ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Detection of Fake Biometric Images using Images Quality Assessment: Application to Face Classification

Nisha S. Shinde[1], Vijay B. Baru[2]

PG Student, Dept. of Electronics, Sinhgad College of Engineering, Savitribai Phule Pune University, Pune, India. [1]

Associate Professor, Dept. of Electronics, Sinhgad College of Engineering, Savitribai Phule Pune University, Pune, India. [2]

ABSTRACT:In biometric authentication significant problem is to ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a, which requires the development of new and efficient protection measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed work presents a very low degree of complexity, which makes it suitable for real-time applications, using 10 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of and 2D face, show that the proposed method is highly competitive compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very efficiently used to discriminate them from fake traits.

KEYWORDS: Image quality assessment, biometrics, security, attacks, Classification.

I. INTRODUCTION

Now a days, there is increase in interest in the assessment of biometric systems security, that's why the creation of many different initiatives are leading and focused on this major field of research.All parties involved in the development of biometrics like researchers, developers and industry gives importance to the improvement of the systems security to bring this rapidly emerging technology into practical use and all the initiatives clearly highlight that importance. There are many types of threats, among the different threats analysed, the so-called direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the face and multimodal approaches in these attacks, the intruder uses some type of synthetically produced artifact (e.g., face mask), to fraudulently access the biometric system. As these types of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital Signature or watermarking) are not effective.

The previous works and other parallel studies have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, improving this way the strength and security level of the systems. As a rough comparison, software-based techniques are lessin general expensive as no extra device is needed, and less obtrusive since their implementation is transparent to the user, while hardware-based systems usually

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

gives a high fake detection rate. In addition, as software-based systems operate directly on the acquired sample (and not on the biometric trait itself), software-based Techniques may be fixed in the feature extractor module and they will be possibly capable of detecting other types of unlawful break-in attempts not necessarily classified as spoofing attacks. Just as, software-based methods can protect the system against the introduction of synthetic or fake samples into the communication medium between the feature extractor and the sensor.

The proposed work is to improve the security of biometric recognition architecture, this is achieved by adding liveness assessment in a fast, non-obtrusive and user-friendly manner, through the use of image quality assessment(IQA). The system will have a very low degree of complexity, which makes it suitable for real-time applications, using 10 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between genuine and pretender samples. The experimental results, obtained on publicly available data sets of 2D face, show that the proposed method is highly combative compared with other state-of-the-art approaches and that the analysis of the general image quality of real biometric samples reveals highly valuable information that may be very systematically used to discriminate them from fake traits.

II. RELATED WORK

Existing protection method performs novel parameterization using 10 general image quality measures. Input biometric sample is classified into one of two classes: real or fake based on simple classifier built using parameterization performed using efficient 10 general image quality measures. The process involves to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image “realism” given the extracted set of features. Support Vector Machine (SVM) Classifiers are used in existing work. It uses Full reference image quality measures, which are selected using four general criteria: performance, complementarity, complexity, speed. General image quality measures are fast and easy tocompute and combined with simple classifiers. This biometric protection method is applicable to multimodality such as face.

Liveness detection methods are generallygrouped into two ways (I) Hardware-based techniques, these techniques add some specific device to the sensor to detect specific properties of a living trait and (II) Software-based techniques, in this techniques the fake trait is detected after the sample has been obtained with a standard sensor means features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself. Proposed technique is software-based technique.

III. PROPOSED METHOD

In this proposed work,to keep its generality and simplicity, the system needs only one input: the biometric sample to be classified as real or fake (i.e., the same image acquired for biometric recognition purposes). Furthermore, as the method operates on the whole image without searching for any trait-specific properties, it does not require any pre-processing steps (e.g. face extraction) prior to the computation of the IQ features. This characteristic minimizes its computational load. Once the feature vector has been generated the sample is classified as real (generated by a genuine trait) or fake (synthetically produced), using some simple classifiers. In particular, for experiments this system considered standard implementations in Matlab. The parameterization proposed in the present work comprises ten image quality measures both reference and blind (as will be introduced in the next sections). Full-reference (FR)Image quality assessment(IQA) methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample.

Algorithm for database creation:

1. Initialize Camera, Total 10 images will be captured and captured image (images will be genuine) will be stored.
2. Waits for any keyboard button to be hit and Next 10 images (images will be fake) will be captured it will be stored.

Algorithm for training:

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

1. Read input image and Convert input image from RGB to grey,create reference smoother image by applying smoothening filters.
2. Extract features of both image input image and reference image and select only those features which are showing interclass variations.
3. Append feature vector of current image to excel data matrix, 1st 10 images belong to class 1 and next 10 to class 0.

Algorithm for testing:

1. Apply steps on query image same as input image till step 3.
2. Apply SVM classifier, it will compare both feature vectors of input image and query image respectively.
3. SVM classifier recognized the query image is genuine (class 1) or fake (class 0).

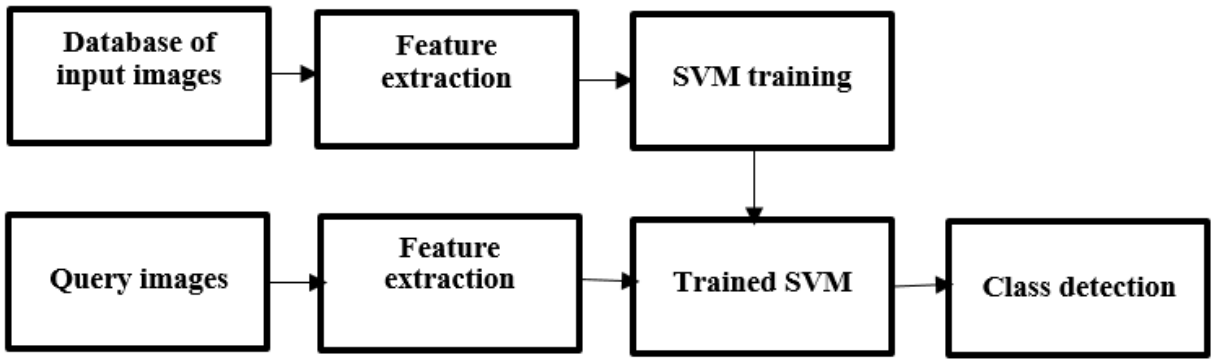

Figure1. Block Diagram of Proposed Face Detection System

Figure above shows the block diagram of Face Detection System. Proposed system uses full reference approach for that there is a need of reference image but input taken by the system is only one image that's why its smoothed version is generated. Now Feature extraction and SVM training is possible. Ten quality measures are taken as follows – Mean square error (MSE), Peak signal to noise ratio (PSNR), Signal to noise ratio (SNR), JPEG quality score, normalised cross correlation (NXC), structural content (SC), structural similarity index (SSIM), Normalised absolute error (NAE), Total edge difference (TED), Max difference(MD). Among them selected features are used to train SVM so that classifier should not get confused due to values crossing the hyperplane of SVM. Same process is valid for query images and trained SVM will detect the class of query image whether it is real or fake.

IV. EXPERIMENTAL RESULTS

Figures shows the results of detection of Biometric images using Image Quality Assessment Then trained SVM classifier will classify the query image is real or fake (image from mobile screen).Fig.2 (a) Show original image. It is obtained from the online database .Fig.2 (b) image is gray image obtained by rgbtogray conversion of original image and its smoothed version obtained by average filtering shown in fig(c) .Using (b) and (c) feature vector is created. That feature vector will used to train SVM.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

(a) (b) (c)

System detectsbelow Fig.2(d) as a Real in controlled scenario .Controlled scenario means while creating database and testing, background and brightness conditions of the image will be fixed. System detect Fig2. (e) As a Real in adverse scenario. Adverse scenario means while creating database and testing, background and brightness conditions of the captured image may not be fixed.

(d) (e)

System detects Fig.2 (f) As Fake image in controlled scenario and Fig.2 (g) As Fakeimage in adverse scenario.

Because both images are captured from mobile screen and not a genuine person. This is nothing but a spoofing or fraudulent attack in the channel between sensor and feature extractor. For this type of attacks cannot help digital protection methods.

(f) (g)

Fig.2 Fake Biometric (Face) Detection (a) Original Image (b) Image after gray conversion(c) Image after smoothing (d) Real image detected by system in controlled scenario (e) real image detected by system in adverse scenario (f) Fake image detected by system in controlled scenario (g) Fake image detected by system in adverse scenario

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

V. CONCLUSION

We have implemented Detection of Fake Biometric Images using Images Quality Assessment: Application to Face Classification. Our algorithm successfully classifies the query image is genuine or fake. We have extracted features of many images and used SVM classifier to detect faces successfully.

REFERENCES

[1] Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez ,"Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition" IEEE transactions on image processing, vol. 23, no. 2, february 2014
[2] 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.
[3] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.
[4] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.
[5] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.
[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] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognition, vol. 43, no. 3, pp. 1027–1038, 2010.
[8] A. K. Jain and D. Zongker, "Feature selection: Evaluation, application, and small sample performance," IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 2, pp. 153–158, Feb. 1997.
[9] 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
[10] 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.
[11] Andre Anjos and Sebastien Marcel," Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline", Idiap Research Institute Centre du Parc - rue Marconi 19 CH-1920 Martigny, Suisse.