Various Quality Measures for Fake Biometric Detection” [REVIEW]

Ruhool Ameen Sheikh
M.TECH student
Department of Electronics
S.B. Jain Institute of Technology, Management and Research
Nagpur

Dr. Sanjay Badjate
Vice Principal
Department of Electronics
S.B. Jain Institute of Technology, Management and Research
Nagpur

Abstract - To ensure the particular presence of a true legitimate trait in distinction to a faux self-manufactured artificial or reconstructed sample could be a vital drawback in biometric authentication, which needs the event of latest and efficient protection measures. In this paper, we tend to gift a unique software-based pretend detection methodology that may be utilized in multiple biometric systems to discover differing types of fallacious access attempts. The target of the projected system is to reinforce the security of biometric recognition frameworks, by adding physiological property assessment in an exceedingly quick, easy, and non-intrusive manner, through the employment of image quality assessment. The planned approach presents a awfully low degree of quality, that makes it appropriate for time period applications, victimization general image quality options extracted from one image (i.e., a similar noninheritable for authentication purposes) to differentiate between legitimate and faker samples.

Keyword: biometric, legitimate trait, image quality assessment.

*****

I. Introduction

IN RECENT years, the increasing interest within the analysis of biometric systems security has junction rectifier to the creation of numerous and really various initiatives centered on this major field of analysis the publication of the many analysis works disclosing and evaluating totally different biometric vulnerabilities indicates that importance of biometrics and to improve the system to be practically used. Fake bioscience suggests that by mistreatment the important pictures of human identification characteristics produce the pretend identities such as fingerprint, iris, and signature on a written paper.

Fake user first of all capture the initial identities of the real user then they create the faux sample for authentication however biometric system have a lot of method to discover the faux users and that’s why the biometric system is safer, as a result of all and sundry have their distinctive characteristics identification. Biometrics system is surely safer than different security ways like password, pin, or card and key. A life science system measures the human characteristics thus users don't have to be compelled to remember passwords or pins which might be forgotten or to carry cards or keys which might be taken.

Biometrics can be broadly classified into two types physiological characteristics and behavioral characteristics usually derived from the human action .Biometrics which are related to physical characteristics of human being includes fingerprint recognition system, iris recognition system, voice recognition system etc whereas the biometrics related to behavior consist of gait and signature recognition system . Biometrics are majorly used for identification and for security purpose in order to prevent the access to system by fake users which leads to design such a system which gives high security and fast access. Multi biometric system is used to overcome the limitations of biometric system. Ample source of information which gives more specific results are used by multi-biometric system.

Researchers and industry have specially made their attention towards liveness detection which distinguishes between real and fake using different physiological properties along with challenge-response method or multi-biometric system. Image assessment is force by supposition that it\'s predictable that a faux image and real sample can have different quality acquisition. Predictable quality variations between real and faux samples could contain: color and luminance levels, general artifacts, amount of data, and amount of sharpness, found in each form of pictures, structural distortions or natural look.

II. LITERATURE SURVEY

In this section we review various studies and development carried out by many researchers. We will also see various detection techniques.

[1]Anil k. jain, Karthik nandakumar, and Abhishek nagar has proposed a high-level categorization of the assorted vulnerabilities of a biometric system and discuss countermeasures that are projected to handle these vulnerabilities they concentrated on biometric model security that is a vital issue giving information that biometric template is prevented from being revoked and reissued though tokens and passwords can be compromised. Template protecting is a difficult as well as a challenging task because of intrauser variability in the acquired biometric traits. To meet all the application requirements protection approach is inadequate using single template. Thus there is a need for developing such

schemes which utilizes the protection approaches of different template.

They have presented various schemes for protecting biometric template discussing their advantages and limitations based on parameters such as security, revocability and accuracy. Providing good security and acceptable recognition performance has thus far remained elusive for template protection scheme.

Developing such scheme is crucial as biometric systems are increasing rapidly into the core physical and information infrastructure of our society.

[2]Abhyankar proposed the technique that developed a single image based on liveness measure. In this work he exploited the difference between live and not live fingerprint images on the basis of inherent texture and density. The energy associated with phase and orientation maps are minimized using the technique of multi resolution texture analysis. He has utilized the statistical measure to analyze cross ridge frequency of fingerprint images and calculated the weighted mean phase.

These completely different options alongside ridge dependability or ridge center frequency ar given as inputs to a fuzzy c-means classifier. The projected rule was applied to a dataset of roughly 58 live, fifty spoof and twenty eight dead body fingerprint pictures, from 3 completely different types of scanners.

[3] nikam has proposed a method to detect the liveness of a system based on curvelet which want just one fingerprint to eliminate the problems occurring from perspiration-based liveness detection algorithms. though Wavelets are terribly effective in representing objects with isolated point singularities, however fail to represent line and curve singularities. Curvelet rework permits representing singularities Ridges bound in several directions in an exceedingly fingerprint image square measure curved; thus curvelets square measure terribly vital to characterize fingerprint texture. Fingerprint image are characterize using textural measures based on co-occurrence signature and energy contained within the curvelet.

Dimensionalities of feature sets square measure reduced by running Pudil’s successive forward floating selection (SFFS) rule along curves in an exceedingly a lot of economical approach than the wavelets. Curvelet energy and co-occurrence signatures area unit severally tested on 3 different classifiers:, support vector machine alternating decission tree and AdaBoost.M1. Finally, the entire said classifiers area unit consolidated exploitation the “Majority Voting Rule” to create an ensemble classifier. A fingerprint info consisting of 185 real, ninety Fun-Doh and one hundred fifty gluey fingerprints is formed by exploitation styles of artificial materials for casts and moulds of spoof fingerprints.

Performance of the new aliveness detection approach is found terribly promising, because it desires solely one fingerprint and no further hardware to sight vitality.

[4]lsmail Avcibas, Sevinc Bayram, Nasir Memon, Mahalingam Ramkumar, Bulent Sankur has proposed a framework for digital images forensics. Doctored image is an image which is used to deceive people and thus there should be a technique to discriminate it from the original image.

They have designed such classifiers that can be used to discriminate between original and processed images. They have proposed a method for measuring the distortion between original image and processed image. Comparing the part of a image which seems to be suspicious part of a image is compared with a particular method using classifiers. They have shown the experimental results showing that which part of an image has undergone the combination of processing methods.

[5]Jonathan connell, nalini ratha, james gentile & ruud bolle has proposed a inexpensive method to determine fake iris pattern in order to enhance the security level of the system. They have also explained the use of designer contact lenses in spoofing the system based on iris recognition system. Structured light projection method has been utilized in recognizing fake items. An algorithm to identify the patterned contact lenses from the acquired images is also described. They also promised improved security with the addition of the proposed system in iris biometric system. Different dimensions of attack and their solutions has also been explained.

Manufacturing of contact lenses at a cheaper rate has promoted the use of various printed lenses for different occasions. By projecting the ray of light on the eyes the results obtained will be different for normal eyes without lens and the eyes with the normal lenses and patterned lenses showing the stripes whether it is straight or curved.

[6] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, *et al.*has proposed a unique evaluation method for comparing different performance of state of art algorithm on same database it consist of six different teams around the world and most of them are using the techniques related to texture analysis and liveness detection. Algorithms used are very much efficient in determining the real access from the various spoofing attack. A complex attack has been also elaborated.

Different teams performance figure in percentage has been given below :

Team	**Development**		**Test**		
	FAR	**FRR**	**FAR**	**FRR**	**HTER**
AMILAB	**0.00**	**0.00**	**0.00**	**1.25**	**.63**
CASIA	**1.67**	**1.67**	**0.00**	**0.00**	**0.00**
IDIAP	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**
SIANI	**1.67**	**1.67**	**0.00**	**21.25**	**10.63**
UNICAMP	**1.67**	**1.67**	**1.25**	**0.00**	**0.63**
UOULU	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**

✓ Corresponds to the technique being utilized as shown in the table below:

Team	**Motion Analysis**	**Texture Analysis**	**Liveness Detection**
AMILAB	✓	✓	✓
CASIA	✓	✓	●
IDIAP	●	✓	●
SIANI	✓	●	●
UNICAMP	✓	✓	✓
UOULU	●	✓	●

[7]J. Galbally • J. Fierrez • F. Alonso-Fernandez • M. Martinez-Diaz has presented significant observations based on the quality of fingerprint images and the results which have been achieved from different operation on sequence of event. They also performed different related significant operations to increase system ability to cope with errors during execution. A fingerprint recognition based study was used to check the vulnerabilities of different attacks determining whether the user has supported the operation or not.

They used two different kinds of attacking technologies that is one based on the gummy fingerprint and the other one is real fingerprint on which the test has been performed using fake imitation.

Thus they have utilized database of real and fake fingerprints which have been implemented on two systems ridge feature-based and other one is minutiae-based. Success rate of attacks in minutiae based system is dependent on the quality of fake samples of fingerprint thus giving up of conclusions that better the captured fake fingerprint sample lower is the system robustness. From the results obtained from two techniques ridge-based system has given more efficient results implemented on the images of high fake quality.

Performance of attacks on minutiae based system:

	FAR	**FRR**
Optical	**0.1**	**0.25**
	1	**0**
	10	**0**
CAPACITIVE	**0.1**	**25**
	1	**16**
	10	**11**
thermal	**0.1**	**18**
	1	**11**
	10	**6**

Performance of attacks on ridge based system:

	FAR	**FRR**
Optical	**0.1**	**61**
	1	**36**
	10	**13**
CAPACITIVE	**0.1**	**96**
	1	**78**
	10	**35**
Thermal	**0.1**	**95**
	1	**82**
	10	**45**

III. CONCLUSION

This paper describes different methods of determining fake biometric along with the techniques to overcome these false intruders making attempts to break the security of the system. Different methods for detecting the fake and real such as fingerprint recognition and iris recognition has been described in this paper. Moreover it will help the designer to be aware of the threats and security issues in the designing of the biometric system using various quality measures.

REFERENCE:

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

[2] A. Abhyankar and S. Schuckers, “Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques,” in *Proc. IEEE ICIP*, Oct. 2006, pp. 321–324.

[3] S. Nikam and S. Argawal, “Curvelet-based fingerprint anti-spoofing,” *Signal, Image Video Process.*, vol. 4, no. 1, pp75–87, 2010.

[4] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, “Image manipulation detection,” *J. Electron. Imag.*, vol. 15, no. 4, pp. 041102-1–041102-17, 2006.

[5] “FAKE IRIS DETECTION USING STRUCTURED LIGHT” Jonathan Connell, Nalini Ratha, James Gentile & Ruud Bolle IBM T. J. Watson Research Center Yorktown Heights, NY 10598 978-1-4799-0356-6/13/$31.00 ©2013 IEEE

[6] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, *et al.*, “Competition on countermeasures to 2D facial spoofing attacks,” in *Proc. IEEE IJCB*, Oct. 2011, pp. 1–6.

[7] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, “Evaluation of direct attacks to fingerprint verification systems,”

[8] Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” *Electron. Lett.*, vol. 44, no. 13,pp. 800–801, 2008.

[9] S. Yao, W. Lin, E. Ong, and Z. Lu, “Contrast signal-to-noise ratio for image quality assessment,” in *Proc. IEEE ICIP*, Sep. 2005, pp. 397–400.

[10] A. M. Eskicioglu and P. S. Fisher, “Image quality measures and their performance,” *IEEE Trans Commun.*, vol. 43, no. 12, pp. 2959–2965, Dec. 1995.

[11] [11] H. R. Sheikh and A. C. Bovik, “Image information and visual quality,” *IEEE Trans. Image Process.*, vol. 15, no. 2, pp. 430–444, Feb. 2006.

[12] R. Soundararajan and A. C. Bovik, “RRED indices: Reduced reference entropic differencing for image quality assessment,” *IEEE Trans. Image Process.*, vol. 21, no. 2, pp. 517–526, Feb. 2012.

[13] X. Zhu and P. Milanfar, “A no-reference sharpness metric sensitive to blur and noise,” in *Proc. Int. Workshop Qual. Multimedia Exper.*, 2009, pp. 64–69.

[14] A. K. Moorthy and A. C. Bovik, “A two-step framework for constructing blind image quality indices,” *IEEE Signal Process. Lett.*, vol. 17, no. 5, pp. 513–516, May 2010

[15] A. Mittal, R. Soundararajan, and A. C. Bovik, “Making a ‘completel blind’ image quality analyzer,” *IEEE Signal Process. Lett.*, vol. 20, no. 3, p. 209–212, Mar. 2013.

[16] Trusted Biometrics Under Spoofing Attacks (TABULA RASA)
[Online]. Available: http://www.tabularasa-euproject.org/

[17] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, *et al.*, “An evaluation of direct and indirect attacks using fake fingers generated from ISO templates,” *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 725–732, 2010.

[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, “A new forgery scenario based on regaining dynamics of signature,” in *Proc. IAPR ICB*, vol. Springer LNCS-4642. 2007, pp. 366–375.

[19] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, “Can gait biometrics be spoofed?” in *Proc. IAPR ICPR*, 2012, pp. 3280–3283.

[20] Z. Wang and A. C. Bovik, “Mean squared error: Love it or leave it? A new look at signal fidelity measures,” *IEEE Signal Process. Mag.*, vol. 26, no. 1, pp. 98–117, Jan. 2009.

[21] B. Girod, “What’s wrong with mean-squared error?” in *Digital Images and Human Vision*. Cambridge, MA, USA: MIT Press, 1993, pp. 207–220.