World Applied Sciences Journal 29 (Data Mining and Soft Computing Techniques): 93-98, 2014
ISSN 1818-4952
© IDOSI Publications, 2014
DOI: 10.5829/idosi.wasj.2014.29.dmsct.17

Counter Measures Against Iris Direct Attacks Using Fake Images and Liveness Detection Based on Electroencephalogram (EEG)

[1]B. Sabarigiri and [2]D. Suganyadevi

[1]Research Scholar of Computer Science, Department of Computer Science,
Sree Saraswathi Thyagaraja College, Palani Main Road, Pollachi-642107, Coimbatore, India
[2]Computer Sciences, Sree Saraswathi Thyagaraja College,
Palani Main Road, Pollachi-642107, Coimbatore, India

Abstract: In current years, IRIS recognition is flattering a very dynamic topic in both research and sensible applications. In this part, fake IRIS is a possible hazard for IRIS based biometric systems. In this paper direct attacks using fake IRIS Images and its performance measures is presented. To improve the performance of the IRIS based biometric system the Electroencephalogram (EEG) is added. A widely presented IRIS recognition system is used for our experiments. This Multi-modality system represents the first endeavor to fuse the IRIS with a novel biometric modality--Electroencephalogram (EEG). Furthermore, it is established that Electroencephalogram (EEG) is an interesting complementary modality to improve the anti-spoofing ability of conservative biometrics based systems. Experimental results demonstrate that the highest identification performance is obtained in the Multi-modality system using IRIS and Electroencephalogram (EEG).

Key words: Anti-spoofing · Direct Attacks · Electroencephalogram (EEG) · Fake IRIS images · Multi-Modalities · Conservative Biometrics

INTRODUCTION

Implementing biometrics-based technologies has improved in current years and plateful to keep the nation and multi-national enterprises by keeping people and assets, more safe and to limit physical right of entry. Biometrics is having the skill to take a bodily trait as images and Signals, compute it and then use it as evidence of "who you are". The concept of personal uniqueness is significant from numerous perspectives. Uniqueness is a key concept in the universal world. The improvement of biometrics is an effect of globalization: the world is now a comprehensive place for commerce, migrations, trusted exchanges of all kind of information and values. Biometrics is radically different from any other system for automatic human ID because recognition and identity confirmation are not based on a token but on the body itself. Biometrics is the systematic authority of measuring appropriate attributes of living individuals or populations to make out lively properties or unique characteristics. IRIS recognition has gained popularity due to factors such as its superficial high accuracy, quick, robust, fast to compare, its non-contact acquisition method and the availability of low cost sensors due to improvements in technology. The IRIS is plainly visible, coloured ring that surrounds the pupil and it has a muscular structure. IRIS controls the amount of light entering the eye. Due to epigenetic nature of IRIS patterns each and every individual has a unique. IRIS is an externally visible internal organ which in turn remains plays a vital role through the human's entire life cycle. The IRIS formation starts at third month of born and the structures creating its pattern are largely complete by the eighth month of born and this formation wouldn't be changed though out the human being life. The two eyes of an individual hold IRIS patterns which are completely independent from one another are advantages of IRIS.

Corresponding Author: B. Sabarigiri, Computer Science, Department of Computer Science,
Sree Saraswathi Thyagaraja College, Palani Main Road, Pollachi-642107, Coimbatore, India.
Tel: +91-97882-06468.

But, there are many false techniques evolved to cheat every IRIS biometric sensor, for the IRIS spoofing methods includes Printed IRIS Images and photographic surfaces, re-played video, fake glass/plastic eye and IRIS texture printed on contact lenses [1-7]. IRIS liveness detection is an important and challenging issue which determines the trustworthiness of biometric system security against spoofing at the time of sensor input [8-11]. Therefore, Generating Liveness Detection measures and anti spoofing Procedures is extremely unavoidable. This Paper provides the valuable input to IRIS direct attacks and Spoofing. At this time, EEG is Novel Modality used for liveness Detection as well as supplementary Biometric Modality to improve the performance of the IRIS Authentication system. To protect our system from direct attacks using Fake IRIS images the integrated Multi modal biometric systems using two individual modalities, like IRIS and Electroencephalogram (EEG) is fused. Electroencephalogram (EEG) is the spatially weighted summation of all these action potentials measured at the surface of the skull. The technique to extract the human brain information provides a new research paradigm as EEG-Based Biometry. The sensor is attacked using artificial biometric samples. The attack is carried out in the analog area. Outside the digital limits of the system, so digital security mechanisms cannot be used [12]. Wavelength reflection coefficient Passive and Pupil Dynamics Active Method for fake IRIS Detection [7, 11, 13, 14] IRIS texture pattern can be used for biometric identification and verification of a person from a large dataset. The authors critically evaluate different IRIS recognition methods [15, 16] for both non-cooperative and cooperative databases. With rapid advance of popularization of biometric applications and electronic technologies, the production cost of much specialized biometric equipment, including eye/IRIS image cameras, has become lower and lower. Simultaneously, the quality of captured eye/IRIS images has become higher and higher [16]. No doubt better IRIS image quality can contribute to even higher performance of IRIS recognition systems [17] and also simplification of IRIS segmentation algorithms without compromising the recognition performance. Because of the accuracy of the camera and robustness [18] of the IRIS algorithm producing fake authentication problems in IRIS Biometric Systems Growing number of publications casing several pioneering authentication approaches and some of them present the perspectives of the EEG-based approaches. This serves to furnish a sudden overview of what has been done in the

Fig. 1: A sight for sore eyes perhaps, but very effective: achieving authentication with someone else's iris by hiding your own pupil behind it.

Fig. 2: Woman putting artificially printed lens and different Colored and textured iris of same eye

field so far. Generating “Pass Thoughts” is the key for personal identification using EEG. This Research argues that such a system is feasible and could work since brain signals from an individual might be unique even when thinking about the same thought as others.

Single modal systems execute person recognition based on single modality. Single biometrics systems have a variety of troubles such as noisy data, individuality, non-universality, High Spoof Rate, High fault rate, Liveness Detection and Direct attacks [12, 19]. The existing biometrics communities are hurdled with confidentiality and unfairness, cancelable biometrics, risk to holder of Secured items. The reasons for the attacks are transform their individual uniqueness, violence, to create criminal actions, frauds; a person can use any one of the above described spoofing techniques to change the identity of a genuine person for e.g. Figure 1, 2 and 3. To overcome the above said inconvenience in the Single Modal biometric systems and develop the performance of biometric security is to be solved by using Multi-Modal Biometrics. These boundaries can be solved by deploying multimodal biometric systems. IRIS and Electroencephalogram (EEG)

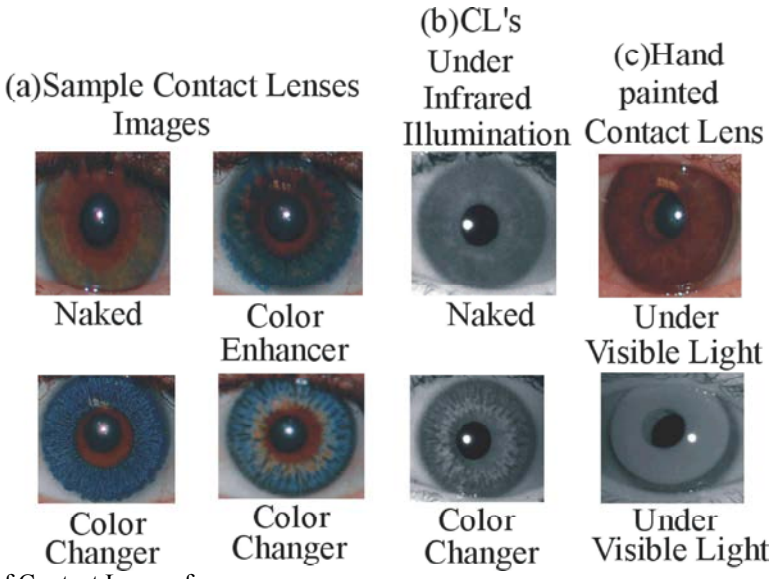

Fig. 3: Different Types of Contact Lenses for same eye

are the first of its kind in the international scenario and which provides outstanding Identification performance and effective anti-spoofing property. Varying lighting conditions, facial expressions, poses and orientations can complicate the face recognition task, masking it one of the most difficult problems in face biometrics. The voice of people can be easily duplicated(i.e. a tape recording) and the voice of people may change if they have pneumonia or bronchitis, illness, fatigue, pitch, surgery involving tampering with the vocal cord, or any combinations of them. Age can also cause changes in the voice. If the surrounding area is noisier this kind of identification can be spoof. In the DNA molecular structures of only a few people have been identified at present. DNA design generated using the Polymerase Chain Reaction (PCR) process. The Preparation kit costs around (OpenPCR) $500. It will take enormous effort and time to identify the type of DNA. The downsides are that DNA samples are contaminated easily and they are hard to control and store. The finger prints of people who work in chemical industries are sometimes diminished. When using finger Prints the following materials used for spoofing. They are Silicone, Moldable plastic, Plaster, Dental molding material, Gelatin, Play-doh, Target-brand gummy bears, Silly Putty, Elmer's Reusable Adhesive Tac 'N Stik, Rose Art Modeling Clay, Crayola Model Magic Soft, Spongy Modeling Materials. The finger prints can be leave everywhere which can be replicated and used to achieve right of entry to any security information. But no one can gain access to the brain signals because it is safely protected inside the skull.

The Proposed integrated Multi modal biometric systems utilize two individual modalities, like IRIS and Electroencephalogram (EEG). An EEG signal of each personality differs in such a way that they are not same even if they do the same work or task. The brain wave of each personality is unique; DNA and living expressions will certainly have a force on human brain structure. It can be said that even if the DNA of two persons are the same but their living experiences will vary. EEG always depends on the living experiences on each personality. Certain biometrics is vulnerable to noisy or bad data, such as dirty fingerprints and noisy voice records, identical twins are not easy to be distinguished by face recognition systems. So, Authenticating users based on their EEG is more accurate than other biometric technologies.

MATERIALS AND METHODS

IRIS Data Collection: Forty healthy volunteers (25 males and 15 females) IRIS images were collected. At the time of Extraction took some efforts to control image quality on eye pictures and as well as appropriate settings such as lighting and distance to camera were adjusted. DM365IPNC Camera used to extract IRIS Patterns in the Effective Manner. The image size is 320×240 pixels and 24 bit depth stored in the bmp file format. For our authentication system only 32 Subjects were taken into account. From each person 5 samples were collected, only 3 samples stored in the data base, all the 5 samples used for testing. First 30 subjects considered as correct persons, Remaining (31^{st}, 32^{nd}) 2 subjects as false persons in the authentication system.

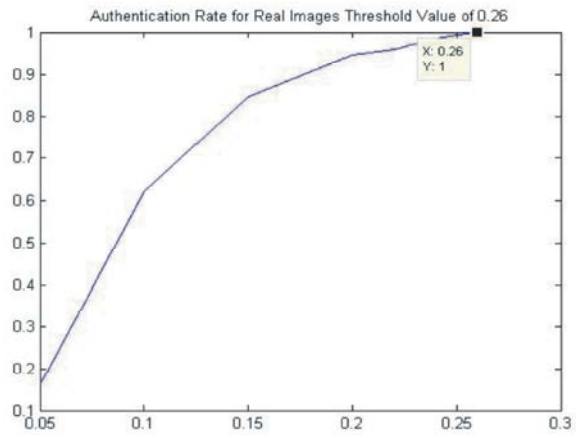

Fig. 4: Authentication Rate for Real Images Threshold Value of 0.26

Iris Recognition System: A widely presented IRIS recognition system (e.g. figure 5) is used for our experiments developed by Libor Masek [20]. It consists of the following steps: Segmentation, Normalization, Encoding and Matching. The following set of functions helps to develop IRIS RECOGNITION SYSTEM. SEGMENTIRIS- Performs automatic segmentation of the IRIS region from an eye image. Also isolates noise areas such as occluding eyelids and eyelashes. FINDCIRCLE- Returns the co-ordinates of a circle in an image using the Hough transform and canny edge detection to create the edge map. LINECOORDS- Returns the co-ordinates of positions along a line. FINDLINE- Returns the co-ordinates of a line in an image using the linear Hough transform and Canny edge detection to create edge map. HOUGHCIRCLE-Takes an edge map image and performs the Hough transform for finding circles in the image. ADDCIRCLE- A circle generator for adding (Drawing) weights in to a Hough accumulator array. NONMAXUP - Function for performing non-Maxima Suppression on an image using orientation image. It is assumed that the orientation image gives feature normal orientation angles in degrees (0-180). ADJGAMMA- Adjust image gamma, Image Gamma value in the range 0-1 enhance contrast of bright regions, HYSTHRESH- Function performs hysteresis threshold of an image. CANNY- Function performs Canny Edge Detection. NORMALIZATION - performs normalization of the IRIS region by unwrapping the circular region into a rectangular block of constant dimensions.

SHIFTBITS - function to shift the bit-wise IRIS patterns in order to provide the best match each shift is by two bit values and left to right, since one pixel value in

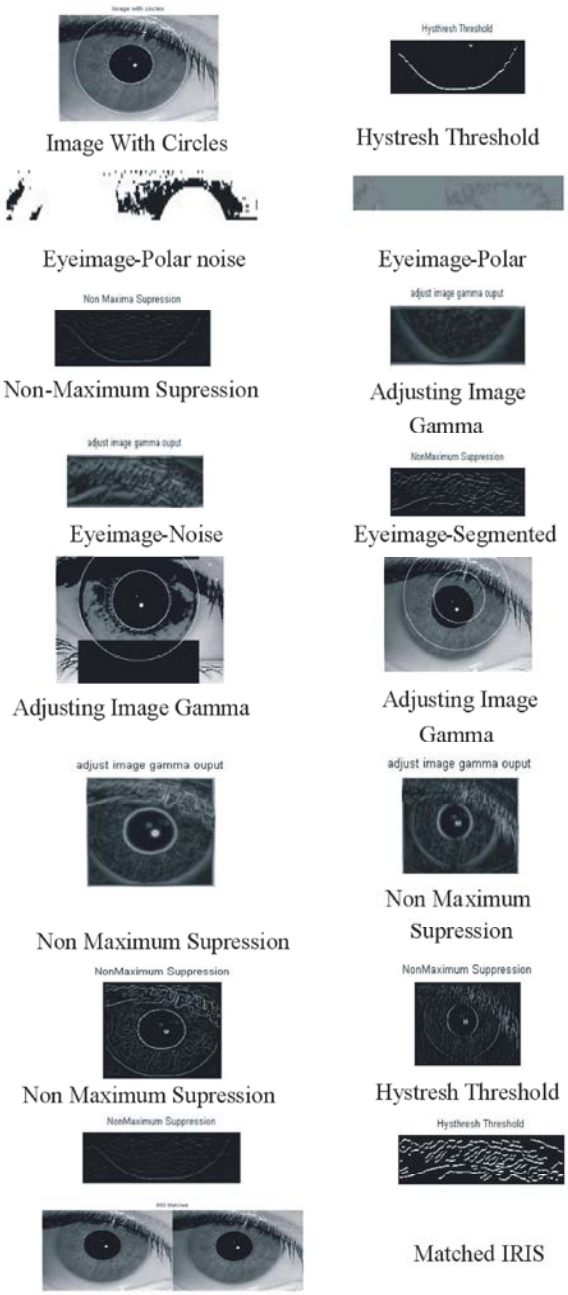

Fig. 5: IRIS Recognition System

the normalized IRIS pattern gives two bit values In the template also takes into account the number of scales used. For Matching, THE HAMMING DISTANCE was distance chosen as a metric for recognition. First the Real images were used for authentication, the total authentication Rate of the system is 100% (Threshold Value is 0.26). After that the fake images produced using FALSE IRIS DATABASE GENERATION METHOD for e.g. Figure. 4 and 5.

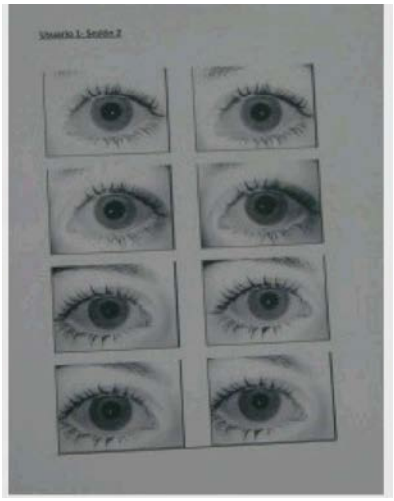

Fig. 6: Fake IRIS Capture Preparation [17]

Fig. 7: Capturing Fake IRIS [17]

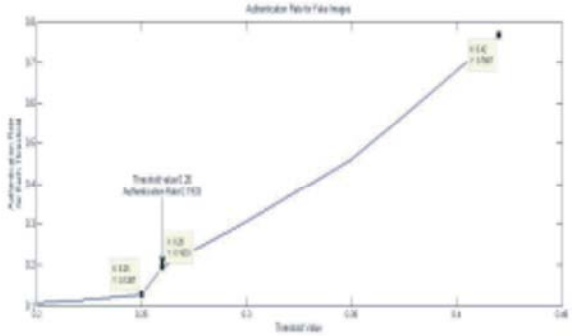

Fig. 8: Authentication Rate for Fake Images Threshold Value of 0.26

RESULTS AND DISCUSSION

Fake IRIS Database Generation

Method 1: (1) At first, the images are processed to progress its quality. (2) Then these images are printed in a regular paper using a usual printer in Figure 6. (3) The printed images are exhibited to the IRIS sensors to carry out a fake authentication presented in Figure 7. Using fake images the Total Authentication Rate of the system is 76.67% (Threshold Value 0.42) in Figure 8.

Table 1: The Hamming Distance Value for Real IRIS Images (5 Subjects, 4 Samples)

	Sample1	Sample2	Sample3	Sample4	Sample5
1	0.07282	0.06450	0.0611	0.1197	0.1340
2	0.075	0.07436	0.097	0.1617	0.1403
3	0.09438	0.11366	0.0928	0.1426	0.1437
4	0.16177	0.16170	0.1879	0.2439	0.2428
5	0.07860	0.07727	0.1047	0.1986	0.1600

Table 2: The Hamming Distance (HD) Value for Fake IRIS Images (5 Subjects, 4 Samples)

	Sample1	Sample2	Sample3	Sample4	Sample5
1	0	0.1633	0.1797	0.1547	0.15774
2	0.3618	0.3901	0.3793	0.4059	0.3741
3	0.4201	0.4352	0.3951	0.3778	0.35365
4	0.4474	0.4465	0.4516	0.4090	0.43128
5	0.4277	0.4236	0.4205	0.4202	0.41308

Method 2: The only thing that was still missing was a printed picture of an IRIS with an appropriate degree of quality. Hence we presented to the Authentication digital image of a human eye that had been sprayed onto mat inkjet paper with a resolution of 2400 x 1200 dpi and into which we had previously cut a miniature hole. This was enough to overcome Authentication resistance: We were granted access to the system under the assumed identity of 'Master False Eye'. It was also possible to enroll with the aid of the 'artificial' eye. From that point onwards anyone in possession of the eye pattern was able to log on to the system. Moreover, the person whose eye had been used to create the pattern was also able to acquire authentication in relation to the picture-generated reference data set with his own live IRIS.

CONCLUSION

The assessment of the vulnerabilities to direct attacks of IRIS-Based Verification systems has been offered. We have built a data base of fake images from 32 persons right eye were prepared. The Results showed that the system is highly vulnerable to the two evaluated attacks. Liveness Detection Procedures are possible countermeasures against directs. Here Electroencephalogram (EEG) is Novel Modality used for liveness detection as well as additional Biometric Modality to the system. The usage of EEG for Biometrics and its Procedures will be presented later.

REFERENCES

1. Zahid Akhtar, Sandeep Kale and Nasir Alfarid, 2011. Spoof Attacks on Multimodal Biometric Systems, 2011 International Conference on Information and Network Technology IPCSIT vol.4 IACSIT Press, Singapore, 2011.

2. Adam Czajka, Przemek Strzelczyk and Andrzej Pacut, 2007. Making IRIS recognition more reliable and spoof resistant, SPIE—The International Society for Optical Engineering.
3. Niladri B. Puhan, N. Sudha and A. Suhas Hegde, 2011. A New IRIS Liveness Detection Method Against Contact Lens Spoofing, IEEE 15th International Symposium on Consumer Electronics.
4. James S. Doyle, Patrick J. Flynn and Kevin W. Bowyer, 2013. Automated Classification of Contact Lens Type in IRIS Images.
5. Hui Zhang, Zhenan Sun and Tieniu Tan, 2010. Contact lens detection based on weighted LBP, IEEE.
6. Naman Kohli, Daksha Yadav, Mayank Vatsa, Richa Singh, 2012. Revisiting IRIS Recognition with Color Cosmetic Contact Lenses.
7. Rajesh Bodade and Sanjay Talbar, 2011. Fake IRIS Detection: A Holistic Approach, International Journal of Computer Applications (0975-8887), 19(2).
8. Hui Zhang, Zhenan Sun, Tieniu Tan and Jianyu Wang, "Learning Hierarchical Visual Codebook for IRIS Liveness Detection", IEEE, 2011.
9. Javier Galbally, Julian Fierrez and Javier Ortega-Garcia, 2007. Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection.
10. Javier Galbally, Jaime Ortiz-Lopez, Julian Fierrez and Javier Ortega-Garcia, 2012. IRIS Liveness Detection Based on Quality Related Features, IEEE.
11. Eui Chul Lee, Kang Ryoung Park and Jaihie Kim, 2005. Fake IRIS Detection by Using Purkinje Image, ICB, LNCS 3832, pp: 397 – 403, Springer-Verlag Berlin Heidelberg.
12. Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez and Javier Ortega-Garcia, 2008. Direct Attacks Using Fake Images in IRIS Verification, Springer-Verlag Berlin Heidelberg, BIOID, LNCS, 5372: 181-190.
13. Jonathan Connell, Nalini Ratha, James Gentile and Ruud Bolle, 2013. Fake IRIS Detection Using Structured Light, IEEE, ICASSP.
14. Xiaofu He, Yue Lu and Pengfei Shi, 2008. A fake IRIS detection method based on FFT and quality assessment, IEEE.
15. Abbasi, A.A. and M.N.A. Khan, 2013. A Critical Survey of IRIS Based Recognition Systems. Middle-East Journal of Scientific Research, 15(5): 663-668.
16. Ling, L.L. and D.F. Brito, 2010. Fast and Efficient IRIS Image Segmentation. Journal of Medical and Biological Engineering, 30(6): 381-392.
17. Yaser Daanial Khan, Farooq Ahmad and Muhammad Waqas Anwar, 2012. A Neuro-Cognitive Approach for Iris Recognition Using Back Propagation World Applied Sciences Journal, 16(5): 678-685, ISSN 1818-4952, IDOSI Publications, 2012.
18. Zyad Thalji and Mutasem Alsmadi, 2013. Iris Recognition Using Robust Algorithm for Eyelid, Eyelash and Shadow avoiding, World applied Sciences Journal, 25(6): 858-865, 2013 ISSN 1818-4952, IDOSI Publications, 2013.
19. Jaime Ortiz-Lopez, Javier Galbally, Julian Fierrez and Javier Ortega-Garcia, 2011. Predicting IRIS Vulnerability to Direct Attacks Based on Quality Related Features, ICCST.
20. Libor Masek, 2003. Recognition of Human IRIS Patterns for Biometric Identification, Ph.D Thesis.