INNOVARE JOURNAL OF SCIENCES

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Vol 7, Issue 4, 2019

ISSN - 2321-5496

Review Article

IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION USING SUPPORT VECTOR MACHINE CLASSIFICATION

LINSHA LUVIS, GNANA KING

Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology, Thrissur, Kerala, India. Email: Linshaluvis96@gmail.com

Received: 16 January 2019, Revised and Accepted: 21 April 2019

ABSTRACT

Biometric security system plays a very important role in everyone's life as security. Biometric system is a security system which provides conditional ways after scanning for unique physical characteristics for authentication. However, fake, synthetic or reconstructed sample is the main problem in biometric authentication. These biometric systems are highly flexible to different types of attacks such as some types of synthetically produced artifact (e.g., fake fingerprints, photo print of iris image, or face mask). Hence, new and effective protection actions based on hardware and software have been developed to resist these attacks. Image quality assessment is one of the techniques used in image processing to decide whether the biometric input is real or synthetic. This paper deals with full reference and no-reference measures used to estimate the quality value of an image. Twenty-five image quality features are takeout using mathematical expressions.

Keywords: Image quality assessment, Biometrics, Security.

INTRODUCTION

Biometric authentication has been receiving much concern over the past years due to the increasing demand for automatic person identification. The term biometric mentions here to automatic recognition of an individual based on behavioral and/or physiological characteristics (e.g., fingerprint, face, iris, voice, signature, etc.) which cannot be taken, lost, or copied. As the use of biometric system in many security purposes, the attacks have also increased. The researchers mainly focused on the evaluation of different biometric vulnerabilities, suggestion of new protection methods, and acquisition of specific datasets. All these clearly highlight the significance given by them to the enhancement of the systems security to bring this technology into practical use. Among the various threats evaluated, the direct and spoofing attacks have motivated to examine the vulnerabilities toward this type of fraudulent actions.

As this type of attacks is executed in analog domain and the interactions with the device are done following the regular protocol, the usual digital security mechanisms (e.g., encryption, digital signature, or watermarking) are not useful. Hence, researches focused on the outline of particular methods to find the fake samples and reject them, thus enhance security level of the system.

Liveness detection methods are usually two types: (i) Hardware-based techniques, which add some particular tools to sensor used to detect specific properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye) and (ii) software-based techniques, the fake trait is detected once the sample has been get with a standard sensor [1]. The combination of these two methods is used to increase the security in biometric recognition. One of the disadvantages of protection measures is lack of generality. The current protection measures are based on the measurement of certain specific properties of a given trait; they may not be executed in recognition systems based on other biometric techniques. In the present work, we deal with software-based multibiometric and multiattack security method. It has been verified on publically available databases of iris, fingerprint, and two-dimensional (2D) face.

RELATED WORKS

Some of the anti-spoofing techniques are based on the skin properties for this, Li *et al.*, [2] proposed a technique to detect the spoofing attack. The live face detection has done by analyses of Fourier spectra of single-face image. When compare to real faces, the photograph is normally smaller size and they would contain less high-frequency components. The results are shown that this method has an encouraging performance.

Maatta *et al.* [3] presented an efficient method for face recognition from single-face images by applying microtexture analysis. In this for liveness detection, they make use of multiscale local binary pattern (LBP). Then, it classified to real or fake by support vector machine (SVM) classifier. In this, they are using publically available database (NUAA photograph imposter database). In this method, the differences between real and fake printed faces are the main concern. The main differences between them are the reflection of light and the quality difference that can be detected with microtexture patterns. Using LBPs, it describes its microtextures and their spatial information. Then, the feature vector fed to SVM classifier which classifies whether it is real or fake. Main advantages are robustness and computationally fast.

Pan *et al.* [4] proposed a blinking-based method. It uses a generic camera and based on the eye blink it classified into real or fake. It does not require the extra hardware and it can finish in a non-intrusive manner. Kollreider *et al.* [5] described a method based on the face motion estimation. It is based on model-based local Gabor feature extraction and SVM classification. To detect a face part, estimated optical flow (OFL) pattern matching and classify using model-based Gabor classification. It is a quick method and robust. Bao *et al.* [6] also used OFL for motion estimation. One main concern of these OFL techniques is that users required to be highly cooperative and it take more time for detection, which will make users uncomfortable.

Tan *et al.* [7] proposed real-time and non-intrusive method to detect the spoofing with photograph and video based on the analysis of Lambertian model. In this paper, they formulate the task of detecting photograph spoof as a binary classification problem. The method extracts latent reflectance features of samples by a variational Retinex technique and difference-of-Gaussians method. Then, these are used for classification process. There is no extra hardware requirement.

Dhole and Patil [8] proposed face identification using curvelet transform method. Using the curvelet transform, the features are extracted. The curvelet coefficients create a feature vector for classification. These coefficients set then used to train gradient decent back propagation neural network. Zhang *et al.* [9] presented multispectral face liveness detection method. The Lambertian model examines multispectral features of human skin versus non-skin. To form training set, the reflectance data of real and synthetic faces at multidistances are selected for classification. SVM classifier is used for classification process.

Więcław [10] proposed minutiae-based fingerprint identification and verification. It consists of two procedures, minutia extraction and matching. Depends on the accuracy of the minutia extraction procedure, the performance is determined. Crossing number concept is the technique used in minutiae extraction. The main concern is the quality of fingerprint image. When the quality of images decreased, increase number of false minutiae point.

Drahansky and Lodrova [11] proposed that method is based on the detection of optical characteristics of the finger surface (skin). In this paper detect motion of papillary lines by two methods based on optical principles. One is based on the close-up view of the fingertip by charge- coupled device camera; the second one is the distance measurement with laser sensor. The fingerprint liveness detection has several methods: The wavelet analysis of the fingertip texture [12], the curvelet analysis of the fingertip texture [13], and the combination of local ridge frequencies and multiresolution texture analysis [14].

Li *et al.* [15] described that new feature descriptors are defined by a multiscale directional transform (Shearlet transform) for both face liveness detection and recognition. In this, they are using CASIA face anti-spoofing database for evaluation. Chen *et al.* [16] proposed iris recognition based on a wavelet quality measure. It has ability to deliver good special adaptively and deals with local quality measures of iris image. Proenca [17] proposed a method to get the quality of visible wavelength iris samples takes in unconstrained conditions. Focus, motion, angle, occlusions, area, pupillary dilation, and levels of iris pigmentation are the factors that determine quality of iris image. Zhou and Kumar [18] described a methodology which suitable for any biometric. Three methods to improve the performance of biometric matchers are described. Quality of sample and confidence in matching scores (CS) are the first two methods and third method only use for discrimination between real and fake matching scores.

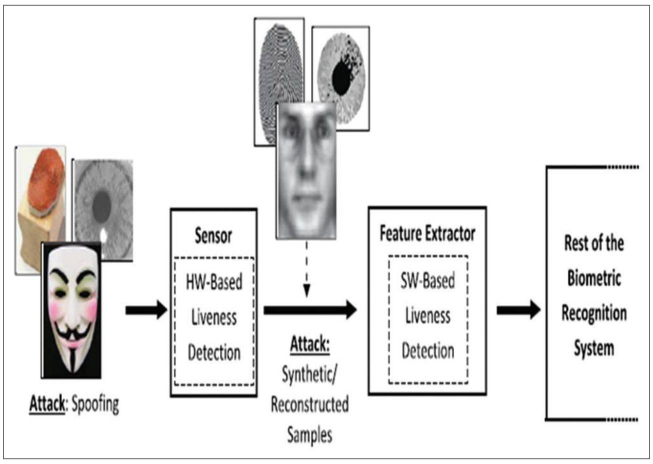
Sensor
HW-Based Liveness Detection
Attack: Spoofing
Attack: Synthetic/ Reconstructed Samples
Feature Extractor
SW-Based Liveness Detection
Rest of the Biometric Recognition System

Fig. 1: Hardware and software-based spoofing detection techniques

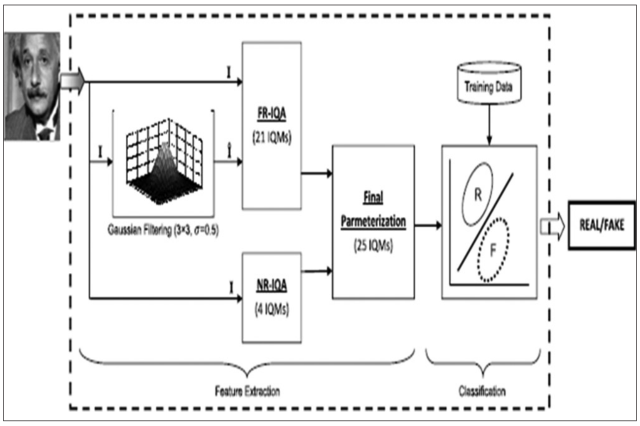

Fig. 2: Block diagram of biometric protection method

Kim *et al.* [19] described the behavior of reflectance in real and fake images. The sensor classifies using Fisher's linear discriminant, and they achieved 97.78 accuracy. Alonso-Fernandez *et al.* [20] reviewed the existing approaches for quality computation of fingerprint image. They are using the MCYT database including 9000 fingerprint images.

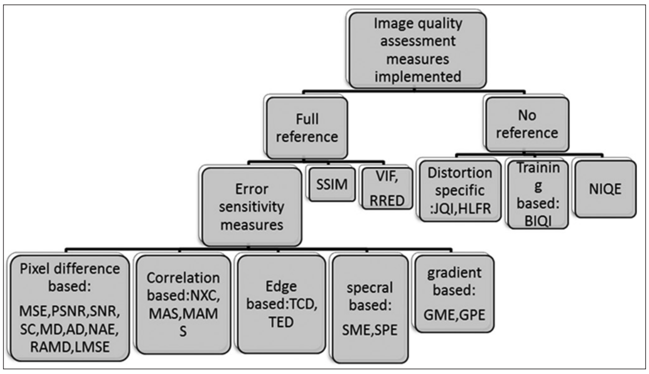
Image quality assessment measures implemented
Full reference
No reference
Error sensitivity measures
SSIM
VIF, RRED
Distortion specific :JQI,HLFR
Trainin g based: BIQI
NIQE
Pixel difference based: MSE,PSNR,SNR, SC,MD,AD,NAE, RAMD,LMSE
Correlation based:NXC, MAS,MAM S
Edge based:TCD, TED
specral based: SME,SPE
gradient based: GME,GPE

Fig. 3: Twenty-five image quality measures classified into full reference and no-reference measures

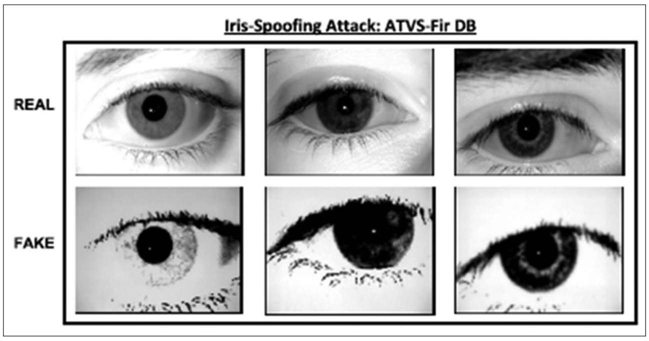

Fig. 4: Typical real and fake iris samples

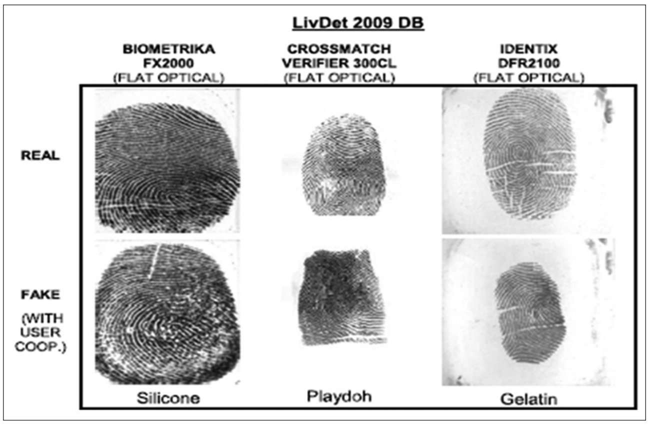
LivDet 2009 DB
BIOMETRIKA FX2000 (FLAT OPTICAL)
CROSSMATCH VERIFIER 300CL (FLAT OPTICAL)
IDENTIX DFR2100 (FLAT OPTICAL)
REAL
FAKE (WITH USER COOP.)
Silicone
Playdoh
Gelatin

Fig. 5: Examples of real and fake fingerprint images

IMAGE QUALITY ASSESSMENT

The use of image quality assessment assumes that: "It is expected that a fake image will have different quality than a real sample." In the proposed system, the input samples are classified into one of two classes: Real or fake. In specific, our experiments implemented in OpenCV in python language of the SVM classifiers. Feature extraction is the method which takes out the desired features from the pre-processed images. The system uses 25 quality features for feature extraction.

Full reference intHelligence quotient (IQ) measures

In full reference, IQ measures the comparison between input and reference image and the features extracted using mathematical functions.

- Error sensitivity measures
  - a. Pixel difference measures
  - b. Correlation-based measures
  - c. Edge-based measures
  - d. Spectral distance measures and
  - e. Gradient-based measures.
- Structural similarity measures
- Information theoretic measures.

Error sensitivity measures

Error sensitivity measures are based on measuring the errors between the distorted and reference images.

Pixel difference measures

It computes the distortion between two images based on the pixel value difference. Here, we consider mean squared error (MSE), signal-to-noise ratio (SNR), peak SNR, maximum difference (MD), structural content, average difference, normalized absolute error, R-averaged MD, and Laplacian MSE.

Correlation-based measures

It considers the similarity between two digital images. This includes normalized cross-correlation, mean angle similarity, and mean angle magnitude similarity.

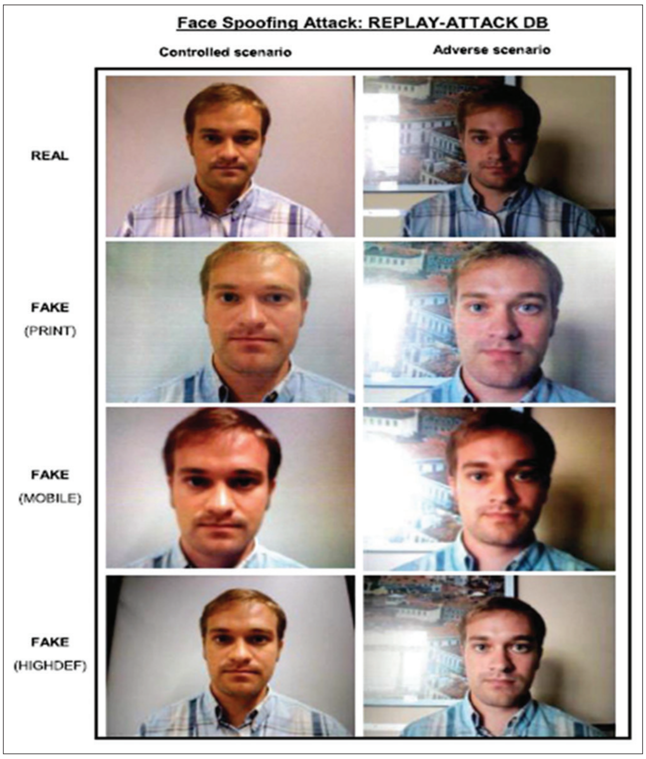

Fig. 6: Examples of real and fake (print, mobile, and highdef) face images

Edge-based measures

The edges are the most informative parts of an image we consider two edge-related measures. Total edge difference and total corner difference edges are detected by Sobel operator and corners are detected by Harris corner detector.

Spectral distance measures

In this, we are applying Fourier transform for image quality assessment. In this, we consider spectral magnitude error and spectral phase error.

Gradient-based measures

In this, structural and contrast changes are considered. We consider gradient magnitude error and gradient phase error.

Structural similarity measures

It considers that there is a variation in lightning contrast or brightness is different in structural image compared to the distorted image. Structural similarity index measure has used in practical applications.

Information theoretic measures

In this, two features are considered the visual information fidelity and the reduced reference entropic difference index.

No-reference IQ measures

The no-reference measures are adopting human visual system. The human visual system does not require the reference image to determine its quality level. No-reference method also does not require reference image. Three approaches are their distortion-specific approaches, training-based approaches, and natural scene static approaches.

Distortion-specific approaches

It contains the joint photographic experts group (JPEG) quality index. JPEG is a block discrete cosine transform-based lossy image coding technique; it evaluates the quality of image the usual block artifacts. The high low-frequency index using the upper and lower frequency of the Fourier spectrum, the sharpness of image is computed.

Training-based approaches

The model is trained using real and fake samples. Then, the quality score computed based on the number of features extracted.

Natural scene static approaches

In this, we are using the natural quality evaluator. It is a blind quality analyzer based on collection of statistical quality features.

SVM CLASSIFICATION

SVM classification is a supervised learning, which the input images are mapped into either one of the two categories as real or fake. It is used only when training set of correctly identified observation available.

Training algorithm

1. Read the sample images from database for training
2. Acquire the image quality features by full reference and no-reference measures
3. Combine all the features and form a feature vector, which contains a number of features that are descriptive of the object
4. Construct a target for SVM classification
5. SVM classifier trained with two categories as real or fake.

Testing algorithm

1. Read the test images
2. Acquire the image quality features from the test image
3. Collect all the features and form a feature vector

4. Feature vector is now compared with the trained feature values using SVM classifier
5. Finally, test image is classified as real or fake.

EXPERIMENTAL SETUP

In this system, we use 25 quality features for feature extraction and SVM classifier for classification. The results are expressed in terms of false genuine rate (FGR), number of false samples which classified as real; and false fake rate (FFR), and number of genuine samples which are considered as fake. The half total error rate (HTER) computed as follows:

HTER = (FGR+FFR)/2

For iris spoofing, the database used for evaluation is from AVTS-Flr DB which acquired from the biometric recognition group – AVTS.

In fingerprint evaluated using LivDet 2009 DB. Using three different optical sensors, the real and fake datasets are constructed: (1) Biometrica FX2000 (569 dpi), (2) Crossmatch Verifier 300CL (500 dpi), and (3) Identix DFR2100 (686 dpi). The gummy fingers are made by silicone, gelatine, or Playdoh materials.

In 2D face, we consider different types of attacks: (1) Print, high-resolution digital photographs, (2) mobile, photos captured by iPhone using iPhone screen, (3) highdef, the photos are displayed using resolution 1024×768.

Qt software is a cross-platform application framework and widget toolkit (graphical user interface [GUI] tool kit). It is a collection of library containing set of graphical control elements. It is used for creating classic and embedded GUI and application. It supports GCC, Python, C++, Visual Studio, etc.

OpenCV is an open source computer vision and machine learning software library. For our experiments, we use in OpenCV in C++ language and the SVM classifier.

CONCLUSION AND FUTURE SCOPE

In this paper, we have introduced a method for biometric detection using image quality assessment and SVM classification. In this method, we are considering the quality variations between real and fake biometric traits. We consider 25 quality features integrate with simple classifier to identify real and fake traits. The most common drawback anti-spoofing method is the absence of generality. The present work is a software base multibiometric and multiattack protection with high performance. The main advantage of this approach: Fast, non-intrusive, user-friendly, cheap, and easy to embed in already functional systems. It has also an added advantage is its speed and very low complexity. It has been verified by publically available databases of iris, fingerprint, and 2D face. There are also possibilities to future work including extension of quality features and can extend this application other image-based protection methods (e.g., hand geometry, vain, palm print, etc.). Video attacks can be also detected using video quality measures.

REFERENCES

1. Galbally J, Marcel S, Fierrez J. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. Vol. 23. IEEE; 2014.
2. Li J, Wang Y, Tan T, Jain AK. Live face detection based on the analysis of fourier spectra. In: Biometric Technology for Human Identification. Orlando: SPIE; 2004. p. 296-303.
3. Maatta J, Hadid A, Pietikainen M. Face Spoofing Detection From Single Images Using Micro-Texture Analysis. IEEE Transaction of Image Processing Conference; 2011.
4. Pan G, Wu Z, Sun L. Liveness detection for face recognition. In: Delac K, Grgic M, Bartlett MS, editors. Recent Advances in Face Recognition. Ch. 9. ???: INTECH; 2008.
5. Kollreider K, Fronthaler H, Bigun J. Non-intrusive liveness detection by face images. Image Vision Comput 2009;27:233-44.
6. Bao W, Li H, Li N, Jiang W. A liveness detection method for face recognition based on optical flow field. In: 2009 International Conference on Image Analysis and Signal Processing. IEEE; 2009. p. 233-6.
7. Tan X, Li Y, Liu J, Jiang L. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In: Proceedings of the 11th European Conference on Computer Vision: Part VI, ECCV'10. Berlin, Heidelberg: Springer-Verlag; 2010. p. 504-17.
8. Dhole SA, Patil VH. Face recognition using curvelet transform. Int J Appl Eng Res 2015;10:33949-54.
9. Zhang Z, Yi D, Lei Z, Li SZ. Face Liveness Detection by Learning Multispectral Reflectance Distributions" Chinese National Natural Science Foundation Project #61070146, National Science and Technology Support Program Project #2009BAK43B26. EEE International Conferenc; 2011.
10. Więcław L. A minutiae-based matching algorithms in fingerprint recognition systems. J Med Inform Technol 2009;13:65-71.
11. Drahansky M, Lodrova D. Liveness detection for biometric systems based on papillary lines. Int J Secu Appl 2008;2:29-38.
12. Moon YS, Ch`n JS, Chan KC, So K, Woo KC. Wavelet based fingerprint liveness detection. Electron Lett 2005;41:1112-3.
13. Nikam S, Argawal S. Curvelet-based fingerprint anti-spoofing. Signal Image Video Process 2010;4:75-87.
14. Abhyankar A, Schuckers S. Fingerprint liveness detection using local ridge frequencies and multiresolution texture analysis techniques. In: Proceeding IEEE ICIP; 2006. p. 321-4.
15. Li Y, Po LM, Xu X, Feng L, Yuan F. Face Liveness Detection And Recognition Using Shearlet Based Feature Descriptors IEEE ICASSP; 2016.
16. Chen Y, Dass S, Jain A. Localized Iris Image Quality Using 2-D wavelets, Advances in Biometrics. Lecture Notes in Computer Science, Vol. 3832. Berlin Heidelberg: Springer; 2011. p. 373-81.
17. Proenca H. Quality Assessment of Degraded Iris Images Acquired in the Visible Wavelength. Vol. 6. IEEE Trans. Information Forensics Secur; 2011. p. 8295.
18. Zhou Y, Kumar A. Contactless Palm Vein Identification using Multiple Representations, Department of Computing. Hong Kong: The Hong Kong Polytechnic University;
19. Kim Y, Na J, Yoon S, Yi J. Masked fake face detection using radiance measurements. J Opti Soc Am A 2009;26:760-6.
20. Alonso-Fernandez F, Fierrez-Aguilar J, Ortega-Garcia J. A review of schemes for fingerprint image quality computation. Eur Co Operat Field Sci Tech Res 2005;