An Overview of Various Human Traits Used for Biometric Recognition

Arun Bhargava

M.Tech student, Indus Institute of Engineering and Technology, Kinana (Haryana), India

Abstract: ***With the advent of technology, almost all the precious assets of humans have gone digitized. This digital treasure needs to be securely stored and access to it must be restricted to the owner or trusted personals only. With this security urgency, there appeared the biometric solutions, which are fast, reliable and highly secure as compared to traditional physical security solutions. These biometric systems exploit the unique physiological and behavioural traits of humans for recognition and authorization. This paper is a small attempt to summarize the commonly used and intended to be used biometric traits. The merits and demerits of some of the biometric traits is being discussed in this paper.***

Keywords: Biometric, security, authorization, recognition, physiological

1. Introduction

The etymological meaning of the word biometric (Gk *bio+metric*) means measurement of living things. As per ISO biometrics is the automated recognition of individuals based on their biological and behavioural characteristics. Biological and behavioural characteristics are those distinguishing, repeatable biometric attributes of an individual from which unique information can be extracted for the purpose of biometric recognition. Use of biometric system in identification and authorization has been there since times immemorial. Biometric systems have become integral and mandatory parts of physical access world. Biometric systems have been classified differently by different researchers. Visual biometrics (face recognition, ear print recognition, iris recognition, retina recognition, fingerprint recognition, finger geometric pattern/spatial recognition), chemical biometrics (DNA recognition), auditory biometrics (voice and speech recognition), olfactory biometrics (odour recognition), behavioural biometrics (gait recognition, handwriting/signature recognition) etc. The advent in technology has made it easier to recognise one or more biometric characteristics of an individual rapidly.

Highly secure identification and personal verification solutions are the need of hour for various industries and services in both government and private sector. Enterprise wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy, and these techniques are becoming inexpensive on each successive hour and are being accepted by society as a replacement of tradition verification systems like Pins and Passwords. Instead of carrying bunk of keys, all those access cards or passwords you carry around with you, your body can be used to uniquely identify you. However identification and verification are two different terms with quite different meanings; where earlier being the claiming of one's uniqueness from amongst multiple subjects and later being one's comparison with the database to prove his claim. Yet in this paper we will use both as a part of recognition. So term 'recognition' will be used simultaneously for both identification and verification.

Basic principle of biometric system remains almost similar in every system which include following steps-

- **Enrolment or Registration:** The process of obtaining, processing, and storing user's data in standard template form for further use in a biometric system is called enrolment or registration process.
- **Biometric Data:** The unprocessed or raw data obtained from user during registration is referred as raw biometric data or biometric sample. Raw biometric data cannot be used without feature extraction process.
- **Presentation:** It refers to the process including the hardware by which user's raw data is acquired. For example a fingerprinting scanner is required to acquire the fingerprints of users.
- **Template:** A mathematical representation of raw biometric data which is obtained after applying a number of feature extraction algorithms. A template size can vary in size as few bytes for hand geometry to several thousand bytes for facial recognition. The template created at the time of registration is called stored template and at the time of authentication is called live template.
- **Feature Extraction:** The process of locating and encoding distinctive characteristics from biometric data in order to generate a template is called feature extraction. Feature extraction takes place during enrolment and verification, any time a template is created.
- **Matching:** A process where stored template is matched with live template at the time of verification and we obtained a score, on the basis of this score we conclude that a user is authenticate human or not.
- This paper is a small attempt to review various biometric systems, their mechanisms and their applications.

2. Review of Existing Biometric Recognition Techniques

Fingerprint Recognition

Fingerprints based identification and verification system has been in use since many centuries and is the most popular, inexpensive, and longest serving method of biometric recognition. A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmer (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. The ridge pattern of each finger is unique and permanent. The patterns are classified in whorls, loop (radial and ulnar), and arch (tented arch) patterns. A single finger or multiple fingers are imaged using a live-scan fingerprint capture device. Optical fingerprint readers are the most common at present. They are based on reflection changes at the spots where the finger papilar lines touch the reader's surface. The compressed and encrypted data is stored in a local or central workstation which is usually known as automatic fingerprint identification system (AFIS) which performs the matching and identifies the sources of fingerprints. The first step in AFIS processing consists of creating a biometric template through a process known as "feature extraction". AFIS uses these 'features' instead the whole images of fingerprints for comparing two fingerprints. Specifically, the image of a biometric sample such as a fingerprint is not used in comparing one fingerprint to another. Rather, a significantly smaller "feature map" or template of the fingerprint, containing only the unique identifying minutiae points on the finger, is used. The features from questioned fingerprint are matched with standard fingerprint templates stored in system.

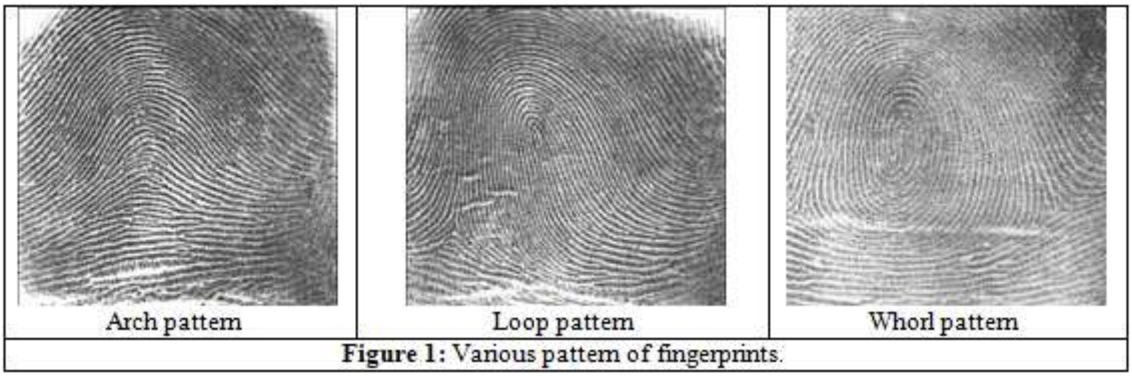
Arch pattern | Loop pattern | Whorl pattern

Figure 1: Various pattern of fingerprints.

Voice Recognition

The generation of human voice involves a combination of behavioural and physiological features which makes the voice a natural choice to authenticate a user (for a mobile phone or even a computer). The physiological component of voice generation depends on the shape and size of vocal tracts, lips, nasal cavities, and mouth. The movement of lips, jaws, tongue, velum, and larynx constitute the behavioural component of voice which can vary over time due to person's age and medical condition (e.g., common cold). With so many factors being responsible for generation of voice, it's obvious that the voice becomes unique to neach individual at any time. Usually Hidden Markov Model is used to build the model of voice based on the intensity, duration, quality, and pitch information. The limitation of voice recognition is that it is highly sensitive to background noise and playback spoofing. Yet voice recognition is highly suitable for applications in tele-banking, voice command based services, mobile phone communications etc. Again, voice biometric is primarily used in verification mode.

Iris Recognition

The iris of the eye is the visible, thin, colored, circular part of eyes which surrounds the pupil and is responsible for quantity of light passing through the pupil. The Iris patterns of everyone including twins is different, even the iris patterns a person's left and right eye is different, and unique too. Research shows that the matching accuracy of iris identification is greater than of the DNA testing. Iris scanning devices have been in use for personal authentication applications for several years. The iris pattern is taken by a special gray scale camera in the distance of 10-40 cm of camera. Once the gray scale image of the eye is obtained then iris is located in the image using the software followed by creation of a net of curves covering the iris. Based on the darkness of the points along the lines the software creates the iris code. While performing authorization, the matching software takes two iris codes and computes the hamming distance based on the number of different bits. The Hamming distance is a score (within the range 0 – 1, where 0 means the same iris-codes), which is then compared with the security threshold to make the final decision. Computing the Hamming distance of two iris-codes is very fast, some modern computers are able to compare over 4,000,000 iris-codes per second. 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. The Iris Access is more advanced. It is auto-focus and has a sensor that checks whether an individual has stepped in front of the camera. It is also able to guide the person audibly into the correct position. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). The artificial duplication of the iris is virtually impossible because of the unique properties. The iris is closely connected to the human brain and is one of the first parts of the body to decay after death. It should be therefore very difficult to forge or create an artificial iris or to use a dead iris to fraudulently bypass the biometric system. The iris verification technology is rapid, and not intrusive, also the technology advent have made it quite inexpensive, so it's use for the recognition and authorization process has increased to a great deal.

Facial Recognition

Facial recognition is the most natural method of biometric identification. Facial recognition system exploits the idea that each person has a particular face structure, and symmetry. Video image or static face image can be used to recognize individual. Facial features such as shape, location and spatial/geometric relationships among facial landmarks such as eyes, mouth, nose, lips and cheek (geometric features) and structural pattern that extracts discriminative information of the face textures (texture features) are exploited for face recognition. The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Most of facial recognition systems require the user to stand a specific distance away from the camera and look straight at the camera. This ensures that the captured image of the face is within a specific size tolerance and keeps the features (e.g., the eyes) in as similar position each time as possible. The first task of the processing software is to locate the face (or faces) within the image. Then the facial characteristics are extracted. Facial recognition technology has recently developed into two areas: facial metrics and Eigen faces. Facial metric technology relies on the positioning of facial features like eyes, nose and mouth and distances between these features. The face region is rescaled to a fixed pre-defined size (e.g. 150-100 points). This normalized face image is called the canonical image. Then the facial metrics are computed and stored in a face template. The Eigen Face method is based on categorizing faces according to the degree of it with a fixed set of 100 to 150 Eigen faces. The Eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern shows how different features of a face are singled out. The image processing and facial similarity decision process is done by the computer software at the moment, this processing requires quite a lot of computing power and so it is not easy to assemble a stand-alone device for face recognition. The special-purpose chip with embedded face recognition instruction set has been created by many companies. The accuracy of the face recognition systems improves with time, but it has not been very satisfying so far.

Hand Geometry Recognition

Individual identification using hand geometry exploits the unique shape of a person's hand which usually does not change after certain age. It uses certain measurements of the hand such as the length and the width of fingers. Various mechanical and optical (more commonly) methods are used to measure the hand. Optical hand geometry scanners capture the image of the hand and using the image edge detection algorithm compute the hand's characteristics. A black-and-white bitmap image of hand's features is created using a low resolution camera. The discriminatory power of hand geometry features is very limited and that is why these systems are employed only for verification applications (1:1 matching) in low security access control and time-and-attendance applications.

Retina recognition

Retina scan recognition technique is another authorization method that uses eyes of subject for verification and identification. It is based on the blood vessel pattern in the retina of the eye and is older technique than iris recognition method. The biggest limitation of retina scan method is its intrusiveness because of an invasive acquisition method. Retina scan is more laborious, complicated and expensive technique than iris recognition method, so its use is quite limited.

Signature Dynamics Recognition

The signature dynamics recognition is based on the dynamics of making the signature which includes the pressure, direction, acceleration and the length of the strokes, number of strokes and their duration, rather than a direct comparison of the signature itself. The most obvious and important advantage of this is that a fraudster cannot glean any information on how to write the signature by simply looking at one that has been previously written. Earlier methodology involved the extraction of ten or more writing characteristics such as the number of times the pen was lifted, the total writing time and the timing of turning points. The matching process was then performed using fairly standard statistical correlation methods. Newer sequential techniques treat the signature as a number of separate events, with each event consisting of the period between the pen striking the writing surface and lifting off again. This approach is much more flexible. There are tablets and special pens which are used to capture the signature dynamics. Tablets can capture a two dimensional coordinates and the pressure of signature, while special pens can capture movement in three dimensions. Most of the signature dynamics systems verify the dynamics only; they do not pay any attention to the resulting signature. So it is possible to successfully forge a signature even if the resulting signature looks so different. The accuracy of the signature dynamics biometric systems is not high and is not recommended now days.

DNA Recognition

Deoxyribonucleic Acid (DNA), the hereditary material of a living organism and is unique to each individual. The human genome is made up of 3 billion nucleotides 99.9% of these are same in humans. DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. DNA based personal identification is not possible in real time. This method of capture still has to be refined. So far the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. The analysis of human DNA is now possible within 10 minutes. As soon as the technology advances so that DNA can be matched automatically in real time, it may become more significant. At present DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being.

Ear Recognition

Ear is relatively new biometric trait. An earprint is a two-dimensional reproduction of the parts of the outer ear that has all the properties that other biometric traits have i.e. uniqueness, universality, performance, reliability and collectability. The outer ear shape, lobes and bone structure can use for characterization. Two ears are not found to be same in any person even amongst the identical twins. Ears are grows uniformly after the first four months of birth and structure of the ear does not change over time. Ear based authentication can be used as a supportive biometric traits means one can combine face with ear or fingerprint with ear etc. just like face recognition method of biometrics, ears are biometric which can be captured easily by the cameras which makes them more feasible. Earprints analysis is considered to be more economical than DNA profiling. Ear biometric consist of 2D gray and 3D color images or combination of both. Recognition performance of the ear biometric is not much different to face. However the use of earprints as in forensic science is still under criticism from some sections of scientific community because of lack of formal protocols for collecting and analysing. Also the individualization process using earprints is subjective.

Other Biometric Systems

Scientists are looking to use the electrocardiogram (ECG), electroencephalogram (EEG) for biometric purposes. Some features like universality, uniqueness, permanency, acceptability, reproducibility and collectability are essentially required for a trait to be used in biometric authorization. Some biometric traits like palm prints, knuckle, dentition, ruguscopy, body odour, gait, keystroke, nailplate etc have been suggested and tested for biometric authorization but their use is limited due to lack of one or two essentially required features or due to lack of formal protocols.

3. Conclusion

Even if the accuracy of the biometric techniques is not perfect yet, the implementation of biometrics in many industries is the need of hour. Proper design and implementation of the biometric system can indeed increase the overall productivity and security. The urgent need of security and authorization in corporate and financial institutions and in government sector demand more reliable and real time biometric solutions. Making a secure biometric systems is, however, not as easy as it might appear. Multimodal biometric systems which use two or more biometric traits for individualization and authorization look more promising and recommended instead of single trait based biometric systems. Alongwith the appraisal of existing biometric solutions, we should also explore more physiological and behavioural traits that can be used in biometric recognition.

References

[1] Tripathi KP. (2011). A Comparative Study of Biometric Technologies with Reference to Human Interface. International Journal of Computer Applications. 14(5):10-15.

[2] Kalyani CH (2017) Various Biometric Authentication Techniques: A Review. J Biom Biostat 8: 371. doi: 10.4172/2155-6180.1000371.

[3] Jain, Anil K., Ross, Arun A., Nandakumar, Karthik. (2011). Introduction to Biometrics. Springer Publishers. XVI. ISBN 978-0-387-77326-1.

[4] Jain, Anil K., Flynn, P. J. and Ross, A. (2007). Handbook of Biometrics. Springer Publishers. ISBN: 978-0-387-71040-2.

[5] Kaur G, Singh G and Kumar V. (2014). A review on biometric recognition. International Journal of Bio-Science and Bio-Technology. 4: 69-76.

[6] Simon Liu and Mark Silverman. (2001). A Practical Guide to Biometric Security Technology. IT Pro. 27-32.

[7] Himanshu Srivastava. (2013). A Comparison Based Study on Biometrics for Human Recognition IOSR Journal of Computer Engineering. 15(1):22-29.

[8] Debnath B (2009) Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology. 3:13-28.

[9] Zdenek Ríha, Václav Matyáš. (2000). Biometric Authentication Systems. FIMU Report Series.