Automation, Greece, Feb. 2007, pp. 91 – 96.

[6] A. K. Jain, A. Ross, and S. Pankanti, "Biometric: A Tool for Information Security", IEEE Trans. InformationForensics and Security, Volume 1, No. 2, Jun. 2006, pp. 125–144.

[7] J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Eds., "Biometric Systems: Technology, Design andPerformance Evaluation", New York: Springer Verlag, 2005.

[8] J. Daugman, "The importance of being random: statistical principles of iris recognition", Journal of PatternRecognition, Elsevier, Volume 36, No. 2, Feb. 2003, pp. 279–291.

[9]OpenCV 2.4.7.0 documentation. Available from: http://docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html

[10]ChiaraTurati, Viola Macchi Cassia, F. S., and Leo, I. *Newborns face recognition: Role of inner and outer facial features. Child Development* 77, 2 (2006), 297–311.

[11] Kanade, T. *Picture processing system by computer complex and recognition of human faces.* PhD thesis, Kyoto University, November 1973

[12]Brunelli, R., Poggio, T. *Face Recognition through Geometrical Features.* European Conference on Computer Vision (ECCV) 1992, S. 792–800

[13] Turk, M., and Pentland, A. *Eigenfaces for recognition.* Journal of Cognitive Neuroscience 3 (1991), 71–86.

[14]Ruud M. Bolle, Jonathan H. Connell, SharathPankanti, Nalini K. Ratha, and Andrew W. Senior, *Guide to Biometrics*. Springer Science + Business Media, Inc, NY 10013, USA, 2004, pp 3 – 6, 31 – 45, 146 – 148.

[15]S. H. Maes, J. Navratil, and U. V. Chaudhari, "Conversational Speech Biometrics," in *E-Commerce Agents, Marketplace Solutions, Security Issues, and Supply Demands*, Berlin: Springer-Verlag, 2001, pp. 166 -179.

[16]G.N. Ramaswamy, "Conversational Biometrics: The Future of Personal Identification," Technical report, IBM Research Division, Yorktown Heights, NY, September 2001.

[17] Tiwalade O. Majekodunmi and Francis E. Idachaba, "A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies", Proceedings of the World Congress on Engineering Vol II WCE 2011, July 6 - 8, 2011, London, U.K.

[18] Samir K. Bandopadhaya, Debnath Bhattacharyya, Swarnendu Mukherjee, DebashisGanguly, Poulumi Das, "Statistical Approach for Offline Handwritten Signature Verification", Journal of Computer Science, Science Publication, Volume 4, Issues 3, May. 2008, pp. 181 – 185.

[19] J. L. Wayman, "Fundamentals of Biometric Authentication Technologies", International Journal of Image and Graphics, World Scientific Publication, Volume 1, No. 1, Jan. 2001, pp. 93-113.

[20] Dr.Pramod Kumar, Mrs. Monika Agarwal, Miss. Stuti Nagar, A Survey on Face Recognition System - A Challenge International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013

[21] Rabiajafri, Hamid R. Arabnia, A Survey of Face Recognition Techniques, Journal of Information Processing Systems, Vol.5, No.2, June 2009

DOI 10.17148/IJIREEICE.2015.3826