ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

A Survey on Biometric Recognition Techniques

ARULALAN.V[1], BALAMURUGAN.G[2], PREMANAND. V[3]

M.TECH, Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India [1]

M.TECH, Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India[2]

M.TECH, Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology, Puducherry, India [3]

Abstract: Biometrics is an evolving technology which is used in various fields like forensics, secured area and security system. Biometric system takes the base for the pattern recognition system that recognise a person with authentication by using different features such as Fingerprint, Retinal Scan, Iris scan, Hand geometry and Face recognition. These are the major biometrics systems. These are used in various applications like ATM, cellular phones, secure access to a building. Biometrics are designed to enhance the security and reduce vulnerability. In this paper different biometrics techniques such as Fingerprint, Iris Scan, Retinal Scan, Face Recognition, Hand Geometry, Voice and Signature are available to implement a biometric system.

Keywords: Biometrics, Biometric Recognition, Techniques.

I. INTRODUCTION

Biometrics system recognise a person using his/her physiological and behaviour characters. Before biometric people identification done with their scar, colour and etc., now the current biometric plays with Iris, veins, voice and finger print. Biometrics takes once step high in security level. For secure identification and personal verification. In future even the internet banking transaction can be done with highly secure to avoid fraudulent finance.

A Biometric can be either Identification (who am I) 1: n or Verification (am I who I claim I am?)1:1

APPLICATION

Finger biometric has been widely used in large number of government application and also in our own laptop for log in, even they were used in international border crossing. In automobile instead of key Finger print biometric is used. Due to increased security threats, ICAO (International Civil Aviation Organisation) has approved to use of e-passport.

SURVEY OF VARIOUS BIOMENTRIC RECOGNITION

Many biometric system are available in various applications. Biometric means "life measurement". Each human acquire some sole physiological characters to identify a person. There is no biometric is optimal; depending upon the application they were used. A brief introduction of commonly used biometrics is given below.

I. Fingerprint Recognition

Fingerprint biometric is widely used in various fields for security. Fingerprint identification are used for past many year by matching. A Fingerprint contains patterns of valley and ridges on the surface of finger lips. Even for twins the Fingerprint won't be same. It is probable that two individual having same fingerprint less than one in billion. The cost of this biometric is low and they were embedded in laptops also. The accuracy of current biometric system is adequate for verification. Only one problem in current biometric that it requires large amount of computational resource, when using in identification mode. Finally the fingerprint biometric is not suitable for some factors like aging, environmental or occupation reason (e.g.: manual workers who use had frequently for their work). The main advantages of fingerprint biometrics are easy to use, economy, very high accuracy and small size for template. The disadvantages are change quickly for children, compose mistake with dryness or dirty in fingers and a cut or scar on finger.

II. IRIS RECOGNITION

Iris recognition is an automated method of biometrics identification that uses mathematical path recognition technique. The visual texture of iris is formed during fetal development and becomes stable in first two years itself. Iris recognition is also widely used, it is feasible in large scale. Each iris are different for twins like finger print. It is extremely difficult to change iris pattern and it'seasy to detect the artificial iris. For iris scan a specialized camera is required. The complete process will take few seconds only. The main advantages of iris recognition are very high accuracy and verification times takes less than five seconds. The disadvantage of this recognition are cost is high, too much movement of head and use of colour contact lens.

III. Face Recognition

A facial recognition is computer application for automatically identify or verify a person from a digital

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

images or a video frame from a video source. One method to proceed by comparing selected facial features from the image and a facial database. Face recognition records the spatial geometry of unique features of the face. This technique is used to identify terrorist and criminal and etc. This is a non-intrusive, cheap technology. Face recognition is a challenging task for the researchers, on one side its applications is used for verification and recognition on other side it is complicated to implement due to all different situation that a human face can be found. Face recognition is including five stages such as extracting the image of individual face, locate image of face, analysis of facial image, comparison and match or no match. Facial recognition ranges from single to multiple background (e.g.: airport).

The most common approach for face recognition is based on either the location, shape of facial attributes such as eyebrows, eyes, nose, lips, and their spatial relationships or the overall analysis of face image that represents a face as a weighted combination of number of canonical faces. For best work of facial recognition system in practise, it should automatically

(i) Detect whether face is available in the acquired image.
(ii) Locate the face if there is only one face and,
(iii) Recognize the face.

Facial, hand and hand vein infrared thermogram: the pattern of heat radiation from human body is a characteristic of an individual and can be capture by infrared cameras. But it is difficult to implement in heat emanating environment like room heater and etc. It is expensive and used with thermograms.

IV. DNA RECOGNITION

Deoxyribo nucleic acid (DNA) is the one dimensional unique pattern for one's individuality but in case of identical twins have identical DNA patterns. This technology is mostly used in forensics application for person recognition. DNA recognition has three main issues to limit the utilization of this biometrics for other application.

(i) Contamination process and Sensitivity module: Easy to take a portion of DNA.
(ii) Automatic recognition issues in real time: The current technology for DNA pattern matching requires cumbersome chemical method involving an expert's skill.
(iii) Privacy issues: With the DNA pattern of a person certain diseases can be gained.

V. HAND AND FINGER GEOMETRY

Hand geometry recognition system are based on a measurements taken from the human hand, which includes shape, size and length and widths of fingers. Commercial hand geometry based verification system were used in various places around the world. This technique is very simple, easy to use and also inexpensive. Environmental factors such as dry weather won't affect the verification accuracy of hand geometry based system. Hand geometry information may not be invariant during growth period of children. In addition, an individual jewellery (e.g.: ring) or limitations in dexterity may leads to further challenges in extracting correct informations.

The size of this device is larger and it can't be embedded in certain devices like laptop or mobiles devices. Instead of using entire hand, there are some verification systems that based on measurement of few fingers.

VI. Palm Print Recognition

Palm print recognition is more or like finger print recognition both contains pattern of ridges and valleys. The size of the palm is larger comparing to the Finger, as a result palm print scanner needs to capture larger area and also they are more expensive.

Human palm contains some additional distinctive features such as principal lines and wrinkles that can be captured with low resolution scanner, which would be cheap. So with the help of high resolutions scanners all features of palm such as hand geometry, ridges and valleys features, principal lines and wrinkles can be extracted to build highly accurate biometric system.

VII. RETINAL SCAN RECOGNITION

Then retinal vasculature is highly rich in structure. It is said to be most secure biometric since it is difficult to change or duplicate the retinal vasculature. The image acquisition done by a person to peep into an eye- piece and focus to find specific spot in visual field.

The image acquisition involves co-operation from the opposite side also. Retinal vasculature can reveal some medical conditions like hypertensions.

VIII. SIGNATURE RECOGNITION

Signature verification method in various fields like government, legal and commercial transactions. Signature is a behavioural biometric that change over a period of time. Signature of some people vary substantially: even successive impressions of their signature looks different. Further professional forgers may able to reproduce signature that freaks the system.

IX. VOICE RECOGNITION

Voice is the combination of physiological and behavioural biometrics. The physiological characteristic of human voice may be unique but the behavioural characteristic of human may change over a period of time due to illness, age, emotional state, etc.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Voice is also not very distinctive and may not be suitable for large scale identifications. Text dependent voice recognition system is based on the pitch of a predetermined phrase. It is more difficult to design a text independent system than a text dependent systems but offers high secure against

Characteristics	Face	Retina	Iris	Hand Geometry	Fingerprints	Signature	Voice
Easy to use	Medium	Low	Medium	High	High	High	High
Error factors	Lighting, age, glasses, hair.	Glasses	Lighting	Hand injury, age	Dryness, dirt, age	Changing signature	Noise, colds
Correctness	High	Very high	Very high	High	High	High	High
Long term permanence	Medium	High	High	Medium	High	Medium	Medium

Fraud. The main disadvantages of voice based recognition is that speech features may be affected by some factors like background noise. Speakers recognition is most appropriate in phone based applications but the voice signal overall phone is typically degraded in quality due to low quality microphones and the communication channels.

BIOMETRIC RECOGNITION ALGORITHMS

I. Fingerprint Recognition Algorithm

A series of ridges and furrows makes the fingerprint on the surface of the finger. Every human possess unique, immutable fingerprint. With the help of furrows and ridges as well as minutiae can be used to determine the inimitability patterns of the fingerprint. Minutiae points are local ridges characteristics that occur at either a ridge ending or ridge bifurcation. To remove noise and irrelevant information fingerprint pre-processing is done. The steps of Pre-processing are Image Normalization, binarization, making of minutiae and etc.

Two algorithms for fingerprint are
1. Pattern segmentation.
2. Minutiae local mapping.

The main factors of fingerprint algorithm are
1. Normalisation.
2. Segmentation.
3. Filtering.

II. Face Detection Algorithm

There are three steps of process for face recognition process. They are:
1. Face detection.
2. Feature extraction.
3. Feature recognition.

The main approaches for face detection algorithms is
1. Texture of unique mapping detection.

III. Iris Recognition Algorithm

The unique details of the individual were collected in Iris Recognition system. There are four modules of Iris Recognition methods.
1. The pupil region were extracted with the help of Morphological Operator. Under Morphological ed
2. Localization of centre and inner boundary.
3. Localization of outer boundary.
4. Sectoring.
5. Normalization.
6. Iris code Generation and Indexing.

IV. Retina Recognition

The Algorithm for Retina Recognition is
1. Orientation of special swing.

CONCLUSION

The Biometric Recognition system uses physical characteristics such as fingerprint, face, voice, hand geometry, iris and retina. Biometric Recognition system replaces the existing security system which are used in some places like ATM, Passport, Credit cards, access control and Etc., the Biometric system are found to be more accuracy and more effective too. These systems can process only in presence of person. Hence these biometric systems are proved to be highly secured system.

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] Zdeněk Říha Václav 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] DeVel, 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. "Oregon DMV is going to start using "facial recognition" software, a new tool in the prevention of fraud, required by a new state law. The law is designed to prevent someone from obtaining a driver license or ID card under a false name."
[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
[12] KresimirDelac, MislavGrgic "A Survey on Biometric methods," IEEE Conf. on Electronics in marine, June 2004.
[13] Sulochanasonkamble, dr. ravindrathool, balwantsonkamble "survey of biometric recognition systems and their applications" Journal of Theoretical and Applied Information Technology, 2005-2010.
[14]K.Rajasri, S.Sathiyadevi, S.Tamilarasi " new algorithm and indexing to improve the accuracy and speed in iris recognition", International Journal of Engineering Research and Development, 2012.

BIOGRAPHIES

ARULALAN.V

Completed Bachelor degree in Computer Science & Engineering at 2012 and pursuing Master Degree in computer science and engineering under Pondicherry university, [MIT] Manakula Vinayagar Institute of Technology.

BALAMURUGAN.G

Completed Bachelor degree in Computer Science & Engineering at 2013 and pursuing Master Degree in computer science and engineering under Pondicherry university, [MIT] Manakula Vinayagar Institute of Technology.

PREMANAND.V

Completed Bachelor degree in Computer Science & Engineering at 2012 and pursuing Master Degree in computer science and engineering under Pondicherry university, [MIT] Manakula Vinayagar Institute of Technology.