Study and Analysis on Biometrics and Face Recognition Methods

1.**Anjani Kumar Singha**
Department of Computer Science and Engineering
Gurukula Kangri Vishwavidyalaya, Haridwar, Uttarakhand

2. **Anshu Singla**
Department of Computer Science
Jamia Millia Islamia, New Delhi

3..**Rajneesh kumar pandey**
Air Force Record Office,
Subroto Park New Delhi

Abstract— **Human Biometrics is a rising technology, which has been broadly used in forensics, safe access and top-security prison. A biometric system is primarily a pattern recognition system that recognizes a person by determining the verification by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are important physiological biometrics and behavioral trait are Voice recognition, keystroke-scan, and signature-scan. In this paper different biometrics techniques such as Iris scan, retina scan and face recognition techniques are discussed.**

Keywords-Biometric; Fingure Print; Voice Recognition; keystroke scan; Signature scan, Biometric techniques, Eigen face, Face recognition.

I. INTRODUCTION

Biometrics is automatic method of recognizing a person based on a physiological or behavioral trait. The past of biometrics include the recognition of people by distinctive body features, scars or a grouping of other physiological criteria, such like height, eye color and complexion. The present features are face recognition, fingerprints, handwriting, hand geometry, iris, vein, voice and retinal scan. Biometric technique is now becoming the basis of a wide array of highly secure recognition and personal verification. As the level of security violation and transaction scam increases, the need for well secure identification and individual verification technologies is becoming apparent. Recent world events had lead to an increase interest in security that will drive biometrics into bulk use. Area of future use hold Internet dealings, workstation and network access, telephone transactions and in travel and tourism. There are different types of biometrics: Some are old or latest technology. The most familiar biometric technologies are fingerprinting, retinal scanning, hand geometry, signature verification, voice recognition, iris scanning and facial recognition

A biometric system can be either an 'identification' system or a 'verification' (confirmation) system, which are defined below.

Identification (1: n) – One-to-Many: Biometrics can be used to establish a person's identity even without his consciousness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can confirm matches that are already store in database.

Verification (1:1) One-to-One: Biometrics can also be used to verify a person's uniqueness. Such as one can allow physical access to a secure area in a building by using finger scans or can award access to a bank account at an ATM by using retina scan.

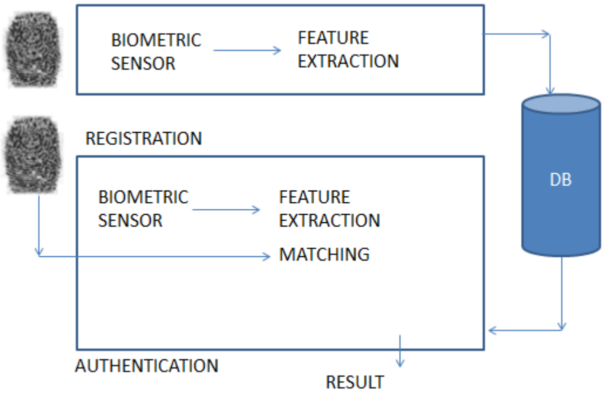

Fig. 1 General Biometric System [1]

II. BIOMETRIC CHARACTERISTICS

"Biometrics" means "life measurement" but the term is generally coupled with the use of unique physiological individuality to identify a person, some other characteristics of biometrics are: ***Universal:*** Every person must possess the characteristic. The trait must be one that is universal and seldom lost to accident or disease. ***Invariance of properties:*** They should be unvarying over a long time. The trait should not be spotlight to significant differences based on age either periodic or chronic disease. ***Measurability:*** This should be suitable for detain without waiting time and must be simple to gather the characteristic data inactively. ***Singularity:*** Each look of the element must be distinct to the person. The distinctiveness should have enough distinctive properties to differentiate one person from other. Height, weight, hair and eye color are all elements that are inimitable assuming a mostly accurate measure, but do not offer enough points of separation to be useful for more than categorizing. ***Acceptance:*** The capturing should be probable in a manner acceptable to a large fraction of the residents. Excluded are particularly persistent technologies, such technologies which is require a part of the human body to be taken or which (apparently) spoil the human body. ***Reducibility:*** The captured data should be able of being reduced to a file which is easy to handle. ***Reliability and tamper-resistance:*** The attribute should be impractical to mask or modify. Process should make sure high reliability and reproducibility. **Privacy:** This process should not break the privacy of the individual. ***Comparable:*** They should be able to diminish the trait to a state that makes it is digitally analogous from others. It has less probabilistic for similarity and more dependable on the identification. ***Inimitable:*** The trait must be irreproducible by other way. The less reproducible the trait, the more likely it will be trustworthy. Biometric technologies: fingerprint, facial features, hand geometry, voice, iris, retina, vein patterns, palm print, DNA, keystroke dynamics, ear shape, odor, signature all satisfy the above requirements.

Table I Characteristic Feature of Biometric Technology [1]

Modality	Fingerprints	Head Geometery	Retina	Iris	Face	Signature	Voice
Use	High	Medium	Low	Medium	Low	High	High
Error	Disease Dirtiness Age	Injury Age	Wearing Glasses	Lightness	Lightness Age Expression	Changing	Noise Cough
Accuracy	High	High	Very High	High	Medium	Medium	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Stability	High	Medium	High	High	Medium	Medium	Medium

In biometrics, biometric system can be classified into following modules-

- Database Preparation Module
- Verification Module.

Database Preparation Module are further alienated into two sub-modules
(a) Enroll Module and (b) Training Module while the other module

Verification module
(a) Matching Module and (b) Decision Module.

III. Biometric Technology

Fingerprint Recognition
• Voice Recognition
• Signature Recognition
• Face Recognition
• Palm scan

- Retina-scan
- Hand geometry
- Signature-scan
- Keystroke-scan

Primary biometric disciplines include: Fingerprint (optical, silicon, ultrasound, touch less), Facial acknowledgment (optical and thermal) Voice recognition (not to be confused with speech), Signature-scan, Iris-scan, Retina-scan, Hand geometry, Keystroke-scan, Palm-scan (forensic use only)

Exploratory stages include: DNA, Ear shape, Odor (human scent), Vein-scan (in back of hand or beneath palm), Finger geometry (shape and structure of finger or fingers), Nailed identification (ridges in fingernails), Gait recognition (manner of walking)

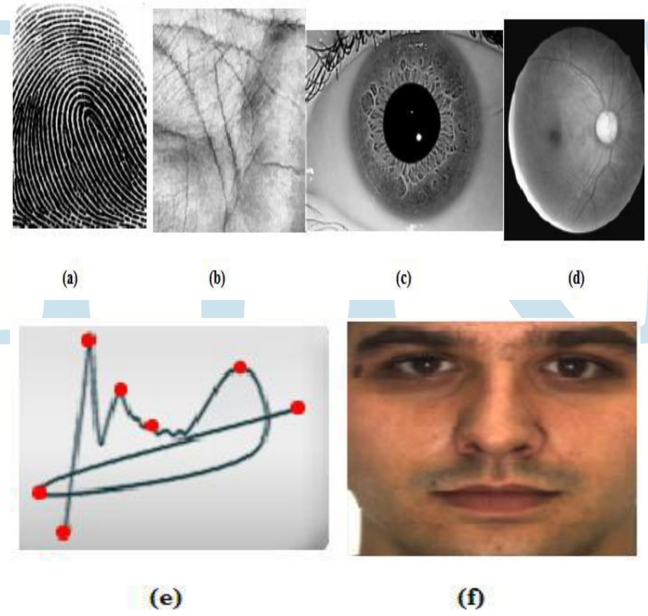

Fig. 2 Biometrics traits: (a) fingerprint, (b) palm, (c) iris, (d) retina, (e) signature and (f) Face.

Fingerprint Recognition: Fingerprint scan is the most widely used biometric tools. Fingerprint (optical, silicon, ultrasound, touch less) distinctiveness can be defined by analyzing the details of a human being. Trivia include sweat pores, distance stuck between ridges, bifurcation. It is probable that the likelihood of two persons having the same fingerprint is less than one in billion. There are a number of sub-methods in fingerprinting, with changeable degrees of accuracy and correctness. Various can even detect when a live finger is present. Fingerprinting method has been developed over the years.

Voice Recognition: Voice recognition technology does not compute the visual features of the human body. In voice recognition sound feelings of a person is measured and compared to an existing dataset. The person to be identified is usually required to speak a secret code, which smooth the progress of the verification process.

Signature recognition: Signature identification is the process used to know an individual's hand-written or signature. Dynamic signature authentication technology uses the behavioral biometrics of a hand written signature to confirm the characteristics of a computer client. Analyzing the speed, shape, stroke, and pen pressure and timing information during the act of signing natural does this.

Palm recognition: In palm recognition a 3-dimensional image of the hand is collected and the feature vectors are extracted and compared with the database feature vectors. These devices are large but recognition is done in a small time.

Hand Geometry Hand: Hand geometry has 3-D image of top and sides of hand and fingers is composed and the feature vectors are take out and compared with the dataset feature vectors. It is identification devices are large but identification is done in a 2-3 second. User places hand, palm-down, on an 8 x 10 metal surface with five guidance pegs. Pegs confirm that fingers are positioned correctly and also verify correct hand position.

Iris scan: The iris scans procedure start to get amazing on film. For this a dedicated camera is required, naturally very close to the subject, not above three feet, uses an infrared imager to light up the eye and capture a very high-resolution photograph. Whole procedure takes only few seconds (approximately 1 to 2 sec) and provides the details of the iris consciously produce, recorded and stored in dataset for future recognition and confirmation. The quality of iris image does not get affected due to the presence of the contact lens and eyeglass. The iris code is evaluated in short time and takes 256 bytes. The probability that 2 different irises could turn out the same iris code is estimated as low as 1: 1078 the probability of two persons with the same iris is very low (1: 1052) [2].

Retina scan: Retina scan is based on the blood vessel prototype in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses a part of the eye. The first retinal scanning systems were launched by Eye Dentify in 1985[3]. Retina is not openly visible and so a rational infrared light source is needed to light up the retina. The infrared energy is absorbed more quickly by blood yacht in the retina than by the neighboring tissue. The image of the retina blood vessel pattern is then analyzed for characteristic points within the pattern. The retina scan is more vulnerable to some diseases than the iris scan, but such diseases are relatively rare [4].

Fingerprint Recognition:
Advantages: Very high accuracy, non-invasive biometric technique. Most economical biometric PC user authentication technique, it is one of the most developed biometrics, Easy to use, Small storage space required for the biometric template and also reduces the size of the database, It is standardized.

Disadvantages: For some people it is extremely intrusive, because is at rest related to criminal verification, it can be compose mistakes with the dryness or dirty of the finger's skin, as well as with the age (is not appropriate with children, because their fingerprint changes quickly), Image captured at 500 dots per inch (dpi). Resolution: 8 bits per pixel. A 500 dpi fingerprint image at 8 bits per pixel demands a large memory space, 240 Kbytes approximately → Compression required (a factor of 10 approximately).

Voice Recognition: *Advantages:* Non intrusive, high social capability, less verification time is about five seconds and not expensive technology. *Disadvantages:* A person's voice can be easily recorded and used for unauthorized PC or network, Low accuracy, an illness such as a cold can change the voice of a person, which makes identification difficult or impossible.

Signature recognition
Advantages: Non-intrusive, less time of verification about 4 to 5seconds, inexpensive technology. *Disadvantages:* Error rate: 1 in 50.

Hand Geometry:
Advantages: It requires special hardware; it can be easily integrated into other devices or systems, It has no public attitude problems as it is associated most commonly with authorized access, a large amount of data are stored in database to uniquely identify a user, allow it to be used with Smartcards. *Disadvantages:* Very expensive, Considerable size, it is not valid for arthritic person; they cannot put the hand on device. ***Iris scan:*** *Advantages:* Very high accuracy, Verification time is generally less than 5 seconds, The eye from a dead person would deteriorate too speedy to be valuable, so no extra protection have to been taken with retinal scans to be sure the user is a living human being.

Disadvantage: Too much movement of head or eye, wear colored contacts.

IV. **FACE RECOGNITION**

In order to recognize a person, one commonly looks at faces, which differentiate one person to another. Fr is used to search for other images with matching features [5]. Eyes in particular seem to tell a story not only about which somebody is, but also about how that person feels, where his/her attention is directed, etc [1]. Face recognition records the spatial geometry of unique features of the face. Main focuses on key features of the face. Face recognition technique is used to identify terrorists, criminals, and other types of persons for law enforcement purposes. This is a non-intrusive, cheap technology. In the 2d recognition of face is affected by vary in lighting, the person's hair, age, and if the people put on glasses, low resolution images [5]. It requires camera as equipment for user identification; thus, it is suspicious to become popular until most pcs include cameras as standard equipment. United States used same technologies to prevent people from obtaining fake identification cards and driver's licenses [9]-[10]. Face recognition has always been a very demanding task for the researches. On the one hand, its applications may be very useful for personal verification and recognition. On the other hand, it has always been very difficult to implement due to all different condition that a human face can be found [8]. Facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. Facial recognition is including five steps to complete their process. *Step1:* ACQUIRING THE IMAGE OF AN INDIVIDUALS FACE; 2 *WAYS TO AQUIRE IMAGE:* 1) Digitally scan an existing photograph; 2) Acquire a live picture of a subject. *Step2:* LOCATE IMAGE OF FACE: software is used to locate the faces in the image that has been obtained. *Step3:* ANALYSIS OF FACIAL IMAGE: software measures face according to is peaks and valleys; focuses on the inner area of the face identified as the "golden triangle", valleys are used to create a face print with their nodal points. *Step4:* COMPARISON: the face print created by the software is compared to all face prints the system has stored in its database.
Step5: MATCH OR NO MATCH: software decides whether or not any comparisons from step 4 are close adequate to declare a possible match.

Facial recognition utilizes unique features of the face - including the upper outlines of the eye sockets, the areas close the cheekbones, the sides of the mouth, and the location of the nose and eyes - to carry out verification and identification. Most technologies are fairly resistant to modest changes in haircut as they do not develop areas of the face located near the hairline. When used in identification mode, facial recognition technology generally returns candidate lists of close matches as opposed to returning a single definitive match (as do fingerprint and iris-scan technologies) [4].
Face Recognition algorithms are Principal Component Analysis(PCA) using eigenfaces, Linear Discriminate Analysis, Elastic Bunch Graph Matching using the Fisherface algorithm, Pseudo 1D Hidden Markov model(HMM), Pseudo 2D Hidden Markov model, Multilinear Subspace Learning using tensor representation, and the neuronal motivated dynamic link matching, Artificial neural network, Support vector machine(SVM) and normalized correlation. The first duty of the processing software is to locate the face (or faces)

inside the image. Then the facial characteristics are extracted. Facial recognition technique is newly developed into two areas: *facial metrics* and *eigenfaces*. Facial metrics technology relies on the measurement of the specific facial features (the systems typically look for the positioning of the eyes, nose and mouth and the distances between these features) [4]. *Eigenfaces* FR technique is based on categorizing faces according to the degree of fit with a fixed set of 150 master eigenfaces. This method has similar policy and methods that are used in creating a portrait, the only dissimilarity is that image processing is automatic and based on a real picture. Every face is assigned a degree of fit to each of the 150 master eigenfaces, only the 40 template eigenfaces with the highest degree of fit are necessary to reconstruct the face with the accuracy of 99%. Improving the algorithms for face position, the current software often does not find the face at all or finds “a face” at an incorrect place. This drastically makes the results inferior. Better results can be achieved if the operator is able to tell the system exactly where the eyes are positioned [4]. Although we can find many other recognition and verification techniques, the main motivation for face recognition is that, it is considered fast, a inactive, non-intrusive system to verify and identify people [6]. There are many other types of identification such as password, PIN (personal identification number) or token systems. Moreover, it is nowadays very instilled the usage of fingerprints and iris as a physiological identification. They are useful if we need an active identification system; the fact is that a person has to expose their body to some device makes people feel being scanned and recognized. The pause and announce interaction is the best method for bank transactions and security areas; people are aware of it, and make them feel comfortable and safe with it [7].

Finally, Section VI draws the concluding remarks and future work.

V. CONCLUSION

Biometrics is a quickly developing technology that is being broadly used in forensics, security; prevent unauthorized access in bank or ATMs, in cellular phones, smart cards, PCs, in workplaces, and computer networks. There are numerous forms of biometrics now being built into technology platforms. It has been implemented in public for short time. There are lots of applications and solutions in biometrics technology used in security systems, which can improve our lives such as: enhanced security, it is reduced con and password administrator costs, easy to use and make life more secure and comfortable.

But it is not likely to definitely state if a biometric technique are successful run, it is essential to locate factors that’s help to reduce affect system performance. The international biometric group Strike System Strikes are: in Fingerprint Dry/oily finger, in Voice recognition Cold or illness that affects voice, in Facial recognition Lighting conditions. Face recognition technology are more consistent, non-intrusive, economical and extremely accurate. Currently Face recognition technology is the most demanding recognition technologies.

.

References

[1] K P Tripathi, *International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011*

[2] Iridian Technologies, http://www.iriscan.com

[3] EyeDentify, http://www.eyedentify.com/

[4] Zdeneˇk R íhaVáclav Matyáš “Biometric Authentication Systems ”, FI MU Report Series, November 2000.

[5] Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.

[6] 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.

[7] Pentland, A.; Choudhury, T. *“Face recognition for smart environments “*, Computer, Volume: 33 Issue: 2, Feb. 2000, Page(s): 50 -55.

[8] De Vel, O.; Aeberhard, S., *“Line-based face recognition under varying pose”*, Pattern Analysis and Machine Intelligence, IEEE Transactions on Volume: 21 Issue: 10, Oct. 1999, Page(s): 1081 -1088.

[9] House, David. "Facial recognition at DMV". Oregon Department of Transportation. Retrieved 2007-09-17.

[10] Schultz, Zac. "Facial Recognition Technology Helps DMV Prevent Identity Theft". WMTV News, Gray Television. Retrieved 2007-09-17. "Madison:The Department of Motor Vehicles is using... facial recognition technology [to prevent ID theft]"

[11]http://www.sony.net/SonyInfo/technology/technology /theme/sface_01.html

Figure 1. Figure 2.

[1]
[2]
[3]