ISSN:0975-9646

Identify Fake and Real User Face by using Client Information for Face Antispoofing

Poonam Nemade[#1] Rekha jadhav[*2]

[1]*M.E Computer Network*
[2]*Professor, H.O.D, Dept. of Comp. Engg*
G.H. Raisoni College of Engineering and Technology, Savitribi Fule pune university
Department of Computer engineering, Pune University
Pune, India

***Abstract*— Client identity checking is a key to secure data, face biometrics is perhaps ideal. Character administration utilizing biometrics has these days turned into a reality primarily due to the biometric travel papers (e-identifications) furthermore due to the vicinity of more biometric empowered applications for PCs. Then again, though the important advancement in the late decades, biometric frameworks are, undesirably, helpless against attacks. A spoofing attack happens when a man tries to take on the appearance of another person by distorting information and along these lines increasing illegitimate get to and focal points. This is at present a major issue for organizations willing to market data security arrangements in view of biometric verification advancements. In this manner, there is a critical requirement for effective and dependable answers for identifying and bypassing spoofing attacks. The regular countermeasure to a spoofing attack is liveness recognition that goes for recognizing some physiological indications of life. That's why the anti-spoofing systems are designed as binary classifiers whose task is to differentiate between real access and spoofing attack samples, without any respect to the client identity. Presently we will concentrate on measure of client particular data and how it influences the execution of antispoofing frameworks. We make utilization of this data to construct two client particular antispoofing arrangements, one depending on a generative and another on a discriminative paradigm.**

Keywords— Biometrics,face antispoofing, liveness recognition

INTRODUCTION

The wide organization of biometric recognition system in the recent years has been frustrated by the discovery of their vulnerability to spoofing attacks :attempts to access the system by displaying a duplicate of the biometric quality of a client. Use of liveness recognition and antispoofing algorithms for many biometric modes. Some of them use a particular hardware device guaranteeing the presence of a living individual in front of the system. Others combine various modalities, assuming this expands the difficulty in spoofing system[4].a client claims an identity and the system utilizes this data to coordinate the information test against a stored model. In a recognizable proof situation, the info test is coordinated against a few stored model whose identities are known. Anti-spoofing system now and again makes usage of this information. More often than not, the anti-spoofing systems are planned as binary classifiers whose undertaking is to segregate between real faces and spoofing attack faces.

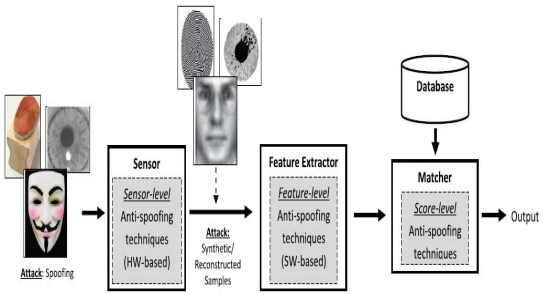


Fig.1 General diagram of a biometric system

II. ANTISPOOFING TECHNIQUES

A. *Sensor -level Techniques:-*

Typically alluded to in the writing by the term equipment based procedures. These techniques add some particular gadget to the sensor so as to distinguish specificproperties of a living attribute (e.g., facial thermo gram, circulatory strain, unique finger impression sweat, or particular reflection properties of the eye).

B. *Feature-level Techniques:-*

Normally alluded to in the writing by the term software based procedures. For this situation the fake quality is distinguished once the sample has been obtained with a standard sensor. In that capacity, features used to recognize real and fake attributes are removed from the biometric sample (normally pictures, as on account of face, or some sort of time-capacities, as on account of discourse), and not specifically from the human body as on account of sensor-level systems. These strategies are coordinated after the sensor, normally working as a major aspect of the feature extractor module [5] .

C. *Score-level techniques:-*

The a third group of assurance routines which falls out of the conventional two-types of classification methods (software and equipment based), has begun to be examined in the field of fingerprint antispoofing favorable circumstances and disadvantages so that, a mix of both would be the most attractive procedure to build biometric security systems.

III. RELATED WORK

In this paper[1] Author implemented two solutions which utilize customer identity data to identify spoofing attack: a generative and a discriminative one. Significant performance gain on different protocols of Replay-Attack face spoofing database. This paper concentrates on the measure of client particular data inside of these components and how it influences the performance of anti-spoofing system. Author makes utilization of this data to fabricate two client-specific antispoofing solutions, one depending on a generative and another on a discriminative paradigm. In paper[2] Author propose a real-time liveness detection methodology is introduced against photo spoofing in a non-meddlesome way for face recognition, which does not require any extra equipment aside for a specific web camera , blinking-based liveness detection has some limitations. In paper[3] Author objective is to recognize the spoofing attacks on such biometric structures, face liveness discovery systems have been made. Different anti-spoofing systems have been created and actualized that might essentially raise the trouble level for photograph, video and combination attacks. In paper[4] presents structural planning for face identification construct framework in light of AdaBoost algorithm using Haar features. Author represents face recognition based on AdaBoost algorithm using Haar features. In paper[5] image quality assessment .The proposed approach displays a low level degree of complexity, which makes it suitable for real-time applications, utilizing 25 general picture quality components separated from one picture (i.e., the same gained for validation purposes)for identifying difference between real and fake samples. In paper[6] Author proposed Three fake face attacks are executed, which incorporate warped photograph attack, cut photograph attack and video attack. Therefore each subject contains 12 recordings (3 real and 9 fake), and the last database contains 600 video clips.In paper[7].motion magnification author presents a novel framework for facial spoofing detection using motion (liveness) and texture (anti-spoofing)features. Author implemented two element extraction algorithms a design of local binary pattern and movement estimation utilizing histogram of oriented optical flow, are utilized to encode texture and movement (liveness) properties separately.

IV.PROPOSED SYSTEM

To overcome the disadvantages that were in the existing system we add to a system that will be exceptionally helpful for any client identity confirmation. Here the system monitors the record number of every cut during the development of identifiable human face and compute maximum number of cuts of the similar record number. Based on this record number program retrieves the similar record of the user identity record and face of user. Based on this record number the project recovers the individual record of the suspect (whose cut constituted the real parts of the developed human face) on practicing the "find" choice.

V.SYSTEM IMPLEMENTATION

A. System Architecture of proposed solution:-

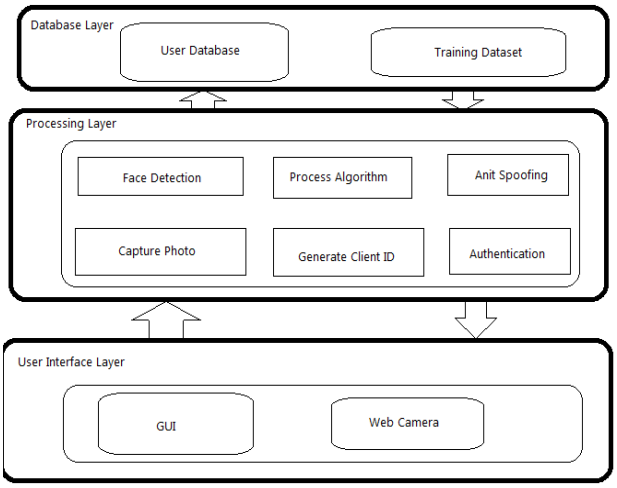


Fig.2 System Architecture of proposed solution

Now a day's biometrics framework playing the part of a password which can't be supplanted if stolen, for example, unique fingerprint detection, iris recognition, the need of setting up counter-measures to biometric spoofing attacks has been created. In any case of the biometric systems, methodology of anti-spoofing systems is to sort the biometric proof in view of elements separate between genuine faces and spoofing attacks. Interestingly, to the best of our insight, this procedure concentrates on the measure of client-specific data inside of these elements and how it influences the execution of anti-spoofing system . We make utilization of this data to construct two client-specific antispoofing systems, one depending on a generative and another on a discriminative worldview. The proposed systems, tried on state of art anti-spoofing features for the face mode, beat the client independant methodologies with changing size of relative change and show better speculation capacities on inconspicuous sorts of spoofing attack.

B. Basic Steps of proposed system:-

- Firstly by using hardware equipment such as web camera capture user photo.
- Addition, Clipping, Construction and updating of the user identity record and face of user.
- Comparing the image with the faces that are there in our database.
- If any new images are found then it should be entered into our database by add image module then it should be segmented into different slice.

C. Algorithm

Step 1: Capture Live video streaming using web camera. Which can be capture image with different gestures.

Step 2: Apply Training set for captured images. (n training examples(x1,y1…xn , yn)).
Step3: Assign initial weight for each hypothesis i.e. features.
Step4: Train each hypothesis for each feature and update Classifier.
Step5: Comparison for captured images with training dataset.

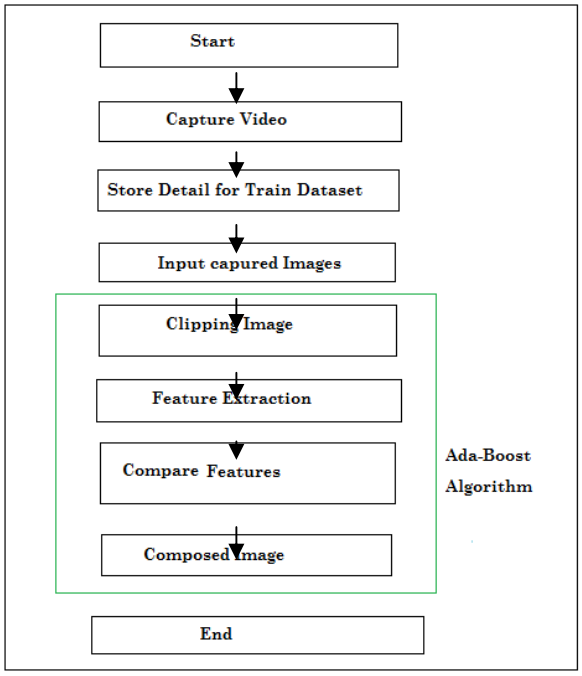


Fig 3.Flow of Ada-boost Algorithm

D. Modules

1] Building android application basic GUI
2] Pre-processing
3] Face detection
4] Face extraction
5] Face matching

E. Security Requirements

The aim for designing the face anti-spoofing system to satisfy following security requirements

(i) **Non-invasive**: these methods should no harmful or not require more contact with the client;

(ii) **Easy to understand**: clients should not be hesitant to interface with them;

(iii)**Fast**: results should be produced in a lessened omission of time as clients' connection with the sensor should be kept as short as possible;

(iv) **Minimal effort**: wide utilize can't be normal in the event that the expense is too much high;

(v) Execution: In addition to a decent fake detection rate, the protection plan should not corrupt the recognition performance of the biometric framework (e.g., false rejection).

F. Mathematical Model

- ***Set Theory:***

Let us consider S as a system for Applications of Client Identity Information For Face Antispoofing.
S= {∑, F, δ, C}
S = Face Recognition for user identity.
∑ = set of input symbols = { Video File, image, character information}
F = set of output symbol = {Match Found then notification to user, Not Found}
δ = 1. Start
2. Read training set of images N*N
3. Resize image dimensions to N^{2*1}
4. Select training set of N^{2*M} Dimensions,
M: number of sample images
5. Find average face, subtract from the faces in the training set,

create matrix

$$\varphi = \frac{1}{M}\sum_{i=1}^{M} \Gamma i$$

Where,
Ψ= average image,
M= number of images, and
Γi= image vector.
`6. Calculate eigenvectors of the c covariance matrix.
7. Calculate faces = No .Of training images no. of classes of eigenvectors.
8. Create reduced face space the selected set of eigenvectors are multiplied by the A Matrix to create a reduced face
9. Calculate eigenface of image in question.
10. Calculate Euclidian distances between the image and the Eigen faces.
11. Find the minimum Euclidian distance.
12. Output: image with the minimum Euclidian distance or image unrecognizable.

VI. **IMPLEMENTED RESULT**

For antispoofing technique we use live image of face of user. Apply training set for face image captured from live web camera. These capture different gestures from video streaming and analyze to match user face expression. System gives expected result as original user identity.

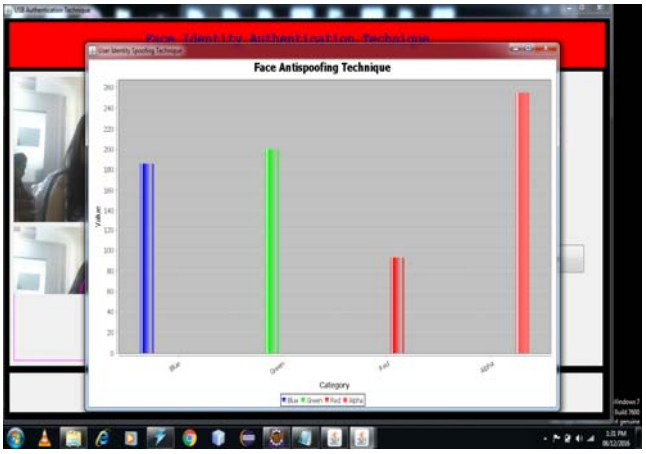
TABLE I

Performance Comparison to Existing System:-

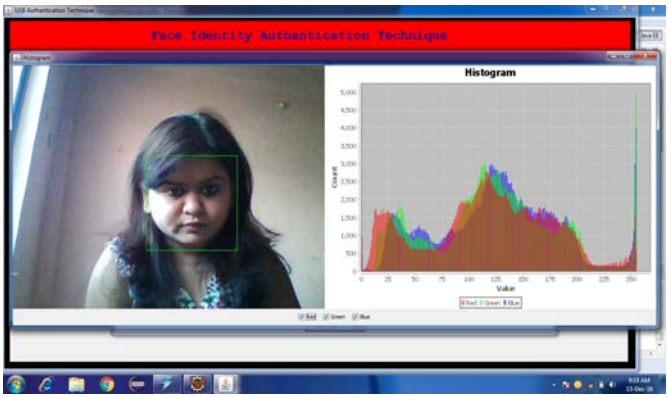
	Grand Test	**Print**	**Digital-photo**	**Video**
Existing System	8.53	5.95	8.74	5.73
Proposed	8.70	9.10	9.58	7.56

GRAPHS

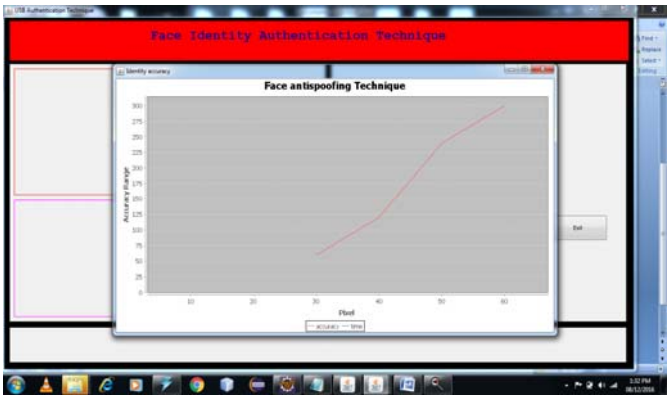
Graph 1:- This graph represents category & values.



Graph 2:-This graph represents histogram to show counting of features matching



Graph 3:- This graph represents pixel & its accuracy range.



CONCLUSION

To utilize an anti-spoofing system, a client is required to display the important biometrics quality to the sensor, which is for this situation a camera. The captured facial images are preprocessed into a satisfactory structure (e.g. For example, through standardization and commotion evacuation systems

ACKNOWLEDGMENT

Our genuine much gratitude goes to GHRIET for giving a strong platform to add to our expertise and abilities. We might want to much appreciate each one of the individuals who specifically or indirectly way help us in presenting the paper. We hereby take this chance to express our heartfelt gratitude towards the general population whose assistance is extremely helpful to finish our project. We might want to express our heartfelt thanks of my guide Prof. Mrs.Rekha Jadhav who's experienced guidance turned out to be extremely important for us.

REFERENCES

[1] Ivana Chingovska and Andr Rabello dos Anjos, "On the Use of Client Identity Information for Face Antispoofing," IEEE Transactions on Information Forensics and Security Vol.10, No. 4, April 2015.

[2] Gang Pan, Zhaohui Wu and Lin Sun,"Liveness Detection for Face Recognition",ISBN 978-953-7619-34- 3, pp. 236, December 2008, I-Tech, Vienna, Austria.

[3]] Sajida Parveen1, Sharifah Mumtazah Syed Ahmad , Marsyita Hanafi1 and Wan Azizun Wan Adnan, "Survey of Face anti-spoofing methods", CURRENT SCIENCE, VOL. 108, NO. 8, 25 APRIL 2015.

[4] M.Gopi Krishna, A. Srinivasulu , "Face Detection System on AdaBoost Algorithm Using Haar Classifiers",Vol. 2, pp-3556-3560 ISSN: 2249-6645 ,Issue. 5, Sep.-Oct. 2012.

[5] J. Galbally, S. Marcel, and J. Fierrez, "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, Feb. 2014.

[6] Z. Zhiwei, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in Proc. 5th IAPR Int. Conf.Biometrics (ICB), New Delhi, India, 2012, pp. 26–31.

[7] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW), Jun. 2013, pp. 105–110.

[8] Javier Galbally, Sbastien Marcel, (Member, Ieee), And Julian Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," Volume 2, Digital Object Identifier 10.1109/Access.2014.2381273.

[9] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in 'liveness' assessment,"

IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 548–558,

Sep. 2007.

[10] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in Proc. Int. Conf. Biometrics (ICB), Jun. 2013, pp. 1–6.

[11] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based face anti-spoofing," in Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl ,Syst. (BTAS), Sep./Oct. 2013, pp. 1–8.

[12] T. de Freitas Pereira et al., "Face liveness detection using dynamic texture," EURASIP J. Image Video Process., vol. 2014, p. 2, Jan. 2014.

[13] G. Zhao and M. Pietikäinen, "Dynamic texture recognition using local binary patterns with an application to facial expressions," IEEE Trans.Pattern Anal. Mach. Intell., vol. 29, no. 6, pp. 915–928, Jun. 2007.

[14] A. Rattani, N. Poh, and A. Ross, "Analysis of user-specific score characteristics for spoof biometric attacks," in Proc. IEEE Comput. Soc.CVPR Workshops, Jun. 2012, pp. 124–129.

[15] S. Marcel, Y. Rodriguez, and G. Heusch, "On the recent use of local binary patterns for face authentication," IDIAP, Martigny, Switzerland,Tech. Rep. Idiap-RR-34-2006.

[16] S. S. Kajarekar and A. Stolcke, "NAP and WCCN: Comparison of approaches using MLLR-SVM speaker verification system," in Proc. ICASSP, 2007, pp. 249–252.

[17] M. McLaren, R. Vogt, B. Baker, and S. Sridharan, "Data-driven backgrounddataset selection for SVM-based speaker verification," IEEE Trans. Audio, Speech, Lang. Process., vol. 18, no. 6, pp. 1496–1507,Aug. 2010.

[18] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in Proc. Int. Conf. Biometrics, 2013, pp. 1-8.