International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Image Quality Assessment for Fake Bio-metric Detection and Replay-Attack in use of Videos

Sunil Nijhawan[1], Dr. Jitender Khurana[2], Dr. R. B. Dubey[3]

[1]Research Associate, BMN University, Rohtak

[2]BMN University, Rohtak

[3]HOD, Hindu College of Engineering, Sonepat

Abstract: ***A biometric framework is acomputer system which is utilized to distinguish the individual on their behavioral and physiological trademark. A normal biometric framework comprises of detecting,matching modules and feature extraction. This research work introduce a new biometric methods which are face detection(Multi Biometric System) in videos and furthermore present the assaults on that framework and by utilizing Image Quality Assessment for Liveness Detection how to shield the framework from fake biometrics. Biometric frameworks experience variability in information that impact capture, treatment, and use of a biometric test. It is basic to first investigate the information and consolidate this comprehension inside of the detection framework, making assessment of biometric quality a vital part of biometrics. This paper proposed a novel procedure use measurements like symmetrical between face features like both sides of face, nose symmetry and so on for identifying fake Images.***

Keywords: Multi Biometric System, fake biometrics, Image Quality Assessment, Live-ness Detection

1. Introduction

Biometric frameworks rather distinguish a person by what he is rather than taking into account something he knows or has. Considering that any bit of material or information can be falsely obtained biometrics can offer a few points of interest over established security strategies. In any case, despite its points of interest, biometric frameworks have a few downsides, including the absence of mystery, the way that a biometric quality can't be supplanted and its helplessness to outside assaults which could diminish their level of security. It is important to remember the security issues when we investigate a radical new universe of potential outcomes in this organized society of these days. Our cell phones are transforming into stockpiles of individual, expert, business, and different sorts of data. This data is expected by the users to be kept classified. [1]

Image quality assessment is a most critical subject in the Image preparing range. Image quality is a characteristic of any Image as a rule contrasted and a perfect or impeccable Image. Computerized Images are liable to a huge scope of twists amid capacity, accomplishment, pressure, handling, transmission and propagation, a few of which might bring about a corruption of visual quality. Imaging frameworks presents some measure of distortioning or antiques which diminishes the quality assessment. As a rule quality evaluation is of two sorts one is subjective visual quality assessment and second one is objective visual quality evaluation [2].Objective Image quality measurements can be ordered on the premise of accessibility of a unique Image, with the mutilated Image is to be thought about.

The objective of this paper is to choose Image quality assessment for liveness location system is utilized to recognize the fake biometrics. Because of Image quality estimations it is anything but difficult to discover genuine and fake users since fake personalities dependably have some distinctive components than unique it generally contain diverse shading and luminance levels, general ancient rarities, amount of data, and amount of sharpness, found in both kind of Images, basic mutilations or regular appearance. Multi Biometric framework is testing framework. Multi biometric framework is utilized for different applications. Also, we get ready for making this framework more secures including the one more biometric framework into this framework and attempting to enhance the framework.

Variables that impact biometric quality

It is essential to value the impacts of different components that influence quality to grow better assessmentalgorithms. While a few variables are unavoidable, others might be natural impediments of the biometric itself. These variables are either user qualities or collaborations in the middle of user and sensors:

- **User characteristics** some critical variables that impact the nature of a biometric test amid capture procedure can be delegated behavioral and physiological qualities of the human users [3]. Behavioral qualities might incorporate inspiration levels, collaboration, and apprehensions. Physiological characteristics incorporate facial hair or affectability to light. While a few practices of users can be confined, it is at the expense of ease of use and expanded impairment. Further, unavoidable variables, for example, age, social traditions, sexual orientation, and wounds can weaken the nature of the caught test. Case in point, fingerprints got from more established age gatherings is of lower intrinsic biometric quality (because of worn edges) when utilizing diverse business unique mark frameworks [4].
- **User-sensor communication and operational imperatives** the second vital element that impacts the nature of contact capture (shut/close field of perspective) based biometrics, for example, fingerprints, palm prints, iris, and retinal, is the

cooperation in the middle of users and sensors. The ease of use of the sensor is significant to quality. Sensors with dynamic user input that are versatile and simple to utilize guarantee great user sensor collaboration, bringing about better quality captures. In any case, natural components, for example, calm, mugginess, and foundations impact this connection, unfavorably influencing the nature of a biometrics.

2. Problem Identification

In order to better comprehend quality evaluation in biometrics, it may be valuable to nearly investigate the distinctive curios that ordinarily show in biometric Images [5].

- **Blurring:** Image obscuring is a typical wonder that happens because of off base center (article is outside the profundity of field), movement, or certain ecological variables. Obscuring impacts edge data, which is fundamental to biometric detection, especially the moment edges of iris examples.
- **Illumination:** Uniform lighting is keys for the capture of a decent quality biometric. On the other hand, unfavorably coordinated lighting definitely influences the execution of iris and face.
- **Noise/Compression:** AnImage might contain clamor because of ecological elements, off base utilization of sensors, and transmission blunder. Clamor pollution radically influences the execution of detection frameworks. Contingent upon the pressure levels, different Image encoding systems produce relics, for example, blockings and ringing impact.
- **Optical distortions:** Nonconformity to rectilinear projection causes mutilation in the caught Image. Such mutilations might happen because of different ecological components or because of the working of sensors. Further, distinction in the sensor models additionally brings about various mutilation profiles, corrupting detection execution.

3. Related Work

The focus of this section is to study or collecting information existing models.

Alanso-Fernandez et al. [6] present a near investigation of a few unique mark quality measurements. These algorithms are isolated into worldwide and nearby measurements relying upon the way of assessment. The study demonstrates a high relationship of unique mark quality measurements among themselves. This appears to show that the concentrated on methodologies encode comparable data from the unique mark Image to anticipate quality. As of late, unique mark quality registered utilizing the edge data as a part of different subbands is appeared to give the best dismissal criteria to enhance execution. The unique mark edge recurrence and introduction were caught utilizing brief time Fourier change. The metric encodes the congruity of the edge range along the introduction of solid edges in the Image. In another examination, self-arranging maps (SOM) are utilized to order neighborhood areas of a unique finger impression to various quality marks.

Chen et al. [7] present a quality metric for iris in light of the ghastly vitality in neighborhood areas. Firstly, iris is portioned utilizing shrewd edge indicator and Hough change. Next, impeded locales that might happen because of eyelashes are uprooted utilizing power thresholding. The 2D Mexican cap wavelet decay is connected, and the result of reactions from numerous scales (typically three) is utilized as the general reaction. The iris locale is apportioned into concentric groups with settled width (8 pixels). The vitality from concentric districts are independently figured and joined into a solitary quality score. Various covering separating of the iris area methodology is fundamental to encode the fine edges displayed by the iris muscle tissue. The methodology is additionally utilized for feature extraction.

In another methodology, Kalka et al. [8] present quality assessment of iris Images in light of the assessment of eight quality parameters (defocus, movement obscure, off-point, impediment, specular reflectance, brightening, and pixel check). These individual quality scores are both Image based and biometric-particular in nature. Further, Dempster-Sheffer hypothesis based combination is utilized to consolidate these individual scores to get a solitary quality worth. The quality measure is assessed on the iris dataset of the West Virginia University (WVU) multimodal biometric database, utilizing the quality receptacles approach talked about already.

Limet al. [9] present a neighborhood feature based quality metric which figures introduction sureness level (OCL), edge recurrence, edge thickness, and edge to-valley thickness proportion. Shen et al. [10] use Gabor channels for quality evaluation. Unique mark Image is decorated into pieces, and Gabor channels with various introductions are connected on every square. For astounding squares, reaction from channels of a few introductions is fundamentally higher than others, while for low-quality hinders, the distinction in reactions from the channels is by and large low. The standard deviation of the reactions in this way shows nearby quality for every piece. The accumulated neighborhood quality is contrasted and scores from visual investigation. So also, Vatsa et al. [11] use repetitive discrete wavelet change (RDWT) to register predominant edge movement to gauge unique mark quality. The quality metric affected colossal execution change when joined into a unique finger impression feature level combination system on a vast genuine database. Olsen et al. [12] likewise exhibit a quality measure in view of assessing Gabor channel reactions of a unique mark Image whose execution is stronger to its parameters.

Wong et al. [13] present a patch-based methodology utilizing the main d low-recurrence segments of the discrete cosine change (DCT) got from every facial patch. A multivariate probabilistic model is created utilizing a preparation set of frontal countenances with worthy enlightenment per patch, and the test Image is thought about, patch-wise, to get the general quality. The general methodology for video face quality evaluation depends on contrasting the information face Image and face models created from perfect sample sets. In another methodology,

Nasrollahi and Moeslund [14] present a straightforward geometrical methodology in view of the measurements of the jumping box of face identification algorithm in a video face detection framework. Since stance is an essential test in such frameworks, this methodology can be considered as a basic posture evaluation strategy.

A comparable methodology is additionally utilized as of late by Long and Li [15] for NIR video face detection. Yao et al. [16] utilize a sharpness measure from casing determination for adetection framework intended for low-determination face recordings. It must be noticed that while face quality evaluation has gotten impressive consideration in video face detection inquire about, the prerequisite in this specific application is for a paired choice (acknowledge/reject) per video outline. Henceforth, such quality measurements may not adequately gauge the nature of the face biometric test.

4. Proposed Work

The fundamental goal of our methodology is to make our system more secure and more fake recognition either in still Images or video based.

A. Proposed Implementation

Two major steps involved in the proposed method of fake face detection in videos that are as follows

a) Fake detection in videos

The enhancement technique along these ways:

1) Extension of the considered 25-feature set with new image quality measures
2) We will use metrics like symmetrical between face features like both sides of face, nose symmetry etc. for detecting fake images
3) Inclusion of temporal information for those cases in which it is available for example camera lighting condition in which the faces were taken, then we can evaluate whether the face image is having those features for corresponding lighting condition
4) Use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB);
5) In video we can detect the fake images by its pose when compared to changes in background.

For that we follow following modules [17]:

Module 1: Face Database Image

Run of the mill illustrations of genuine face Image can be found in people in general REPLAY-ATTACK DB and fake examples will be arranged by obscuring method

Module 2: Still face Images based methods

The methodology consolidates a few Image quality measurements and face-particular measurements utilizing facial element discovery. Outward appearance like great, terrible, revolting sets can be anticipated by utilizing halfway minimum square relapse between Image based elements (sharpness, tone, and force) and geometric characteristics of a face (acquired utilizing dynamic appearance displaying)

Module 3: Video Face coordinating

An imperative utilization of value assessment in face biometrics is in video face coordinating. Here, face detection is performed on a video stream as opposed to a solitary still Image. A multivariate probabilistic model is created utilizing a preparation set of frontal countenances with worthy enlightenment per patch, and the test Image is thought about, patch-wise, to get the general quality.

Module 4: Evaluating quality assessment

Quality score will be utilized to adjust the component space to enhance coordinating. The proposed work join tests taken quality assessment metric (processed for both display and test) in the plan of Hamming separation matcher to indicate enhanced results when contrasted with basic Hamming separation.

b) Replay attacks in videos

The Image quality estimation based component extraction is a standout amongst the best and generally utilized systems as a part of the space of discourse and Image handling. Along these lines, enlivened by its wide achievement in different discourse and Image preparing ranges, we propose its investigation to evaluate the presentation assault location in biometric frameworks [18].

Figure 1: Replay attacks for fake detection in videos

Most of the assaults are introduced by making a biometric ancient rarity as either a photograph or replaying a video before capturing gadget. Subsequently these introduced antiques when caught by the gadgets (or cameras) will tend to display bigger recurrence parts when contrasted with that of genuine biometric tests. Following these high frequencies can be more accentuated exploring so as to utilize Image quality estimation the non-uniform binning of the phantom data it is our attestation that, the utilization of Image quality estimation components can introduce complete data which thusly can be utilized to distinguish the appearance assaults on the biometric framework.

B. Proposed Algorithm

Steps

1) Take reference image and split to symmetrical halves (we are splitting to four but it can split to any)
2) A=Calculate the symmetrical distance between blocks
3) Take image to authenticate and split to symmetrical halves (we are splitting to four but it can split to any)
4) B=Calculate the symmetrical distance between blocks
5) Check for consistency between A and B

If the consistency is more, then image to authenticate is real image, else it is fake image

5. Results

Results of experimental work are shown below:

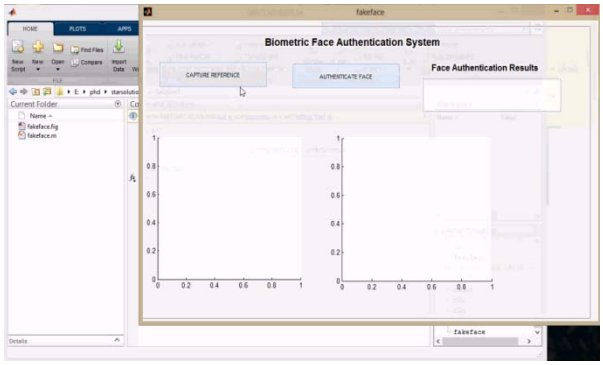

Figure 2: Fake face detection in videos

The Fig.2 illustrates GUI for proposed model of fake face detection.

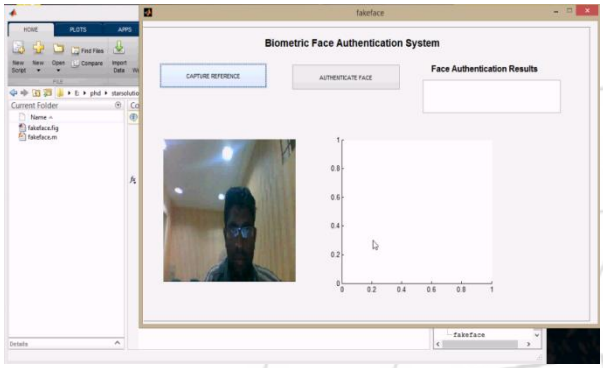

Figure 3: Face detection through video captured by camera

Fig.3illustratesthe process of fake face detection in case of videos. First click the CAPTURED REFERENCE button to capture the videos through camera usage. It will capture the original face.

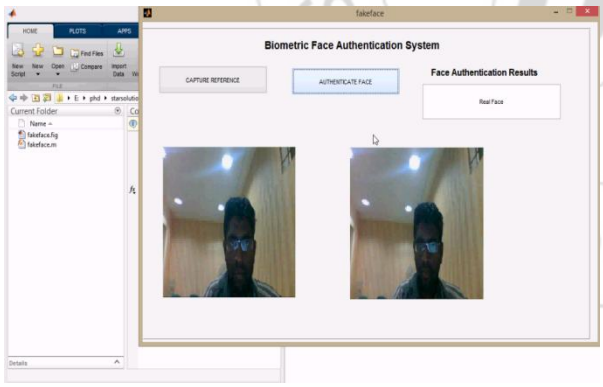

Figure 4: Face authentication that detect the face and real face or fake face

Fig. 4 representsthe process of fake or real face detection. For that again capture the video through camera and click on the AUTHENTICATE button; it will match the face with original video and detect the fake or real face. The reply-attack is detected through the multiple click on AUTHENTICATE button for one face detection in multiple videos.

6. Conclusions

Image quality evaluation for liveness recognition system is utilized to identify the fake biometrics. Because of Image quality estimations it is anything but difficult to discover genuine and fake users since fake personalities dependably have some distinctive components than unique it generally contain diverse shading and luminance levels, general antiquities, amount of data, and amount of sharpness, found in both sort of Images, basic distortions or regular appearance. In this paper learned about work, including: i) expansion of the considered 25-feature set with new Image quality measures; ii) assessment on other Image based modalities (e.g., palm print, hand geometry, vein); iii) incorporation of worldly data for those cases in which it is accessible (e.g., frameworks working with face recordings); iv) Use of video quality measures for video access endeavors in different applications.

In future for making this framework more secures including the one more biometric framework into this framework and attempting to enhance the framework. Additionally Real time usage of Iris and face Image application in biometric should be possible in proficient way.

References

[1] Javier Galbally, Sébastien Marcel. (February 2014).—Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition", Member, IEEE, and Julian Fierrez vol. 23, no. 2.

[2] Rohit Kumar, Vishal Moyal. (2013).—Visual Image Quality Assessment Technique using FSIM", International Journal of Computer Applications Technology and Research Volume 2– Issue 3, 250 - 254, www.ijcat.com.

[3] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al. (2009) —First international fingerprint liveness detection competition— LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. pp. 12–23.

[4] A Mittal, AK Moorthy, AC Bovik. (2012).—No-reference image quality assessment in the spatial domain", IEEE Trans. Image Process. 21(12), 4695–4708.

[5] S Yendrikhovskij. (April 1999).—Image quality: between science and fiction", in Proceedings of Conference of Image Processing, Image Quality, Image Capture, Systems, Georgia, 25–28, pp. 173–178

[6] F Alanso-Fernandez. (2007).—Biometric quality assessment and its application in multimodal authentication systems". Thesis, Universidad Politécnica deMadrid, Madrid.

[7] Y Chen, S Dass, A Jain. (2008).—*Localized iris image quality using 2-D wavelets, Advances in Biometrics", Lecture Notes in Computer Science*, vol. 3832. (Springer, Berlin Heidelberg), pp. 373–381

[8] ND Kalka, J Zuo, N Schmid, B Cukic. (2010).—Estimating and fusing quality factors for iris biometric images", IEEE Trans. Syst. Man Cybern. 40(3), 509–524.

[9] E Lim, X Jiang, W Yau. (September 2002).—Fingerprint quality and validity analysis", in *Proceedings of IEEE/IAPR International Conference on Image Processing* (Rochester, New York, 22–25), pp. 469–472

[10] L Shen, AKot, W Koo.(June 2001). ―Quality measures of fingerprint images", in *Proceedings of Audio and Video Based Biometric Person Authentication* (Halmstad, Sweden), pp. 266–271
[11] M Vatsa, R Singh, ANoore, MM Houck. (2009).―Quality-augmented fusion of level-2 and level-3 fingerprint information using DSm theory". Int. J. Approximate Reasoning 50(1), 51–61.
[12] MA Olsen, H Xu, C Busch. (2012).―Gabor filters as candidate quality measure for NFIQ 2.0", in *Proceedings of IAPR International Conference on Biometrics* (New Delhi, India), pp. 158–163
[13] Y Wong, S Chen, S Mau, C Sanderson, BC Lovell. (June 2011).―Patch-based probabilistic image quality assessment for face selection and improved video-based face recognition", in *Proceedings of IEEE International Conference on Computer Vision and Pattern Recognition Workshops* (Colorado Springs), pp. 74–81
[14] K Nasrollahi, T Moeslund. (2008).―*Face quality assessment system in video sequences. Biometrics and identity management", Lecture Notes in Computer Science*, vol. 5372. (Springer, Berlin Heidelberg). pp. 10–18
[15] J Long, S Li.(August 2011). ―Near infrared face image quality assessment system of video sequences", in *Proceedings of International Conference on Image and Graphics* (Hefei, China, 12–15), pp. 275–279
[16] Y Yao, B Abidi, M Abidi. (2007).―*Quality assessment and restoration of face images in long range/high zoom video", Biometrics and Identity Management. Lecture Notes in Computer Science*, vol. 5372. (Springer, Berlin Heidelberg). 43–60
[17] E Tabassi, CL Wilson, CI Watson.(2004).―Fingerprint image quality", (NISTIR 7151).
[18] H Fronthaler, K Kollreider, J Bigun. (June 2006).―Automatic image quality assessment with application in biometrics", in Proceedings of IEEE Computer Vision and Pattern Recognition Workshops,New York, p. 30