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

Applications of Client Identity Information for Face Antispoofing

Poonam Nemade[1], Deeksha Bhardwaj[2]

[1]ME Computer Network, G.H. Raisoni College of Engineering and Technology, Savitribi Fule Pune University
Department of Computer Engineering, Pune, India

[2]Professor, H.O.D of Computer Engineering, G.H. Raisoni College of Engineering and Technology, Savitribi Fhule Pune University
Department of Computer Engineering, Pune, India

Abstract: ***Lately, facial biometric frameworks have gotten expanded organization in different applications, for example, reconnaissance, access control and measurable examinations. On the other hand, one of the confinements of face antispoofing framework is the high probability of the framework being hoodwinked or mock by non-genuine faces, for example, photo, video clasps or sham countenances. With a specific end goal to recognize the caricaturing assaults on such biometric frameworks, face liveness discovery methodologies have been produced. Along these lines, the present methodology is to coordinate liveness recognition inside of facial biometrics by utilizing life sign markers of individual elements. This paper introduces a survey of best in class strategies in face liveness identification, which are arranged into two gatherings, to be specific meddlesome and non-nosy methodologies. Here, each strategy is talked about as far as its execution, qualities and impediments, and also signs on.***

Keywords: Biometrics, face antispoofing, meddlesome, liveness recognition, non-nosy

1. Introduction

Biometrics alludes to advancements that measure and investigate human body characteristics [1] . Biometrics attributes can be arranged into two classes, to be specific physical qualities, for example, fingerprints, confronts or iris designs furthermore, behavioral attributes, for example, voice, signature or strolling examples (walk). overwhelming challenges in numerous biometric antispoofing frameworks is the likelihood of data fraud, which is thoughtfully known as caricaturing assault [1].

Some stolen biometrics information can be effectively abused and emulated by impostors to increase unapproved access to the biometric framework, without the assent of the veritable client. Illustrations of mocking assaults on biometrics frameworks incorporate the utilization of fake fingers, contact lens with retinal examples and recorded voice. Research endeavors on distinguishing proof of satirizing assault have been produced using different points

In this article, the cutting edge satirizing recognizable proof strategies for facial biometrics in view of liveness recognition are exhibited.

By and large, fake countenances can be arranged into two classes: positive and negative. The positive class, moreover known as the honest to goodness face, has constrained variety, where as the negative class incorporates the parody faces on photos sham or recorded recordings. Figure 1 appears samples of fake confronts made of silica gel, elastic, photograph what's more, video replay [2][3].

Honest to goodness photos or shams, playing video recording and so forth before the camera. A human photo speaks to planar articles with one and only static facial expression. In any case, it does not have the three-dimensional (3D) data and gives less physiological signs than recordings. These impediments of still photos are frequently misused in liveness recognition for facial biometrics. In any case, the difficulties in facial recognition increment for satirizing assaults that include the utilization of camcorders. These days, recordings of a certifiable client with outward appearances, eye flicker and head development can be effortlessly caught utilizing top notch cameras. To the extent 3D structure is concerned, a 3D human model of a client has itemized 3D data that photographs and recordings don't have. The biometric framework can be ridiculed by utilizing a 3D physical model which is known as amalgamation assault. Sham models can for the most part repeat inflexible head development by revolution yet can't emulate the lip development, eye squint furthermore, outward appearances[3][4].

As of late, studies on the face liveness discovery have been generally investigated keeping in mind the end goal to handle the issue of caricaturing assaults. Face liveness location includes a procedure of checking whether the face picture displayed to antispoofing framework is genuine (i.e. alive) example or has been imitated artificially and is therefore false.

1.1. Facial Biometric Liveness Detection System Architecture

The essential square outline of a face liveness identification framework is appeared in Figure 1. To utilize a hostile to parodying framework, a client is required to show the pertinent biometrics attribute to the sensor, which is for this situation a camera. The caught facial pictures is preprocessed into a worthy form(e.g. for example, through standardization and clamor evacuation methods) thusly unmistakable "live" facial components can later be extricated at the element extraction module. The yield of the element extraction is a biometric layout which contains noticeable elements which

have the capacity to recognize live specimens from caricature partners. Just live examples will be handled for biometric recognizable pieces of proof, though parody validation endeavors are consequently dismisses.

1.1 a) Sensor

An assortment of procurement sensors has been considered in distinctive writing. For the most part, the same kind of sensors is utilized to give info tests into the face liveness identification framework and facial biometrics. Unmistakable light cameras are among the most usually utilized gadgets[3], as they are less expensive, speedier, higher in determination and simple to use. However, such cameras are constrained to catching just pictures that are in noticeable light range. In addition, several investigations have likewise used warm and 3D sensors for face liveness detection. Warm sensors are not restricted to just noticeable range; thus, they can catch objects in dull region. In any case, translating the pictures can be a troublesome assignment. Also, the sensors are extremely costly, obstructing modest biometrics arrangement. Then again, 3D sensors have high information obtaining rate, free of encompassing light, sub micron precision in miniaturized scale ranges. 3D sensors may be influenced by computation, measurement time, expense and quality anticipated from estimation. represents a synopsis of distinctive sorts of procurement frameworks utilized as a part of the writing for face liveness discovery[5].

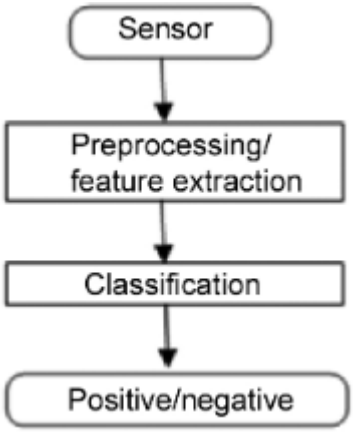

Figure 1: Block Diagram of face liveness detection system [8].

1.2. Preprocessing/Feature Extraction

Face liveness discovery frameworks may be impacted by variability in lighting, posture and picture quality. To expand the adequacy of liveness location, a few frameworks have received preprocessing. Preprocessing for the most part includes the expulsion of commotion from the picture and every so often standardization ventures with a specific end goal to upgrade the visual appearance of the facial pictures for highlight extraction. The methods may incorporate smoothing, obscuring, sharpen, edge discovery or scaling. At that point, the preprocessed tests are sent to the element extraction module to remove the remarkable components in separating live examples from satire partners.

2. Advantages

a) Face recognition is a generally utilized biometric approach.
b) Face recognition innovation has grown quickly as of late and it is more straightforward, easy to understand and helpful contrasted with different routines.

3. Disadvantages

a) Face recognition frameworks are defenseless against satire assaults made by non-genuine countenances.
b) It is a simple approach to satire face acknowledgment frameworks by facial pictures, for example, representation photos.

4. Discussion

Written works, we construed that nonintrusive methodologies, for example, surface based plans are suitable for ease liveness identification frameworks. These frameworks require no additional equipment however trade off on picture or video quality. Movement based hostile to mocking plans, which are named meddling methodology, are a decent alternative for medium-expense face liveness discovery systems. These plans are extremely successful and autonomous of surface varieties. The primary burden of such mocking strategies lies in their affectability to the brightening changes. The affectability may be repaid by utilizing excellent pictures or recordings. To expand the security level and handle the issues connected with low furthermore, medium expense hostile to caricaturing plans, the utilization of life pointers in an against parodying framework is a sufficient solution. Such frameworks require additional equipment to create astounding pictures or recordings which make such frameworks costly and equipment subordinate, however the frameworks give better execution and are extremely hard to parody.

References

[1] Wayman, J. L., Jain, A., Maltoni, D. and Maio, D., Biometric Systems Technology, Design and Performance Evaluation, Springer Science Business Media, Springer-Verlag, London, 2005.
[2] Zhang, Z., Yi, D. Lei, Z. and Li, S. Z., Face liveness detection by learning multispectral reflectance distributions. Automatic Face and Gesture Recognition and Workshop, IEEE, Santa Barbara, CA, 2011, pp. 436–441.
[3] Bai, J., Ng, T. T., Gao, X. and Shi, Y. Q., Is physics-based liveness detection truly possible with a single image? In Proceedings of the IEEE International Symposium. Circuits and Systems (ISCAS), Paris, France, 30 May–2 June 2010, pp. 3425–3428.
[4] Nixon, K. A., Aimale, V. and Rowe, R. K., Spoof Detection Schemes. Handbook of Biometrics, Springer, New York, 2008, pp. 403–423.
[5] Kollreider, K., Fronthaler, H., Faraj, M. and Bigun, J., Real time face detection and motion analysis with application in liveness assessment. Trans. Infor. Forensics and Security, IEEE, 2007, 2(part 2), 548–558.

[6] Javier Galbally1 , Sebastien Marcel2 , (Member, IEEE), And Julian Fierrez3,Biometric Antispoofing Methods: A Survey in Face Recognition, Digital Object Identifier 10.1109/ACCESS.2014. 2381273
[7] Bao, W., Li, H., Li, N. and Jiang, W., A liveness detection method for face recognition based on optical flow field. In International Conference on Image Analysis and Signal Processing IASP, IEEE, 2009, pp. 233–236.
[8] Sun, L., Huang, W. B. and Wu, M. H., TIR/VIS correlation for liveness detection in face recognition. In Computer Analysis of Images and Pattern, Springer, 2011, pp. 114–121.
[9] Hatture, S. M. and Karchi, P. R., Prevention of spoof attack in biometric system using liveness detection. Int. J. Latest Trends Eng. Technol., 2013, Special Issue-IDEAS-2013, pp. 42–49.
[10] J . Komulainen, A. Hadid, and M. Pietikainen, in *Proc."* "Context based face anti-spoofing," *IEEE 6th Int. Conf. Biometrics, Theory, Appl.,Syst. (BTAS)*, Sep./Oct. 2013, pp. 18.
[11] Kant, C. and Sharma, N., Fake face recognition using fusion of thermal imaging and skin elasticity. IJCSCIJ, 2013, 4(1), 65–72; ISSN-0973-7391
[12] Erdogmus, N. and Marcel, S., Spoofing in 2D face recognition with 3D masks and anti spoofing with Kinect. In 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS), IEEE, Arlington, VA, 2013.

Author Profile

Ms. Poonam Nemade student of ME computer network second Year from G.H .Raisoni College of Engineering and Technology Savitribai Phule Pune university .pursued B.E in Computer Engineering from Godavari College of Engineering North Maharashtra University.

Prof. Deeksha Bhardwaj received the MTech degree 2007 from Dept of Computer Science and pursuing PhD in Ad-Hoc Network. She is working as HOD in Comp Department in GHRIET, Pune. She has 8 publications in her research area. Her research interests include Networking - Ad Hoc Network.