Techniques of Face Spoof Detection: A Review

Ramandeep Kaur
MTech(CSE)
D.A.V Institute of
Engineering &Technology

P. S. Mann
Assistant Professor(CSE)
D.A.V. Institue of
Engineering &Technology

ABSTRACT
To automatically recognition of face is wide used in several applications like authentication of mobile payment. Automatic face recognition has raised issues concerning face spoof attacks (biometric sensor presentation attacks), in which a photograph or video of an authorized person's face will be used to gain access.There are variety of face spoof detection techniques are proposed, their generalization ability has not been adequately addressed. The intention of this paper is to review and acknowledge numerous face detection ways and to sort them into totally different classes.

Keywords
Face recognition, spoof detection, image distortion analysis and svm classifier.

1. INTRODUCTION
Automatic face recognition has attracted increasing attention in several get to regulate applications, significantly for mobile unlocking. Like fingerprint authentication, with the release of face unlocking practicality within the Android mobile operating system package, face recognition turns into another biometric identification technique for mobile phones(Touch ID) within the iOS system. Not in any respect like fingerprint authentication, face recognition doesn't need any further detector since each single advanced mobile come back equipped with a front end camera. Be that because it might, like different biometric modalities, we have to handle worries concerning face parody assaults on face recognition systems, particularly in free police investigation and uncooperative subject things[8].In spite of the very fact that a trivial task for the human brain, face recognition has turned to be greatly exhausting to imitate by artificial means, since the commonalities do exist between faces, they differ imposingly in terms age,skin,color and gender. The matter is additional wooly-minded by different image qualities, facial expressions, facial article of furniture, background and illumination conditions. The function of this step is to see [16]

1) Whether or not human faces seem n an exceedingly given image, and
2) Wherever these faces are located at.

For every person some pictures are taken and their features are extracted and can store in database. Than we have a tendency to perform face detection and have extraction, and Compare its feature to each face category stored in database. Several explore and algorithms are planned to contend with this classification downside, and we will discuss them in later sections. There are 2 general applications of face recognition, identification and verification. In Face identification, we had like the system to tell who he/she is; in face verification, given a face image and a guess of the identification, we had like the system to tell true or false regarding the guess [11]. To produce a system for recognition, we have a tendency to need data sets for building classes and compare similarities between the check information and each class. Check information is usually known as a "query" in image retrieval written works, and that we can utilize this term throughout this report. Starting from the data set facet, we have a tendency to initial perform dimension reduction on the hold on data by data-driven ways and domain knowledge ways, which can be mentioned later. Once dimension reduction, each data within the data sets is reworked (transformed) into a collection of features , and therefore the classifier is for the foremost half trained on these feature representations. At the purpose once a question comes in, we have a tendency to perform an identical dimension reduction procedure on that and enter its options into the trained classifier. The yield of the categoryifier are going to be the best class (some of the time with the classification accuracy) label or a rejection note (return to manual classification) [13].

1.1 Face Spoofing
Biometrics alludes to technologies that measure and analyze human body characteristics. Biometrics traits will be categorized into 2 categories, specifically physical characteristics, for instance, fingerprints, faces or iris patterns and activity characteristics, for instance, voice, signature or strolling patterns (step). Be that because it might, a standout amongst the foremost predominant challenges in varied biometric recognition systems is that the chance of fraud, that is fairly referred to as spoofing attack. Some purloined stolen data will be effectively exploited and mimicked by impostors to realize unauthorized access to the biometric system, while not the consent of the real user. Examine endeavors on identification of spoofing attack are created mistreatment totally different views [9]. The progressive spoofing identification technique for facial statistics in lightweight of physiological property detection is bestowed during a portion of the work. Generally, false faces will be categorized into 2 classes: positive and negative. The positive category, otherwise referred to as the real face, has restricted variation, although the negative category incorporates the spoof faces on pictures, dummy or recorded videos.

1.1.1 Methods for Face Spoofing Detection
There are completely different faces Spoof detection algorithms that shift as indicated by their strengths and limitations in terms of:

(i) Lustiness and speculation ability, and (ii) real time response and usefulness.As per differing types of cues utilized as a vicinity of face spoof detection, revealed ways are often classified into four groups:

i. motion based methods
ii. texture based methods
iii. methods based on image quality analysis, and
iv. methods based on other cues [2].

(i) Motion based methods:

These methods, planned primarily to counter printed photo attacks, catch a significant sign for vitality: the subconscious motion of organs and muscles in an exceedingly live face, for instance, eye blink, mouth development and head rotation.

(ii) Texture based methods: To counter printed photo and

Replayed video attacks, texture based mostly ways were projected to extract image artifacts in spoof face pictures. Not like motion based methods, texture based methods need simply one image to find a spoof [4].

(iii) Methods based on image quality analysis: A recent work projected a biometric physiological property detection strategy for iris, distinctive mark and face pictures utilizing 25 image quality measures, as well 21 full-reference measures and 4 non-reference measures. By quality, the projected approach intends to boost the speculation ability underneath cross-database things; that has rarely been explored within the biometric community [1].

(iv)Methods based on other cues: Face spoof countermeasures utilizing cues derived from sources aside from 2D intensity image, for instance, 3D depth, IR image, spoofing context, and voice has likewise been projected. Be that because it might, these ways impose additional needs on the user or the face recognition framework, and so have a narrower application vary.

2. THE REVIEWED APPROACHES ON FACE DETECTION

In this [3] the strategy relies exclusively on colors, significantly hue, while not requiring any geometrical parameter information. One in all the fundamental concepts is to match the intensity power differentiation of specular-free pictures and input pictures iteratively. The specular-free image may be a pseudo-code of diffuse elements which will be generated by shifting a pixel's intensity and hue nonlinearly whereas holding its hue. All processes within the methodology square measure done regionally, involving a most of solely 2 pixels. The experimental results on natural pictures show that the planned methodology is correct and robust below renowned scene illumination hue. In contrast to the prevailing ways that use one image, our methodology is effective for rough-textured objects with advanced multicolor scenes. In [5] a robust face detection technique at the side of mouth localization, process each frame real time (video rate), is bestowed. Moreover, it is exploited for motion analysis onsite to verify "liveness" moreover on accomplish lip reading of digits. A method novelty is that the instructed

quantal angle options ("quangles") being designed for illumination changelessness while not the requirement for preprocessing(e.g. histogram equalization). This can be achieved by victimization each the gradient direction and also the double angle direction (the structure tensor angle), and by ignoring the magnitude of the gradient. Boosting techniques square measure applied in a very quantal feature house. A significant profit is reduced interval (i.e., that the coaching of effective cascaded classifiers is possible in terribly short time, less than 1 h for data sets of order $10^{4)}$. Scale changelessness is enforced through the employment of a picture scale pyramid. We tend to propose "liveness" verification barriers as applications that a major quantity of computation is avoided once estimating motion. Novel ways to avert advanced spoofing makes an attempt (e.g., replayed videos that embrace person utterances) square measure incontestable. We tend to present favorable results on face detection for the YALE face check set and competitive results for the CMU-MIT frontal face check set moreover as on "liveness" verification barriers. It [6] may be a common spoof to use a photograph to fool face recognition algorithm. In light-weight of variations in optical flow fields generated by movements of two-dimensional planes and three-dimensional objects, we tend to plan a brand new aliveness detection methodology for face recognition. Below the idea that the check region may be a two-dimensional plane, we are able to acquire a reference field from the particular optical flow field knowledge. Then the degree of variations between the 2 fields may be accustomed distinguish between a three-dimensional face and a two-dimensional photograph. Empirical study shows that the the planned approach is each possible and effective. This [7] paper presents a brand new rule for nonlinear spatial property reduction (NLDR). Our rule is developed below the abstract framework of compatible mapping. Every such mapping may be a compound of a tangent space projection and a bunch of splines. Tangent space projection is calculable at every information on the manifold, through that the information purpose itself and its neighbors square measure pictured in tangent space with native coordinates. Splines square measure then made to ensure that every of the native coordinates may be mapped to its own single world coordinate with relevance the underlying manifold. Thus, the compatibility between native alignments is ensured. In such a piece setting, we tend to develop associate improvement framework supported reconstruction error analysis, which may yield a worldwide optimum. The planned rule is additionally extended to insert out of samples via spline interpolation.

In this paper [10] we tend to present multispectral Experiments on toy knowledge sets and real-world knowledge sets illustrate the validity of our methodology.

Face aliveness detection methodology that is user cooperation free. Moreover, the system is adaptation to numerous user-systems distances. Victimization the Lambertian model, we tend to analyze multispectral properties of human skin versus non-skin, and also the discriminative wavelengths square measure then chosen. Coefficient data of real and fake faces at multi-distances square measure chosen to make coaching set. Associate SVM classifier is trained to be told the multispectral distribution for a final Genuine-or-Fake classification. Compared with previous works, the planned methodology has the subsequent advantages: (a) the need on the user's cooperation is not any longer required, creating the aliveness detection user friendly and quick. (b) The system will work while not restricted distance demand from the target being analyzed. Experiments square measure conducted on real versus planar face data, and real versus mask face data. Furthermore a comparison with the visible challenge-response aliveness detection methodology is additionally given. The experimental results clearly demonstrate the prevalence of our methodology over previous systems. They [12] Identity spoofing may be a competition for high-security face-recognition applications. With the arrival of social media and globalised search, peoples face pictures and videos square measure wide-spread on the web and might be doubtless accustomed attack biometric systems while not previous user consent. Yet, analysis to counter these threats is simply on its infancy - the authors lack public customary databases, protocols to live spoofing vulnerability and baseline ways to observe these attacks.

The contributions of this work have 3-fold: 1st, the authors a in public out there PHOTO-ATTACK database with associated protocols to live the effectiveness of counter-measures is introduced. Supported the data out there, a study is conducted on current progressive spoofing detection algorithms supported motion analysis, showing they fail under the light of this new dataset. By last, the authors propose a brand new technique of countermeasure exclusively supported foreground/backgr-ound motion correlation victimization optical flow that outperforms all alternative algorithms achieving nearly excellent evaluation with associate equal error rate of 1.52% on the out there available data. The source code files resulting in the according results are formed out there for the dependableness of findings during this study.

They [14] approach a brand new face anti-spoofing approach that relies on analysis of distinction and texture characteristics of captured and recaptured pictures is planned to observe photograph spoofing. Since photograph image may be a recaptured image, it's going to show quite completely different distinction and texture characteristics compared to a true face image. In a very spoofing try, image rotation is sort of potential. Therefore, during this paper, a rotation invariant native binary pattern variance (LBPV) primarily based methodology is chosen to be used. The approach is tested on the in public out there NUAA photo-impostor database, that is built below illumination and place amendment. The results show that the approach is competitive with alternative existing ways tested on identical database. It is particularly helpful for conditions once photos square measure control by hand to spoof the system. Since associate LBPV primarily based methodology is employed, it's sturdy to illumination changes. It's non-intrusive and straightforward. They [15] planned that User authentication is a crucial step to shield information and during this field face biometry is advantageous. Face biometry is natural, simple to use and fewer human invasive. Tragically, recent work has disclosed that face biometry is at risk of spoofing attacks utilizing low-tech low-cost provides. This text presents a measure against such attacks supported the LBP-TOP operator consolidating each space and time information into one multi-resolution texture descriptor. Experiments did with the REPLAY ATTACK database demonstrate Half Total Error Rate (HTER) improvement from 15:16% to 7:60%. Remark that results with SVM classifier have to be compelled to be soft on care as a result of with the rise of the multi-resolution vary, the SVM classifier tends to over-train on the knowledge. Be that because it might, experiments with easier classifiers, as an example, LDA, incontestable that the LBP-TOP multi-resolution approach still incontestable an out of this world potential against face spoofing in numerous type of attacks things, beating the state of art results. They [17] discovered that for a robust face biometric system, a reliable anti-spoofing approach should be deployed to bypass the print and replay attacks. Many techniques are planned to counter face spoofing, but a robust answer that's computationally efficient is still unavailable. This paper presents another approach for spoofing detection in face videos utilizing motion magnification. Eulerian motion magnification approach is employed to boost the facial expressions normally exhibited by subjects in a much captured video. Next, 2 varieties of feature extraction Calculations Square measured proposed: (i) a configuration of LBP that gives improved performance compared to alternative computationally, expensive texture primarily based approaches and (ii) motion estimation approach utilizing HOOF descriptor. The HOOF descriptors noninheritable from motion enlarged videos give progressive performance on the Print Attack and Replay Attack datasets in terms of preciseness and procedure potency. On the Print Attack and Replay Attack spoofing datasets, the planned framework improves the state-of-art performance; significantly the state-of-art performance; significantly HOOF descriptor yielding a close to excellent Half Total Error Rate of 0% and 1.25% on an individual basis. They [18] propose a component-based face coding approach for aliveness detection. The planned methodology consists of 4 steps: (1) locating the elements of face; (2) writing the low-level features for all the elements ;(3) derivation the high-level faces illustration by pooling the codes with weights derived from Fisher criterion; (4) concatenating the histograms from all components into a classifier for identification. The planned framework makes sensible use of small variations between real faces and fake faces. Meanwhile, the inherent look variations among completely different elements square measure maintained. In depth experiments on 3 revealed customary databases demonstrate that the strategy can do the most effective aliveness detection performance in 3 databases. This [19] paper emphasized on face recognition, that is security-critical, has been wide deployed in our everyday life. However, ancient face recognition technologies in observe may be spoofed simply, as an example, by employing a simple printed photograph. During this paper, we tend to propose a completely unique face aliveness detection approach to counter spoofing attacks by convalescent thin 3D facial structure. Given a face video or many pictures captured from over 2 viewpoints, we tend to observe facial landmarks and choose key frames. Then, the thin 3D facial structure may be recovered from the chosen key frames. Finally, a Support Vector Machine (SVM) classifier is trained to differentiate the real and fake faces. Compared with previous works, the planned methodology has the subsequent benefits. First it offers excellent aliveness detection results that meet the safety demand office biometric system. Second it is independent on cameras or systems that work well on completely different devices. Experiments with real faces versus planar photograph faces and crooked photograph faces demonstrate the prevalence of the planned methodology over the progressive aliveness detection ways. To [20] make sure the actual presence of a true legitimate attribute in distinction to a fake self-manufactured artificial or reconstructed sample may be a vital downside in identification, which needs the event of latest and economical protection measures .During this paper, we tend to present completely unique software based fake observation methodology which will be utilized in multiple biometric systems to detect differing kinds of dishonorable access makes an attempt. The target of the planned system is to boost the safety of biometric recognition frameworks, by adding aliveness assessment in a very quick, easy, and non-intrusive manner, through the employment of image quality assessment. The planned approach presents a really low degree of quality, that makes it appropriate for period applications, victimization 25 general image quality options extracted from one image(i.e., identical noninheritable for authentication purposes) to differentiate between legitimate and cheater samples. The experimental results, obtained on in public out there knowledge sets of fingerprint, iris, and 2D face, show that the planned methodology extremely competitive

compared with alternative progressive approaches which the analysis of the final image quality of real biometric samples reveals highly valuable information which will be very expeditiously accustomed discriminate them from fake traits. They [21] discovered that Automatic face recognition is presently wide utilized in applications starting from de-duplication of identity to authentication of mobile payment. This quality of face recognition has raised issues regarding face spoof attacks

(Otherwise known as biometric sensor attacks). Wherever a

photograph or video of a certified person's face can be used to gain access to offices or services. Whereas variety of face spoofs detection techniques are planned, their speculation capability has not been adequately addressed.

We tend to propose associate economical and rather robust face spoof detection rule supported Image Distortion Analysis (IDA). Four completely different options (specular reflection, haziness, chromatic moment, and color diversity) are extracted to frame the IDA feature vector. A gathering classifier, comprising of varied SVM classifiers trained for various face spoof attacks (e.g., printed photograph and replayed video), is employed to differentiate amongst real and spoof faces. The planned approach is extended to multi-frame face spoof detection in videos utilizing a voting based scheme. We tend to collect a face spoof database, MSU Mobile Face Spoofing info (MSU MFSD), utilizing 2 mobile devices (Google Nexus five and MacBook Air) with 3 varieties of spoof attacks (printed photograph, replayed video with iPhone 5S and iPad Air). Experimental results on 2 public-domain face spoof databases (Idiap REPLAY-ATTACK and CASIA FASD), and also the MSU MFSD database demonstrate that the planned approach outperforms progressive ways in spoof detection. Our results likewise highlight the problem in separating real and spoof faces, significantly in cross-database and cross-device situations.

Table 1: Table of Comparison

Author	Year	Description	Outcomes
R.Tan [3]	2005	Color chromaticity based method	Accurate, robust
K. Kollreider [5]	2007	Motion based method	Good generalization ability
W.Bao [6]	2009	To distinguish between 2d and 3d images for face detection	Feasible, effective
N.Kose [14]	2012	To contrast between captured and recaptured images	Non intrusive and Simple
T. de Freitas Pereira [15]	2012	Texture based method	Fast response (< 1s) Low computational Complexity
J.Yang [18]	2013	Face Liveness Detection method	Best performance for liveness detection
J. Galbally [20]	2014	Image quality analysis based methods to detect fake faces	Good generalization ability,Low degree of complexity
Di Wen, Hu Han [21]	2015	Feature extraction based method	Good generalization ability Fast response (< 1s) Low computational complexity

3. CONCLUSION

In this work, it is been concluded that face spoof detection is the technique which is been applied to improve security of the bio-metric system. In the face spoof detection techniques, the technique is been applied which will detect the fake images which are given as input to take access of the data of the bio-metric system. In the paper, various techniques of spoof detection is been reviewed in terms of description and outcome.

4. REFERENCES

[1] B. E. Boser, I. M. Guyon, and V. N. Vapnik, 1992. "A training algorithm for optimal margin classifiers," in Proc. 5th ACM Workshop on Computational Learning Theory.

[2] P. Marziliano, F. Dufaux, S. Winkler and T. Ebrahimi, 2002 "A no-reference perceptual blur metric," in Proc. ICIP, vol. 3.

[3] R. Tan and K. Ikeuchi, Feb. 2005."Separating reflection components of textured surfaces using a single image". IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178–193.

[4] Y. Chen, Z. Li, M. Li, and W.-Y. Ma, 2006 "Automatic classification of photographs and graphics," in Proc. ICME .

[5] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, 2007. "Real-time face detection and motion analysis with application in "liveness" assessment," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558.

[6] W. Bao, H. Li ,N. Li, and W. Jiang,2009. "A liveness detection method for face recognition based on optical flow field," in Proc. IASP.

[7] C. Zhang, F. Nie, and S. Xiang, 2010."A general kernelization framework for learning algorithms based on kernel PCA," Neurocomputing, vol. 73,no. 4–6, pp. 959 – 967.

[8] Q. Yang, S. Wang, and N. Ahuja,2010. "Real-time specular highlight removal using bilateral filtering," in Proc. ECCV.

[9] X. Gao, T.-T. Ng, B. Qiu, and S.-F. Chang, 2010. "Single-view recaptured image detection based on physics-based features," in Proc. ICME.

[10]Z. Zhang, D. Yi, Z. Lei, and S. Z. Li ,2011."Face liveness detection by learning multispectral reflectance distributions," in Proc. pp. 436–441. FG.

[11] J.-F. Lalonde, A. A. Efros, and S. G. Narasimhan, 2011. "Estimating the natural illumination conditions from a single outdoor image," Int. J. Comput. Vision, vol. 98, no. 2, pp. 123 – 145.

[12] A. Anjos and S. Marcel 2011. "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IJCB.

[13] H. Han, S. Shan, X. Chen S. Lao, and W. Gao, 2012." Separability oriented preprocessing for illumination-insensitive face recognition," in Proc. ECCV.

[14] N. Kose and J.-l. Dugelay, 2012."Classification of captured and recaptured images to detect photograph spoofing," in Proc. ICIEV.

[15] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, 2012." LBP-TOP based countermeasure against face spoofing attacks," in Proc. ACCV Workshops.

[16] V. Christlein, C. Riess,E. Angelopoulou, G. Evangelopoulos, and I. Kakadiaris, 2013. "The impact of specular highlights on 3D-2D face recognition," in Proc. SPIE.

[17] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh,2013. "Computationally efficient face spoofing detection with motion magnification," in Proc.CVPR Workshops. IEEE Trans. Image Process. vol. 23, no. 2, pp. 710–724.

[18] J. Yang and S. Z. Li,2013. "Face Liveness Detection with Component Dependent Descriptor," in Proc. IJCB, pp. 1–6.

[19] C. Hou, F. Nie, C. Zhang, D. Yi, and Y. Wu, 2014. "Multiple rank multi-linear SVM for matrix data classification," Pattern Recognition, vol. 47, no. 1, pp. 454 – 469.

[20] J. Galbally, S. Marcel, and J. Fierrez, 2014."Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," IEEE Trans. Image Process. vol. 23, no. 2, pp. 710–724.

[21] Di Wen, Hu Han, and Anil K. Jain, 2015." Face Spoof Detection with Image Distortion Analysis", IEEE Transactions on information Forensics and Security, Vol. 4No. 3.