|| Volume 6 || Issue 3 || March 2021 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

FACE BIOMETRIC ANTI-SPOOFING

Ratnadeep Tayade[1], Pratiksha Kamble[2], Santosh Meshram[3], Pooja Choudhari[4], Akansha Rajgure[5]

Department of Electronics And Telecommunication, JDIET, Yavatmal[1,2,3,4,5]

[1] ratna726728@gmail.com [2]pkamble.ytl123@gmail.com [3]meshramdadu494@gmail.com
[4]Choudharipooja24@gmail.com[5]rajgureakansha@gmail.com

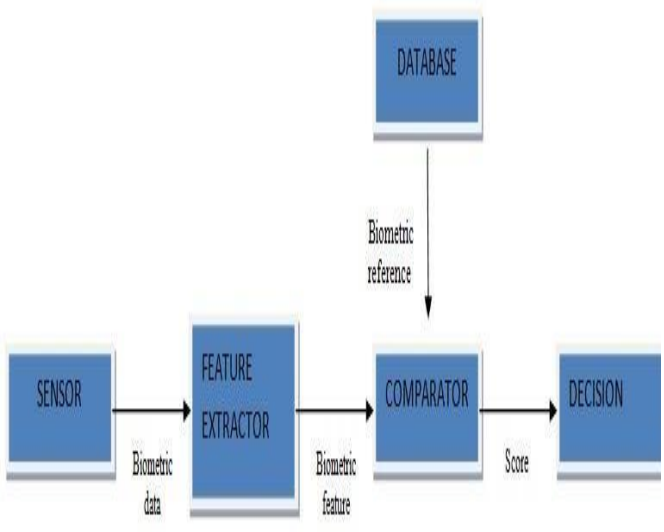
Abstract: - recent decades, we've witnessed the evolution of biometric technology from the primary pioneering works in face and voice recognition to the present state of development wherein a good spectrum of highly accurate systems could also be found, starting from largely deployed modalities, like fingerprint, face, or iris, to more marginal ones, like signature or hand. This path of technological evolution has Naturally led to a critical issue that has only began to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, especially, to spoofing. Spoofing, mentioned by the term presentation attack in current standards, may be a purely biometric vulnerability that's not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor. The entire biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient protection methods against this threat. The goal of this paper is to supply a comprehensive overview on the work that has been administered over the last decade within the emerging field of anti- spoofing, with special attention to the mature and largely deployed face modality. The work covers theories, methodologies, state-of-the-art techniques, and evaluation databases and also aims at providing an outlook into the longer term of this very active field of research.

Keywords- *Biometric, Vulnerability, Attacks, Counter measures, Eigen face Algorithm, Spoofing, Raspberry pi, OpenCV, Python.*

I.INTRODUCTION

Biometrics is that the specialized term for body estimations and counts. It alludes to measurements identified with human attributes. Biometrics validation (or sensible confirmation) is utilized as a part of software engineering as type of recognizable proof and access control. Biometric verification is any method by which a person are often interestingly recognized by assessing a minimum of one recognizing organic attributes. Fig.1 shows the overall diagram for a biometric system. Interesting identifiers incorporate fingerprints, hand geometry, ear cartilage geometry, retina and iris designs, voice waves, DNA, and face. The most established sort of biometric confirmation is fingerprinting. Biometric check has progressed extensively with the looks of modernized databases and therefore the digitization of straightforward information, considering relatively momentary individual distinguishing proof. Iris and retina-design validation techniques are, as of now utilized in some bank programmed teller machines. Voice waveform acknowledgment, a strategy for confirmation that has been utilized for a long time with tape accounts in phone wiretaps, is presently being utilized for access to exclusive databanks in look into offices. Facial recognition innovation has been utilized by law implementation to choose people in vast group with extensive unwavering quality. Hand geometry is being utilized as a part of industry to give physical access to structures. Ear cartilage geometry has been utilized to invalidate the personality of individuals who claim to be somebody else (wholesale fraud). Signature correlation isn't as dependable, independent from anyone else, as the other biometric confirmation techniques however offer an additional layer of check when utilized as a part of conjunction with at least one different strategy(1). This paper is concentrated on face biometrics, the varied spoofing and anti spoofing methods.

Face biometrics is that the second largest biometric used, with fingerprint being the primary . Hence, it is more open to spoofing attacks or direct (presentation) attacks in which intruders use synthetically produced artefact try to mimic the behavior of genuine users, to fraudulently gain access to the biometric system. Certain countermeasures need to be implemented within the sort of anti spoofing methods so as to form.



biometric verification safer. An anti-spoofing technique is normally acknowledged to be any procedure, which can consequently recognize genuine biometric attributes displayed to the sensor from fake biometric characteristic.

II.BIOMETRIC SPOOFING

In spite of some ongoing efforts and proposals to reach a unifed and standardized nomenclature for vulnerability related concepts, the biometric community has still not reached a general agreement on the best terminology to be used in each case. In light of the absence of a closed definition, this article will follow the specialised literature where biometric spoofing is widely understood because the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting to the sensor a synthetic forged version (i.e., artefact) of the original biometric trait. Such attacks, also referred to in some cases as direct attacks fall within the larger category `presentation attacks", defined in the latest draft of the ISO/IEC 30107 standard as ``presentation of an artefact or human characteristic to the biometric capture subsystem during a fashion that would interfere with the intended policy of the biometric system". Such a wider group of attacks also includes the presentation to the acquisition device of human characteristics (and not only synthetic artefacts) like dead fingers, mutilated traits, real living traits under coercion or a different living trait (i.e., zero-effort impostor attempts that try to take advantage of the False Acceptance Rate, FAR, of biometric systems).

Therefore, spoofing consists in using an artificial trait to impersonate a different user or to create a new genuine identity. Several scenarios are typically conceived for spoofing attacks counting on the sort of biometric system considered. (i) Verification system: within the commonest case, spoofing is administered at the time of authentication by presenting to the sensor a fake physical copy of the genuine's user trait. Such artefact is acquired and matched to the enrolled real template of the genuine user.

(ii) Verification system/Identification system in closed set: Spoofing may also be performed at the enrolment stage by generating a new identity with an artifact (not necessarily imitating any real user's trait) which may later be employed by different users to access the system. (iii)Identification system in open set: Typically this case corresponds to look-up systems where a new identity is created using the spoofing artefact to avoid being found in a watch list (e.g., to get a VISA for illegally entering a country).

III .THREE TYPES OF SPOOFING ATTACKS

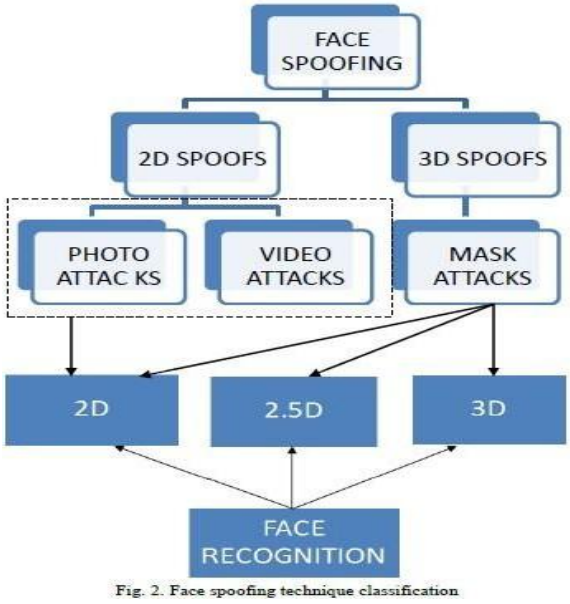


Fig. 2. Face spoofing technique classification

1.Photo Attack

The photograph of a real user could also be taken by the attacker employing a camera , or maybe retrieved from the web [3]. Another sort of photo-attack is that the use of photographic masks. These are high resolution printed photographs where eyes and mouth are cut out Liveness detection are often bypassed as certain facial movements like blinking of the attention are reproduced. The image can then be printed on a paper (i.e., print attacks, which were the primary to be systematically studied within the literature) or could also be displayed on the screen of a digital device like a mobile or a tablet (i.e., digital- photo attacks). a rather more advanced sort of photo-attack that has also been studied is that the

2.Video Attacks

Also referred to as replay attacks, may be a sophisticated version of the straightforward photo spoofs. during this case, the attacker doesn't use a still image, but replays a video of the real client employing a digital device (e.g. mobile , tablet or laptop) [4], [5].

during this case, the attacker doesn't use a still image, but replays a video of the real client employing a digital device (e.g., mobile , tablet or laptop). Such attacks appeared as an extra step within the evolution of face spoofing and are harder to detect, as not only the face 2D texture is copied but also its dynamics.

3.Mask Attacks

The spoofing artefact may be a 3D mask of the real client's face, which makes it difficult to detect impostors. Although, the likelihood to bypass a biometric system wearing a mask imitating the face of a special user is a thought that has been circulating for a few time [6]. These attacks are far less common than the previous two categories thanks to increase in cost to breed the artefact.

IV.ANTI SPOOFING TECHNIQUES:

Luckly, there are some counter-measures for these spoofing techniques. Using these techniques we can protect the information.

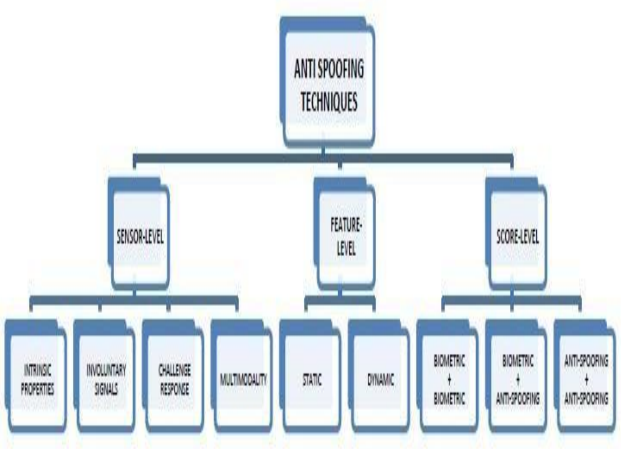


Fig.3. Anti Spoofing Techniques

1.Sensor-Level Techniques

Otherwise mentioned as hardware-based techniques where a selected device is integrated within the biometric sensor which helps to detect specific properties of a living trait It measures one among three characteristics. Namely: Involuntary signals of a living body eg. vital sign , perspiration, electric heart signals. Intrinsic properties of a living body - which could include properties like physical, electrical, spectral or visual properties.

Responses to external stimuli, also mentioned as challenge-response methods, which needs the cooperation from the user as these responses are supported detecting voluntary (behavioral) or involuntary (reflex reactions) to an external signal. Eg.When light is switched on the pupil contracts (reflex), or the top moves following a random path determined by the system (behavioral). Multi-biometric anti spoofing is predicated on the idea that the blending of varied biometrics will decrease the vulnerability to assaults, as in theory , producing multiple fake characteristics is harder than generating a private fake characteristic. supported this assumption, multimodal approaches fuse different modalities.

The strategy is using complementary traits for eg. Finger print and finger veins, this strategy requires additional hardware devices, therefore, these techniques could also be included within

multibiometric system has already been shown to be untrue as, in many cases, bypassing only one of the unimodal subsystems is enough to realize access to the entire application. Hence, multibiometry by itself doesn't necessarily guarantee a better level of protection against spoofing attacks.

i.Sensor Level Interfacing

Sensor Level Interfacing is nothing but, Connection between sensor to Controller or processor. So in this type of Interfacing we use a pi cam module. Pi cam module is one of the best and precise module and we interface Raspberry Pi as a processor to direct Pi cam module.

Connection of Raspberry Pi processor and Pi cam module is easy, there is a slot for Pi cam module to interface with the Raspberry Pi

Processor. After connecting the processor we have to train the processor to detect authorized person using Pi cam module. For to do so, we write some couple of lines of code. Here we use python language to Train our processor. By using OpenCV module we are able to capture images. Now we capture some images of authorized person and store in a particular folder, in this folder we capture various face expression, angles of face, simple face images. We train processor in that way of, the newly captured image is get compared with already captured image, if the captured image is 75% same to stored image then it is authorized person.

2.Feature-Level Techniques

Otherwise mentioned as software-based techniques, here, the biometric data is acquired with a typical sensor and therefore

the distinction between fake and real faces is software based. Under Software based techniques there are two methods for anti spoofing - static and dynamic. Static features may present some degradation in performance but remains preferred over dynamic techniques because it's faster and fewer intrusive as they require less cooperation from the user. Static anti spoofing methods work on single images while dynamic anti spoofing methods work on video sequence. In feature level technique, multimodality are often implemented. From only one single high resolution image of a face, both face and iris recognition are often performed.

It not only detects spoofing attacks but it is also capable of detecting other sorts of illegal break- in attempts. For eg. Feature level techniques protects the system against the injection of reconstructed or synthetic samples (9). the benefits of Feature-level dynamic are it's high accuracy level. It exploits spatial and temporal features during a video sequence. it's known to be very effective against photo attacks. The

disadvantages are - can't be utilized in single image scenario instances. it's comparably slow. Accuracy is lost against video attacks. the benefits of Feature-level static are - It can't only be used with a video sequence but can also be used for single images. Faster in comparison to Feature level dynamic technique. it's totally transparent to the user. The disadvantages are-It is predicated only on image spatial information which reduces the accuracy.

i.Eigen Face Algorithm

Principal component analysis transforms a group of knowledge obtained from possibly correlated variables into a group of values of uncorrelated variables called principal components. the amount of components are often but or adequate to the amount of original variables. the primary principal component has the very best possible variance, and every of the succeeding component has the very best possible variance under the restriction that it's to be orthogonal to the previous component. we would like to seek out the principal components, during this case eigen vectors of the covariance matrix of facial images.

The first thing we'd like to try to to is to make a training data set. 2D image Ii are often represented as a 1D vector by concatenating rows [2]. Image is transformed into a vector of length N = mn.

$$I = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ . & . & . & \\ . & . & . & \\ . & . & . & \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix}_{mn} = x$$

Let M such vectors xi (i = 1, 2, ..., M) of length N form a matrix of learning images, X. to make sure that the primary principal component describes the direction of maximum variance, it's necessary to center the matrix. First we determine the vector of mean values Ψ, then subtract that vector from each image vector.

$\Psi = \Sigma x$, (1)

$\varphi = x - \Psi$. (2)

Averaged vectors are arranged to make a replacement training matrix (size N×M);

$M = (\varphi 1, \varphi 2, \dots \varphi M)$.

The next step is to calculate the covariance matrix C, and find its eigenvectors ei and eigenvalues λi.

Covariance matrix C has dimensions N×N. From that we get N egeinvalues and eigenvectors. For a picture size of 128×128, we might need to calculate the matrix of dimensions 16.384×16.384 and find 16.384 eigenvectors. it's not very effective since we don't need most of those vectors. Rank of covariance matrix is restricted by the amount of images in learning set — if we've M images, we'll have M–1 eigenvectors like non-zero eigenvalues. one among the theorems in algebra states that the eigenvectors ei and eigenvalues λi are often obtained by finding eigenvectors and eigenvalues of matrix C1 = ATA (dimensions M×M) [3]. If νi and μi are eigenvectors and eigenvalues of matrix ATA.

3.Score level techniques

It is the foremost recently introduced anti spoofing technique. This method focuses on the study of bio system of weights and measures at score level so as to propose fusion strategies that increase their resistance against spoofing attempts. they're often considered as a supplementary to sensor level and have level techniques thanks to their limited performance. The scores to be combined may come from a)two or more unimodal biometric modules

b)unimodal biometric modules and anti - spoofing techniques, or c)only results from anti- spoofing modules. the benefits of Sensor-level are it's highly acurate against all kinds of spoofing attacks like photo, video and mask.

The disadvantages are - it's generally slower. Higher level of cooperation is required from the user. it's expensive thanks to the extra hardware that's required to process the biometric traits. The diagram Fig.4. Shown below specifies the modules utilized in biometric system that's the Sensor level, Feature level and Score level. It not only shows the protection offered against spoofing attacks but also shows the protection offered against attacks administered with synthetic or reconstructed samples.

V.CONCLUSION

within the anti spoofing techniques, the sensor level presents a better fake detection rate, whilst feature level techniques are less costly , less intrusive and more user friendly, since their implementation is hidden from the user. The score level protection technique presents a way lower performance in comparison to the sensor level and has level protection measures. Hence, they're designed only as a support to the sensor level and have level techniques. Although significant amount of labour has been administered within the field of biometric anti- spoofing. the extent of hacking methodologies have also evolved becoming more sophisticated. As a result, there are still improvements to be made to the present anti spoofing techniques which will challenge the evolving direct attacks so as to form the system safer .

REFERENCES

[1] Javier Galbally, Ssebastien Marcel, (Member, IEEE). and Julian Flerrez.-Biometric Anti-spoofing Methods: A Survey inFace Recognition'.

[2]A. Dantcheva, C. Chen, and A. Ross, "Can facial cosmetics affect the matching accuracy of face recognition systems?" in Proc. IEEE 5th Int. Conf. Biometrics, Theory, Appl. Syst (BTAS), Sep. 2013, pp. 391-398.

[3] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng. "Understanding OSN-based facial disclosure against face authentication systems," in Proc. ACM Asia Symp. Inf., Comput. Commun. Security (ASIACCS), 2014. pp. 413-424.

[4]1. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE int. Conf. Biometrics interest Group (BIOSIG), Sep. 2012. pp. 1-7. [5]Z. Zhang. J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face anti-spoofing database with diverse attacks," in Proc. IAPR Int. Conf. Biometrics (ICB), Mar JApr. 2012. pp. 26-31.

[5]Biometric Antispoofing Methods: A Survey in Face Recognition JAVIER GALBALLY1, SÉBASTIEN MARCEL2, (Member, IEEE), AND JULIAN FIERREZ31Joint Research Centre of the ecu Commission, Institute for the Protection and Security of the Citizen, Ispra 21027, Italy.

[6]SERBIAN JOURNAL OF EE Vol. 9, No. 1, February 2012, 121-130 Face Recognition Using Eigenface Approach* Marijeta Slavković, Dubravka Jevtić