Review Paper on Biometrics Authentication based on Liveness Detection Methods

Bibin Varghese
Dept. of Computer Science & Engineering
Amal Jyothi College of Engineering,
Kanjirapally

Abstract

Nowadays, biometrics is widely used for the purpose of authentication than state of art methods because it provides much higher security and convenience. However, biometric authentication can be easily bypassed by using a fake synthetic or reconstructed sample which is substantial problem and need to be resolved quickly. In this paper, a study of various attacks in the field of different types of biometrics and different software based fake detection methods which are used to detect the different types of unauthorized attacks especially spoofing attacks is reviewed.

Keywords—Biometrics, Biometric Authentication, Spoofing Attacks, Live Detection Methods, Image Quality Assessment.

I. INTRODUCTION

In the new era of technology, Biometric systems are emerging technology which is widely used in the authentication. However, with increasing interest in biometric systems, attackers are developing numerous ways which can be used to bypass the authentication and may get access to valuation information. Hence, various methods are proposed to detect and evaluate the vulnerabilities which are present in the current biometric systems [6]. Also novel methods have been proposed to provide protection from different types of attacks.

Biometrics is a trait which can be used to identify an individual based on the unique physiological characteristics. Each individual have their own personal behavioral patterns that serves as a biometric characteristics. Numerous biometric traits have been developed which can be used to authenticate a person's identity. Hence, in order to identify a person, exceptional characteristics such as features that are extracted from face, iris, fingerprint etc are used [2].

Biometric systems are used to detect or recognize the pattern by using the special unique traits present in the individual and can be used to the purpose of identifying a person. A biometric system verifies the authentication of a person by analyzing the specific physiological or behavioral characteristic possessed by the individual. A biometric system can be used as either an identification system or authentication system. In the case of identification system, a person's identity can be determined even without the person consent or knowledge. For example, a camera can be used to capture the image of an individual in a crowd and with a help of face recognition technology, image can be matched against a known database. In case of verification, biometric systems can determine person's identity. For example, a person can gain access to bank account through a retinal scan or a finger print scan. A biometric system is more convenient than the traditional authentication system which uses passwords and tokens to gain access because the biometric system does not needed lengthy passwords or physical object such as token need to be carried at every time to gain authorized access [3].

II. BIOMETRIC SYSTEMS

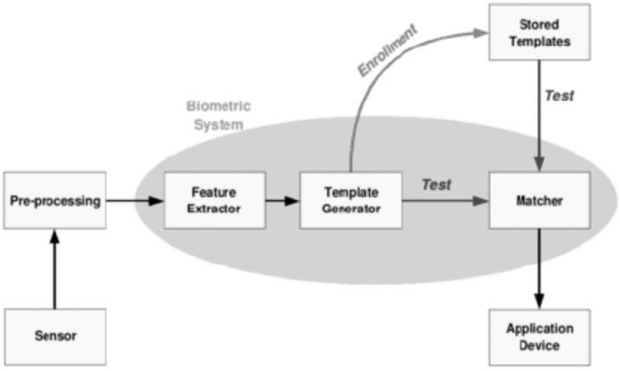

Fig. 1. General block diagram of a biometric system [4].

The figure 1 shows the basic block diagram of a biometric system. Here, biometric data is collected through the sensors, and then it is passed to pre-processing steps. Features are extracted from the preprocessed data and using the extracted features, the biometric template is generated and stored. When authentication is performed the template stored in the database is matched against the biometric query template extracted in this moment. If the templates are matched, the user is authorized one[4].

III. ATTACKS ON BIOMETRIC SYSTEMS

A. Spoof Attacks

Spoofing is type of attack which is done at sensor level where the biometric sample of the individual is replaced by an impostor sample. An attacker in order to deceive the system may try to imitate the biometric trait of an authorized person. This type of attack is mostly done in the case when signature or iris traits are used for authentication. Physical traits are also very much lively to attacked using spoofing. For example, attackers may use synthetic biometric traits such as High quality printed image of iris or gummy fingers

can be used to gain access by bypassing the authentication[1].

From the analysis of different types of attacks/threats, it is found that the direct or spoofing attacks makes the biometric community to learn about the vulnerabilities so that attack can be prevented against traits such as iris, fingerprint, signature, face, etc. Usually the intruder may try to attack the biometric system using some type of artifact which is produced by synthetic methods. Synthetic products can be a gummy finger, face mask or an iris image which is printed. By using these products, intruder makes an attempt to imitate the behavior of the user who is genuine (eg: gait, signature) and tries to gain access in a fraudulent manner. These types of attacks are done in analog domain using regular protocols. Hence, the digital protection mechanisms (such as water marking, encryption, etc) are not very effective against these types of attacks. So researchers need to focus on mechanisms which can be used as counter measures against attacks which can detect fake and hence provide much better security and robustness to the system.

IV. LIVENESS DETECTION

Liveness detection method is an anti spoofing method which uses different types of physiological properties of an individual in order to determine whether the sample is fake or real. Liveness assessment methods are a challenging task in the engineering field and it needs to satisfy certain conditions. Some of them are

i) Methods which should not have an excessive contact with the individual and it should produce any undesirable effect on the user.

ii) It should user friendly so that every individual are not afraid to use the method.

iii) It should be of low cost.

iv) Results produced should be fast in a desirable manner.

v) It should contain good fake detection rate. However, it also should have good recognition performance.

type

Liveness detection methods are classified into two

i) Hardware – based techniques

ii) Software – based techniques

In the case of hardware based techniques, along with the sensors, some specific devices are added along in order to detect certain properties of living trait. For example, blood pressure, fingerprint sweat etc. In software based techniques, first a sample is taken with the help of a standard sensor. Then required features are extracted and stored in the database. These extracted features are used to distinguish between a real and fake person.

Generally, Hardware based methods provide a higher fake detection rate than the software based techniques. But software based techniques are less expensive because there is no need extra devices required. These software based methods may be attached to a feature extractor module which makes the system to identify the other types of unauthorized break-in attempts which are not types of spoofing attacks.

The main problem of most of the anti – spoofing techniques is that there is no generality. Usually, a proposed anti spoofing technique is found to be provides a high performance result in detecting a certain category of spoofs. For example, if the system is designed to detect gummy fingers which are made from silicone material, system produces a high detection rate. But if the attacker uses a gummy finger produced from gelatine, system may not able to identify it. Hence error rate will be increased and testing condition increases heavily. Besides most of state of art protection methods uses measurement of given trait based on the measurement of certain specific properties, for example pupil dilation of the eye or frequencies of ridges and valleys in the fingerprints etc. Hence these systems cannot provide much interoperability.

V. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

Quality of an image is very important and image quality is property or characteristics of an image that can be used to measure the degradation of perceived image. Imaging systems which are used to capture images may produce distortions which may degrade the image; hence quality assessment is a very important factor.

Image quality assessments [5] are methods which are used to find the quality of an image. These use several techniques and metrics and are measured and evaluated automatically with the help of a computer program. There are different types of image quality assessment methods. They are classified as

i) Full Reference (FR) methods

ii) No Reference (NR) methods

In FR methods, a reference image is compared with a test image and quality is tested in assumption that the images are of perfect quality. In NR methods, metrics are used to assess the quality of an image without using any reference image.

There are certain ways in which expected quality of real image and fake samples are different. Some of them may be : luminance levels, color levels, degree of sharpness, artifacts which are present locally, the quantity of data or information which is found in both types of images, ie, entropy, different structural distortions etc. For example, if the image is captured used a mobile device and trembling occurs, then that image may be blurred or out of focus. Sometime image captured can be over exposed or under exposed. Also, fingerprint image is captured from a gummy finger; it may contain local acquisition artifacts such as patches or spots. Usually, an attacker if want to gain unauthorized access to system, then image which is produced synthetically can be directly injected to the communication channel even before extraction of feature occurs.

There are three factors that is used to support the use of IQA features for liveness detection

i) In forensic field, quality of image is successfully used in detection of image manipulation[7] and steganalysis[10]. For example, printed iris image or face image which is used to spoof attack can be considered as type of manipulation in image and with the help of different quality features present in image, fake can be detected

ii) In forensic field, using different trait specific qualities, it is easy to use in liveness detection method. Fingerprint

spoofing can be easily detected if ridge and valley frequency is measured properly. Also iris spoof can be detected by using amount of occlusion in the eye. However, there is no generality for finding the spoofing even though separately each trait can be used to detect spoofing[11].

iii) Different metrics and methods which are designed for IQA intends to estimate in an objective and reliable way the perceived appearance of images by humans.

In order solve this problem of not having generality in biometric systems, if certain quality measures from each biometric systems is taken into consideration and it can be easy to classify whether the input is real or fake. According to authors in [1], 25 IQA measures are used to solve this problem of not having generality in biometric systems. Some of the IQA measures taken into consideration are:

A. Full Reference (FR) measures

The Full Reference (FR) methods usually rely on the availability of a good, neat and undistorted quality reference image which can be used to calculate quality of the test sample. In the problem of fake detection addressed, rreference images are unknown and the detection system only has access to the input sample. In order to solve this limitation, the strategy used for image manipulation detection and for steganalysis [9] is be implemented. Here, authors [1], used the input grey-scale image and is filtered with a low-pass Gaussian kernel in order to create a smoothed version of the image. Then, the quality between both images is computed according to the corresponding full reference IQA metric provided. This approach works on the assumption that the loss of quality produced by gaussian filtering makes it easy find the difference between real and fake biometric samples

1) FR-IQMs: Error Sensitivity Measures – State of art perceptual assessment of image quality approaches are usually based on computing the errors between the distorted images and images which are used as references. These features need to be classified and here it is classified into different groups based on the image property which is measured as Pixel Difference measures. These features can be used to calculate the distortion between two images in accordance with their pixel wise differences. Here, authors [1] include: Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Structural Content (SC), Maximum Difference (MD), Average Difference (AD), Normalized Absolute Error (NAE), R-Averaged Maximum Difference (RAMD) and Laplacian Mean Squared Error (LMSE) methods to classify the real and fake images.

Correlation-based measures - The correlation function are mostly used to find if there is any similarity between two digitally produced images. If the statistics of the angles between the pixel vectors of the real and irregular images is considered, the variant of correlation based measures can be easily acquired. The authors [1] include features such as Normalized Cross-Correlation (NXC), Mean Angle Similarity (MAS) and Mean Angle- Magnitude Similarity (MAMS).

Edge-based measures – Typical edges and corners of digital images are some of the part where huge amount of information is present. The structural distortion of an image is tightly connected with its edge degradation, hence, here authors have considered two edge-related quality measures: Total Edge Difference (TED) and Total Corner Difference (TCD)[1].

Spectral distance measures - Another type of conventional image processing tool which has been applied to the field of image quality assessment measurement is the Fourier transform. Features used in [1] are the Spectral Magnitude Error (SME) and the Spectral Phase Error (SPE).

Gradient-based measures – Generally, gradients emits most important visual information which can be of greater use for the objective of quality assessment. Most of the distortions that can affect an image are usually reflected by a change in its gradient. Hence, if such kind of information is used, then structural and contrast changes can be effectively captured easily. Two most simple gradient based features are used in the biometric system protection are Gradient Magnitude Error (GME) and Gradient Phase Error (GPE)[1]

2) FR-IQMs: Structural Similarity Measures – FR-IQMs : Structural similarity methods are a new paradigm for image quality assessment based on structural similarity was used which follows the hypothesis that the human visual system is very much likely to adapted for extracting structural information from the viewing field. Therefore, distortions in an image that emits from variations in lighting, such as contrast or brightness should be dealt differently from structural ones. Among these recent objective perceptual measures, the Structural Similarity Index Measure (SSIM) has the simplest formulation.

3) FR-IQMs: Information Theoretic Measures: In this FR technique, source of images transmits to a receiver through a channel that limits the quantity of information that could flow through it; hence usually occurrence of distortions can be considered. The aim is to associate the visual quality of the test image to the amount of information shared between the test and the reference signals. The VIF metric generally measures the quality fidelity as the ratio between the total quantity of information ideally fetched by the brain from the total irregular image and the final information provide from within the complete reference image. This metric holds on to the assumption that the natural images of any high class quality, if no distortions is present, it will pass through the human visual system (HVS) of an observer before entering the brain, and fetches cognitive information from it. In the case of irregular digital images, it is hypothesized that the reference signal has passed through another “distortion channel” before entering the HVS. The VIF measure is derived from the ratio of combined information of two quantities: the combined information between the input and the output of the HVS channel when there is no distortion channel is to be present and the mutual information between the input of the distortion channel and the output of the HVS channel for the different test images. Therefore, in order to calculate the VIF metric, the entire reference image is required as quality and is assessed on a global basis. The RRED metric proceed towards the issue of QA from the perspective of measuring the amount of local information difference between the reference image and the projection of the distorted image onto the space of natural images, for a given sub band of the wavelet domain. Hence, the RRED algorithm calculates the average dissimilarity between local entropies which are scaled of wavelet coefficients of

reference and projected distorted images in a distributed fashion. Hence, for the RRED it is not required to have access the entire reference image but only to a reduced part of its facts or information. If all the scaled entropy terms in the selected wavelet sub band are considered in one single block, then this required information can even be reduced to only one single scalar [1].

B. Full Reference (FR) measures

In general, the human visual system does not require of a reference sample to determine the quality level of an image. Using this same type of principle, automatic no-reference image quality assessment (NR-IQA) algorithms are used to manage the very complex and complicated problem of assessing the visual quality of any images, if there is any absence of references. Currently, NR-IQA methods are usually used to roughly calculate the quality of the test image according to some statistical models which are pre- trained. Depending on the images which are needed to be train this model and based on a priori knowledge requirement, the methods are roughly divided into the following three trends.

Distortion-specific approaches - These techniques mainly relies on data or knowledge which are acquired earlier about the type of visual quality loss resulted by a specific distortion. Hence, the final quality measure is calculated based on a model trained which are from clean images and the images affected by this distinct distortion. The JPEG Quality Index (JQI), is used to assess the quality in images affected by the usual block artifacts which are found in most of the compression algorithms running at low bit rates such as the JPEG. The High-Low Frequency Index (HLFI), which was inspired by previous work and it considers local gradients as a blind metric to detect blur and noise in image. Also, the HLFI feature is very sensitive to the sharpness of the image by calculating the difference between the power in the lower and upper frequencies of the Fourier Spectrum.

Training-based approaches - In this type of techniques a model is trained using clean, neat and irregular images. Then, the quality score is calculated based on a number of features which are extracted from the test image and related to the general model used. However, unlike the former approaches, these metrics are intended to provide a general quality score which are not related to a specific distortion. Up to now, the statistical models are trained with images which are affected by different types of distortions. The BIQI uses a two-stage framework in which the individual measures of different distortion-specific experts are grouped together to create one global quality score.

Natural Scene Statistic approaches – This approach is also a blind IQA technique. This blind IQA technique uses a knowledge which is known priori and is taken from natural scene distortion-free images to train the initial model. In this case, no distorted images are used. The main reason behind this trend is that it relies on the hypothesis that undistorted images of the natural world presents certain regular properties which fall under the category of a certain subspace of all possible digital images. If it is quantified correctly, deviations which occur from the regularity of natural statistics can help to evaluate the perceptual quality of an image. Also, this approach is followed by another the Natural Image Quality Evaluator (NIQE) and is used. The NIQE technique is a total blind image quality analyser which is based on the creation of a quality aware cluster of statistical features which are derived from a group of natural undistorted images related to a multi-variate Gaussian natural scene statistical model [1].

VI. CONCLUSION AND FUTURE WORK

By using different IQA including blind measures, authors [1] were able to develop a system which can be used for multi-attacks such as spoofing attacks. Cconsistency performance at a high level for different biometric traits are also achieved and are able to adapt to different types of attacks providing for all of them a high level of protection Hence, the system was able to generalize well to different databases, acquisition conditions and attack scenarios. The present research also opens new possibilities for future work which includes using more than the considered 25-feature set with new image quality measures. Also further evaluation can be provided on other image-based modalities such as palm print, hand geometry, vein etc. If temporal information is included, then for those cases in which it is available such as systems working with face videos. Use of video quality measures for video attacks e.g., Trying illegal access gain attempt considered in the REPLAY-ATTACK DB [1].

REFERENCES

[1] Javier Galbally, Sébastien Marcel, ”Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face recognition”,pp. 710 - 724 ,2014

[2] 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] 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.

[4] Carmen Sanchez Avila, “Biometric Fuzzy Extractor Scheme for IRIS Templates”, International Conference on Security & Management, SAM 2009, Las Vegas Nevada, USA, 2 Volumes, July 2009

[5] 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.

[6] T. Matsumoto, “Artificial irises: Importance of vulnerability analysis,” in Proc. AWB, 2004.

[7] 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.

[8] 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.

[9] Avcibas, N. Memon, and B. Sankur, “Steganalysis using image quality metrics,” IEEE Trans. Image Process., vol. 12, no. 2, pp. 221–229, Feb. 2003

[10] S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar. 2006.

[11] 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