Review Paper on Biometric Authentication

Kavita Gupta
Department of Electronics & Communication
Vivekananda Institute of Technology, Jaipur
Jaipur, India

Abstract: **Nowadays we come across a number of cases of cybercrime, data leak, manipulation of data by unauthenticated users, hacking of personal accounts etc. due to traditional password based security systems which could be hacked. So this has created a even secure system requirement which could eliminate these security related issues, the alternate solution for which could be seen in biometric authentication technology which could not be hacked as this system consists of software which identifies or validates the user by matching the data being fed with the digital images of the unique characteristics of the user .This data cannot be copied or hacked, so it makes the identification more reliable.**

Keywords: Biometrics, Authentication, Hacking, Iris, Retina

INTRODUCTION

Biometrics comes from the words 'bio' meaning Life and 'matron' meaning Measurement. It is therefore the identification /authentication by use of measurement of some unique traits of the user. So the process of validation of user to sign in to the account or getting access to personal data etc. by using the unique characteristics of user i.e. fingerprint scan, facial imaging, signature, voice recognition, is the Biometric Identification. Verification of Identity occurs when the user is already registered or user's data is already enrolled in the system software. In this case the user's input data being fed is compared with the previously fed input data, if the data i.e. the physiological or behavioral characteristic matches with already enrolled characteristic, then the user is verified and allowed to get access to or sign in. In case if user is not enrolled, and is enrolling for the first Time, then the characteristic data is fed and saved in the software for any further access. This system provides better reliability then the traditional PIN or any other Identity or document based system as:

1. The person needs not to carry any identity card or remember any passwords or login-ids.
2. The person in regard needs to be present at the point of time and place, the system is one to one interface, so more secure.
3. Biometric authentication can be classified into two classes of identification schemes:
4. A. Behavioral characteristics
5. B. Physiological characteristic

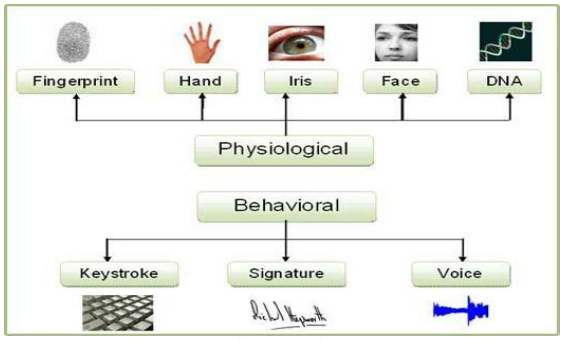

Fig: classification of biometrics

Fingerprints Identification: It is oldest Biometric characteristic used. In this technology the digital imaging of fingerprints is carried out. It scans the friction ridge skin impression of the human fingers. The sensor senses the unique curves, bifurcations of the skin of fingers. Same happens in palm scanning.

Eye Scanning

There are two methods for eye recognition:

Retina scanning: The user has to look in a device that performs laser-scanning of his retina. The device analyzes the configuration of blood vessels of the user. The blood vessels configuration of a person is unique. It poses a difficulty as user has to fix a point till the laser is analyzing his eye.

Iris Scanning: Unlike the Retinal scanning the person needs not to be close to the device. In this, the imaging is done by a camera. The iris patterns are obtained through a video-based imaging system. The image so acquires is analyzed by the device. The image contains 266 different spots, these spots are based on the characteristics of iris, i.e. furrows and rings. The iris is stable throughout the life. No timely updation of image is required.

Face Recognition

In face recognition, a good resolution simple camera or a web camera is used. Facial recognition in visible light acquires features from the central portion of face image. These characteristics do not change over time. Superficial features such as facial expressions, hairs are avoided. The representation is compared with Existing database, which if matched, the user is authenticated.

Handprint Imaging

In this method, the picture of a user's hand is being scanned. Characteristics like distance between fingers, length of fingers, length of hand are extracted and saved

with the help of digital signal processing algorithms. The templates are generated. The characteristics are with these templates for verification. Hand geometry is scanned mostly by optical scanners.

Palm print Recognition

Features like minutiae, ridges, principle lines, creases, orientation, and vein geometry are extracted for recognition. For different individuals, vein geometry is distinct. For authentication, hand is placed on the screen, infrared light is used for scanning of the veins. It captures image of hand, a pattern of veins is extracted, which is the bright and dark pattern. The darker pattern is formed due to absorbing of infrared light by veins of hand.A template of this biological pattern is saved in the device. This image is converted into digital image by transducer for matching and comparison purpose.

DNA Analysis

This Method of verification is mostly used in criminal cases. DNA of the user in the form of blood, tissue, hair, nails is collected for confirming. DNA analyzing takes time. DNA also is unique characteristic but a hair or nail can be stolen.

Voice Verification

In voice verification, user is asked to speak a phrase or a secret code. His vocal characteristics are measured i.e. both physiological (shape and size of vocal cords) and behavioural (pitch of voice) characteristics. The verification process is different from voice identification process. In verification sample of speaking style pattern is saved and is compared with the same person's speech but identification is rather many to one or one too many process. The verification system is been trained for a particular speaker's voice verification.

Signature scanning

It is the dynamic analysis of the shape, size of signature, writing speed, time taken for signing, pressure applied by user's hand on the screen while signing etc. Though signature may be copied but the traits while signing may not be.

Keystroke: It is basically the way of pressing the key. The measurable traits are the time for which key is pressed, releasing time, sound made while pressing and releasing.

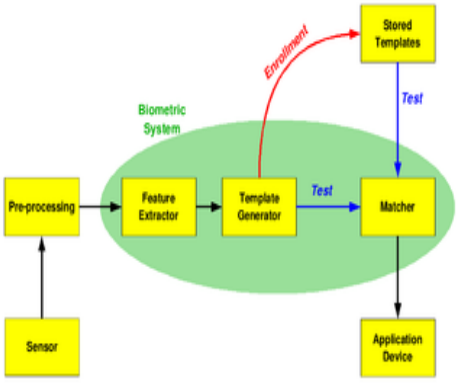

Fig: Mechanism of biometric operation

Advantages of Biometric Authentication:

1. No remembering of passwords or login ID's is required.
2. Better alternate of saving time and resources.
3. Only Legitimate user can get access to the personal data or accounts.
4. Elimination of need of carrying authorized documents

Disadvantages of Biometric Verification

1. Some of these methods are limitation for physically challenged people.
2. Changing of amount of light entering into eye due to pupil contraction may lead to system showing error.
3. DNA analysis takes time, retina scanning requires expensive device.
4. Some characteristics of face or palm may change with time and age

CONCLUSION:

The biometric system may find applications in attendance system, security systems, and identification purposes and may find even more applications in the time to come. The prevalent systems would be worked upon and modified for error free secure system. The accuracy levels need to be increased for efficient security system. Proper selection of technique has to be considered according to the requirement. Scientific work is being carried out for future applications and progress in the biometrics.

REFERENCE:

[1] https://www.engineersgarage.com/blogs/biometrics-technology-and-its-scope-future
[2] http://www.biometricsinstitute.org/pages/types-of-biometrics.html
[3] https://www.ieee.org/about/technologies/emerging/biometrics.pdf