International Journal of Applied Research 2017; 3(5): 822-823

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2017; 3(5): 822-823
www.allresearchjournal.com
Received: 28-03-2017
Accepted: 29-04-2017

Sunita Roy
Ph.D. Scholar in the Department of Computer Science & Engineering, University of Calcutta, Kolkata, India

Samir K Bandyopadhyay
Professor of the Department of Computer Science & Engineering, University of Calcutta, Kolkata, India

Correspondence
Sunita Roy
Ph.D. Scholar in the Department of Computer Science & Engineering, University of Calcutta, Kolkata, India

Iris recognition using biometric techniques

Sunita Roy and Samir K Bandyopadhyay

Abstract
Data Security and Biometric systems found its application in present day lifestyle and it is being used in securing communication and identity around the world. Data security encompasses the realms of encryption, steganography, masking, erasure. and some others whereas biometric systems spearheads the protection of one's individuality by ensuring identity by means of distinguishable traits like- face, hand imprint, fingerprints, DNA, retina, etc. This paper utilized biometric systems that guarantees Security and Authenticity.

Keywords: Iris recognition, biometrics recognition, wavelet technology, hybrid technique and feature extraction

Introduction
In today's world of growing technology security is of utmost concern. Present status of the world says that everything that can be thought off can be done with the help of the internet. Even the monetary transactions are also done using the internet. With the amount of internet users rising up, everything that is transferred through internet is under serious threat. It has become important to use various security methods to protect the data that we exchange. Biometrics are automated methods of recognizing a person based on a physiological or behavioural characteristic.

The security field for authentication such as password, PIN, a card key, smart card, token or a biometric. Of these, the method of identification based on biometric characteristics is preferred for various reasons such as: The person to be identified is required to be physically present at the time-of-identification.

A biometric system makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic"[1].

Biometrics "Biometrics" is usually determine unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometrics identification has eventually a much broader importance as computer interface is becoming more natural. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc. Image processing broadens the spectrum of biometric systems. Biometric system means the following:

Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent.

Verification - One to One: Biometrics can also be used to verify a person's identity. Biometric verification requires comparing a stored or enrolled biometric sample with a newly captured biometric sample.

During the beginning of the process, a raw biometric is captured by a sensing device such as a fingerprint scanner or photo camera and the image is fed as an input to the processing software.

The second phase of processing is to extract the distinguishing characteristics from the raw biometric image and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrolment and it is used for future processing that are needed for authentication.

Image processing is the study of any algorithm that takes an image as input and returns an image as output. Digital image processing performs image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It helps to avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems. It includes the following:

- Image display and printing
- Image enhancement
- Feature detection
- Image compression
- Image editing and manipulation

This paper proposed biometric systems that guarantees Security and Authenticity.

Review Works

Biometrics studies face, iris, fingerprints, voice, palms, hand geometry, retina, handwriting, gait etc. [3]. Recognition algorithms requires preprocessing of input image to get better quality of data by tracking various feature points of iris. Biometric systems captures the feature taking a digital image for iris recognition. A biometric is characterized by use of a feature that is decidedly unique – so that the chance of any two human having the same features will be minimal [1-2]. Person identification based on iris recognition gives one of the most reliable results [4]. Iris texture features provides a unique high dimensional information that explains why iris recognition based verification has the lowest false acceptance rate among all types of biometric verification systems [5-6].

Proposed Method

The major challenges of automated iris recognition by biometric techniques requires to capture a high-quality image of the iris. After getting the input image, the next step is to identify the circular edge in the region of interest. Finally the iris region of eye is detected. The output is shown in Figure 1 to Figure 4.

Fig 1: Original Image

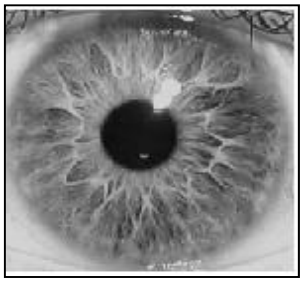

Fig 2: Gray image

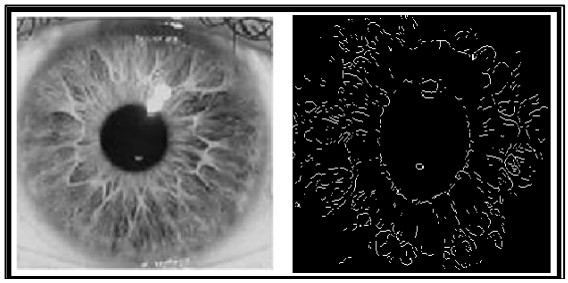

Fig 3: GrayImage and Edge Detected Image

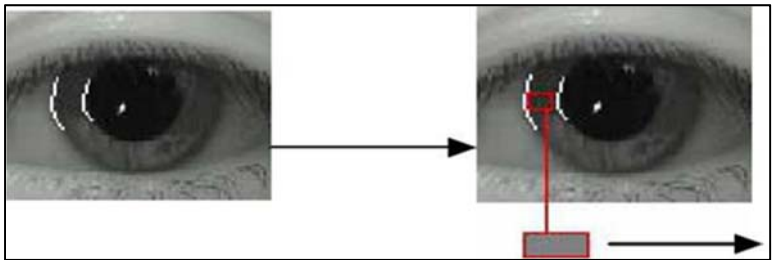

Fig 4: IRIS Effective Region Extracted

Conclusions

Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition. In this paper we highlighted the detection of iris using biotechnology technique.

References

1. Jain AK, Bolle RM, Pankanti S. (eds.): Biometrics: Personal Identification in Net-worked Society. Kluwer, Norwell, 1999.
2. Prabhakar S, Kittler J, Maltoni D, O'Gorman L, Tan T. Introduction to the SpecialIssue on Biometrics: Progress and Directions. IEEE Trans. Pattern Anal. Mach. Intell. 2007; 29(4):513-516.
3. Xiaofu He *et al*. A New Fake Iris Detection Method, M. Tistarelli and M.S. Ni Algirdas Bastys, Iris Matching by Local Extremum Points of Multi scale Tayl or Expansion, ICB2009, LNCS5558, 2009, 1070-1079. Springer-Verlag Berlin Heidelberg.
4. Daugman J, Dowing C. Epigenetic randomness, complexity, and singularity of human iris patterns. In: Preceding soft the Royal Society, B, 268, Biological Sciences, 2001, 1737-1740.
5. Daugman J. Statistical richness of visual phase information: update on recognizing Persons by iris patterns. Int. J. Comput. Vis. 2001; 45(1):25-38.
6. Pradnya Shende M, Dr. Milind Sarode V. Fake Biometric Detection Using Liveness Detection System Applications: Iris and Fingerprint Recognition System. International Journal of Research in Advent Technology (E-ISSN: 2321-9637) Special Issue 1st International Conference on Advent Trends in Engineering, Science and Technology ICATEST. 2015.