ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Biometric Cryptosystems: for User Authentication

Shobha. D

Assistant Professor, Department of Studies in Computer Science, Pooja Bhagavat Memorial Mahajana Post Graduate Centre, K.R.S. Road, Metagalli, Mysuru, Karnataka, India

ABSTRACT: Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioral characteristic. There are number of emerging developments that are important to the continued commercial growth of the biometrics industry. Biometrics offers greater security and convenience than traditional methods of personal recognition. Person could be identified based on “who she/he is" rather than "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). In this paper, a brief overview of biometric methods will be presented.

KEYWORDS: Biometrics, Recognition, Verification, Identification, Security, authentication.

I. INTRODUCTION

Representations of identity such as passwords and cards no longer suffice. Further, passwords and cards can be shared and thus cannot provide non-repudiation. In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes. (Biometrics, which refers to automatic recognition of people based on their distinctive anatomical e.g., face, fingerprint, iris, retina, hand geometry and behavioral e.g., signature, gait, characteristics, could become an essential component of effective person identification solutions because biometric identifiers cannot be shared or misplaced, and they intrinsically represent the individual's bodily identity.)

A biometric is a physiological or behavioral characteristic of a human being that can distinguish one person from another and that theoretically can be used for identification or verification of identity. Since the beginning of civilization, identifying fellow human beings has been crucial to the fabric of human society. Consequently, person identification is an integral part of the infrastructure needed for diverse business sectors such as finance, health care, transportation, entertainment, law enforcement, security, access control, border control, government and communication.

II. BIOMETRIC SYSTEMS

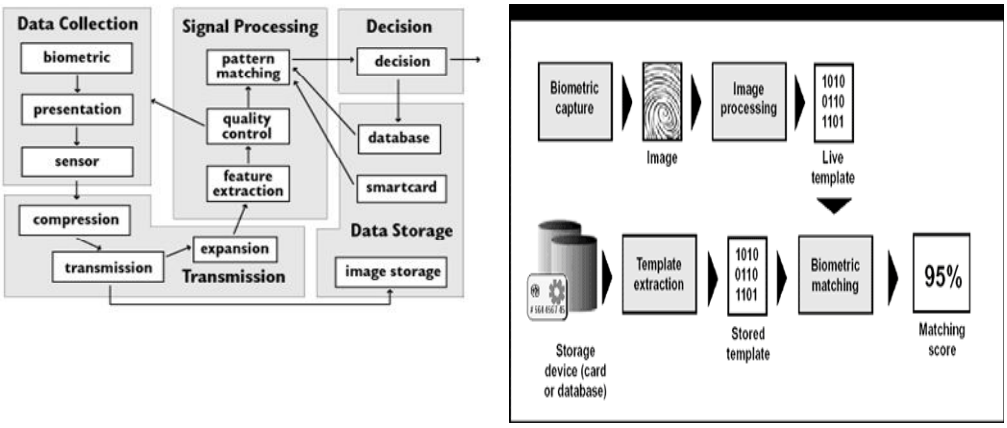
A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses [1]. Depending on the application context, a biometric Authentication Process typically operates in one of two modes: verification or identification through Acquisition, Creation of Master characteristics, Storage of Master characteristics, Acquisition(s), Comparison ,Decision. That is the hardware captures the salient human characteristic, the software interprets the resulting data and determines acceptability.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015



In verification mode, the system validates a person's identity by comparing the captured biometric characteristic with the individual's biometric template, which is prestored in the system database. In such a system, an individual who desires to be recognized. In identification mode, the system recognizes an individual by searching the entire template database for a match. The system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database). The question being answered is, "Who is this person?" Identification is a critical component of *negative recognition* applications, in which the system establishes whether the person is who she (implicitly or explicitly) denies being.

III. BIOMETRIC AUTHENTICATION CAPABILITY

Biometrics cannot be lost or forgotten.... They are difficult for attackers to forge and for Users to repudiate. To attack a biometric-based system, however, the hacker must generate (or acquire) a large number of samples of the biometric (for example, fingerprints); this is more difficult than generating a large number of PINs or passwords. Finally, system administrators can arbitrarily reduce a biometric system's false match rate for higher security—at the cost of the increased inconvenience to users resulting from a higher false nonmatch rate .

A biometric scanning device takes a user's biometric data, such as an iris pattern or fingerprint scan, and converts it into digital information a computer can interpret and verify. Since it is more difficult for a malicious hacker to gain access to a person's biometric data.Biometrics can be used for both physical access to corporate buildings and internal access to enterprise computers and systems.

IV. COMMONLY USED BIOMETRICS DEVICES

- Retina scanning
- Iris scanning
- Fingerprint scanning
- Hand scanning
- Face recognition
- Voice recognition & DSV
- Signature recognition

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

- Keystroke recognition

Retina Scanning

User Looks into a Viewer and Focuses on a Point; Infrared Light Scans Retina. Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature, this is one of the most secure biometric. Image acquisition requires a person to look through a lens at an alignment target; therefore it implies cooperation of the subject.

Iris Scanning

User looks at a camera (distance from camera increasing rapidly to 2-3 feet) , Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette [4]. Iris is colored and visible from far ,no touch required , overcomes retinal scanner issues ,contact lenses an issue? Iris and retinal scans are considered to be a more secure form of biometric authentication, since copying a person's retinal pattern is a much more difficult task than copying a fingerprint.

Finger Scanning

Fingerprint scanners are one of the oldest forms of biometrics and have been largely reliable when it comes to authentication. These systems are easy to use, which makes them favorable among users. It is widely known that the fingerprint is unique, and invariant with aging, which implies that user authentication, can be relied on the comparing two fingerprints [2]. A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high [3]. In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points [4]. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template.

Hand Scanning

The essence of hand geometry is the comparative dimensions of fingers and the location of joints, shape and size of palm. The technique is very simple, relatively easy to use and inexpensive. Geometry of users hands, more reliable than fingerprinting, Balance in performance and usability, it need Very large scanners.

Facial Recognition

Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. The most popular approaches to face recognition are based on either: 1) the location shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces [2]. Performance of commercially available systems is reasonable there is still significant room for improvement since false reject rate (FRR) is about 10% and false accept rate (FAR) is 1% [5].

Voice Recognition & DSV

The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state. User speaks into a microphone or other device, such as a telephone handset. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrollment time, and more than one enrollment session is often necessary .

Signature Recognition

User signs name on a device Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Keystroke Recognition

User types standard sample on keyboard, Keystroke dynamics is a behavioral biometric; for some individuals, one could expect to observe large variations in typical typing patterns. Advantage of this method is that keystrokes of a person using a system could be monitored unobtrusively as that person is keying information

Comparison of several biometric technologies

BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Worn ridges; hand or finger impairment	None	Hand impairment	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Permanence	High	Medium	Medium	High	Low
Collectibility	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low
Acceptability	Medium	High	Medium	Low	High
Potential for circumvention	Low	High	Medium	Low	High

Technique	Strengths
Retina	Highly accurate
Iris	Highly accurate ; Works with eyeglasses; more acceptable to users than retina scan
Fingerprint	Mature technology; highly accurate; low cost; small size, becoming widely acceptable.
Hand/Finger Geometry	Accurate and flexible; widely acceptable to users
Face Recognition	Widely acceptable to users; low cost; no direct contact; passive monitoring possible
Voice Recognition	Usable over existing telephone system; good for remote access and monitoring;
Signature Recognition	Widely acceptable to users
Keystroke Recognition	Widely acceptable to users; low cost; uses existing hardware

V.CONCLUSION

Any system assuring reliable person recognition must necessarily involve a biometric component. Because of the unique person identification potential provided by biometrics, they have and will continue to provide useful value by deterring crime, identifying criminals, and eliminating fraud. The identification of new uses for biometric devices given the potential for very low cost over the longer term. Biometrics is one of the important and more interesting pattern recognition applications with its associated unique legal, political and business Challenges. An emerging technology such a biometrics is typically confronted with unrealistic performance expectations and not fairly compared with existing alternatives (e.g., passwords) that we have resigned to tolerate. A successful biometric solution does not have to be 100% accurate or secure. A particular application demands a *satisfactory* performance justifying the additional investments needed for the biometric system; the system designer can exploit the application context to engineer the system to achieve the target performance levels.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

In this work, we have explored the fundamental roadblocks for widespread adoption of biometrics as a means of automatic person identification.

REFERENCES

[1] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy, March/April 2003, pp. 33-42
[2] Jain, L.C., Halici, U., Hayashi, I., Lee, S.B., Tsutsui, S.: Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press LLC, (1999)
[3] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, A. K. Jain, "FVC2002: Fingerprint verification competition" in Proc. Int. Conf. Pattern Recognition (ICPR), Quebec City,QC, Canada, August 2002, pp. 744-747
[4] J. Daugman, "How Iris Recognition Works", IEEE Trans. on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 21-30, January 2004
[5] P. J. Philips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, J. M. Bone, "FRVT2002: Overview and Summary," available at: http://www.frvt.org/FRVT2002/documents.htm.
[6] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec. 2003, pp. 2019-40.
[7] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 24, No. 8, pp. 1010-1025, August 2002.
[8] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric Cryptosystems: Issues and Challenges", Proceedings of the IEEE, Special Issue on Enabling Security Technologies for Digital Rights Management, Vol. 92, No. 6, June 2004.