International Journal of Web Technology
Volume: 04 Issue: 02 December 2015 Page No.100-102
ISSN: 2278-2389

Facial Feature Recognition Using Biometrics

Brindha T,MS Josephine

Research scholar,Dr MGR Research institute and Educational University,Maduravoyal, Chennai
Prof Dept of MCA,Dr MGR Research institute and Educational University,Maduravoyal, Chennai
brindhatsambandam@gmail.com

Abstract-Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness. Biometric requires no physical interaction on behalf of the user. Biometric allows to perform passive identification in a one to many environments. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However individuals biological traits cannot be misplaced, forgotten, stolen or forged.

Keywords— Face recognition, low intrusiveness, corrupted, Pins

I. INTRODUCTION

Face recognition is not perfect and struggles to perform under certain condition. A researcher at the Carnegie Mellon Robotics Institute, describe one obstacle "Face recognition has been getting pretty good at full frontal faces and 20 degrees off, but as soon as u go towards profile, there have been problems".Other conditions where face recognition does not work will include poor lighting, sunglasses, long hair or other objects partially covering the subjects face and low resolution images. Another serious disadvantage is that many systems are less effective if facial expressions vary. The effectiveness is critics of the technology complain that the London borough of New ham giving disappointing results. User interface captures the analog or digital image of the persons face. In the enrollment module the obtained sample is preprocessed and analyzed. This analyzed data is stored in the database for the purpose of future comparison.As compared with other biometrics systems using finger print/palm print and iris, face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified and the identification does not require interacting with the person. It uses existing hardware infrastructure, existing cameras and image capture. Devices will work with no problems. In addition, face recognition serves the crime deter rant purpose because face images that have been recorded and archived can later help identify a person.Face recognition technology may solve this problem since a face is undeniably connected to its owner except in the case of identical twins. It's non-transferable. The system can then compare scans to records stored in a central or local database or even on a smart card.

Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness. From time to time we hear about the crimes of credit card, fraud, and computer break-ins by hackers, security breaches in a company or government building. In the year 1998, sophisticated cyber crooks caused well over US$100 million in losses. In most of these crimes, the criminals were aware taking advantage of a fundamental flaw in the conventional access control systems. The systems do not grant access by "who we are", but by "what we have", such as ID cards, keys, passwords, PIN numbers, or mother's maiden name. None of these means really define us. Rather, it is a means to authenticate us. This technology is based in a field called "biometrics". Biometric access control are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics, such as finger prints or facial features, or some aspects of the persons behavior like his/her handwriting style or key stroke patterns. Since biometric systems identify a person by biological characteristic they are difficult to forge.A biometric is a unique, measurable characteristic of a human being that can be used to automatically recognize an individual or verify an individual's identity. Biometrics can measure both physiological and behavioral characteristics. Physiological biometrics (based on measurements and data derived from direct measurement of a part of the human body) include:
a. Finger-scan

b. Facial Recognition
c. Iris-scan
d. Retina-scan
e. Hand-scan
Behavioral biometrics (based on measurements and data derived from an action) include:
a. Voice-scan
b. Signature-scan
c. Keystroke-scan
A "biometric system" refers to the integrated hardware and software used to conduct biometric identification or verification. Anonymously and passively captures passenger's facial features as they enter airport and then tracks them through their journey. Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness.

II. FACE RECOGNITION OVER OTHER BIOMETRIC

In this section we review the features that are used for face recognition section 2 discusses the face for recognition.

A. Face recognition features

There are number reasons to choose face recognition. This includes the following
a. It requires no physical interaction on behalf of the user.

b. It is accurate and allows for high enrolment and verification rates.

International Journal of Web Technology
Volume: 04 Issue: 02 December 2015 Page No.100-102
ISSN: 2278-2389

c. It does not require an expert to interpret the comparison result.
d. It can use your existing hardware infrastructure, existing cameras and image capture
Devices will work with no problems
e. It is the only biometric that allow you to perform passive identification in a one to many environments (e.g.: identifying a terrorist in a busy Airport terminal). People are more comfortable signing their names or speaking to a microphone than placing their eyes before a scanner or giving a drop of blood for DNA sequencing. Passwords and PIN's are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten , purloined or duplicated; magnetic cards can become corrupted and unreadable. However, and individual's biological traits cannot be misplaced, forgotten, stolen or forged.

Figure 1. Face for recognition

The facial identification is based on facial features left eye and the right eye, eyebrow, position of the nose, position of the mouth, chin shape, face width at nose position and face width halfway between nose tip and eyes. Figure 1 shows the features for recognition.Biometric based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm iris, retina, ear and voice) and behavioral traits (such as gait, signature and key stroke dynamics).Face recognition appears to offer several advantages over other biometric methods, a few of which are outlined here: all the technologies require voluntary action by the user.As compared with other biometrics systems using finger print/palm and iris face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified and the identification does not require interacting with the person. In addition, face recognition serves the crime deterrent purpose because face images that have been recorded and archived can later help identify a person.Anonymously and passively captures passenger's facial features as they enter airport and then tracks them through their journey. Face recognition is one of the few biometric methods that possess the merits of both high accuracy and low intrusiveness.

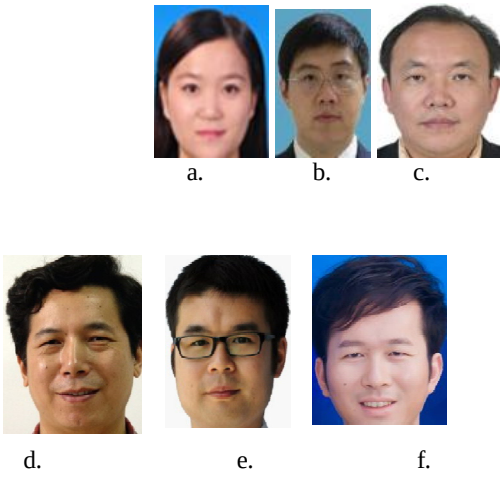

Figure 2. Features of the face

The figure 2 includes facial features of different persons. Figure 2 a. showing a female having front fore head with hair.The figure 2b. with person with hair at front and having spectacles worn. Figure 2 c. having bald at front face.Figure 2d. showing the face of a male having bulged chin.Figure 2e. showing the face of male with thick spectacles. Figure 2 f. showing the person of male with hair at forehead .From time to time we hear about the crimes of credit card, fraud, and computer break-in-ins by hackers, security breaches in a company or government building in the year 1998, sophisticated cyber crooks caused well over US$100 million in loss. In most of these crimes, the criminals were taking advantage of a fundamental flaw in the conventional access control systems. The systems do not grant access by "who we are ", but by " what we have", such as ID cards, keys, passwords, PIN numbers or mother's maiden name. None of these means really define us. Rather, it is a means to authenticate us. This technology is based in a field called "biometrics". Biometric access control are automated methods of verifying or recognizing living person on the basis of some physiological characteristics, such as finger prints or facial features , or some aspects of the persons behaviour like his/ her handwriting style or key stroke patterns. Since biometric systems identify a person by biological characteristic they are difficult to forge.

B. Use face for recognition

People are more comfortable signing their names or speaking to a microphone than placing their eyes before a scanner or giving a drop of blood for DNA sequencing. Passwords and PIN's are hard to remember and can be stolen or guessed; cards, tokens, keys, and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged.Face recognition appears to offer several advantages over other biometric methods, a few of which are outlined here: All the technologies require voluntary action by the user. The human face plays an important role in our social interaction, conveying people's identity. Using the human face as a key to security, biometric face recognition technology has received significant attention in the past several years due to its

International Journal of Web Technology
Volume: 04 Issue: 02 December 2015 Page No.100-102
ISSN: 2278-2389

potential for a wide variety of applications in law enforcement and non-law enforcement.As compared with other biometrics systems using finger print/palm print & iris face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person being identified, and the identification does not require interacting with the person. In addition, face recognition serves the crime deterrant purpose because face images that have been recorded and archived can later help identify a person.Biometric can measure both physiological and behavioral characteristics. Face recognition technologies have been associated generally with every costly top secure applications. Today the core technologies have evolved and the cost of equipment's is going down due to the increasing processing power. Certain applications of face recognition technology are now cost effective, reliable and highly accurate.

III. CONCLUSION

This paper discusses the unique measurable characteristic of a human being that can be used automatically recognize an individual or verify an individual's identity. Face recognition technologies have been associated generally with every costly top secure applications. In pattern recognition the feature extraction is one technique that is widely deployed due to its user friendliness.

REFERENCES

[1] Jain ,A.K.,Kumar,A.,2012 Biometric recognition: An overview, in : my ordim,E .,Tzovaras, D.(Eds), second generation Biometric: The ethical, legal and social context. Springer Netherlands Volume II of The International Library of Ethics, Law and Technology, pp 49-79.

[2] Math Works MATLAB, 2013. Computer Vision System Toolbox: 2013b - Video Stabilization Using Point Feature Matching. The Math Works Inc., Natick, Massachusetts, United States.

[3] T Wang, P Shi, Kernel Grassmannian distances and discriminant analysis for face recognition from image sets. Pattern Recogn.Lett. 30(13), 1161-1165(2009)

[4] K Koh, SJ Kim, S Boyd, l1_ls: simple Mat lab solver for l1-regularized least squares problems,(2008).http://www.stanford.edu/~boyd/l1_ls/.Accessed 13 January 2014

[5] K Fukui,O Yamaguchi, Face recognition using multi-viewpoint patterns for robot vision, in Robotics Research, ed. By Dario, R Chatila (Springer, Heidelberg, 2005), pp.192-201

[6] Zhifeng Li, Member, IEEE, Unsang Park and Anil K.Jain 'A Discriminative Model for Age Invariant Face Recognition'

[7] Young H.Kwon and Niels da Victoria Lobo 'Age Classification from Facial Images'