International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 3, March-2014, pp: (296-299), Impact Factor: 1.252, Available online at: www.erpublications.com

Biometric Technology - A Review

Navya Garg[1], Sukhwinder Singh[2]
[1]Student, E&EC Dept., PEC University of Technology, Sector-12, Chandigarh, (INDIA)
[2]Assistant Professor, E& EC Dept., PEC University of Technology, Sector-12, Chandigarh, (INDIA)

Abstract: Biometrics is a growing technology, which has been widely used in forensics, secured access and prison security. A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different biological features i.e. Fingerprint, retina-scan, iris scan, hand geometry, and face recognition are leading physiological biometrics and behavioral characteristic 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, Biometric Technology, Fingerprint Identification, verification, Recognition, Signature Recognition.

I. INTRODUCTION

With the rapid proliferation of technologies, data processing, electronic transaction and service delivery affecting everyday life in multiple ways , a strong need for new identification practices has emerged. In numerous contexts technologically mediated and automated economic and social interaction replaces physical and face to face encounters, depriving the interacting partners of traditional , trusted ways of establishing each other who they are . Also , the ever higher levels of complexity in society generate a wide variety of problems relating to public and private security, bureaucratic and administrative control and surveillance. Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. The past of biometrics includes the identification 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.

vein ,voice and retinal scan. Biometric technique is now becoming the foundation of a wide array of highly secure identification and personal verification[6]. As the level of security breach and transaction scam increases, the need for well secure identification and personal verification technologies is becoming apparent. Recent world events had lead to an increase interest in security that will impel biometrics into majority use. Areas of future use contain Internet transactions, workstation and network access, telephone transactions and in travel and tourism. There have different types of biometrics: Some are old or others are latest technology. The most recognized 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' (authentication) system, or a recognition system which are defined below.

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

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

Recognition is a generic term and does not necessarily apply with verification or identification. All biometric systems perform recognition.

II. BIOMETRIC CHARACTERISTIC

"Biometrics" means "life measurement" but the term is generally coupled with the use of unique physiological characteristics 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 constant over a long time. The trait should not be focus to considerable differences based on age either episodic or chronic disease.

Measurability: This should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

Singularity: Each expression of the element must be distinctive to the person. The characteristics should have adequate distinctive properties to distinguish one person from other. Height, weight, hair and eye color are all elements that are unique 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 possible 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) impair 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 reduce the trait to a state that makes it is digitally comparable 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 reliable.

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.[5].

III. Biometric Technology

- Fingerprint Recognition
- Voice Recognition
- Signature Recognition
- Face Recognition
- Palm scan
- Iris-scan
- Retina-scan
- Hand geometry
- •Signature-scan

Primary biometric disciplines include: Fingerprint (optical, silicon, ultrasound, touch less), Facial recognition (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), Nail bed identification (ridges in fingernails), Gait recognition (manner of walking)

Fingerprint Recognition: Fingerprint scan is the most widely used biometric technology. Fingerprint (optical, silicon, ultrasound, touch less) uniqueness can be defined by analyzing the trivia of a human being. Trivia include sweat pores, distance stuck between ridges, bifurcation. It is probable that the likelihood of two individuals having the same fingerprint is less than one in billion. There are several 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 measure the visual features of the human body. In voice recognition sound sensations 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 facilitate the verification process.

Signature recognition: Signature recognition is the process used to recognize an individual's hand-written or signature. Dynamic signature verification technology uses the behavioral biometrics of a hand written signature to

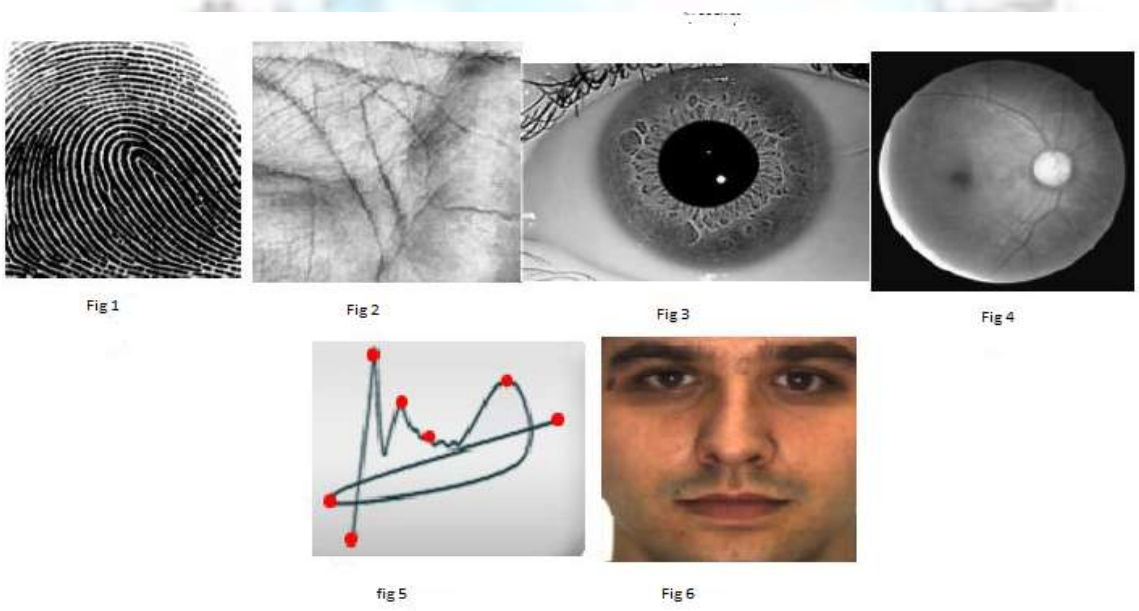
confirm the identity of a computer client. Analyzing the speed, shape, stroke, and pen pressure and timing information during the act of signing natural does this.[3]

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 bulky but identification is done in a short time.

Hand Geometry Hand: Hand geometry has 3-D image of top and sides of hand and fingers is collected and the feature vectors are extract and compared with the dataset feature vectors. It is recognition devices are bulky 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 process start to get something on film. For this a specialized camera is required, naturally very close to the subject, not above three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. Complete process takes only few seconds (approximately 1 to 2 sec) and provides the details of the iris knowingly produce, recorded and stored in dataset for future identification and verification. 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 produce 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 pattern 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 directly visible and so a coherent infrared light source is necessary to illuminate the retina. The infrared energy is immersed more rapidly by blood yacht in the retina than by the surrounding tissue. The image of the retina blood vessel pattern is then analyzed for characteristic points within the pattern. The retina scan is more susceptible to some diseases than the iris scan, but such diseases are relatively rare [4]



Biometrics traits: Fig1. Fingerprint Fig2. Palm Fig3. Iris Fig4. Retina Fig5. Signature and Fig6. Face

IV. Advantages and Disadvantages

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[6].

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.

V. Conclusion

Biometrics is a rapidly evolving technology that is being widely 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: improved security, it is reduced con and password administrator costs, easy to use and make life more secure and comfortable. But it is not possible 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, in Iris-scan Too much movement of head or eye, in Hand geometry Bandages, and in Signature-scan Different signing positions. Face recognition technology are more reliable, non-intrusive, inexpensive and extremely accurate. Currently Face recognition technology is the most challenging recognition technologies.

Acknowledgment

I would like to thank Mr. Sukhwinder for giving me this opportunity to present this review paper and my parents and my friends for their invaluable assistance.

References

[1]. Tripathi, K P, 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]. Zdeněk R íhaVáclavMatyáš "Biometric Authentication Systems ", FI MU Report Series, November 2000.
[5]. Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.
[6]. Vaclav Matyas, ZdenekRiha, "Biometric Authentication Systems".
[7]. Bhatia Renu, "Biometrics and Face Recognition Techniques", Pattern Analysis and Machine Intelligence, IEEE Transactions on Volume 3, Issue 5, May 2013.
[8]. Introduction to biometrics page at www.biometrics.gov.