Biometric Mistreatment Image Quality Assessments for Spoofing Detection

S. Sivaranjani[1], K.C. Ramya[2], S. Sheeba Rani[3]
[1]Assistant Professor
[2,3] Associate Professor
[1,2,3] EEE Department, Sri Krishna College of Engineering and Technology, Coimbatore, India.
[1]sivaranjanis@skcet.ac.in,[2]ramyakc@skcet.ac.in, [3]sheebaranis@skcet.ac.in

Article Info
Volume 83
Page Number: 8701 - 8707
Publication Issue:
March - April 2020

Article History
***Article Received**: 24 July 2019*
***Revised**: 12 September 2019*
***Accepted**: 15 February 2020*
***Publication**: 09April 2020*

Abstract

Face appearance, iris and finger impression are most promising biometric authentication system that can be identified and analysed a person's unique features that can be immediately obtained from the recognition process. To confirm the real existence of an original authentic feature in difference to a fake or recreated model is an significant difficulty in biometric confirmation, which necessities the expansion of innovative and competent security methods. Biometric systems are susceptible to tricking attack. A trustworthy and well-organized counter measure is required to contest the epidemic growth in uniqueness holdup. The Biometric recognition and verification agreements with non-ideal circumstances such as distorted images, replications and also forged by others. For this motive, image quality valuation methods to instrument forged finding process in multimodal biometric systems. Image quality assessment approach is used to build the feature vectors that comprise quality parameters such as likeness, fuzziness level, color variety, error degree, noise degree, resemblance values and so on. These structures are stored as vectors in database. Then implement Multi level Support Vector Machine classification algorithm to predict forged biometrics.

Keywords: *Multimodal biometrics, Image Quality, Spoofing attack, Fake detection, Feature Vector*

I. INTRODUCTION

Biometric is a rapid growing technology for programmed response or confirmation of the distinctiveness of an individual being using distinctive physical or behavioral characteristics listed as finger impressions, facial appearance, iris, retina, voice, hand geometry and sign etc. To develop an individual unique identity Biometric depends on - who is a person or what a person does, as disagreeing to what one can recall - such as a Personal Identification Number or conceal keyword or what an individual do use -such as an Identification card. Though, important developments have been comprehended in Biometrics, numerous spoofing procedures have been recognized to mislead the Biometric systems, and the defense of these systems against attacks is still an open challenge. Amongst the altered threats inspected, the direct or spoofing attacks have activated the biometric communal to learn the accountabilities in flaw of this type of tricky activities in acts for instance the finger impression, the face appearance, the sign, and also the bearing and multimodal tactics. Spoofing occurrences rise when an individual attempts to pretense as somebody and thereby forging the Biometric information which are limited by the sensor in an effort to avoid a Biometric system and leads to a head illegal use and benefits. Few category of falsely formed objects e.g. iris image print, gummy finger, facial appearance mask, photo, audiovisual, 3 dimensional visual Model or reproduce the actions of the authentic operator (e.g., gait, sign) etc., are handled by the pretender to forge the biometric scheme.

Subsequently, there is a growing critical to notice such efforts of occurrences to biometric systems. Liveness finding is the most prevailing countermeasure in the flaw of spoofing attack. It targets at physiological symbols of individual being in biometric image such as eye blinking, mouth actions, blood pressure, sweating of finger skin, face appearance expression changes, particular imitation characteristics of the eye etc., by gathering exceptional sensor devices to biometric system. Another helpful countermeasure in flaw of spoofing attack is usage of multimodal features. Merging face appearance or iris or finger impression recognition by means of additional biometric modalities such as bearing and language is perception of multimodal scheme. Certainly, multimodal schemes are fundamentally trickier than Uni-modal scheme. Single modal systems are less complex than the Multimodal systems. The multimodal biometrics system is illustrated in figure 1.

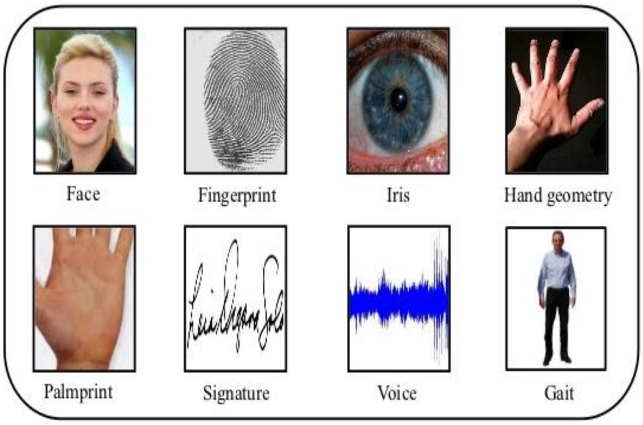

Figure 1. Multimodal Biometric scheme

So, to plug those attacks to biometric systems cumulative Multimodal is required. If spoofers (users who do not have an authorization to enter the structure) have permission to scores the respective system, the spoofer can simply bypass the arrangement. However, it is harder to undertake this type of attack. Then the acquisition sensor is the most susceptible portion (every individual can have right to admit in this part of the system), spoofing attack procedures have turned out to be more attractive for pretenders.

II. RELATED WORK

Julian Fierrez, et.al [3] proposed a new parameterization by superior events which are verified on a thorough liveness recognition structure. Any of the subsequent features are computed for Image quality evaluation: frame strength or directionality, veracity of the ridge-valley structure ridge continuity, ridge clearness, or projected authentication act when using the appearance at hand. Properties are measured by a number of information those are: (i) direction field angle information,(ii) pixel intensity of the gray-scale image, (iii) representation of other implementation direction angle by Gabor filters, and power spectrum. (iv) Finger impression feature can be evaluated not only by reviewing the picture in a holistic method but also merging the local non-overlapped blocks picture effectiveness.

J. Galbally, et.al [4] studied two processes for attack detection in face appearances. The major model inspected the efficacy of the Bayesian-based hill-climbing attack on an Eigen face appearance-based system. The subsequent model used the formerly establish optimal alignment to attack a GMM Parts based system. Through the similar optimal safety alignment between studies, it can be concluded that the performance of the attack is highly reliant on the values of the parameters nominated.

Javier Galbally, et.al [10] obtained liveness detection solutions for great significance in the biometric field as they support to elude straight attacks those accepted out by means of synthetic traits, and highly tough in identifying, improving the mode of level of the safety provided to the receiver end.

Jaime Ortiz-Lopez,et.al, familiarized a widely existing databank, procedures and a typical procedure to guesstimate counter measures to spoofing occurrences in face appearance recognition systems. It appears to survive no consensus on finest processes and methods to be situated on attack exposure by non-intrusive systems. An important trace to this problem is the deficiency of typical databases to test counter-measures, trailed by a set of rules to assess the output and agree for impartial assessment.

Alessandra Lumini, et.al [5] projected the image reestablishment method deeds the evidence deposited in the pattern to recreate an accurate image by guessing numerous features of the real unknown finger impression by four processing stages. The attacking state measured in this effort supposed that the mandatory evidence only deposited in an Impression Particulars Record of the ISO pattern is existing.

Lacey Best-Rowden, et al., [1] implemented face appearance quality actions to define when the fusion of resource sources will support identification. The superior actions are also employed to allocate weights to transformed resources in synthesis structures.

III. CRITERIA IMAGE DISTORTION ANALYSIS BASED FACE APPEARANCE SPOOFING DETECTION

Biometrics offers tools and methods created on behavior, chemical and physical qualities to distinguish persons in an exclusive and auto style. Best communal prompts are finger impression, face appearance, eye iris, palm and finger geometry, veins of hand, sign, vocal sound and Deoxyribonucleic Acid. Because of modern arrangement developments applied to face appearance identification, biometric systems have been mostly implemented to complications, including right to use control, surveillance and convict identity. All together that noteworthy developments are being attained in biometrics, numerous spoofing methods are also established to trick the biometric systems, and those structures against attacks is an open issue still.

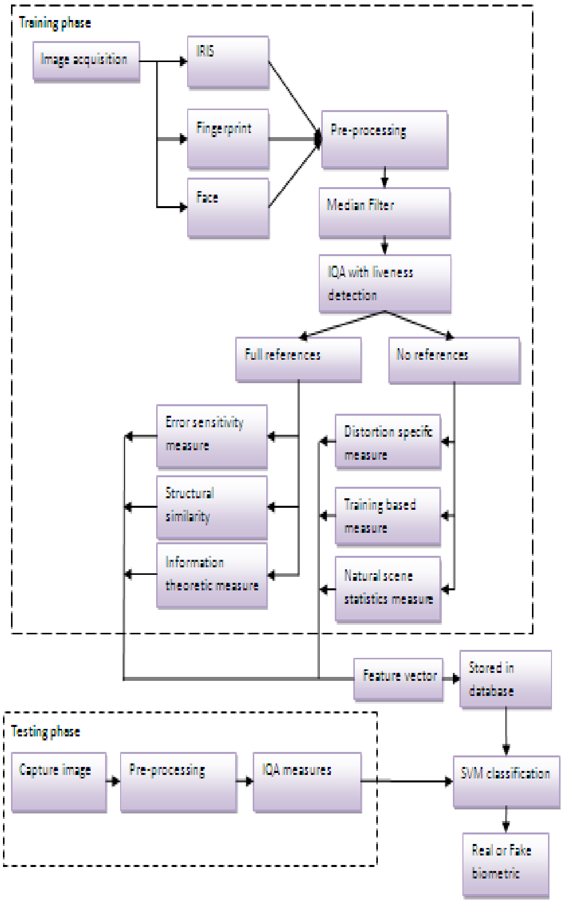

Figure 2. Proposed Framework

Spoofing attacks happen when a person attempts to pretense as somebody forging the biometrics statistics. Attacks are apprehended by the specific sensor in an effort to improvise the security of a biometric system. Foremost anxiety for today's situation is Security. A notable industry practices Personal Identification Numbers like first digit finger impression, face appearance, vocal sound, eye iris, etc. Hence, countless safety arrangements are existing.

Nevertheless it is not so reliable. At this time the emerging structure which is too accurate and trustworthy. The structure has two phases which is rooted system. Even if any phase is split incorrectly, unofficial access can be recognized. Current framework investigated an image distortion analysis approach to recognize the forged face appearances. IDA comprises specular reflection, chromatic moment, blurriness and color diversity). Specular

Reflection Features examine illumination of the images.

Then vagueness is obtained based on the variance between the real image and its imprecise form. Then change the regularized facial appearance from the RGB space into the HSV (Hue, Saturation, and Value) space and the mean, deviation, and skew ness of every network as a chromatic appearance is calculated. Finally color reproduction loss in input images is investigated. Multiple SVM classifiers are provided with Feature vectors. The proposed structure is to attain a new steady face appearance spoof recognition structure.

IV. MULTIMODAL BIOMETRIC IMAGE QUALITY ASSESSMENT SYSTEM

To assure the genuine incidence of an actual correct attribute in difference to a false self-designed imitation or redesigned test model is a chief worry in biometric validation. It needs the enhancement of novel as well as active safety methods. Contextual to finger impression recognition labels the biometric practice of finger impressions scanning is also done by biometric tools. The motive of the projected structure is to improve the safety of biometric verification structures, by including liveness validation in a speedy, easy and non-intrusive way, by the way of image validation. Image validation is categorized into full-reference and no-reference methods.

Full-Reference (FR) Image Quality Assessment approaches trust on the existence of a fresh accurate base image to evaluate the eminence of the test model. FR IQA comprises three kinds of measurements such as error sensitivity measures, structural likeness measures and information theoretic measures. No-Reference IQA measures do not need of an example structure to normalize the eminence level of an image. The measurement contains measures based on distortion, training and natural scene information. Then implement image fusion method to associate all biometric structures that comprises iris, face appearance and finger impression features. And finally QDA based classification technique can be implemented to conclude whether image is real or forged.

V. RESULTS AND DISCUSSION

A. Finger impression Recognition System:

Impression of all fingers of an individual person is deliberately distinctive; Twins even have dissimilar finger impression. Finger impression identification is the best classical biometric identification. Finger impressions are being implemented from long for recognizing persons. Finger impressions comprise of a series friction ridges and recessed on the pads of the fingers and thumbs. Now finger impression identification method is incorporated in mobile, and also it is employed everywhere abundantly.

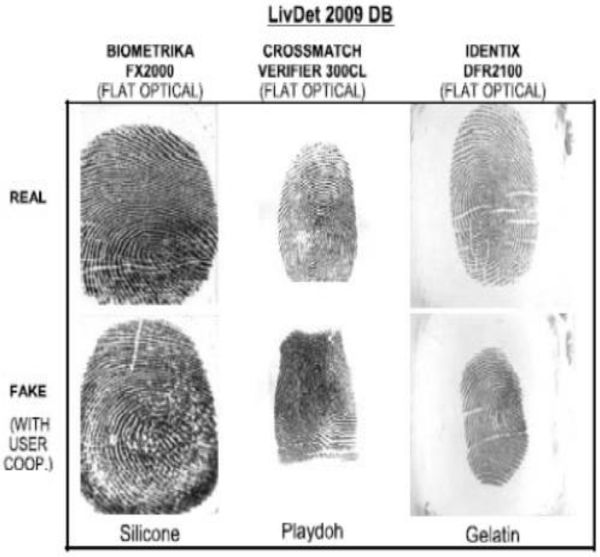
LivDet 2009 DB
BIOMETRIKA FX2000 (FLAT OPTICAL)
CROSSMATCH VERIFIER 300CL (FLAT OPTICAL)
IDENTIX DFR2100 (FLAT OPTICAL)
REAL
FAKE (WITH USER COOP.)
Silicone
Playdoh
Gelatin

Figure 3. Finger impression datasets

But muggers exploit on finger impression identification method. Impostors first preserve actual finger impression then they generate false finger impression by means of silicon, gelatin, playdoh and attempt to intrude the system.

B. Iris Identification Method:

Iris identification is a digitalized process of biometric recognition. It practices numerical typical identification procedures on individual eyes irises visual images. Those are distinct, random multidimensional configurations and being viewed from certain distance. Detection of a person's identity can be accomplished by Iris cameras. The iris recognitions practice to get image approximately on the film. It adds digital vision, statistical data, configuration of identity and optics.

Eye iris is the underlined ring around the pupil of every being and resembles a snowflake. All are unique. An attack on the iris is not so stress-free but how to violence on the system is as shown below. Iris is manipulated by three steps.

1) For the best quality, new images are captured

2) Images are produced on a dissertation by a feasible printer

3) At the iris sensor, printed images are presented.

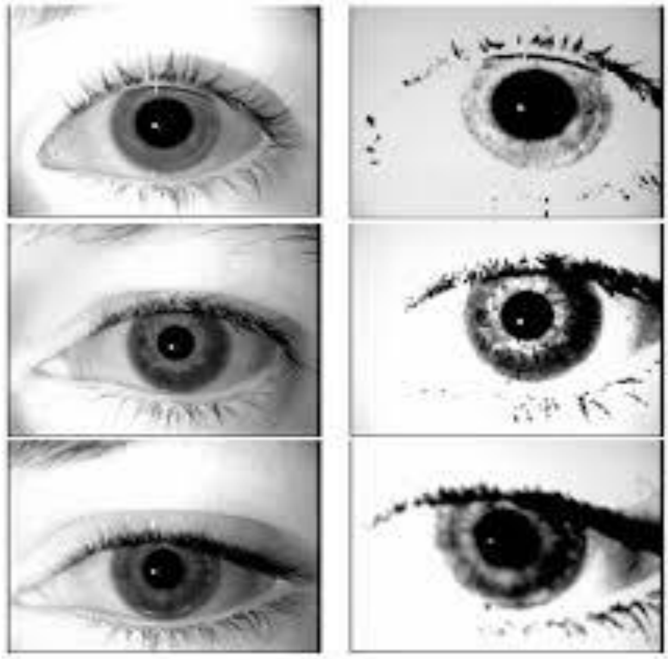

Figure 4. IRIS datasets

CASIA database is used to collect iris datasets and the images are in figure 4.

C. Face appearance Recognition System:

The best chosen biometrics is recognition of face appearance, since it is the most common procedures of records in which individuals employ visual communications and acquirement of face appearances. Face appearance identification methods create diverse among the contextual and appearance of the face. It is utmost considerable when a face appearance within a crowd is categorized by the system. It then generates a person's facial structures in terms of its heights, valleys, milestones and indulgences which are lumps and being equated and planned in contradiction of those deposited in arrangement's record.

About 80 lumps are encircling the face appearance print. It comprises the depth of eye orbit, muscular jaw line length, space between two eyes, outline of malar bone, and also size of the nose. This recognition method distinguishes the special markings of facial terminologies, oldness and minor differences in atmosphere of imaging.

Variation in the facial look identification structure is presented in the Figure 5. Figure depicts the forged and actual picture images and those pictures are discovered thro' different methods of identification. In the identification structure, false manipulators do malpractice on the system by impeding the image into the phone or camera and attempt to check. Possible states in face appearance database are displayed in figure 5.

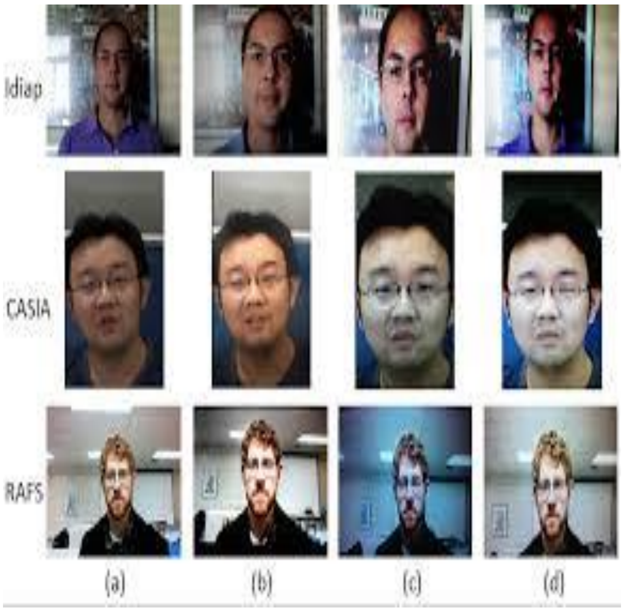

Figure 5. Face appearance datasets

The performance of the system is dignified using False Fake Rate and False Genuine Rate.

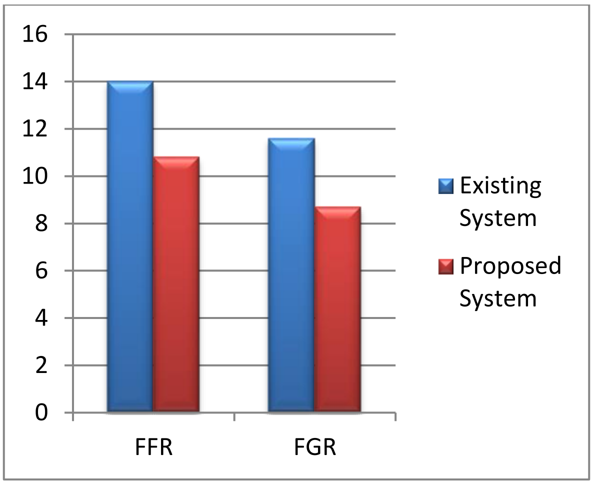

Figure 6. Performance evaluation

Compared to present system, our work provides reduced number of FFR and FGR. The graphical representation is exhibited in figure 6.

VI. CONCLUSION

Forged biometrics is identified through Image quality assessment. As a result of Image dimensions, it is modest to find out actual and forged users. Since false individualities often have certain dissimilar structures than the actual as it constantly enclosed dissimilar luminance, color points, common artifacts, evidence extent, magnitude of acuity, identified in both category of pictures and natural appearance or structural distortions. Multi-Biometric system is a thought-provoking method. It is further protected than Uni-biometric system. Multi- Biometric system can investigate multi modal biometric system with image fusion approach. Image fusion approach is implemented to combine both biometrics (finger impression and iris, iris and face appearance, face appearance and finger impression). It proves that image fusion technique can fuse all biometric features as in one image format. This method is implemented to improvise the confidence in database level. The dynamic IQA is a very encouraging technique in creating recognition system as it is more robust against fake based spoofing attempts to provide alert system and also to intimate mobile message to the person who are authorized by the system.

REFERENCES

[1]. 2014, Best-Rowden L., Han H., Otto C., Klare B., and Jain A. K., “Unconstrained face appearance recognition: Identifying a person of interest from a media collection,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157.

[2]. 2013, Evans N., Kinnunen T., and Yamagishi J., “Spoofing and countermeasures for automatic speaker verification,” in Proc. INTERSPEECH, pp. 925–929.

[3]. 2013, Erdogmus N. and Marcel S., “Spoofing in 2D face appearance recognition with 3D masks and anti-spoofing with Kinect,” in Proc. IEEE BTAS, pp. 1–6.

[4]. 2012, Galbally J., Alonso-Fernandez F., Fierrez J., and Ortega-Garcia J., “A high performance finger impression liveness detection method based on quality related features,” Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321.

[5]. 2012, Rattani A., Poh N., and Ross A., “Analysis of user-specific score characteristics for spoof biometric attacks,” in Proc. CVPR Workshops, pp. 124–129.

[6]. 2012, Chingovska I., Anjos A., and Marcel S., “On the effectiveness of local binary patterns in face appearance anti-spoofing,” in Proc. IEEE BIOSIG, pp. 1–7.

[7]. 2011, Bowyer K., Boult T., Kumar A., and Flynn P., Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press.

[8]. 2011, Zhang Z., Yi D., Lei Z., and Li S. Z., “Face appearance liveness detection by learning multispectral reflectance distributions,” in Proc. FG, pp. 436–441.

[9]. 2011, Anjos A. and Marcel S., “Counter-measures to photo attacks in face appearance recognition: A public database and a baseline,” in Proc. IJCB, pp. 1–7.

[10]. 2010, Galbally J., McCool C., Fierrez J., Marcel S., & Ortega-Garcia J., “On the

vulnerability of face appearance verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027–1038.

[11]. 2010, Tan X., Li Y., Liu J., and Jiang L., "Face appearance liveness detection from a single image with sparse low rank bilinear discriminative model," in Proc. ECCV, pp. 504–517.

[12]. 2009, ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792.

[13]. 2009, Marcialis G. L., Lewicke A., Tan B., Coli P., Grimberg D., Congiu A., "First international finger impression liveness detection competition— LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716, pp. 12–23.