Detection and Spoofing Methods of Face Recognition using Visualization Dynamics: A Review

Mandeep Kaur
Research scholar
Department of IT
GNDEC, Ludhiana

Hanit Karwal
Assistant Professor
Department of IT
GNDEC, Ludhiana

Kulvinder Singh Mann, PhD
Professor
Department of IT
GNDEC, Ludhiana

ABSTRACT

Biometric systems have claimed to become one of the sore subjects in the present epoch when it comes to validation or recognition of an individual. Biometric system mainly focuses on identification of traits of an individual. The foundation of face recognition, globally, is laid on a set of unique and specific recognizable or valid data. This data can be in the form of digital images or video frames. In spite of being ubiquitous, face recognition data is prone to spoofing attacks as face recognition data introduces a high probability of breach allowing a fraudulent user to masquerade as a registered user to gain illegitimate access and privileges. It has, thereby, become highly unlikely to avoid the prevention of such frauds by developing reliable and robust methods. This paper intends to review and acknowledge numerous face detection ways and to sort them into totally different classes.

Keywords

Biometrics, Face spoofing, Spoofing Attacks, 2D, Face Recognition, Detection ways, Visualization Dynamics.

1. INTRODUCTION

The biometric framework is an innovative framework that uses different traits of an individual to uniquely identify that individual [1]. In the present epoch, there is no compelling reason to carry a unique identity proof or a secret password to get to a security framework, an individual could himself be a secret key to get to a security system. It is a system for the measurement of physiological and biological characteristics of an individual. The physiological features are determined as fingerprint, face, and iris, whereas bio-logical features include voice, pattern, and speech [2]. Biometric system is related to normal biometrics such as fingerprint, iris, palm, and so forth. In past research, a mechanized system for the identification of an individual relies upon the functional and biological features which can be the tallness, complexion, or color of the eye of an individual. In current innovations, biometric structures can be finger impression, geometrical view of the hand, iris, vocal analysis and so forth [3]. The applications of the biometric systems are inclusive of identification, airport, checking, computer or mobile device log-in, building and critical infrastructure access control, digital multimedia right control, etc. The modality of biometrics is dependent on the biometrics modality applications', practically [4].

Below fig 1 described that the biometric process used in digital image processing. Fig 2 shows the types of biometrics features and traits.

Face spoofing is an effort to access rights to some other person's privileges through a photograph, moving object, or some other method [5]. Spoofing is a fake biometric used by an intruder that endeavors to access a biometric sensor. The biometric traits introduced by a live person or some other source to access some other verified client are known as spoof detection.

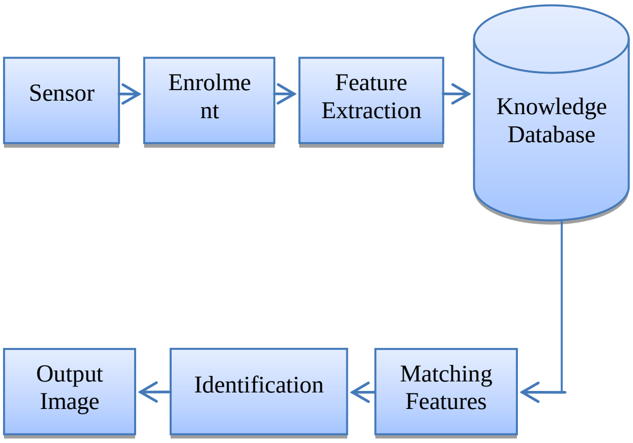

Fig. 1 Biometric System

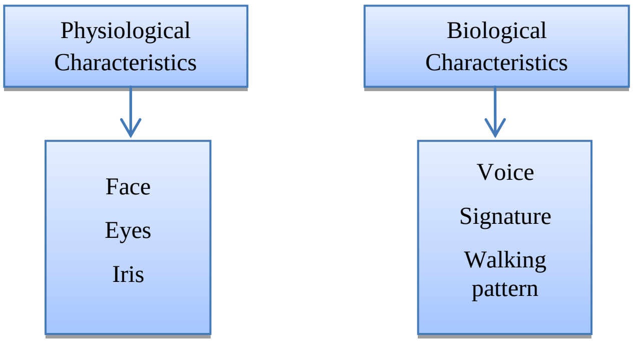

Fig. 2 Biometric characteristics

As its expanding use in dynamic and challenging zones in computer vision research, the awareness towards face recognition frameworks is begun to pay all-around cautiously. The judgment of the living from the non-live discovery has turned into an issue [6]. In spite of the fact that the face spoofing is a challenging issue, so it winds up important to develop a robust and efficient method for face spoofing detection. A spoofing attack is a method for fake endorsement wherein intruders yield a false proof to biometric scheme to achieve identification. An intruder may access the authorized person by doing some illicit activities [7].

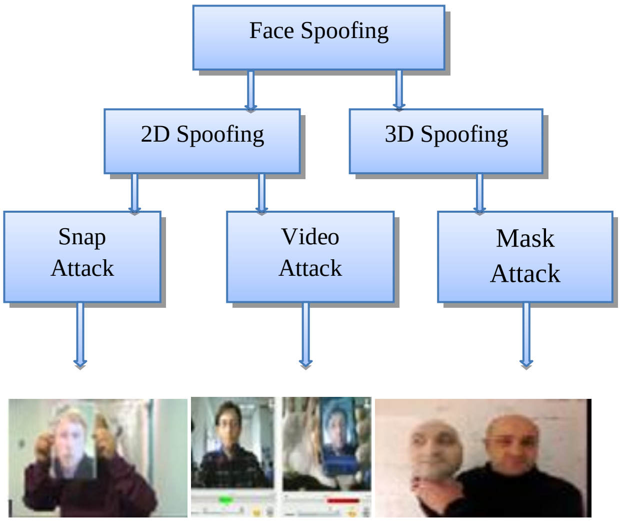

Fig. 3 Face Spoofing Detection System [15]

1.1. Photo Attack

In this method, intruder utilizes photographs of some other bona fide individual in order to gain access to a biometric framework. This type of attack is classified under 2D spoofing wherein the attackers use photos on mobile phones, tablets and laptops to access the system modality. Digital cameras are used to capture pictures by attackers or they can be hacked from social media sites such as Facebook, Instagram or Twitter [8]. Thenceforth, that photograph is imprinted on some paper to generate a photographic mask with improved resolution and quality. The attacker uses this mask in such a way that the blinking of eyes and the movement of lips can be duplicated at the season of perception of face at biometric system [9].

1.2 Mask Attack

In a three-dimensional mask attack, intruder creates a 3-D mask of the authentic person's face. These attacks are extremely hard to detect as the counter measures to be taken against the attackers using 3-D masks are difficult [10]. The attackers use the 3-D mask they make of the people from the videos or the photos which are made up of the silicon, paper or the plastic. In this kind of threat, the 3-D structure of the face is replicated utilizing its profundity signs [11]. These profundity signs are normally missed in photograph attack and video attack as they utilize just 2-D surface. In this manner, Mask attack is the propelled version of the photo attack and video attack and is hard to distinguish. But these attacks are less regulated when contrasted with photograph and video attacks. [14].

1.3 Video Attack

In this method, intruder may capture the video of the victim through digital camera, mobile phone or tablet.. Intruder replays that captured video at the time of recognition of face at biometric system to gain access to that system's modality. This method guarantees conduct and face motion of a person [12]. Because of the best possible development of the face in the replayed video, it turns out to be difficult to distinguish these sorts of attacks [13].

2. LITERATURE REVIEW

Jayan, T. J. et al., 2018[15] proposed an exploration on the quick and robust calculation for the location of the phony appearances from the pictures taken from the cameras that were likewise shared on the internet based life. The face sections are detected through various shading spaces and gauges to light up the guide of the area. Besides, the picture quality parameters of the parts and foundation areas were looked at in this paper. The element vectors were produced utilizing the picture quality parameters. In this examination, Quadratic Discriminant Analyser (QDA) classifier was utilized for the discovery of the phony pictures. **Patel, K., Han, H and Jain, A. K. et al., 2016[16**] tended to the issue of the face spoofing acknowledgment, in contrast, to picture and moving item based on the perils, picture claimers, design acknowledgment. They built up the satire assault dataset that comprises more than 1000 classes. Distributed and reiteration risk was discovered utilizing far and closer cameras. They analyzed the deriving of the uproar and risks utilizing quality models which are RGB and dark scale picture, a region of the face, spellbinding highlights. They built up a solid parody investigator plan utilizing machine gadgets. The trial approach was made on the dataset, for example, CASIA and MSU-MFSD dataset through which farce recognition was reliable for test approaches. **Fourati, E. et al., 2017[17]** shows the counter ridiculing answer for the picture quality appraisal to separate the genuine and the phony pictures. The picture quality appraisal was dependent on the extraction of the edges and low intricacy classifiers. The picture quality countermeasures are the face of satirizing assaults. In this exploration, the first spotlight on the face mocking assaults utilizing photographs, recordings, and 3d veils pictures. The liveness face was identified using the introduction assault location dependent on the picture quality evaluation. **Li, H., Wang, et al., 2016[18**] proposed an examination on the picture quality relapse system to beat the issues of face parodying location. Initially, the groups of the equivalent (camera model component) and diverse quality classifiers based were extricated through the picture quality appraisal. The relapse capacity maps from the highlights of the picture quality appraisal. The order was finished utilizing the classifiers, and the expectation was accomplished for the check of the face. In this examination, the investigations were completed using single class classifiers. **Galbally, J et al., 2014[19]** displayed a novel methodology face discovery strategy and different misrepresentation endeavors utilized in multi-biometric frameworks. The primary objective of this exploration was to build the security of the biometric structure by including the liveness picture evaluation. The principle issues might be assaulted or the blunder measurements because of the confound of the pictures. The continuous applications utilize the 25 general pictures, highlights for the extraction of a picture and contrasting that and different examples. In this examination, the exploratory outcomes are thought about utilizing condition of a quality approach and genuine quality biometric frameworks. In this exploration, programming based was used for the discovery of the misrepresentation endeavors to pictures and different sorts of the assaults. **De Marsico. et. al., 2012[20]** proposed an exploration on the identification of the charges and a sufficient answer for issues of face satirizing. Face confirmation was powerless methodology in the parodying assaults. Subsequently, a method was executed by joining 3D verification. The discovery of the complex parodying record was dependent on the recorded recordings. In this examination, Analyses shows viability and productivity location of caricaturing using a 3D moving facial veil.

3. DETECTION METHODS IN FACE SPOOFING

3.1 Techniques for detection of face spoofing

Anti-spoofing method is an approach to differentiate between veritable client's biometric attribute and phony biometric attribute delivered artificially. The detection of face spoofing is done through various techniques which are described as:-

3.1.1 Movement-based technique

In this technique, the pattern of the movement of the external parts of the lively face such as blinking of the eyes, movement of mouth and motion of the head is determined. This method fundamentally depends upon the supposition that the movement of 2D objects for example planer items is entirely unexpected from the development of 3D objects for example genuine human appearances. Movement based anti-spoofing technique thus made the spoofing by 2D images exceptionally hard to continue [21]. Movement based anti-spoofing procedure at times hard to use as it requires a video of the veritable client. But, the client's conduct may now and again shift from one to other; at that point it might give false rejection to a veritable user. The movement analysis relies on the optical stream which is determined from video groupings.

3.1.2 Texture-based technique

This method deals with the premise of surface highlights like shape and details of the face to recognize spoof from two-dimensional pictures. In this technique, there is extraction of the artifacts from 2D images to detect spoof from that image. It is supposed that there is considerable difference in the texture features developed by the real face and texture features generated by a face printed on paper. Texture based technique also helps in the differentiation of the face of a person in life from the face printed on paper two-dimensionally. These strategies have been utilized for both face confinement and location. Different techniques like Local Binary Pattern and power spectrum are used for the extraction of texture and frequency information of a face. Local Binary Pattern calculates the relative intensity difference of the pixel from center and pixels in its neighborhood where neighboring pixels are at the same distance from the center pixel. A 2-D Discrete Fourier Transform is used to convert the facial image into the frequency domain to extract the frequency information. A one dimensional feature vector is calculated by summing up by frequency bands [22].

3.1.3 Life Sign Detection Based Analysis

The detection of life sign depends on two different ways. One requires user interaction whereas other one not. In the first, one needs to perform some tasks to demonstrate its face aliveness to gain authentication to the system. In the later, movements of the facial parts play an important role instead of requirement to interact with the user. Lip movements and eye blinking are considered as life sign indicators in the second type. The primary advantage of life sign detection technique is that it is free of texture analysis. The only hindrance it has, it requires user interaction. By utilizing this method, it will be difficult to spoof with 2D or 3d photographic masks [23].

3.1.4 Optical flow based technique

In this technique, the summation of basic movement types to generate optical flow, are considered as rotation movement, translation movement, moving movement and swing movement for the analysis. These optical flow properties are generated by 2D and 3D objects. The first three movement properties fall under one category that generate same kind of optical flow fields for 2D images and 3D images as well. Whereas swing movement falls under a different category which produces different optical flow fields from 2D images and 3D images as compared to the optical flow fields generated by first three properties. A reference field can be acquired from the optical stream field where a 2D plane image is used as a test image [23]. Then the differentiation of 3-D face from 2-D image is done on the basis of distinction between both the fields. It percepts that the focus on the central parts of the face is more than the outer parts of the face when it comes to generate 2-D motion through a 3-D face. As the central parts of the face are more close to the camera, it moves in a different way when compare to outer parts of the face which are not much closer to the camera. Thus the information about the position of the face parts and their velocities during motion are used to contrast their relationship and one another. This data helps in separating a 3-D live face from a 2-D phony face picture [24].

3.1.5 Geometrical based technique

In this method, the general information of the face is acquired to recognize the symmetrical location boundary, shape and pattern of the face. Face consists of the various organ parts of the body which are eyebrows, nose, eyes, and mouth in symmetrical face picture in different sections, an upper and lower portion of the eye, leftward and sideward of nose [25].

3.2 Detection of Face Spoofing Using Visualization Dynamics

Face spoofing is an effective approach to deceive a face recognition mechanism through 2D and 3D spoof attacks. The detection of these attacks can be possible by using different visualization dynamics methods. The methods are described in three steps:-

3.2.1 Dynamic Mode Disintegration

3.2.2 Creation of the LBP Histogram

3.2.3 Organization using SVM classifier

3.2.1 Dynamic Mode Disintegration

In this approach, a video frame is used as an input for the generation of set of frames, on which Dynamic mode Disintegration (DMD) is done. Eigen values are then calculated from the generated set of frames to create dynamic modes. A unique dynamic mode image having angle equal to zero or nearest to it, is selected. Dynamic mode Disintegration (DMD) can extricate the effective facial highlights and in this manner security of the biometric framework can be successfully and efficiently taken care of.

3.2.2 Creation of the LBP Histogram

The local binary pattern leads to a representation of the picture pattern in an exact manner. The histogram is built that corresponds to the dynamic mode whose stage point is zero or the nearest value. The division of the acquired dynamic approach is segmented into various groups. Histograms are built for every group. Each histogram is evaluated and by connecting the highlights, a feature histogram is generated that corresponds to the unique dynamic mode [26].

3.2.3 Classification using SVM Classifier

The support vector machine has dual classification leading to segmentation of actual and spoofed moving objects. The classifier is reliant on the threshold variable group in the scheme. The displacement of the data from the support vector machine is calculated, and if the output is positive, the required video is determined. However, if the result is negative, then output is a spoofed image. Following figure demonstrates the spoof recognition through Dynamic Mode Visualization.

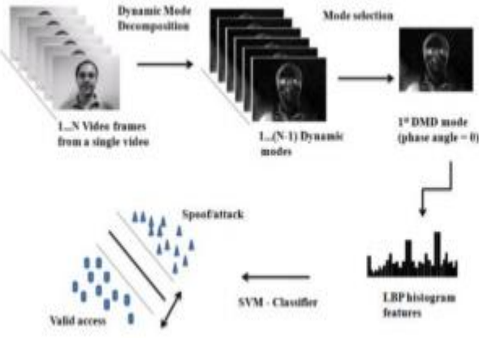

Fig 4. Spoof recognition using Dynamic Mode Visualization [26]

4. CONCLUSION AND FUTURE SCOPE

It is inferred from the investigation that the prominence of the biometric system is expanding on account of its ease to use as it is easy to understand. But the major issue in utilizing these biometric frameworks serenely is that it is highly prone to the spoofing attacks. In the face recognition system, vulnerabilities to face spoof attacks create a significant impact on the systems [3]. However, the recognition of face spoofing is still a challenging issue due to the problems in the judgment of the discriminative and computationally inexpensive features. It is necessary to develop a robust and efficient method which can detect the spoofing in a well-generalized manner with specific imaging conditions. In this paper, various spoofing attacks and numerous anti-spoofing techniques are reviewed and acknowledged. Researchers described various categories of detection of face spoofing. On the other hand, Dynamic Mode Disintegration, Creation of the LBP Histogram Organization using SVM classifier is used for recognition of spoofed videos and validated videos. It is concluded that this method can extricate liveness attributes as well as spoofing artifacts at the same time. Dynamic Mode Disintegration hence prompts giving better execution, better security and better accuracy of the system. As a future work, one can implement the typing pattern of an individual and voice recognition in a biometric system for superior security and authentication. In this way, detection of spoofed and real speaker can be analyzed by checking their voice characteristics.

5. REFERENCES

[1] Gressel, C. D. (2001). *U.S. Patent No. 6,311,272*. Washington, DC: U.S. Patent and Trademark Office.

[2] Negin, M., Chmielewski, T. A., Salganicoff, M., Von Seelen, U. M., Venetainer, P. L., and Zhang, G. G. (2000). An iris biometric system for public and personal use. *Computer*, vol *33*(2), pp. 70-75.

[3] Gamboa, H., and Fred, A. (2004, August). A behavioral biometric system based on human-computer interaction. In *Biometric Technology for Human Identification* (Vol. 5404, pp. 381-393). International Society for Optics and Photonics.

[4] Lee, J. C. (2012). A novel biometric system based on palm vein image. *Pattern Recognition Letters*, vol *33*(12),pp. 1520-1528.

[5] Määttä, J., Hadid, A., and Pietikäinen, M. (2011, October). Face spoofing detection from single images using micro-texture analysis. In *2011 international joint conference on Biometrics (IJCB)* (pp. 1-7). IEEE.

[6] Erdogmus, N., and Marcel, S. (2013, September). Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. In *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)* (pp. 1-6). IEEE.

[7] Boulkenafet, Z., Komulainen, J., and Hadid, A. (2016). Face spoofing detection using colour texture analysis. *IEEE Transactions on Information Forensics and Security*, vol *11*(8), pp. 1818-1830.

[8] De Marsico, M., Nappi, M., Riccio, D., and Dugelay, J. L. (2012, March). Moving face spoofing detection via 3D projective invariants. In *2012 5th IAPR International Conference on Biometrics (ICB)* (pp. 73-78). IEEE.

[9] Chingovska, I., Anjos, A., and Marcel, S. (2012, September). On the effectiveness of local binary patterns in face anti-spoofing. In *2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG)* (pp. 1-7). IEEE.

[10] Komulainen, J., Hadid, A., Pietikäinen, M., Anjos, A., and Marcel, S. (2013, June). Complementary countermeasures for detecting scenic face spoofing attacks. In *2013 International conference on biometrics (ICB)* (pp. 1-7). IEEE.

[11] Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., and Li, S. Z. (2012, March). A face antispoofing database with diverse attacks. In *2012 5th IAPR international conference on Biometrics (ICB)* (pp. 26-31). IEEE.

[12] De Freitas Pereira, T., Anjos, A., De Martino, J. M., and Marcel, S. (2012, November). LBP− TOP based countermeasure against face spoofing attacks. In *Asian Conference on Computer Vision* (pp. 121-132). Springer, Berlin, Heidelberg.

[13] Lu, Y., Zhou, J., and Yu, S. (2012). A survey of face detection, extraction and recognition. *Computing and informatics*, vol *22*(2), pp. 163-195.

[14] Manjani, I., Tariyal, S., Vatsa, M., Singh, R., and Majumdar, A. (2017). Detecting silicone mask-based presentation attack via deep dictionary learning. *IEEE Transactions on Information Forensics and Security*, vol *12*(7), pp. 1713-1723.

[15] Jayan, T. J., and Aneesh, R. P. (2018, July). Image Quality Measures Based Face Spoofing Detection Algorithm for Online Social Media. In *2018 International CET Conference on Control, Communication, and Computing (IC4)* (pp. 245-249). IEEE.

[16] Patel, K., Han, H., and Jain, A. K. (2016). Secure face unlock: Spoof detection on smartphones. *IEEE Transactions on Information Forensics and Security*, vol

11(10), pp. 2268-2283.

[17] Fourati, E., Elloumi, W., and Chetouani, A. (2017, August). Face anti-spoofing with image quality assessment. In *2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART)* (pp. 1-4). IEEE.

[18] Li, H., Wang, S., and Kot, A. C. (2016, December). Face spoofing detection with image quality regression. In *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)* (pp. 1-6). IEEE.

[19] Galbally, J., Marcel, S., and Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE transactions on image processing*, vol *23*(2), pp. 710-724.

[20] De Marsico, M., Nappi, M., Riccio, D., and Dugelay, J. L. (2012, March). Moving face spoofing detection via 3D projective invariants. In *2012 5th IAPR International Conference on Biometrics (ICB)* (pp. 73-78). IEEE.

[21] Boulkenafet, Z., Komulainen, J., and Hadid, A. (2016). Face spoofing detection using colour texture analysis. *IEEE Transactions on Information Forensics and Security*, vol *11*(8), pp. 1818-1830.

[22] Ramachandran, V., and Nandi, S. (2005, December). Detecting ARP spoofing: An active technique. In *International Conference on Information Systems Security* (pp. 239-250). Springer, Berlin, Heidelberg.

[23] Bao, W., Li, H., Li, N. and Jaing, W. (2009). A liveness detection method for face recognition based on optical flow field. *International Conference on Image Analysis and Signal Processing*, pp. 233-236. IEEE.

[24] Chakraborty, S., and Das, D. (2014). An overview of face liveness detection. *arXiv preprint arXiv:1405.2227*.

[25] Wen, D., Han, H., and Jain, A. K. (2016). Face spoof detection with image distortion analysis. *IEEE Transactions on Information Forensics and Security*, vol *10*(4), pp. 746-761.

[26] VS, S. and Linda, M. A Survey on Facial Spoofing Detection. *International Journal of Science and Technology Research,* vol 5(1), pp. 49-53.