International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Robust Framework for Antispoofing Face Recognition Mechanism for Mitigating Image Attacks

Jignesh N Solanki[1], Chirag R Patel[2], Vijaysinh K Jadeja[3]
[1, 2, 3] *Assistant Professor*
[1]*Information Technology Deprtment*
,[2]*Computer Engineering Department,*
[3]*Information Technology Department*
[1]*C U Shah College of Engineering and Technology, Wadhwan City, India*

Abstract: ***The challenge here is that the appearance of human face can change drastically due to various illumination conditions and there are also many camera-related factors that may influence the quality of images, which makes it hard to differentiate images from a live person from those from photos. Due to these, simply asking "what's in the image (e.g., human skin)" tends to be unreliable. Another strategy is to use various image processing techniques to extract features that highlight the difference between images from live human faces and those from photographs.***
Work on fraud detection capabilities for face is still limited and a substantial part of it is based on the flatness of the captured surface in front of the sensor during an attack. This is also true for approaches that examine the 3D nature of the face by employing additional devices, which is much more realistic now with the introduction of affordable consumer depth cameras. With the help of the advancements in 3D manufacturing technologies, easily attainable facial masks take the spoofing attacks one step further and introduce new challenges for counter measure studies. The lack of protection against biometric spoofing attacks is not exclusive to face biometrics [2].
While it is possible to spoof a face authentication system using make-up, plastic surgery or forged masks; photographs and videos are probably the most common threats. Moreover, due to the increasing popularity of social network websites, a great deal of multimedia content, specially videos and photographs, is available on the web that can be used to spoof a face authentication system. To mitigate vulnerabilities, effective countermeasures against face spoofing must to be deployed.
Keywords: Anti- spoofing, Mitigating, Biometric.

I. INTRODUCTION

Biometric techniques, which rely on the inherited biometric traits taken from the user himself for authentication, have gained wide range of applications recently. Unfortunately, once such biometric data is stolen or duplicated, the advantages of biometrics become disadvantages immediately. This situation is most commonly found in a face recognition system, where one or some photos of a valid user can be easily obtained without even physically contacting with him/her, say, through internet downloading or simply capturing them using a camera. A 2D-image based facial recognition system can be easily spoofed by these simple tricks and some poorly-designed systems have even been shown to be fooled by very crude line drawings of a human face. Actually, it is a very challenging task to guard against spoofs based on a static image of a face, while most effort of the current face recognition research has been paid on the "image matching" part of the system without caring whether the matched face is from a live human or not [1].
Basically there are two main categories of face anti-spoofing techniques, the facial motion detection category and facial texture analysis category. Facial motion detection techniques expect subjects to exhibit specific facial motion, the detection of which determines the liveness. Facial texture analysis techniques believe that fake faces probably lack some high frequency information during the reproduction process, and by analyzing and learning the facial texture information, genuine and fake faces can be classified properly. Here the term "texture" represents the high frequency details in face images, and without ambiguity, the study treats "texture" equally with "high frequency information".

II. LITERATURE STUDY

This section discusses about the significant studies being carried out most recently about the prime domain of the proposed study. Fumera et al. [3] have introduced the issue of multimodal anti-spoofing, and gave an overview of state-of-the-art anti-spoofing measures. The problem considered is multimodal biometric verification systems, whose aim is to verify a claimed identity on the basis of different biometric traits submitted by the user. One of the most recent studies of superior level is proposed by Erdogmus and Mercel [4] who have introduced first public spoofing database with facial masks, called 3D Mask Attack Database. The author have used Morpho database and 3D Mask Attack Database (3DMAD) is a face spoofing database which currently contains 76500 frames of 17 different users, recorded using Microsoft Kinect sensor for both real access and spoofing attacks using 3D facial masks. The same author has discussed about the same issues in [5]. Pereira et al. [6] assesses how well existing face anti-spoofing countermeasures can work in a more realistic condition. The authors have introduced test protocol using the only two video face anti-spoofing databases publicly available.

Kollreider et al. [7] have used a lightweight novel optical flow, which is especially applicable in face motion estimation based on the structure tensor and inputs of a few frames to assist in a biometric authentication framework, by adding liveness awareness in a non-intrusive manner. Experimental results on the proposed system are presented on both a public database and spoofing attack simulations. Pinto et al. [8] have presented a solution to video-based face spoofing to biometric systems using noise signatures generated by the recaptured video to distinguish between fake and valid access.

Kose and Dugelay [9] used a 2D+3D face mask attack database which was prepared for TABULA RASA research project. Suhr et al. [10] have proposed a system which assesses the recognizability of facial images of ATM users to determine whether their faces are severely occluded using component-based face candidate generation and verification approach to handle various facial postures and acceptable partial occlusions. Matta et al. [11] proposed an architecture that analyzes the texture of the facial images using multi-scale local binary patterns thereby providing a unique feature space for coupling spoofing detection and face recognition. Tronci et al. [12] have performed both video and static analysis in order to employ complementary information about motion, texture and liveness and consequently to obtain a more robust classification.

However, after reviewing the recent development, it can be found that current researches only concentrate on fake face with little variations. Another shortcoming in variation is the quality of attacks where algorithms extract the high frequency information to detect liveness. But as this high frequency information highly depends on the image quality, how will they perform on good quality and bad quality images. It can be seen that due to the lack of variational data, many questions remain unanswered. Majority studies were found to propose local binary pattern-based countermeasures to spoofing attacks based on the hypothesis that real faces present different texture patterns in comparison with fake ones. However, the techniques analyse each frame in isolation, not considering the behaviour over time.

Another interesting research against photo spoof is to use a user-specific key to generate a random matrix to distort the face template, so that a ”stolen” face image without the key will be almost of no use. This kind of method, however, mainly focuses on the security of biometric templates instead of face liveness detection. Hence, it can be seen that inspite of various literature archival, there is a significant tradeoffs and research gap in this regards.

III. PROPOSED METHOD

The preliminary phase of the study focuses on the methods which rely on a single static image to do spoof detection. Such methods can also be directly applied to deal with video spoof or be integrated with a video-based face liveness detection method for better performance. The challenge here, is that the appearance of human face can change drastically due to various illumination conditions and there are also many camera-related factors that may influence the quality of images, which makes it hard to differentiate images from a live person from those from photos.

In this phase, the anti-photo spoof problem is formulated as a binary classification problem, thus the statistics from the whole set of images consisting both live human faces and photographs can be fully exploited. To evaluate this design, the system will use a publicly available large photograph-imposter database containing massive number of images from multiple subjects. The study will use Retinex approach, in which the luminance is first principally sought within the total variational framework and the reflection coefficient will be estimated through Retinex approach discussed by Fu et al. [13]..

The next phase of the study will focus on designing a baseline algorithm to give a preliminary study. For fake faces, the reproduction process such as printing or displaying will inevitably degrades the quality of facial texture. So the high frequency information may be a strong proof of liveness. The system will use multiple effective filters to extract the high frequency information and exclude the low frequency information and noise. Then a supervised learning algorithm / classifier will be used for

training on the filtered image, which outputs the final decision. The system formulate considers one fact that the facial motion is a crucial liveness clue for anti-spoofing, and it is necessary to provide them just like in a challenge-response strategy used in facial motion detection methods. The motion type of blink is chosen because it is more natural and user-friendly than other motion types such as head movement and mouth movement.

The next phase of the study is focused on an in-depth analysis on the use of dynamic texture for face liveness description using a unified experimental setup and evaluation methodology. In this case, each frame of the original frame sequence was gray-scaled and passed through a face detector using modified census transform features. After the face detection step, the local binary patterns operators were applied for each image plane and the histograms will be computed and then concatenated. After the feature extraction step, binary classification can be used to discriminate spoofing attacks from real access attempts. In order to explore the dynamic texture information more carefully, the study will introduce the multiresolution approach. The multiresolution approach can be performed by concatenating the histograms in the time domain. Finally, the outcome of the proposed system is compared with the study of Erdogmus and Marcel [4] to evaluate the level of effectiveness in proposed solution.

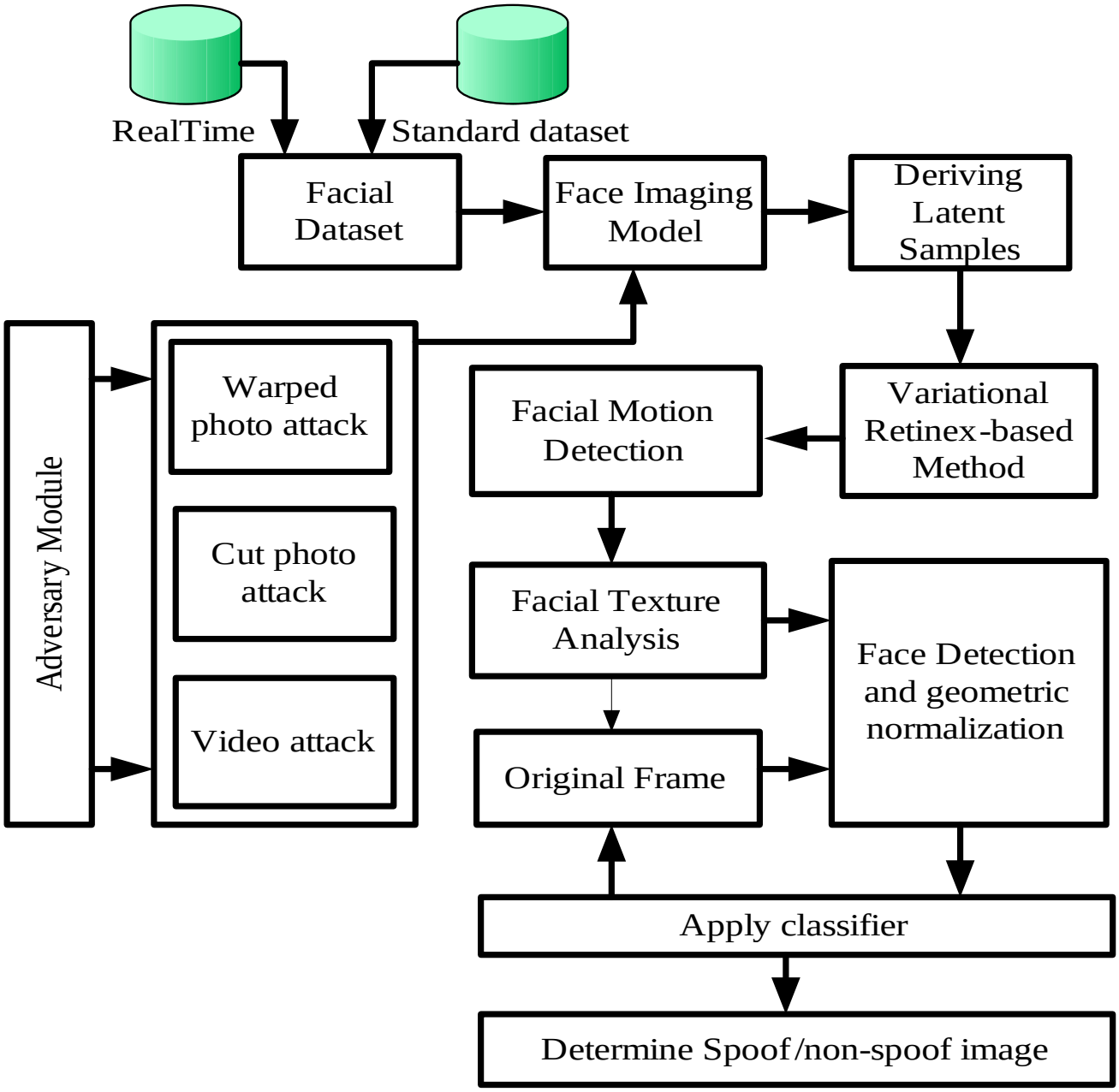

Figure 1 Indicative Architecture of Proposed Study

IV. CONCLUSION

A. The possible outcomes of the proposed system are as follows:

1) Enhanced Detection Performance: The proposed study will use optimization theory for strengthening the detection and mitigation techniques for forged images, hence precise percentage of detection (genuine and fake) facial images are expected as an outcome.

2) Algorithm Robustness: The entire dataset will be subjected for quality test, fake face test, and overall test under various illumination condition to anticipate effective algorithm that is compliant of time and space complexity.

3) Anti-Spoofing Accuracy: The proposed framework will used false acceptance rate and false rejection rate for marking the effective trials being performed on various images and higher accuracy is anticipated as an outcome.

REFERENCES

[1] .N. Rodrigues, “Face Modeling and Biometric Anti-Spoofing Using Probability Distribution Transfer Learning”, BiblioBazaar, 2012
[2] S. Lina, R. Latha, “Detecting Masquerade in Face Recognition System – A Literature survey”, IOSR Journal of Computer Engineering, Vol.16, Iss.1, Ver. IV, pp.01-05, 2014
[3] G.Fumera, G.L. Marcialis, B. Biggio, F. Roli and S. C. Schuckers, “Multimodal Anti-Spoofing in Biometric Recognition Systems”, Springer, 2014
[4] N. Erdogmus, S. Marcel, “Spoofing Face Recognition With 3D Masks”, IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, July 2014
[5] N. Erdogmus and S. Marcel, “Spoofing in 2D Face Recognition with 3D Masks and Anti-spoofing with Kinect”, IEEE Sixth Conference on Biometrics, pp.1-6, 2013
[6] T. F. Pereira, A. Anjos, J.M. Martino, S. Marcel, “Can face anti-spoofing countermeasures work in a real world scenario?”, IEEE International Conference on Biometrics Compendum, pp.1-8, 2013
[7] K. Kollreider, H. Fronthaler, J. Bigun, “Non-intrusive liveness detection by face images”, ACM Digital Library, Image and Vision Computing, vol.27, pp.233–244, 2009
[8] A. S.Pinto, H. Pedrini, W.R. Schwartz, A. Rocha, “Video-Based Face Spoofing Detection through Visual Rhythm Analysis”, IEEE, 2012
[9] N. Kose, J-L Dugelay, “On The Vulnerability Of Face Recognition Systems To Spoofing Mask Attacks”, IEEE, 2013
[10] J.K. Suhr, S. Eum, H. G. Jung, G. Li, G. Kim, J. Kim, “Recognizability assessment of facial images for automated teller machine applications”, Pattern Recognition, Elsevier, 2012
[11] J. Maatta, A. Hadid, M. Pietikainen, “Face Spoofing Detection From Single Images Using Micro-Texture Analysis”, IEEE, 2011
[12] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, “Fusion of multiple clues for photo-attack detection in face recognition systems”, IEEE, 2011
[13] X. Fu, Q. Lin, W. Guo, Y. Huang, D. Zeng and X. Ding, “A Novel Retinex Algorithm Based On Alternating Direction Optimization”, International Symposium on Precision Mechanical Measurements, Vol. 8916, 2013