Find Pretend Biometric Mistreatment Image Quality Assessment for Animateness Detection

P. Suresh

Assitant Professor
Electronics and Communication Department, PRIST University
Trichirapalli, Tamil Nadu, India
psureshengineer@gmail.com

Abstract-**A biometric system could be a system that is employed to acknowledge the person on their behavioural and physiological characteristic. This paper introduce 3 biometric techniques that ar fingerprint recognition, iris recognition, and face recognition (Multi Biometric System) and additionally introduce the attacks on it system and by exploitation Image Quality Assessment for physiological property Detection a way to shield the system from pretend statistics. The experimental results, obtained on publically offered information sets of iris ,face, and fingerprint, show that the planned technique is extremely competitive compared with different progressive approaches which the analysis of the overall image quality of real biometric samples reveals highly valuable info which will be very with efficiency accustomed discriminate them from pretend traits.**

Keywords: **Biometrics, attacks, image quality assessment.**

I. INTRODUCTION

The security field uses three different types of authentication: Something you know a password, PIN, or piece of personal information, something you have a card key, smart card, or token (like a Secure ID card), something you are a biometric. Fake biometrics means by using the real images of human identification characteristics create the fake identities like fingerprint, iris on printed paper. In general biometric systems work in two modes: Enrolment mode: In this mode biometric user data is acquired. This is mostly done with some type of biometric reader. The gathered information is stored in a database where it is labeled with a user identity to make possible authentication. In authentication mode again biometric user information is acquired and used by the system to either verify the users claimed identity. When identification involves the process of comparing the user's biometric information 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. However, inspite of its advantages, biometric systems have some disadvantage, including the need of secrecy, the fact that a biometric trait cannot be replaced and its vulnerability to external attacks which could decrease their level of security. At the same time that significant advances have been achieved in biometrics, several spoofing techniques have been developed to deceive the biometric systems, and the security of such systems adjacent to attacks is still an open problem. Spoofing attacks occur when a person tries to masquerade as someone else falsifying the biometrics data that are captured by the acquisition sensor in an attempt to circumvent a biometric system. Therefore, there is a rising need to detect such attempts of attacks to biometric systems. A multi biometric system means a biometric system is used more than one biometric system for one multi-biometric system. It uses the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. In this Survey Base seminar report Image quality assessment for liveness detection technique is used for find out the fake biometrics. Image assessment is force by supposition that it is predictable that a fake image and real sample will have different quality acquisition. Image quality assessment is a most important topic in the image processing area. Biometrics can be divided into two broad categories-Behavioral and Physiological. Behavioral biometrics are based on unique ways people do things such as talking, walking, typing on a keyboard or signing their name. By contrast, physiological biometrics are based on a person's physical characteristics which are not unchanging such as fingerprints, iris patterns and facial features.

II. RELATED WORK

A new vulnerability prediction scheme for direct attacks to iris recognition systems is presented. The objective of the novel technique, based on a 22 quality related parameterization, is to discriminate beforehand between real

samples which are easy to spoof and those more resistant to this type of threat. The system is tested on a database comprising over 1,600 real and fake iris images proving to have a high discriminative power reaching an overall rate of 84% correctly classified real samples for the dataset considered. Furthermore, the detection method presented has the added advantage of needing just one iris image (the same used for verification) to decide its degree of robustness against spoofing attacks.

In this paper, we use a hill- climbing attack algorithm based on Bayesian adaption to test the vulnerability of two face recognition systems to indirect attacks. The attacking technique uses the scores provided by the matcher to adapt a global distribution computed from an independent set of users, to the local specificities of the client being attacked. The proposed attack is evaluated on an eigenface-based and a parts-based face verification system using the XM2VTS database. Experimental results demonstrate that the hill climbing algorithm is very efficient and is able to bypass over 85% of the attacked accounts. The security flaws of the analyzed systems are pointed out and possible countermeasures to avoid them are also proposed

A new software-based liveness detection approach using a novel fingerprint parameterization based on quality related features is proposed. The system is tested on a highly challenging database comprising over 10,500 real and fake images acquired with five sensors of different technologies and covering a wide range of direct attack scenarios in terms of materials and procedures followed to generate the gummy fingers. The proposed solution proves to be robust to the multi-scenario dataset, and presents an overall rate of 90% correctly classified samples. Furthermore, the liveness detection method presented has the added advantage over previously studied techniques of needing just one image from a finger to decide whether it is real or fake. This last characteristic provides the method with very valuable features as it makes it less intrusive, more user friendly, faster and reduces its implementation costs.

Fingerprint recognition systems are vulnerable to artificial spoof fingerprint attacks, like molds made of silicone, gelatin or Play-Doh. "Liveness detection", which is to detect vitality information from the biometric signature itself, has been proposed to defeat these kinds of spoof attacks. The goal for the LivDet 2009 competition is to compare different methodologies for software-based fingerprint liveness detection with a common experimental protocol and large dataset of spoof and live images. This competition is open to all academic and industrial institutions which have a solution for software-based fingerprint vitality detection problem. Four submissions resulted in successful completion: Dermalog, ATVS, and two anonymous participants (one industrial and one academic). Each participant submitted an algorithm as a Win32 console application. The performance was evaluated for three datasets, from three different optical scanners, each with over 1500 images of "fake" and over 1500 images of "live" fingerprints. The best results were from the algorithm submitted by Dermalog with a performance of 2.7% FRR and 2.8% FAR for the Identix (L-1) dataset. The competition goal is to become a reference event for academic and industrial research in software-based fingerprint liveness detection and to raise the visibility of this important research area in order to decrease risk of fingerprint systems to spoof attacks

III. FINGER PRINT RECOGNITION

Fingerprint Recognition means taking an image of a person's finger and records its characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae.

Advantages:

- Subjects have Multiple Fingers.
- Easy to use, with some training.
- Some systems require little space.
- Large amounts of existing data to allow background and/or watchlist checks
- Has proven effective in many large scale systems over years of use.
- Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime.

Disadvantages:

- Privacy concerns of criminal implications.
- Health or social concerns with touching a sensor used by countless individuals.
- Collection of high quality nail-to-nail images requires training and skill, but current flat reader technology is very robust.
- An individual's age and occupation may cause some sensors difficulty in capturing a complete and accurate fingerprint image.

IV. IRIS RECOGNITION

Iris scan biometrics employs the unique characteristics and features of the human iris, which remains unchanged throughout an individual's life span, in order to verify the uniqueness of an individual. The iris is the main area of the

eye where the pigmented or colored circle, usually brown, green, grey or blue, rings the dark pupil of the eye.

Advantages:

- No contact required
- Protected internal organ, less prone to injury
- Believed to highly stable over lifetime

Disadvantages:

- Difficult to capture for some individuals
- Easily obscured by eyelashes, eyelids, lens and reflections from the cornea.
- Public myths and fears related to "scanning" the eye with a light source.
- Acquisition of an iris image requires more training attentiveness than most biometrics.
- Lack of existing data deters ability to use for background or watch list checks.
- Cannot be verifies by human.

V. FACE RECOGNITION

Human face detection plays an important role in applications such as video observation, human computer interfaces, face detection, and face image databases. To enable this biometric technology it requires having at least a video camera, PC camera or a single-image camera. However, 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 location, the direction, the environment and the size of a face is variable is a very hard task and many algorithms have been worked on to solve this problem. Other problems with face detection occur whenever faces are partially covered by beards, glasses, hair style or hats; because a lot of information just stays hidden.

Advantages

- No contact required
- Commonly available sensors
- Large amounts of existing data to allow background and/or watchlist checks
- Easy for humans to verify results.

Disadvantages:

- Face can be obstructed by hair, glasses, hats, scarves, etc.
- Sensitive to changes in lighting, expression, and pose.
- Faces change over time.
- Propensity for users to provide poor-quality video images yet to expect accurate results.

VI. IMAGE QUALITY ASSESSMENT

The use of image quality assessment for liveness detection is motivated by the statement that: It is expected that a false image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was considered. Predictable quality differences between real and false samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both types of images. For example, iris image captured from a printed paper or out of focus due to trembling; it is common that fingerprint images captured from a sticky finger present local acquisition artifacts such as spots and patches. List of image quality measures are gives below:

Full-reference: That a complete reference image is unspecified to be known.

No-reference: The reference image is not present, and a no-reference or "blind" quality assessment approach is attractive.

Reduced-reference: The reference image is only incompletely presented, in the form of a set of extracted features made available as side data to help calculate the quality of the distorted image.

Mean Square Error (MSE)

The large value of MSE means that image is poor quality. MSE is defined as follow:

$$MSE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(x(m,n) - \hat{x}(m,n)\right)^2 \quad (1)$$

Mean Average Error (MAE)

The large value of MAE means that image is poor quality. The MAE is defined as follow:

$$MAE = \frac{1}{MN}\sum_{m=1}^{M}\sum_{n=1}^{N}\left| x(m,n) - \hat{x}(m,n) \right| \quad (2)$$

Peak Signal to Noise Ratio (PSNR)

The small value of PSNR means that image is poor quality. The PSNR is defined as follow:

$$PSNR = 10 \log \frac{L^2}{MSE} \quad (3)$$

Structural Content (SC)

The large value of SC means that image is poor quality. The SC is defined as follow:

$$SC = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} x(m,n)^2}{\sum_{m=1}^{M} \sum_{n=1}^{N} \widehat{x(m,n)^2}} \quad (4)$$

Maximum Difference (MD)

The large value of MD means that image is poor quality. The MD is defined as follow:

$$MD = Max\left(\left| x(m,n) - \hat{x}(m,n) \right| \right) \quad (5)$$

Normalized Absolute Error (NAE)

The large value of Normalized Absolute Error (NAE) means that image is poor quality. NAE is defined as follow:[4]

$$NAE = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} \left| x(m,n) - \widehat{\hat{x}(m,n)} \right|}{\sum_{m=1}^{M} \sum_{n=1}^{N} \left| x(m,n) \right|} \quad (6)$$

Laplacian Mean Square Error (LMSE)

This measure is based on the importance of edges measurement. The large value of Laplacian Mean Square Error (LMSE) means that image is poor quality. LMSE is defined as follow: [4]

$$LMSE = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} \left[L\left(x(m,n)\right) - L\left(\hat{x}(m,n)\right) \right]^2}{\sum_{m=1}^{M} \sum_{n=1}^{N} \left[L\left(x(m,n)\right) \right]^2} \quad (7)$$

Structural similarity index (SSIM)

Given the observable restrictions of the mean squared error, propose a more clever solution to the problem of image quality assessment. Made up of three conditions, the structural similarity (SSIM) index estimates the illustration impact of shifts in image luminance, changes in photograph difference, as well as any other remaining errors, cooperatively identified as structural changes. The metric is based on a top-down supposition that the HVS is highly modified for extracting structural data from the scene, and so a measure of structural comparison should be a good approximation of perceived image quality For original and coded signals x and y, in that order SSIM index is definite as:

$$SSIM(x,y) = [l(x,y)]^{\alpha} [c(x,y]^{\beta} [s(x,y)]^{\gamma} \quad (8)$$

VII. CONCLUSION

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years. Image quality assessment for liveness detection technique is used to detect the fake biometrics. This interest has led to big advances in the field of security-enhancing technologies for Biometric-based applications. Multi-Biometric system is challenging system. It is more secure than unibiometric system. In this paper studied about the three biometric systems that are face identification, iris identification, fingerprint identification, and the attack on these three systems. In future for making this system more secures adding the one more biometric system into this system and trying to improve the system.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.

[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.

[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.

[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.

[7] ISO/IEC 19792:2009, Information Technology— Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., "First international fingerprint liveness detection competition LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009, pp. 12–23.

Author's Profile:

P. Suresh: Assistant Professor of ECE Department in PRIST University. He completed his B.E, Electronics Engg and M.E Communication Engineering from Muthayammal Engineering College and M. Kumarasamy College of Engineering, Karur, Tamilnadu. He is having 2 years Industry experience in database management systems. His area of interest includes image processing and advanced database systems.