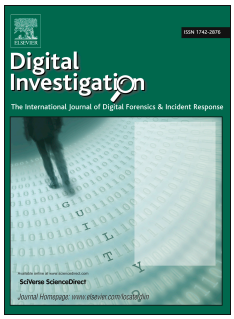
Accepted Manuscript



Detecting fake iris in iris bio-metric system

Vijay Kumar Sinha, Anuj Kumar Gupta, Manish Mahajan

PII: S1742-2876(17)30384-5

DOI: 10.1016/j.diin.2018.03.002

Reference: DIIN 749

To appear in: *Digital Investigation*

Received Date: 7 December 2017

Revised Date: 15 February 2018

Accepted Date: 12 March 2018

Please cite this article as: Sinha VK, Gupta AK, Mahajan M, Detecting fake iris in iris bio-metric system, *Digital Investigation* (2018), doi: 10.1016/j.diin.2018.03.002.

Detecting Fake Iris in Iris Bio-metric System

Vijay Kumar Sinha[1] , Dr. Anuj Kumar Gupta[2] , Dr. Manish Mahajan[3]
[1]Research Scholar , Punjab Technical University, Jalandhar, Punjab, India
Cecm.cse.vk@gmail.com
[2]Professor, CGCCOE , IKGPTU , Punjab, India anuj21@hotmail.com
[3]Professor & Head CSE , CGCCOE , IKGPTU , Punjab, India
cgccoe.hodcse@gmail.com

ABSTRACT

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irises of an individual's eyes, whose complex random patterns are unique and can be seen from some distance. Now days, Iris is being used widely by several organizations, including governments, for identification and authentication purposes. Aadhar, India's UID project uses Iris scan along with fingerprints to uniquely identify people and allocate a Unique Identification Number. Most of the work done in the area of Iris pattern recognition systems emphasizes only on matching of the patterns with the stored templates. Security aspects of the system are still unexplored. The available security algorithms provide only some cryptographic solutions that keeps the template database in a secret cryptographic form.We successfully enhanced the detection of fake iris images and add the provision of detection of false of scanned iris images as template. This enhanced significantly the performance of the system in terms of security and reliability. We use Flash and motion detection of natural eye to detect the liveliness of real iris images before matching from stored templates.

Keywords: Iris; Template; Luster, Cryptography; Biometrics; UID

1. INTRODUCTION

In today's general public, security is a noteworthy concern and is turning out to be progressively vital. Cryptography has ended up a standout amongst the best ways and has been perceived as the most mainstream innovation for security purposes. History demonstrates that people can recall just short passwords; most clients even have a tendency to pick secret word that can be effectively speculated utilizing lexicon or animal power systems. This confinement has set off the utilization of biometrics to create solid cryptographic key. Biometrics is interesting to every person and it is solid. For a considerable length of time, information/individual security in the business world has been generally taking into account passwords, PINs, or a security question, for example, mother's last name by birth or singular's date of conception and so on. This security/ID highlight is effectively overlooked, stolen, shared or split. Biometrics is an estimation of the human body natural or physical qualities to decide the human character. There are diverse sorts of biometric advances accessible today which incorporate fingerprints, face, iris/retina, hand geometry, signature, DNA, keystroke and tongue and so forth. Biometrics offered an inseparable connection from the authenticator to its proprietor, which can't be overcome by passwords or tokens, since it can't be loaned or stolen. Biometrics is utilized to improve the protection and security shortcomings that exist in the present security innovation, for example, straightforward watchword or PIN validation. Another favorable position of biometrics is that it can distinguish and keep different IDs. Despite the fact that biometrics is one of a kind among all people, it is unrealistic to utilize biometrics as an immediate cryptography key for the framework because of the distinction bits that happen in the format amid each verification. At the end of the day, every time the filtered biometric picture varies in minor extent. Biometric pictures or layouts are variable by nature which implies each new biometric test is constantly distinctive. Clamors and blunders may happen in the caught picture because of burst or foundation mistake and subsequently the produced format is diverse amid each confirmation. There is additionally mindfulness concerning the protection and the security of individual data because of the stockpiling of the biometric layouts. The misfortune or trade off of biometric layouts may wind up in unusable biometric. Iris acknowledgment biometric frameworks apply scientific example acknowledgment procedures to pictures of the irises of a singular's eyes.

2. THE PRINCIPLE

The structure of the human eye is appeared in Fig 1. Iris is the external dull segment

(chestnut, dark, blue or green) encompassing the focal part called the understudy behind which lies the lens. The white segment (called sclera) encompasses the iris.

Fig. 2 demonstrates the point of interest of the iris (alongside focal understudy). The examples of the iris are unmistakably obvious in Fig 2. These examples are special in each human and are additionally exceptional in every eye i.e. left and right eye of the same person. These novel examples of the individual's eyes can be utilized to recognize the individual.

In iris acknowledgment framework a singular's eyes are filtered by a high determination scanner (Fig. 3) and after that these pictures are handled by the PC to make secure and dependable advanced formats and put away in the information base.

For confirmation, the pictures of the objective individual's iris are contrasted and the formats put away in the databank. In the event that the match happens, the check procedure is fruitful generally not.

With the expanding necessities for higher security level, biometric frameworks have been generally utilized for some applications [22-24]. Biometric acknowledgment or, essentially, biometrics alludes to the programmed acknowledgment of people in view of physiological or behavioral qualities. Biometrics including face, iris, fingerprints, voice, palms, hand geometry, retina, penmanship, walk and so forth have been utilized for the security applications and have numerous preferences contrasted with the conventional security frameworks, for example, recognizable proof tokens, secret key, individual distinguishing proof numbers (PINs) and so forth. Iris acknowledgment is a standout amongst the most encouraging routines in light of the fact that the iris has