ISSN 2395-1621

Implementation of Image Quality Assessment for Fake Biometric Detection for Face

[#1]Ms.Vandana Kumari, [#2]Ms. Priti Agarkhed, [#3]Ms.Shital Joshi,
[#4]Ms. Monika Kharasamble, [#5]Prof. Mrs. Savitri Patil

[1]kvandana767@gmail.com
[2]agarkhedpriti@gmail.com
[3]shitaljoshi13@gmail.com
[4]mkmonika90@gmail.com

[#12345]Department of Information Technology
G.H.R.C.E.M, Wagholi, Pune.

ABSTRACT

Biometric measures the human Characteristics. Biometric system includes finger print, Iris ,face Detection. Face Detection makes it possible to use the facial images of a person to authenticate him into secure system, for criminal identification, for passport verification etc. It is done by PCA(Principle component Analysis).Face Images are protected onto a face space that encodes best variation among known face images. In the algorithm, initially we preprocessing on that image after we apply for classification algorithm in this process we check different angle for face image. Finally we feature extract and analyse the input image is valid or not.

Keywords: Biometric System, Face Detection.

ARTICLE INFO

Article History

Received: 3rd June 2017

Received in revised form :

3rd June 2017

Accepted: 5th June 2017

Published online :

5th June 2017

I. INTRODUCTION

The In last few years, the study of image analysis and its use in face recognition applications has gained significant attention from the worldwide research community. Facial recognition is a popular research area in pattern recognition and computer vision due to its wide range of commercial and law enforcement applications, including passports, credit cards, drivers' licenses, biometric authentication, video surveillance, and information security.

These applications demands user- friendly automatic systems that can secure our assets and protect our privacy without losing our identity. Although researchers in various fields like psychology, neural sciences and engineering, image processing and computer vision have investigated a number of issues related to personal identification and machines, it is still difficult to design an automatic system for this task.

Although extremely reliable methods of biometric personal identification exists, e.g., fingerprint analysis and retinal or iris scans, these methods have yet to gain acceptance from the general population. Thus, facial recognition is a very challenging problem and, to date, there is no technique that provides a robust solution to all situations and different applications that facial recognition may encounter.

In addition, the applications involve a huge number of situations. Although there are many other identification and verification techniques, the main motivation for facial recognition is because it is considered a passive, nonintrusive system for verifying and identifying people. Other types of identification include password, PIN (personal identification number) or token systems, use of fingerprints and iris as a physiological identification system. They are very useful when we need an active identification system; where a person has to expose their body to some device to scan and identify them.
For bank transactions and security areas, a pause-and declare interaction is the best method of identification, where people feel conscious, comfortable and safe with it. However, sometimes in cases like a store that wishes to recognize customers or a house that has to identify people that live there, we need not interact with people for identification purposes. For such applications, facial as well as voice verification are very desirable.

Face recognition technique:

Feature-based approaches: Facial recognition based on feature-based approaches relies on the detection and characterization of individual facial features and their geometrical relationships. Such features generally include the eyes, nose, and mouth. The detection of faces and their

features prior to performing verification or recognition makes these approaches robust to positional variations of the faces in the input image.

Holistic or global approaches: Facial recognition based on holistic approaches, on the other hand, involves encoding the entire facial image and treating the resulting facial "code" as a point in a high dimensional space. Here, it is assumed that all faces are constrained to particular positions, orientations, and scales.

II. PROBLEM STATEMENT

The normal operation scenario for which the sensor was designed. "Image quality is a characteristic of an image that measures the perceived image degradation (typically, compared to an ideal or perfect image). Imaging systems may introduce some amounts of distortion or noises in the signal, so the quality assessment is an important problem.

III. LITERATURE SURVEY

Javier Galbally, Sébastien Marcel,Member, IEEE, and Julian Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, fingerprint, and Face Recognition," 2015, in this paper, approach presents a very low degree of complexity, which makes it suitable for real- time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D face.

Rohit Kumar, Vishal Moyal, Visual Image Quality Assessment Technique using FSIM, 2013, the experimental results show that the image quality assessment method has a higher accuracy than traditional method and it can accurately reflect the image visual perception of the human eye. In this paper, he propose an image information measure that quantifies the information that is present in the reference image and how much of this reference information can be extracted from the distorted image. The use of image quality assessment for liveness detection is motivated by the assumption that: "It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in

Valerio Mura, Luca Ghiani, Gian Luca Marcialis, Fabio Roli, "LivDet 2015 Fingerprint Liveness Detection Competition", 2015, the Fingerprint Liveness Detection Competition (LivDet) goal is to compare both software-based and hardware-based fingerprint liveness detection methodologies. The competition is open to all academic and industrial institutions. The number of competitors grows at every LivDet edition demonstrating a growing interest in the area.

IV. PROPOSED WORK

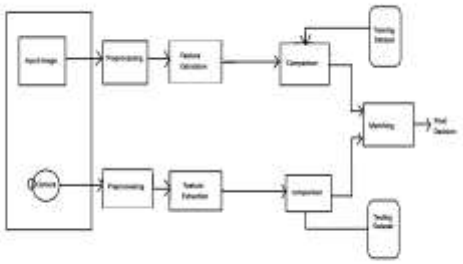

Fig 1. System architecture

A digital image or a video frame from a video source a person can be identified through the face recognition system. This can be done by comparing selected facial features from the image and a facial database. For this purpose PCA is used. This algorithm identifies facial features by extracting landmarks, or features, from an image of the subject's face. These features are then used to search for other images with matching features.

Image quality assessment for detection technique is used to detect the fake image detection. Due to Image quality measurements it is easy to find out real and fake users because fake identities always have some different features than original it always contain different color and luminance, artifacts, quantity of information, and quantity of sharpness, found on both type of images, structural distortions or natural appearance.

The system application is widely used for facial recognition system, there is a tremendous scope in India. This system can be effectively used in ATM's ,identifying duplicate voters, passport and visa verification, driving license verification, in defense, competitive and other exams, in governments and private sectors.

Proposed flow:

Step 1: Read the Test Image from the database we also can implement live face detection using webcam.

Step 2: Fond selected Image Quality Measures for the test image. Example: peak signal to noise ratio, average difference, maximum difference and other quality features.

Step 3: Combine all Quality Measure as a feature.

Step 4: Feature compared with trained Feature using classification.

Step 5: Final result given test image is fake or real image.

V. APPLICATION

- Office for authentication
- It can be used in many industries for security purpose
- This application used in voting system
- It is used in Bank and Medicals

- This application is used in aeronautical fields for high level security purpose
- Vehicle Security
- Research LABs security
- Military Applications
- Industrial Security

V. CONCLUSION

Image quality assessment for detection technique is used to detect the fake image detection. Due to Image quality measurements it is easy to find out real and fake users.

REFERENCES

[1] Javier Galbally, Sebastian Marce, and Julian Fierrezvol, Image Quality Assessment for Fake Biometric Detection: Application to Iris, fingerprint, and Face Recognition,IEEE transactions on image processing vol.23, no. 2, February 2015.

[2] Rohit Kumar CsvtubhilaiSscetbhilai India, Vishal MoyalCsvtubhilaiscetbhilai, Visual Image Quality Assessment Technique using FSIM, Vol.2– Issue 3, 250 - 254, 2013.

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

[4] A. K. Jaon, K. Nandakumar, and A. Nagar, Biometric template security, EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan, 2008.

[5] J. Galbally, F. AlonsoFernandez, J. Fierrez, and J. Ortega-Garcia, A high performance fingerprint liveness detection methods based on quality related features, Future Generat. Comput.Syst., vol. 28, no. 1, pp. 311–321, 2012.

[6] K. A. Nixon, V. Aimale, and R. K. Rowe, Spoof detection schemes, Handbook of Biometrics. New York, NY, USA: Spronger- Verlag,pp. 403–423, 2008.

