A Review on Fake Biometry Detection

Monika Pawase ,Sumedh Gade,Akshay Memane,Author Prof. Poonam Yewale

Dept. of Electronics and Telecommunication ,Keystone School Of Engineering,Pune

Abstract -Face recognition technology has developed rapidly in recent years and it is more direct, user friendly and convenient compared to other methods. To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. Face recognition systems are vulnerable to spoof attacks made by non-real faces. 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 experimental results, obtained on publicly available data sets of iris 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.

1.INTRODUCTION

The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology and it is more direct, user friendly and convenient compared to other methods. Therefore, it has been applied to various security systems.

Prompted by personal information attacks and threats, criminals are able to obtain pictures or videos from legitimate users to engage in fake face attacks. This behaviour is a serious threat to personal property security and public safety. One of the negative implications of increased technological advancement is the ease with which,one can spoof into a biometric identification system. Face or iris recognition systems can be spoofed by spoofing techniques have been developed to deceive the biometric systems, and the security of such systems against 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 an increasing need to detect such attempts of attacks to biometric systems. As this type 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. static facial or iris images. Liveness detection methods are usually classified into one of two groups *(I)* Hardware- based techniques, *(II)* Software-based techniques.

The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to theuser. In the present work we propose a novel software-based multi-biometric and multi-attack protection method which targets to overcome part of these limitations through the use of image quality assessment (IQA). It is not only capable of operating with a very good performance under different biometric systems (multi-biometric) and for diverse spoofing scenarios, but it also provide a very good level of protection against certain non-spoofing attacks (multi-attack). Moreover, being software-based, it presents the usual advantages of this type of approaches: fast, as it only needs one image (i.e., the same sample acquired for biometric recognition) to detect whether it is real or fake; non-intrusive; user-friendly (transparent to the user); cheap and easy to embed in already functional systems (as no new piece of hardware is required). An added advantage of the proposed technique is its speed and very low complexity, which makes it very well suited to operate on real scenarios (one of the desired characteristics of this type of methods). As it does not deploy any trait-specific property (e.g., minutiae points, iris position or face detection), the computation load needed for image processing purposes is very reduced, using only general image quality measures fast to compute, combined with very simple classifiers. It has been tested on publicly available attack databases of iris, fingerprint and 2D face, where it has reached results fully comparable to those obtained on the same databases and following the same experimental protocols by more complex trait-specific top-ranked approaches from the state-of-the-art

2.LITERATURE SURVEY

There are many approaches implemented in Face Liveness Detection. In this section, some of the most interesting liveness detection methods are presented.

Frequency and Texture based analysis

This approach is used by Gahyun Kim et al [1]. The basic purpose is to differentiate between live face and fake face (2-D paper masks) in terms of shape and detailedness. The authors have proposed a single image- based fake face detection method based on frequenc and texture analyses for differentiating live faces from 2-D paper masks. The authors have carried out powerspectrum based method for the frequency analysis, which exploits both the low frequency information and the information residing in the high frequency regions. Moreover, description method based on Local Binary Pattern (LBP) has been implemented for analyzing the textures on the given facial images. They tried to exploit frequency and texture information in differentiating the live face image from 2-D paper masks. The authors suggested that the frequency information is used because of two reasons. First one is that the difference in the existence of 3-D shapes, which leads to the difference in the low frequency regions which is related to the illumination component generated by overall shape of a face. Secondly, the difference in the detail information between the live faces and the masks triggers the discrepancy in the high frequency information.

The texture information is taken as the images taken from the 2-D objects (especially, the illumination components) tend to suffer from the loss of texture information compared to the images taken from the 3-D objects. For feature extraction, frequency-based feature extraction, Texture-based feature extraction and Fusion-based feature extraction are being implemented.

For extracting the frequency information, at first, the authors have transformed the facial image into the frequency domain with help of 2-D discrete Fourier transform. Then the transformed result is divided into several groups of concentric rings such that each ring represents a corresponding region in the frequency band. Finally, 1-D feature vector is acquired by combining the average energy values of all the concentric rings. For texture-based feature extraction, they used Local Binary Pattern (LBP) which is one of the most popular techniques for describing the texture information of the images. For the final one i.e. fusion-based feature extraction, the authors utilizes Support Vector Machine (SVM) classifier for learning liveness detectors with the feature vectors generated by power spectrum-based and LBP-based methods. The fusion-based method extracts a feature vector by the combination of the decision value of SVM classifier which are trained by power spectrum-based feature vectors and SVM classifier which are trained by LBP-based feature vectors. Similar technique of face spoofing detection from single images using micro-texture analysis was implemented by Jukka et al. [2]. The key idea is to emphasize the differences of micro texture in the feature space. The authors adopt the local binary patterns (LBP) which is a powerful texture operator, for describing the micro-textures and their spatial information. The vectors in the feature space are then given as an input to an SVM classifier which determines whether the micro-texture patterns characterize a fake image or a live person image.

Variable Focusing based analysis

The technique of face liveness detection using variable focusing was implemented by Sooyeon

Kim et al. [3]. The key approach is to utilize the variation of pixel values by focusing between two images sequentially taken in different focuses which is one of the camera functions. Assuming that there are clear and others are blurred due to depth information. In contrast, there is little difference between images taken in different focuses from a printed copy of a face, because they are not solid. The basic constraint of this method is that it relies on the degree of Depth of Field (DoF) that determines the range of focus variations at pixels from the sequentially taken images. The DoF is the range between the nearest and farthest objects in a given focus. To increase the liveness detection performance, the authors have increased out focusing effect for which the DoF should be narrow. In this method, Sum Modified Laplacian(SML) is used for focus value measurement. The SML represents degrees of focusing in images and those values are represented as a transformed 2nd-order differential filter.

In the first step, two sequential pictures by focusing the camera on facial components are being. One is focused on a nose and the other is on ears. The nose is the closest to the camera lens, while the ears are the farthest. The depth gap between them is sufficient to express a 3D effect. In order to judge the degree of focusing, SMLs of both the pictures are being calculated. The third step is to get the difference of SMLs. Forone-dimensional analysis, sum differences of SMLs (DoS) in each of columns are calculated. The authors found out that the sums of DoS of real faces show similar patterns consistently, whereas those of fake faces do not. The differences in the patterns between real and fake faces are used as features to detect face liveness. For testing, the authors have considered False Acceptance Rate (FAR) and False Rejection Rate (FRR). FAR is a rate of the numbers of fake images misclassified as real and FRR is a rate of the numbers of real images misclassified as fake. The experimental results showed that when Depth of Field (DoF) is very small, FAR is 2.86% and FRR is 0.00% but when DoF is large, the average FAR and FRR is increased. Thus the results showed that this method is crucially dependent on DoF and for better results, it is very important to make DoF small.

Movement of the eyes based analysis

The technique based on the analysis of movement of eyes was introduced by Hyung-Keun Jee et al. for embedded face recognition system [4]. The authors proposed a method for detecting eyes in sequential input images and then variation

of each eye region is calculated and whether the input face is real or not is determined. The basic assumption is that because of blinking and uncontrolled movements of the pupils in human eyes, there should be big shape variation

3.PROPOSED METHODOLOGY

A.Blockdiagram

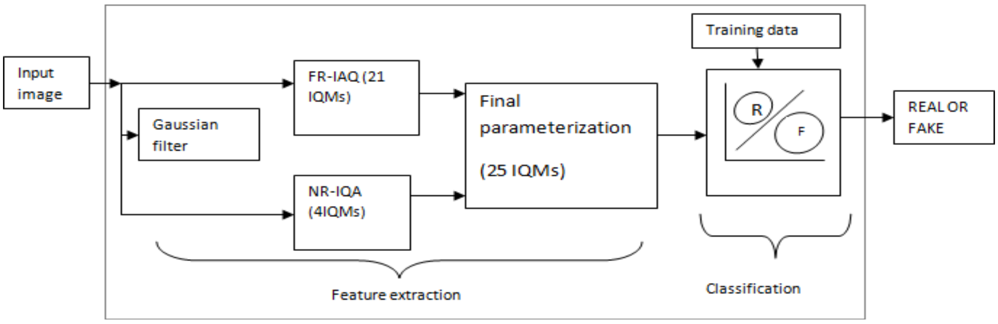

Fig.1. Block diagram

Image Quality Assessment

We use image quality assessment for liveness detection based on the statement that : " It is assumed that a fake image captured during the attacks will have different quality from the real image acquired during normal operation." The quality differences may include difference in color and luminance levels, general artifacts, quantity of information, sharpness, structural distortions or natural appearance. The fake sample will lack the properties found in original images. The usage of IQMs for image quality properties allow detection of quality differences between real and fake samples.We extract some general image quality measures, for simplicity system takes only one image and extract quality measuring features for the image itself rather than trait specific features.This method reduces the computational load to the system and these quality measured features are used to distinguish between real and fake samples. IQMs are classified according to four general criteria.

- Performance -Tested for good performance for various applications.
- Complementarity - The complementary properties like sharpness, structure are used to make system
- Speed – it is related to complexity and it should not take long time for the response.
- Complexity- Features should be less complex to reduce computations.

For each of the scenarios a specific pair of real-fake databases is used. Databases are divided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the paper) of 50 users randomly classifier used for the two scenarios is based on Quadratic Discriminant Analysis (QDA) as it showed a slightly better performance than Linear Discriminant Analysis (LDA), which will be used in the face-related experiments, while keeping the simplicity of the whole system.

Results: 2D Face

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY- ATTACK DB [57] which is publicly available from the IDIAP Research Institute.The database contains short videos (around 10 seconds in mov format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320 × 240 resolution webcam of a 13-inch MacBook Laptop. The recordings were carried out under two different conditions:

i) controlled, with a uniform background and artificial lighting; and

ii) adverse, with natural illumination and non-uniform background.

Three different types of attacks were considered:

i) print, illegal access attempts are carried out with hard copies of high-resolution digital photographs of the genuine users;

ii) mobile, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen;

iii) highdef, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with resolution 1024 × 768.

In addition, access attempts in the three attack subsets (print, mobile and highdef) were recorded in two different modes depending on the strategy followed to hold the attack replay device (paper, mobile phone or tablet): i) hand-based and
i i) fixed-support.

selected from the BioSec baseline corpus.It follows the same structure as the original BioSec dataset, therefore, it comprises 50 proposed protection method. In all cases the final results (shown in Table II) are obtained applying two-fold cross validation.

Results: Iris-Spoofing

The database used in this spoofing scenario is the ATVS-FIr DB which may be obtained from the Biometric Recognition Group-ATVS.1 The database comprises real and fake iris images (printed on BioSec baseline corpus.It follows the same structure as the original BioSec dataset, therefore, it comprises 50 proposed protection method. In all cases the final results (shown in Table II) are obtained applying two-fold cross validation.
The users × 2 eyes × 4 images × 2 sessions = 800 fake iris images and its corresponding original samples. The acquisition of both real and fake samples was carried out using the LG IrisAccess EOU3000 sensor with infrared illumination which
captures bmp grey-scale images of size 640 × 480 pixels.

In Fig. 2 we show some typical real and fake iris images that may be found in the dataset. As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and their corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other 50 eyes available in the dataset. The liveness detection results achieved by the proposed approach under this scenario appear in the first row of Table II, where we can see that the method is able to correctly classify over 97% of the samples. In the last column we show the average execution time in seconds needed to process (extract the features and classify) each sample of the two considered databases.

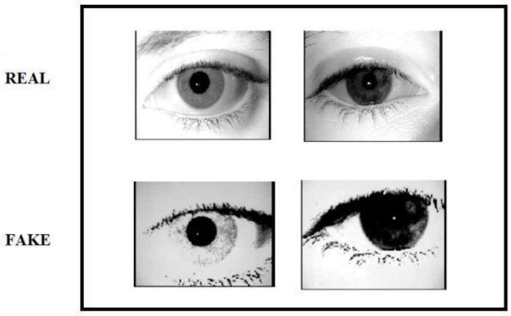

Fig 2.Typical real iris images(top row) and their corresponding fake samples(bottom row)

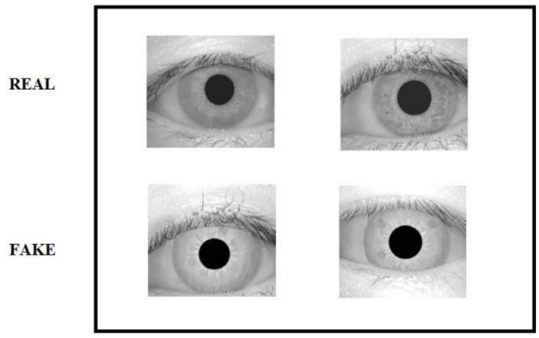

Fig 3.Typical real iris images (top row) and their corresponding fake samples(bottom row)

This time was measured on a standard 64- bit Fig. 3. Typical real iris images from CASIA-IrisV1 (top row) and fake samples from WVU-Synthetic Iris DB (bottom row), used in the iris-synthetic experiments. The databases are available at Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB R2012b. As no other iris liveness detection method has yet been reported on the public ATVS-FIr DB, for comparison, the second row of Table II reports the results obtained on this database by a self-implementation of the anti-spoofing method proposed in [28]. It may be observed that the proposed method not only outperforms the state-of-the-art technique, but also, as it does not require any iris detection or segmentation, the processing time is around 10 times faster. 2) Results: Iris-Synthetic: In this scenario attacks are performed with synthetically generated iris samples which are injected in the communication channel between the sensor and the feature extraction module (see Fig. 1). The real and fake databases used in this case are: • Real database: CASIA-IrisV1. This dataset is publicly available through the Biometric Ideal Test (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA).2 It contains 7 greyscale 320×280 images of 108 eyes captured in two separate sessions with a selfdeveloped CASIA close-up camera and are stored in bmp format. • Synthetic database: WVU-Synthetic Iris DB. Being a database that contains only fully synthetic data, it is not subjected to any legal constraints and is publicly available through the CITeR research center.3 The synthetic irises are generated following the method described in [23], which has two stages. In the first stage, a Markov Random Field model trained on the CASIA-IrisV1 DB is used to generate a background texture representing the global iris appearance. In the next stage, a variety of iris features such as radial and concentric furrows, collarette and crypts, are generated and embedded in the texture field. Following the CASIA-IrisV1 DB, this synthetic database includes 7 greyscale 320 × 280 bmp images of 1,000 different subjects (eyes). We show some typical real and fake iris images that may be found in the CASIA-IrisV1 DB and in the WVU-Synthetic Iris DB. It may be observe that, as a consequence of the training process carried out on the CASIAIrisV1 DB, the synthetic samples are visually very similar to those of the real dataset, which makes them specially suitable for the considered attacking scenario. The last column indicates, in seconds, the average execution time to process each sample. In the experiments, in order to have balanced training classes (real and fake) only 54 synthetic eyes (out of the possible 1,000) were randomly selected. This way, the problem of overfitting one class over the other is avoided. The test set comprises the remaining 54 real eyes and 946 synthetic samples. The results achieved by the proposed protection method based on IQA on this attacking scenario are shown in the bottom row of Table II. In spite of the similarity of real and fake images, the global error of the algorithm in this scenario is 2.1%. The experiments reported in this Section IV-A show the ability of the approach to adapt to different attacking scenarios and to keep a high level of protection in all of them. Therefore, the results presented in Table II confirm the "multi-attack" dimension of the proposed method.

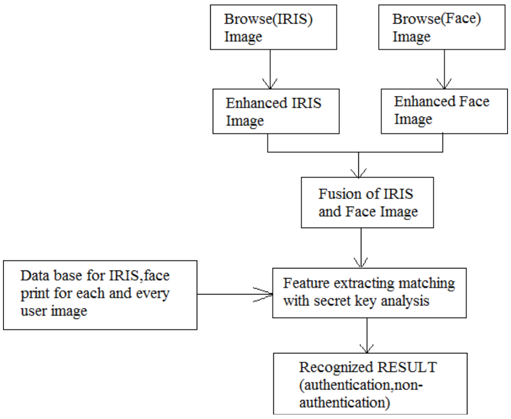
Browse(IRIS) Image
Browse(Face) Image
Enhanced IRIS Image
Enhanced Face Image
Fusion of IRIS and Face Image
Data base for IRIS,face print for each and every user image
Feature extracting matching with secret key analysis
Recognized RESULT (authentication,non-authentication)

Fig 4. Block diagram explaining the proposed work

The block diagram above in Fig 4 shows that the input image is first browsed and it is enhanced for the noise removal every time. The fusion of enhanced iris and face images is done by using some fusion technique then the fused image is again applied for fusion with the enhanced palm print image. Then the final image obtained is the fusion of all three iris, face and palm print images. The image quality features are taken from the final fusion image and its is checked with database every time for the matching to classify as authenticate or non authenticate person.

4.CONCLUSION

Current face biometric systems are very vulnerable to spoofing attacks and photographs are probably the most common sources of spoofing attacks. Inspired by image quality assessment, characterization of printing artifacts and by differences in light reflection, we proposed an approach for spoofing detection based on learning the micro-texture patterns that discriminate live face images from fake ones. Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar and even the human eye may find it difficult to make a distinction between them after a short inspection. Yet, some disparities between the real and fake images may become evident once the images are translated into a proper feature space. These differences come from the fact that biometric traits, as 3D objects, have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (paper, gelatin, electronic display) or synthetically produced samples do not possess. Furthermore, biometric sensors are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3D trait. If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact (2D, different material, etc.), the characteristics of the captured image may significantly vary. We have also evaluated our approach in a real world application (face based access control) by performing various 2D face spoofing attacks using good quality face prints and also high resolution displays. The results were promising. We believe that our approach can also be extended to detect spoofing attacks using masks or 3D models of the face because skin has a very particular texture with, for example, pores whereas fake faces have seldom such a level of detail.

5.REFERENCE

[1] G. Kim, S.Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim, Face liveness detection based on texture and frequency analyses, 5th IAPR International Conference on Biometrics (ICB), New Delhi, India. pp. 67-72, March 2012.

[2] J. Maatta, A. Hadid, M. Pietikainen, Face Spoofing Detection From Single images Using Micro-Texture Analysis, Proc. International Joint Conference on Biometrics (UCB 2011), Washington, D.C., USA.

[3] Sooyeon Kim, Sunjin Yu, Kwangtaek Kim, Yuseok Ban, Sangyoun Lee, Face liveness detection using variable focusing, Biometrics (ICB), 2013 International Conference on, On page(s): 1 – 6, 2013.

[4]J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271–276

[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] M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–496, Sep. 2010.\

[7] D. Brunet, E. R. Vrscay, and Z. Wang, "On the mathematical properties of the structural similarity index," IEEE Trans. Image Process., vol. 21, no. 4, pp. 1488–1499, Apr. 2012.

[8] 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.

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

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

[11] M. G. Martini, C. T. Hewage, and B. Villarini, "Image quality assessment based on edge preservation," Signal Process., Image Commun., vol. 27, no. 8, pp. 875–882, 2012.