International Journal of Information and Computation Technology (IJICT)
ISSN 0974-2239 Volume 3, Number 10 (2013)

PERFORMANCE COMPARISON OF FAKE IRIS DETECTION METHODS

Smriti Rastogi[1], Dr. D. Malathi[2]

[1] *M Tech Scholar, Department of Software Engineering*
SRM University, Kattankulathur, Chennai

[2]*Professor, Department of Computer Science and Engineering*
SRM University, Kattankulathur, Chennai

ABSTRACT

Among several available biometric systems –Iris Recognition Systems are said to be the most secure system because the iris patterns are unique and texture of the iris is hard to make a copy of it. But now by using colored lenses and textured lenses miscreant can breach the secure system and can access the confidential information of the legitimate user. So there should be some efficient methods to detect the lens wore by the user. In this paper four existing methods of detecting coloured texture lenses and high resolution iris images in iris recognition systems, are compared and analyzed based on -False Acceptance Ratio (FAR), False Reject Ratio (FRR), Correct classification Rate (CCR).

Keywords- Biometric systems; Contact lens; Correct Classification Rate (CCR); False Acceptance Ratio (FAR); False Reject Ratio (FRR); Spoofing attacks; Spoof detection;

1. INTRODUCTION

THE security field uses three different types of authentication [3]: *Something you know*—a password, PIN, or piece of personal information (such as your mother's maiden name), *Something you have*—a card key, smart card, or token (like a Secure ID card), *Something you are*—a biometric. The word biometrics comes from two Greek words “bio” and “metrics” which means life measurement. Any characteristic can be used as a biometric identifier if every person possesses the characteristic, it varies from person to person, its properties do not change considerably over time, and it can be measured manually or automatically. Biometrics is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. With the increasing requirements for higher security level, biometric systems have been widely used for many applications. Iris recognition is one of the most promising methods because the iris has the great mathematical advantage that its pattern variability among different persons is enormous. In addition, as an internal (yet externally visible) organ of the eye, the iris is well protected from the environment and stays unchanged as long as one lives.

In general biometric systems work in two modes [1]: *Enrolment mode:* In this mode biometric user data is acquired. This is mostly done with some type of biometric reader. Afterwards the gathered information is stored in a database where it is labeled with a user identity (e.g. name, identification number) to facilitate authentication. *Authentication mode:* Again biometric user data is acquired first and used by the system to either *verify* the users claimed identity or to *identify* who the user is. While *identification* involves the process of comparing the user’s biometric data against all users in the database, the process of *verification* compares the biometric data against only those entries in the database which are corresponding to the users claimed identity.

Biometrics can be divided into two broad categories-Behavioral and Physiological. Behavioral biometrics are based on unique ways people do things such as walking, talking, signing their name, or typing on a keyboard (speed, rhythm, pressure on the keys, etc).By contrast, physiological biometrics are based on a person’s physical characteristics which are assumed to be relatively unchanging such as fingerprints, iris patterns, retina patterns, facial features, palm prints, or hand geometry.

Types of biometric systems are:

1.1 Bertillonage System

The first type of biometrics came into form in 1890, created by an anthropologist named Alphonse Bertillon [5]. He based his system on the claim that measurement of adult bones does not change after the age of

Fig. 1.*Bertillonage System*

Fig. 2. *Fingerprint Recognition*

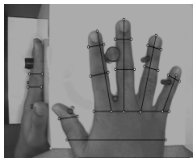

Fig. 4. *Hand Geometry Recognition System*

Fig. 5. *Image of Iris*

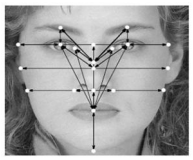

Fig. 6. *Face Recognition*

20.The method consisted of identifying people by taking various body measurements like a person's height, arm length, length and breadth of the head, the length of different fingers, the length of forearms, etc. using calipers. The Bertillonage System is shown in *figure 1*. However, the methodology was unreliable as non-unique measurements allowed multiple people to have same results, decreasing the accuracy and hence is no longer used.

1.2 Fingerprint Recognition

It involves taking an image of a person's fingertips and records its characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae [2]**.**The Fingerprint Recognition System is shown in *figure 2.*

1.3 Hand Geometry

Hand geometry involves analyzing and measuring the shape of the hand [2] [5]. This biometric offer a good balances of performance characteristics and is relatively easy to use. The Hand Geometry Recognition System is shown in *figure 4.*

1.4 Retina Recognition

A retina-based biometric involves analyzing the layer of blood vessels situated at the back of the eye. An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina.

1.5 Iris Recognition

Iris scan biometrics employs the unique characteristics and features of the human iris [as shown in *figure 5*], which remains unchanged throughout an individual's lifetime, in order to verify the identity of an individual [2]. The iris is the area of the eye where the pigmented or colored circle, usually brown, green, grey or blue, rings the dark pupil of the eye.

1.6 Face Recognition

Human face detection plays an important role in applications such as video surveillance, human computer interfaces, face recognition, and face image databases [2]. To enable this biometric technology it requires having at least a video camera, PC camera or a single-image camera. Nevertheless, this biometric approach still has to deal with a lot of problems and cannot work with acceptable identification rates unless certain restrictions are being considered. Finding a face in a picture where the position, the orientation, the background and the size of a face is variable is a very hard task and many algorithms have been worked on to solve this problem. Face Recognition process is shown in *figure 6.* Other problems with face detection occur whenever faces are partially covered, as with beards, glasses, hair style or hats; because a lot of information just stays hidden.

1.7 Signature Recognition

Signature verification is the process used to recognize an individual's hand-written signature. The Signature

Fig. 7. *Signature Recognition*

Recognition device is shown in *figure 7*.Dynamic signature verification uses behavioral biometrics of a hand written signature to confirm the identity of a person [2]. This can be achieved by analyzing the shape, speed, stroke, pen pressure and timing information during the act of signing. On the other hand there is the simple signature comparison which only takes into account what the signature looks like. So with dynamic signature verification, it is not the shape or look of the signature that is meaningful, it is the changes in speed, pressure and timing that occur during the act of signing, thus making it virtually impossible to duplicate those features. Devices which enable dynamic signature verification store the behavioral factors and the captured signature image itself for future comparison in their database. These devices account changes in one's signature over time by recording the time and the dynamic features each time a person uses the system.

1.8 Voice Recognition

Voice authentication is not based on voice recognition but on voice-to-print authentication, where complex technology transforms voice into text. Voice biometrics has the most potential for growth, because it requires no new hardware—most PCs already contain a microphone. However, poor quality and ambient noise can affect verification.

1.9 DNA Recognition

DNA Recognition employs Deoxyribo Nucleic Acid, which is the one dimensional ultimate unique code for ones individuality, except for the fact that identical twins have identical DNA patterns. However, it is currently mostly used in the context of forensic applications. The basis of DNA identification is the comparison of alleles of DNA sequences found at loci in nuclear genetic material. A set of loci is examined to determine which alleles have been identified

Biometrics are unique identifiers but they are not really the secrets [4] [6] e.g., fingerprints are left on everything to touch, facial geometry and iris patterns are visible while voices are being recorded. A sample of biometric can be acquired covertly by synthetic reproduction of anatomical identities e.g., acquisition of facial and iris images, lifting of latent fingerprints, or imitation of behavioral identity e.g., producing similar voice and prepare the digital artifacts. The digitized artifact is the cloned of a legitimate user's identity. The digital clone then is presented to the biometric system to get access as a legitimate individual and deceive the system.

Compared with other biometric modality, iris pattern has been regarded as one of the most accurate biometric modalities for its uniqueness, stability and non-intrusiveness. However, as other biometric systems, iris system is also under threat of forged iris attack. Efficient iris spoof detection can improve security of iris recognition systems. Some artifacts have been considered to spoof iris recognition system, such as paper printed iris, cosmetic contact lens, and redisplayed videos. Cosmetic contact lens is a contact lens with color texture printed on it. The *figure 9* shows different colour texture lenses. Spoof caused by wearing a cosmetic contact lens is particularly dangerous. It is easily accepted by the system and hard to detect.

Fig. 9. *Coloured Textured Lenses*

Following methods are useful for fake iris detection:

2. FAST FOURIER TRANSFORM AND QUALITY ASSESMENT

Authors discussed that the Daugman method of using Fast Fourier Transform (FFT) to check printed iris pattern which uses the characteristics of periodic dot printing [8] to detect fake iris can be failed if at input the counterfeit iris is defocused and blurred purposely. A new approach for detecting fake iris based on analysis of 2D Fourier spectra together with iris image quality assessment is proposed.

To evaluate the quality of non-clear or defocused and motion blurred fake iris images Laplacian of Gaussian (LoG) operator is used. The 2-D LoG function centered on zero with Gaussian standard deviation given in equation (1):

$$LoG(x,y) = -\frac{1}{\pi\sigma^4}\left[1 - \frac{x^2+y^2}{2\sigma^2}\right] e^{-\frac{x^2+y^2}{2\sigma^2}} \qquad (1)$$

where σ is the Gaussian standard deviation.
Different values of σ are set to get the different LoG operators. To simplify the computation 5x5 Laplace operators is selected. The non-clear feature of the fake iris is defined as the power of the convolution result given in equation (2):

$$f(I)=\frac{1}{W\times H}\sum_x\sum_y |C(x,y)| \qquad (2)$$

where *W* and *H* are the width and height of the image respectively. *I* denotes the iris image and *x*, *y* are variables denoting the pixel location. *C* is the convolution result with LoG filter. The larger the *f(I)* is, the clearer the image. Threshold θ_1 is set to detect non-clear iris.

If the fake iris is clear, there will four middle frequency high spots in the frequency spectral. In this case, first the Fourier transformation of the clear fake iris is done, which result in Fourier spectrum of the iris and in that Fourier spectrum there will be four highlighted middle frequencies in vertical and horizontal direction exist.

3. IRIS EDGE SHARPNESS (IES)

Textures that are printed on contact lens usually distributed over the outer half iris region i.e. on the edge and so these lenses make the iris edge sharper than the live one. Iris Edge Sharpness (IES) [9] is measured by the following formula equation (3):

$$IES=\sum_{\theta=0}^{2\pi}\left(I(r_{i+\xi},\theta)-I(r_{i-\xi},\theta)\right) \qquad (3)$$

where $I(r, \theta)$ is an iris image in polar coordinates, r_i is the iris radius and θ is the angle from an edge point to iris center, $I(r_{i+\xi}, \theta)$ and $I(r_{i-\xi}, \theta)$ represent pixel values in sclera and iris region , respectively.

4. REFLECTANCE RATIO BETWEEN IRIS AND SCLERA

This method [9] is based on the changing reflectance property between the iris and the sclera with variations of wavelengths of incident light. The wavelength of incident light is varied from 750nm to 850 nm.

In real iris, the reflectance of iris depends on the amount of melanin in the anterior border layer and the reflectance of melanin slightly increases as the wavelength of illumination increases from 750 nm to 850 nm. So for the real eye the reflectance ratio of iris to sclera is greater at longer wavelength than at shorter wavelength.

In fake iris the iris and sclera are made from same material so there is no change in reflectance ratio of iris and sclera.

5. DYNAMIC IRIS LOCALIZATION

This method [3] emphasizes on the segmentation and localization of the iris in iris recognition which affects more than half the efficiency of iris recognition. The assumption that the center of iris and pupil is same and iris is perfectly circular in shape is incorrect and it leads to loss of texture data near to pupil and/or outer boundary at segmentation and localization step. The irises have wide variations with respect to eye color and texture. This method uses two iris images at different light intensities. The iris localization consists of three steps: Outer boundary detection, Inner boundary detection and Normalization.
For outer boundary, tracing can be started from any corner of the image leading to a complete or incomplete circle. For inner boundary, the two images of iris taken at different light illumination are compared or subtracted. The iris part of the two images are same, result of subtraction will give 0 values. The region where nonzero values are obtained is the region of pupil. Tracing the inner boundary and selecting region outside inner boundary and below outer boundary will give the exact iris with minimum losses. Normalization of the image will give rectangular image which will be used as input for feature extraction.

6. COMPARISON

By FFT method and Quality assessment photo iris and print iris can be well detected. However, if the input counterfeit iris is defocused and blurred purposely, the counterfeit iris may be accepted as live one. This method has to be tested under large database to evaluate stability and reliability of this method.

Iris Edge Sharpness (IES) is simple measurement but highly dependent on segmentation accuracy. It gives better performance on database of contact lenses having similar texture color and pattern.

By using reflectance ratio between iris and sclera, it is possible to detect fake iris images with high accuracy. This method does not cause inconvenience to user since it can detect fake iris image at a very fast speed. It perfectly distinguished the live iris from fake iris made by not only high resolution inkjet and laser printers but also eye and gray and yellow contact lens. This method cannot always distinguish live iris from blue contact lens.

Dynamic Iris localization method showed the very high accuracy rate of iris segmentation and at comparable timing cost. It does not assume the centre of pupil and centre of iris as against other methods hence it is practical to use. Since it is based on comparison of two iris images at different light levels to detect the change in pupil size it is promising technique for making iris recognition systems more robust. The comparison table of the above mentioned methods based on FAR (False Acceptance Ratio), FRR (False Reject Ratio) and CRR (Correct Classification Ratio) is shown in *Table 1*.

Table 1. *Comparison of the four methods*

Methods	FAR (%)	FRR (%)	CCR (%)
FFT and Quality Assessment	-	-	Printed nonclear Iris-98.18
			Printed clear Iris-98.57
Iris Edge Sharpness (IES)	1.87	2.5	76.8
Reflectance Ratio between Iris and Sclera	Blue color Lens-40 and for others -0	0.28	-
Dynamic Iris Localization	-	-	-

7. CONCLUSION

In this paper, the four fake iris detection methods are compared. Even though the FFT method can detect photo and print iris it fails to detect under large database to evaluate stability and reliability. IES gives better performance on database of contact lenses having similar texture color and pattern but it is highly dependent on segmentation accuracy. The reflectance ratio between iris and sclera detect fake iris images with high accuracy, but it cannot always distinguish live iris from blue contact lens. The dynamic iris localization is a very promising technique in making iris recognition system more robust against fake iris based spoofing attempts. These methods can be combined and used in iris recognition system to develop a more secured system.

8. REFERENCES

[1] Anil K. Jain, Arun Ross and Salil Prabhakar, “An introduction to Biometric Recognition”, IEEE Transactions on circuits and systems for video technology vol. 14, no.1, January 2004.

[2] Igor B’ohm and Florian Testor, “Biometric Systems”, ResearchGate

[3] Rajesh Bodade and Rajesh Bodade, “Dynamic Iris Localisation: A Novel Approach suitable for Fake Iris Detection”, IEEE 2009.

[4] Sanjay Kumar Singh and Yogendra Narain Singh, “Vitality Detection from Biometrics: State-of-the-Art”, IEEE 2011.

[5] Siddhesh Angle, Reema Bhagtani, Hemali Chheda, “Biometrics: A Further Echelon of security”, 2005.

[6] Simon Liu and Mark Silverman, “A Practical Guide to Biometric Security Technology”, 2001.

[7] Sung Joo Lee, Kang Ryoung Park, Jaihie Kim, “Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera”, IEEE 2006.

[8] Xiaofu He, Yue Lu, Pengfei Shi, “A fake iris detection method based on FFT and quality assessment”, IEEE 2008.

[9] Zhuoushi Wei, Xianchao Qiu, Zhenan Sun and Tieniu Tan, “Counterfeit Iris Detection Based on Texture Analysis”, IEEE 2008.