International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Survey on Face Spoofing Detection

Farsana N U[1], Selin M[2]

[1]M.Tech Student, KMEA, Computer Science and Engineering, Mahatha Gandhi University, Kerala, India

[2]Associate Professor, KMEA, Computer Science and Engineering, Mahatma Gandhi University, Kerala, India

Abstract: ***Spoofing attack against biometric systems is still an important problem. Face spoofing is a form of attack that is presenting a fake sample to the acquisition sensor with facial information of a valid user. In this paper, we present a comparison between different methods for face spoofing attack detection.***

Keywords: Face spoofing attack detection, liveness detection, local binary pattern, independent component analysis

1. Introduction

The protection of personal data is the basic requirement of security. Traditionally authentication mechanisms used are knowledge-based methods (e.g., password, secret question) token-based methods (e.g., smart cards, token codes). These methods do not verify who is requesting the access. Since the information can easily be lost, shared or manipulated. So as an alternative, biometrics can be used. Biometrics is also an authentication mechanism, which is more reliable and natural. Biometrics overcomes the disadvantage of the traditional authentication mechanism. i.e, Biometrics verifies who is the person requesting the access. Based on the behaviour, physical or chemical traits, being fingerprint, face, iris, hand geometry, hand vein, voice and DNA biometrics provides methods for providing humans automatically. But attacks are also present in the biometric systems. One of the major attack present in biometric systems is face spoofing.

Face spoofing is a form of attack that is, presenting a fake sample to the acquisition sensor with facial information of a valid user including showing photographs, video, 3D facial model of a valid user etc. Face spoofing attacks may be image-based or video-based. In-order to detect the spoofing attack, there are lots of methods are available that detect whether a biometric sample is original or not. These methods include frequency-based approaches, texture-based approaches and motion-based approaches.

During the capturing process of synthetic biometric data, there are noise information and artifacts are present such as blurring effect, printing artifacts and banding effects. These noise information and artifacts are enough to determine the spoofing attacks.

2. Literature Survey

There are many approaches implemented in face spoofing detection. The existing methods for face spoofing detection can be classified into four groups: user behaviour modelling, user cooperation, methods that require additional software and hardware and methods based on data-driven characterization.

The first method user behaviour modelling captures the user behaviour with respect to acquisition sensor (e.g., eye blinking or small head and face movements) to determine whether a captured biometric sample is synthetic. In this method attack is detected based on eye blinking modelling under the assumption that a spoofed attack with photographs differs from valid access by the absence of movements.

The second method user cooperation is used to detect spoofing by asking challenging questions or by asking the user to perform specific movements which adds extra time and removes the naturalness inherent to biometric systems.

The third method that require additional hardware (e.g., infrared cameras or motion and depth sensors) use the extra information generated by these sensors to detect possible clues of an attempted attack.

The final method based on data-driven characterization looking for clues and artifacts that may detect attempted attack and exploit only the data captured by acquisition sensor. Methods that require additional hardware have the disadvantage of not being possible to implement in computational devices that do not support them, such as smartphones and tablets.

In the data-driven categorization method we can again subdivide it into three approaches: frequency-based approaches, texture-based approaches and motion-based approaches.

2.1 Frequency-Based Approaches

2.1.1Video-Based Spoofing Detection

Pinto et al. [1] proposed a method for detecting video-based spoofing attacks using visual rhythm analysis. Based on the principles of authors, in a video-based spoofing attack, a noise signature is added to the biometric samples during the recapture process. Authors used a low-pass filter to isolate the noise signals and to capture the temporal information of the video, authors used visual rhythm technique.

This is the first method proposed for video-based spoofing attack detection. During the viewing or recapture process of videos, there are artifacts and noises are added to the biometric samples. Here, authors assumed that both noise and

artifacts are enough to detect the spoofing attack. Fig. 1 illustrates the video-based spoofing attack detection using visual rhythm technique.

It involves five steps. In the first step, noise residual video for all videos in the training set is calculated. In the second step, Fourier spectrum is calculated. The third step is calculating the visual rhythms of each Fourier spectrum video. Visual Rhythm is a technique that can capture the temporal information and summarize the video contents in a single image. There are two types of visual rhythm are generated for each video: Vertical visual rhythm; formed by the central vertical lines Horizontal visual rhythm; formed by the central horizontal lines. In the next step, visual rhythm is arranged as a texture map. Finally, two machine learning techniques are used to classify the patterns that are extracted from the visual rhythms. The machine learning techniques used are Partial Least Squares (PLS) and Support Vector Machine (SVM).

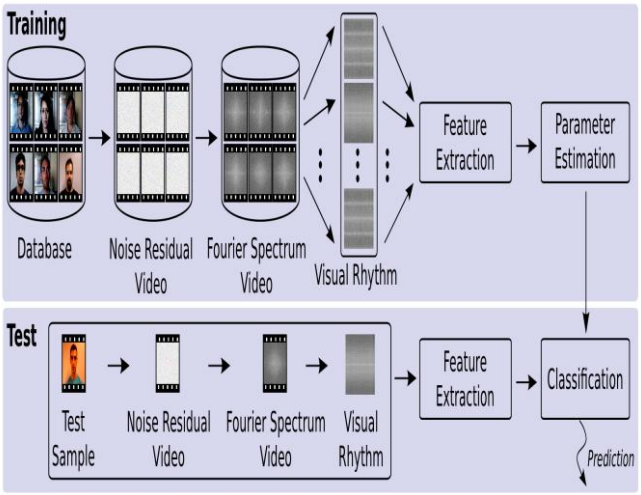

Figure 1: The video-based spoofing attack detection based on the visual rhythm technique. Result is predicted based on both training and testing phase.

2.1.2 Liveness Detection Using Frequency Entropy

Lee et al. [2] proposed a method based on frequency entropy of images. In this paper, the colour video of the face region is captured and split into RGB channels to obtain the time sequences of each colour channel. To find the face region, a face verification algorithm is used. Then by using Independent Component Analysis (ICA), three RGB sequences are analysed to eliminate the cross-channel noise caused by interference from the environment. Finally, the authors calculated the power spectrum. These power spectra are verified through entropy calculation and based on a threshold value the authors decide whether a biometric sample is synthetic or real to validate the liveness or spoofing attack. Fig. 2 illustrates the liveness detection using frequency entropy of image sequences.

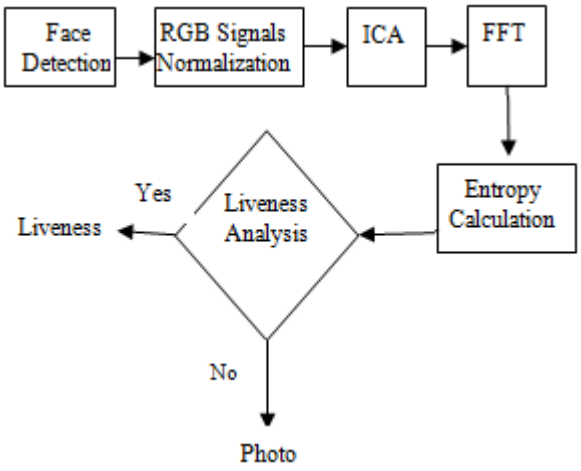

Figure 2: Liveness detection using frequency entropy of image sequences.

2.1.3Liveness Detection in Face Recognition Systems

Nalinakshi et al. [3] proposed a method for detecting liveness of the user with the help of local facial features like eye blinking, lip movement, forehead and chin movement pattern of the face detected with real-time generic web camera. First step is capturing the image of face with low resolution camera. Then by using Viola Jones method, localization of facial portion is carried out. To extract the face features LBP operator is applied on the localized face. The extracted features are called templates, which is securely stored in database. Each facial image is divided into 256 cells. Feature vector is generated from all the 256 gray values computed from the histogram generated by the individual instances of the face images.

During the identification step, the templates stored in the database and generated feature vector of the user is compared by using template matching. Template matching is one-to-many matching which is carried out using Manhattan distance. Best matching of facial image is identified using the min Manhattan distance. If the matching is successful, then perform the liveness check using variations in local regions of facial features like eyes, lips, forehead and chin area. If there is any variation in these local features, then we can conclude that the user is alive. Otherwise user is not alive. Aliveness is calculated by taking the mean and standard deviation of each of the local regions. This method provides security in two phases: authentication and liveness checks. Fig. 3 illustrates the liveness detection technique for prevention of spoof attack in face recognition system.

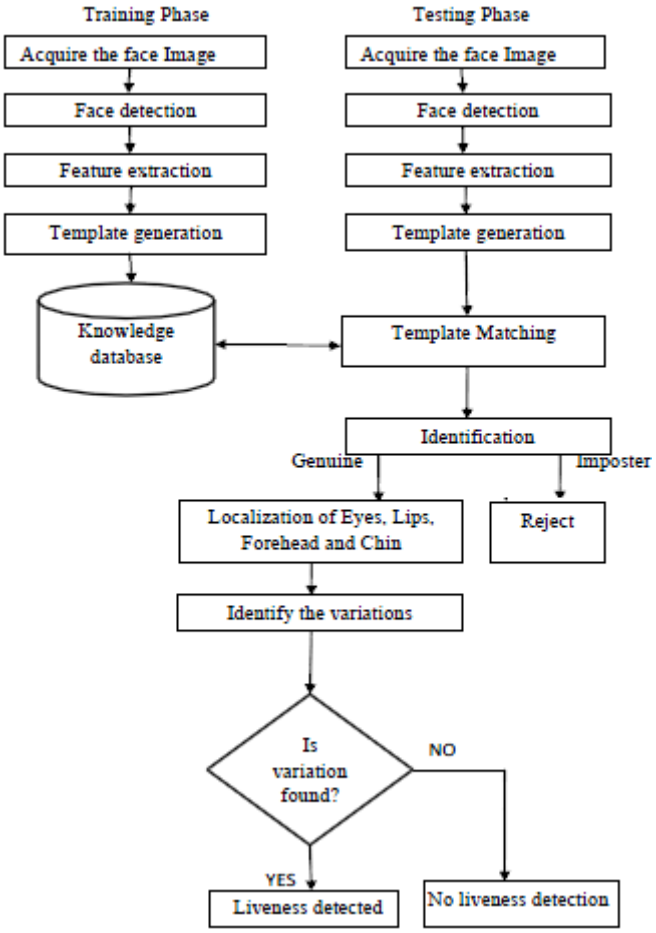

Figure 3: Liveness detection technique for prevention of spoof attack in face recognition system.

2.2 Texture-Based Approaches

2.2.1Face Spoofing Detection Using Micro-Texture Analysis

Määttä et al. [4] explored micro textures for spoofing detection using the Local Binary Pattern (LBP). The authors make use of different LBP operators such as tLBP, dLBP and mLBP. Then by using χ^2 histogram comparison, Linear Discriminant Analysis and Support Vector Machine histograms were classified from these descriptors. Fig. 4 illustrates face spoofing from single images using micro-texture analysis.

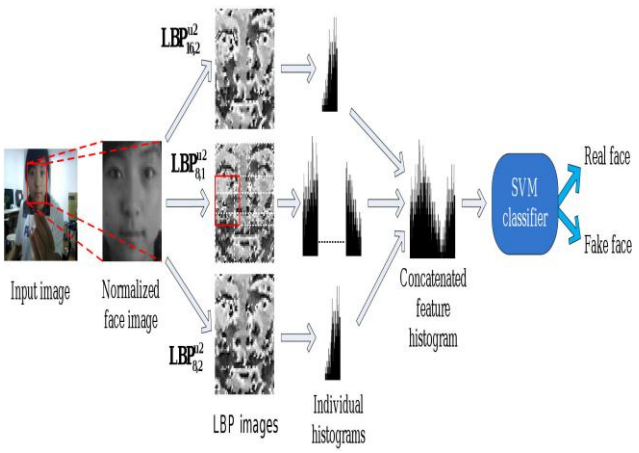

Figure 4: Face spoofing from single images using micro-texture analysis

The face images are captured from the photographs may look very similar to the images captured from real faces. To separate live and fake classes suitable feature space is needed. This method aims at learning the small differences between the real images and those of photographs and then creating feature space; which categorize these differences.

2.3 Motion-Based Approaches

2.3.1Fusion of Multiple Clues

Tronci et al. [5] proposed a method based on the motion information and clues that are take out from the scene by combining two types of processes, referred to as static and video-based analysis. The static analysis consists of combining different visual features such as colour, edge, and Gabor textures. The video-based analysis combines simple motion-related measures such as eye blink, mouth movement, and facial expression change.

The static analysis is used to find the abnormalities related to the input samples at verification process. The hypothesis is that differences are present in the visual data between images captured from real scene, and from photograph. These differences can be found directly from a single image or frame by frame if we are using a video.

The video analysis combines the simple measures of movement. Fusion was carried out at score level by using a weighted sum. Photo detection gives a higher weight in combination. Movement measures contribute only very little weight.

3. Conclusion

Several attack techniques have been developed to deceive the biometric systems. Our face is the biometric data more exposed. Face spoofing attacks can occur when a person tries to masquerade as someone else falsifying the biometric data that are captured by the acquisition sensor. i.e., showing a photograph of a valid user, showing a video of a valid user and showing a 3D facial model of a valid user. There are many works to solve the photo-based spoof attack detection.

In this paper, we discussed different methods for detecting face spoofing attacks that take advantages of noise and artifacts that are added to the fake biometric samples during the recapture process. These methods identify the user being real or not, in face biometric security systems.

References

[1] A. da Silva Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha, "Video-based face spoofing detection through visual rhythm analysis," in *Proc. 25th SIBGRAPI Conf. Graph., Patterns Images*, Aug. 2012, pp. 221–228.
[2] T.-W. Lee, G.-H. Ju, H.-S. Liu, and Y.-S. Wu, "Liveness detection using frequency entropy of image sequences," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, May 2013, pp. 2367–2370.
[3] Nalinakshi B. G, Sanjeevakumar M. Hatture, Manjunath S.Gabasavalgi, Rashmi P. Karchi, " Liveness Detection

Technique for Prevention of Spoof Attack in Face Recognition System," in *Proc. IJETAE Int.* vol. 3. Dec. 2013, pp. 627-633

[4] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE Int. Joint Conf. Biometrics*, Oct. 2011, pp. 1–7.

[5] R. Tronci *et al.*, "Fusion of multiple clues for photo-attack detection in face recognition systems," in *Proc. IEEE Int. Joint Conf. Biometrics*, Oct. 2011, pp. 1–6.

Author Profile

Farsana N U received the Bachelor of Technology degree in Computer Science and Engineering from Calicut University in 2013 and currently doing Master of Technology in Computer Science and Engineering from Mahatma Gandhi University.