IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. IV (Jan. 2014), PP 01-05
www.iosrjournals.org

Detecting Masquerade in Face Recognition System – A Literature survey

Lina. S[#1], Dr. R. Latha[*2]
[#]*Research scholar, Department of Computer Applications, Bharathiar University, Coimbatore, Tamilnadu, India.*
[#]*Assistant Professor, Department of Computer Science, Women's Christian College, Chennai, Tamilnadu, India.*

Abstract: *A masquerader is an (often external) attacker is one who, after succeeding in obtaining a legitimateuser's credentials, attempts to use the stolen identity to carry out malicious actions.Automatic detection of masquerading attacks is generally undertaken by approaching theproblem from an anomaly detection perspective: a model of normal behaviour for eachuser is constructed and significant departures from it are identified as potentialmasquerading attempts.The most common techniqueto masquerade a face recognition system is to use a photo print or a video of a valid user to gain illegitimate access. There exist methods in literature addressing this issue. This paper presents an analysis of masquerade detection algorithms in face recognition system.*

I. Introduction

Face recognition has been an active research area in computervision research because facial information providesmeans for non-intrusive and natural interaction, identityverification and recognition. Although wide range of viewpoints,ageing of subjects and complex outdoor lighting arestill research challenges, face recognition is beginning to bemature enough for biometric-enabled applications. However, vulnerability to direct attacks is the most crucial problemfor companies willing to market 2D face based biometricidentity management solutions.

The use of facial photographs of a valid user to spoofface recognition is the most common attack method, as the photographs of the users are widelyavailablethrough websites like social networks.Even videos ofthe users can be easily captured from distant cameraswithout prior consent. To make face recognition as asuccessful biometric identification technology, there exists the necessity of answering the spoofing attack problem.

Figure1. Examples of real accesses attempts (leftmost column)and corresponding scenic fake face attacks i.e. face spoof with both faceand background scene, from the Replay-Attack Database

One traditional way of classifying insiders is as traitors andmasqueraders (Ben Salem et al., 2008). A traitor is a user whoalready enjoys some privileges within the system and whosepurposes will affect negatively the security properties of theorganisation's information and systems. A masquerader, onthe contrary, is an often external attacker who succeeds inobtaining a legitimate user's credentials and attempts to usethe stolen identity to carry out malicious actions (e.g. creditcard fraudsters).

A masquerader'sintent is to masquerade the attacks to avoid detection. A masquerade detectionsystem is designed to detect such masquerades.Virtually all existing masquerade detection approachesrely upon one key observation: "behaviour is not somethingthat can be easily stolen" (Ben Salem et al., 2008).

II. Survey Of Related Work

While challenge-response approach [9, 12, 7], multimodalanalysis [8, 12] and multi-spectral imaging [25, 18,21] provide efficient means for discriminating real facesfrom fake ones, they are also rather impractical due to interactionor unconventional imaging requirements. In this section,reviews only anti-spoofing techniques requiring nouser-cooperation and using conventional imaging systemsbecause these properties make them appealing to use withinthe existing face authentication systems. Another advantageis that usually it is not known which visual cues areused when the system is harder to deceive.

Typical non-intrusive 2D face anti-spoofing technique isliveness detection that aims at detecting physiological signsof life, such as eye blinking, facial expression changes andmouth movements. For instance Pan et al. [17] exploitedthe observation that humans blink once every 2-4 secondsand used Conditional Random Field (CRF) framework tomodel and detect eye blinking. In general, motion analysisis a commonly used countermeasure since it can be assumedthat the movement of planar objects, e.g. video displays andphotographs, differs significantly from real human faceswhich are complex 3D objects. Kollreider et al. [11] presentedan optical-flow based method to capture and trackthe subtle movements of different facial parts, assumingthat facial parts in real faces move differently than on photographs.

In another work [4], Bao et al. also used opticalflow based motion estimation for describing the movementof planar objects such as prints or screens. Anjos etal. [1] presented a countermeasure to scenic face attacks bymeasuring the motion correlation between the face and thebackground regions through simple frame differences. Eventhough motion is an important visual cue, vitality and nonrigidmotion detectors are powerless under video-replay attacksif interaction is not employed.

Another category of anti-spoofing methods are based onthe analysis of skin properties such as reflectance and texture.Assuming that photographs are usually smaller in sizeand they would contain fewer high frequency componentscompared to real faces, Li et al. [14] described a methodbased on the analysis of 2D Fourier spectra. In a recentwork, Tan et al. [22] considered the Lambertian reflectancemodel and extracted two types of latent reflectance featuresusing a variationalretinex-based approach and differenceof-Gaussians (DoG) filtering to discriminate between the2D images of face prints and 3D live faces.

The aforementionedapproaches may work well for down-sampled photosbut are likely to fail for higher-quality images. Bai et al. [3]extracted micro-textures from the secularity component ofan image to detect recaptured images. The major drawbackof this method is that it requires high resolution input imagesin order to discriminate the fine micro-texture of the used spoofing medium. Maatta et al. [15] and Chingovskaet al. [6] addressed this issue by exploring the structure offacial micro-textures using local binary patterns (LBP) [16]on conventional webcam-quality images.

However, the natureof texture patterns varies a lot due to different acquisitionconditions and spoofing media, thus diverse datasetsare needed for training the micro-texture based methods.Recently, Komulainen et al. [13] extended the microtextureanalysis based spoofing detection into spatiotemporaldomain. In addition to analysing the structure of facialmicro-textures, local binary patterns from three orthogonalplanes (LBP-TOP) [26] were applied for describing specificdynamic events, e.g. facial motion and sudden characteristicreflections of planar spoofing media, and scenic cueswhich might differentiate real faces from fake ones. Similar visual cue was considered in the work by Pinto et al. [19]as the dynamic artefacts of display devices were exploited for detecting video-replay attacks. More specifically, visualrhythms were computed from the Fourier spectrum of theextracted video noise signatures and the resulting texturalinformation was compressed with gray level co-occurrence matrices (GLCM).

Fusion of anti-spoofing measures has not been studiedmuch and mainly combination of highly correlated motioncues [10] has been considered.Tronci et al. [23]and Schwartz et al. [20] were able to obtain impressiveperformance using motion and texture information but atthe cost of complexity.In [23], many visual features andsupport vector machines (SVM) were needed for detectingsimple print-attacks, whereas in [20] temporal informationfrom videos was accumulated by concatenating descriptionsof individual frames which results in very highdimensionalfeature vectors.

Conversely, Yan et al. [24]wanted to achieve better generalization capabilities and proposednovel liveness clues with clear semantic definitionsin order to avoid just extracting specific feature and traininga ”black box” classifier. However, the algorithm utilizedmainly two uncorrelated motion cues, non-rigid motion andface-background consistency analysis, while the only spatialcue, banding analysis, was discarded unless uniformbackground was observed, since both face and backgroundregions were used for image quality assessment.Indeed, many directions for non-intrusive spoofing detectionhave been already explored but none of them is aloneable to capture the nature of every face spoofing scenario.

Therefore, the problem of spoofing attacks should be brokendown into attack-specific subproblems that can be solvedefficiently with a proper combination of countermeasures. To follow this principle proposes fusion of motion andtexture based methods for detecting various scenic face attacks.Furthermore, whenmultiple anti-spoofing measures are used in parallel, computational efficiency is very importantcriteria.In addition to the used spoofing medium type, such asphotograph and video display, 2D fake face attacks can becategorized into two groups, close-up and scenic attacks,based on how the fake face is represented with the spoofingclassificationsschemes on individual countermeasures.

III. Detecting Fake Face

Both types of 2D face spoofs have common and, more importantly, their own distinctive visual cues that canbe exploited in spoofing detection schemes.A close-up spoof describes only the facial area which ispresented to the sensor. The main weakness with the tightlycropped fake spoofs is that the boundaries of the spoofingmedium, e.g. a video screen frame, photograph edges, orthe attacker's hands are usually visible during the attack,thus can be detected in the scene [13]. However, these visualcues can be hidden by incorporating background scenein the face spoof and placing the resulting scenic face spoofvery near to the sensor. Fortunately, the proximity betweenthe spoofing medium and the camera might cause the recapturedface image to be out-of-focus and reveal also other facialtexture quality issues, like degradation due to the usedspoofing medium. Furthermore, for stationary systems, itshould be possible to observe high correlation between theoverall motion of the face and the background regions.

This workconcentrates on detecting scenic spoofingattacks by exploiting the aforementioned two visual cues.More specifically, the fusion of tworecently proposed countermeasures based on motion [1] andmicro-texture analysis [6, 15] that have individually shownmoderate discriminative power.

3.1. Motion correlation analysis

Anjos and Marcel [1] proposed a straightforward
motion-based anti-spoofing technique to measure the correlationsbetween the client head movements and the backgroundscene. The main idea of the algorithm is to ignorethe direction of the movements and focus only on intensityinformation. Thus, an area-normalized sum of the framedifferenceis computed separately for both regions to formtwo signal patterns that describe the total motion within theregions. The resulting motion signals are divided into timewindows of N frames from which five quantities are extractedto form a compact motion representation. A multilayerperceptron (MLP) classifier is then used for evaluatingwhether excessive motion (hand-held attack) or no movement(fixed support photo-attack) is observed during thetime window of N frames.

3.2 Facial texture analysis

Maatta et al. [15] and Chingovska et al. [6] foundthat degradation in facial skin texture quality and disparitiesin reflectance properties can be captured by analysingfacial micro-textures using local binary patterns (LBP) [16].More specifically, uniform patterns (LBPu2) consideredwhen only the labels which contain at most two 0-1or 1-0 transitions are utilized instead of all possible LBPcodes. Like in [6, 15], we describe the facial texture propertiesby computing LBP over normalized face of 64 X 64pixels. However, we extract only the global description ofthe facial texture using LBPu2operator instead of dividingthe face into several blocks. The resulting 59-bin featurehistogram is then fed to a support vector machine (SVM)classifier that decides whether the texture description correspondsto the properties of genuine face or not.

3.3. Fusion strategies

The motion correlation analysis based technique is efficientfor measuring synchronized shaking of hand-held attackswithin the scene. However, a drawback is that it canget confused between a fixed support photo-attack and amotionless person while being recognized [1]. Moreover,the method was originally proposed for detecting photoattacks,while the assumption of decorrelated movementbetween face and background is unfortunately true also incase of video replay-attacks. On the other hand, the performanceof LBP based countermeasures is not dependenton the spoofing attack scenario if disparities in the facialtexture properties exist. More importantly, the two countermeasuresexploit independent visual cues, motion and texture,thus intuitively they should be able to provide complementaryinformation about the nature of the observed accessattempt.

The environmental conditions and possible spoofing scenariosare unpredictable in real world applications. It can beassumed that the generalization ability and stability of theindividual countermeasures could be improved by reducing the complexity of individual countermeasures. Thus,we also considered to utilize linear discriminant analysis(LDA) instead of the complex classifiers (MLP and SVM)used in the original methods to avoid overfitting and possiblyincreasing robustness in real-world applications.

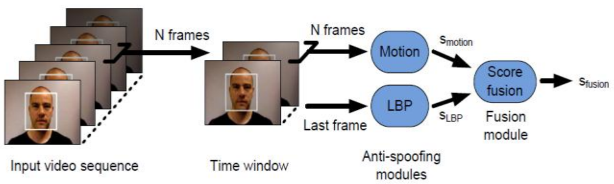

Figure2. Block diagram of the used fusion strategy.

The block diagram of the proposed fusion strategy isillustrated in Fig 2. In order to combine the motionand micro-texture analysis based techniques, the video sequencesare divided into overlapping windows of N frameswith an overlap of N-1 frames and each observation generatesan independent score of the rest of the video sequence.For the sake of simplicity, the LBP based face description iscomputed only for the last frame, whereas the five quantitiesare extracted over the whole time window for evaluating themotion correlation as in [1]. The fusion of the two visualcues is then performed at score level using linear logisticregression (LLR).

	Motion	LBP	Mutual
Devel	11.13	14.72	**2.25**
Test	12.22	12.51	**1.37**

Table1. Overall error rates (%) of time windows for individualmethods with complex classifiers (MLP for motion and SVM forLBP) compared to the percentage of mutual errors over all samples.

	Motion	LBP	Mutual
Devel	15.16	19.07	**2.27**
Test	16.89	15.69	**1.76**

Table2. Overall error rates (%) of time windows for individualmethods with LDA classifier compared to the percentage of mutualerrors over all samples.

IV. Experimental Analysis

The purpose of the experimental analysis is to first determineif the two countermeasures have fusion potential andthen see what the actual fusion performance under scenic spoofing attacks is. More importantly, the study of how the reducedcomplexity of the individual methods affects the performanceof the anti-spoofing framework.

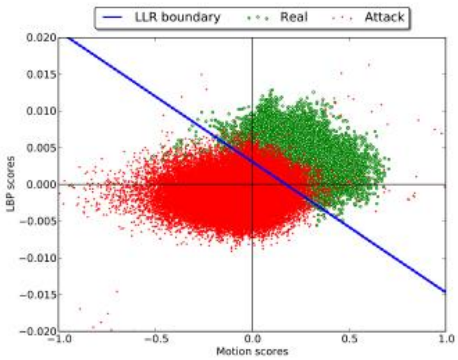

Figure3. Scatter plot of the two countermeasures with LLR decisionboundary.

V. Conclusion

The motion analysis, texture analysis, and liveness detectionare three important means to obtain the clues for detecting print based spoof attacks. The usage of one ormultiple techniques for detection appears to be a common trend. However, the usage of a single techniquealso has shown to be efficient.A possible future investigation would be to compute performance by combining two or more clues.

References

[1] A. Anjos and S. Marcel. Counter-measures to photo attacksin face recognition: a public database and a baseline. InProceedings of IAPR IEEE International Joint Conferenceon Biometrics (IJCB), Washington DC, USA, 2011.

[2] A. Anjos, L. E. Shafey, R. Wallace, M. G¨unther, C. McCool,and S. Marcel. Bob: a free signal processing and machinelearning toolbox for researchers. In 20th ACM Conference onMultimedia Systems (ACMMM), Nara, Japan. ACM Press,Oct. 2012.

[3] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi. Is physics-based livenessdetection truly possible with a single image? In IEEEInternational Symposium on Circuits and Systems (ISCAS),pages 3425–3428, 2010.

[4] W. Bao, H. Li, N. Li, and W. Jiang. A liveness detectionmethod for face recognition based on optical flow field. In2009 International Conference on Image Analysis and SignalProcessing, pages 233–236. IEEE, 2009.

[5] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, D. Muntoni,G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, F. Roli,J. Yan, D. Yi, Z. Lei, Z. Zhang, S. Z.Li, W. R. Schwartz,A. Rocha, H. Pedrini, J. Lorenzo-Navarro, M. Castrill´on-Santana, J. M¨a¨att¨a, A. Hadid, and M. Pietik¨ainen. Competitionon counter measures to 2-d facial spoofing attacks. InProceedings of IAPR IEEE International Joint Conferenceon Biometrics (IJCB), Washington DC, USA, 2011.

[6] I. Chingovska, A. Anjos, and S. Marcel. On the effectivenessof local binary patterns in face anti-spoofing. In IEEEBIOSIG 2012, Sept. 2012.

[7] M. De Marsico, M. Nappi, D. Riccio, and J.-L. Dugelay.Movingface spoofing detection via 3D projective invariants.In ICB 2012, 5th IAPR International Conference on Biometrics,29 March-1 April 2012, New Delhi, India, New Delhi,INDIA, 03 2012.

[8] R. W. Frischholz and U. Dieckmann.Bioid: A multimodalbiometric identification system. Computer, 33(2):64–68,Feb. 2000.

[9] R. W. Frischholz and A. Werner.Avoiding replay-attacksin a face recognition systenm using head-pose estimation.InProceedings of the IEEE InternationalWorkshop on Analysisand Modeling of Faces and Gestures, 2003.

[10] K. Kollreider, H. Fronthaler, and J. Bigun.Verifying livenessby multiple experts in face biometrics. In IEEE Conferenceon Computer Vision and Pattern Recognition Workshops :CVPR 2008, pages 1200–1205, 2008.

[11] K. Kollreider, H. Fronthaler, and J. Bigun.Non-intrusiveliveness detection by face images.Image and Vision Computing,27:233–244, 2009.

[12] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun.Realtimeface detection and motion analysis with application inliveness assessment. Trans. Info. For. Sec., 2(3):548–558,Sept. 2007.

[13] J. Komulainen, A. Hadid, and M. Pietik¨ainen. Face spoofingdetection using dynamic texture. In International Workshopon Computer Vision With Local Binary Pattern Variants- ACCV, 2012.

[14] J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detectionbased on the analysis of fourier spectra. In In BiometricTechnology for Human Identification, pages 296–303, 2004.

[15] J. Maatta, A. Hadid, and M. Pietikainen. Face spoofing detectionfrom single images using micro-texture analysis. InProceedings of IAPR IEEE International Joint Conferenceon Biometrics (IJCB), Washington DC, USA, 2011.

[16] T. Ojala, M. Pietik¨ainen, and T. Maenpaa.Multiresolutiongray-scale and rotation invariant texture classification withlocal binary patterns. IEEE Transactions on Pattern Analysisand Machine Intelligence, 24:971–987, July 2002.

[17] G. Pan, Z.Wu, and L. Sun. Liveness detection for face recognition.In K. Delac, M. Grgic, and M. S. Bartlett, editors,Recent Advances in Face Recognition, page Chapter 9. INTECH,2008.

[18] I. Pavlidis and P. Symosek. The imaging issue in an automaticface/disguise detection system. In Proceedings ofthe IEEE Workshop on Computer Vision Beyond the VisibleSpectrum: Methods and Applications (CVBVS 2000), pages15–, Washington, DC, USA, 2000. IEEE Computer Society.

[19] A. d. S. Pinto, H. Pedrini, W. R. Schwartz, and A. Rocha.Video-based face spoofing detection through visual rhythmanalysis. In Conference on Graphics, Patterns and Images(Sibgrapi), 2012.

[20] W. R. Schwartz, A. Rocha, and H. Pedrini.Face SpoofingDetection through Partial Least Squares and Low-Level Descriptors.In International Joint Conference on Biometrics,2011.

[21] L. Sun, W. Huang, and M. Wu. Tir/vis correlation for livenessdetection in face recognition. In Proceedings of the14th international conference on Computer analysis of imagesand patterns - Volume Part II, CAIP'11, pages 114–121,Berlin, Heidelberg, 2011. Springer-Verlag.

[22] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detectionfrom a single image with sparse low rank bilinear discriminativemodel. In Proceedings of the 11th European conferenceon Computer vision: Part VI, ECCV'10, pages 504–517, 2010.

[23] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia,M. Ristori, and F. Roli.Fusion of multiple clues forphoto-attack detection in face recognition systems.In Proceedingsof IAPR IEEE International Joint Conference onBiometrics (IJCB), Washington DC, USA, 2011.

[24] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li. Face livenessdetection by exploring multiple scenic clues. In 12th InternationalConference on Control, Automation, Robotics andVision, (ICARCV2012), 2012.

[25] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li. Face liveness detectionby learning multispectral reflectance distributions. In InternationalConference on Face and Gesture, pages 436–441,2011.

[26] G. Zhao and M. Pietik¨ainen.Dynamic texture recognitionusing local binary patterns with an application to facial expressions.IEEE Transactions on Pattern Analysis and MachineIntelligence, 29(6):915–928, 2007