Assessment and Improvement of Image Quality using Biometric Techniques for Face Recognition

Rupali Patil[1], Prof. Aarti Deshpande[2]
[1]Dept.-Computer Engineering, G. H. Raisoni College Of Engineering, Pune, India
[2]Dept.-Computer Engineering,G. H. Raisoni College Of Engineering,
Pune, India

ABSTRACT

Biometrics is broadly used in Forensic, highly secured control access and prison security. By making use of this system one can recognizes a person by determining the authentication by his or her biological and physiological features such as Fingerprint, retina-scan, iris scans and face recognition. The determination of the characteristic function of quality and match scores shows that a careful selection of complimentary sets of quality metrics can provide much more benefit to various benefits of biometric quality. Face recognition is a challenging approach to the image quality analysis and many more security applications. Biometric face recognition is the well known technology which is used by the government and civilian applications such Aadhar cards, Pan cards etc. Face recognition is a Behavioral and physiological feature of a human being. Nowadays the quality of an biometric image is the measure concern. There are many factors which are directly or indirectly affects on the image quality hence improvement in image quality has to be done by making the use of some biometric techniques for face recongnion.This paper presents some important techniques for fake biometric detection and improvement of facial image quality.

Keywords: *Image quality assessment, biometrics, face recognition.*

I. INTRODUCTION

Biometric is the various famous method of recognizing a human being depending upon their physiological and behavioral features .There are various features used for identification and verification purpose such as face recognition, iris scan, fingerprint, retina scan etc. But here we only concentrated on face recognition. The face recognition is the most recognized biometric technologies. There is need of higher level of identification of verification for managing the higher level of security. There are various incidents happens which leads to increase in the biometric technique. There various areas where we can use the biometric system or we can say it as the face recognition system for security purpose or for the fake detection such as airports, railway stations, ATMs, international banks etc.

The biometric means the term which is used for the unique identification. For achieving this purpose there may be some characteristics are used which are mainly depending upon the physiological behavior. They can be universal, invariance of properties, measurability, singularity, Acceptance, Reducibility, Reliability and tamper-resistance, privacy etc .By making the use of biometric face recognition technique we can achieve the high universality, uniqueness. Spatial geometry which is unique features of face which is recorded by face recognition. The 2d face is affected by the conditions of light, age, wearing glasses (someone wear glasses).There are various steps which includes face recongnion such as capture image, locate correct face, detect the face, recognize the face and finally identify the person. There are some functions which is considered for recognition such as pose estimation, part detection, trait classification. We can identify faces by making the use of some specific patterns. It means we can divide the facial image into certain pattern and then we can fix that image into certain pattern and we can immediately identify the image which is claim to be. The pattern may be binary pattern and we can divide the particular image into the pixel or we can have the matrix of an image also we can have the graph of an image by making the use of graph we can identify the closest part of an image.

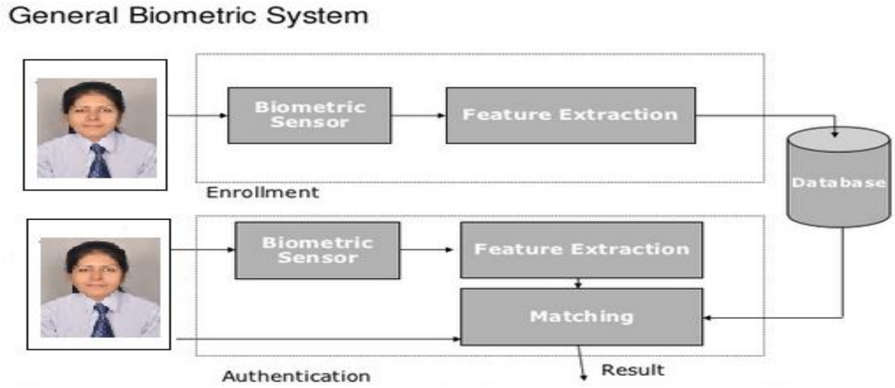

Figure 1: Basic Biometric System Related to Face

The one of the most important challenge in image quality of biometric system or facial biometric system is the performance degradation. There is another important factor which also degrades the performance. The examples of performance degradation of the face recognition in the uncontrolled illumination conditions and different image compression methods for the controlled conditions. In the case of face recognition the performance degradation may be cause by making the use of web cam image because that image may be causing or having the outdoor environment such as different day-night lightening conditions. When we are talking about the biometric sample quality, there are some biometric sample quality components can be used such as character, fidelity and utility .These components are used for the better verification and identication of a facial image. The factors which are related to signal quality of a biometric system are directly referenced to the users, user interactions, the acquisition sensors and the system. There is an effective algorithm for improvement of the signal quality of an facial image for the capture point design also system design. There is an algorithm which is Quality Assessment Algorithm which is used for measuring the properties of facial image such as brightness, contrast, background, uniformity, resolution, focus, frontlines etc.

II. APPLICATIONS

Two primary tasks used for face recognition are –

1. Verification(one-to-one matching)
2. Identification (on-to-many matching)

Verification task ascertains the individual user who claims of identity with an image of his face. The identification task compares and encodes input image with an image in the database for the known users.
There are many applications which use this technology for face recognition –
Security – In offices, Airports, ATM etc
Surveillance - CCTVs
General Identification System – Banking, Passport, Driving License
Image Database Investigations – Missing Children

III. LITERATURE SURVEY

Facial biometrics determines the identity of a person by using his/her physiological or behavioral characteristics. In wavelet based face recognition presents varying illumination.

- **a.** Wavelet Transforms (WTs) – This divides a signal into low and high frequency components. It provides a multi-resolution analysis of the signal.
- **b.** WTs in face recognition – A sub-band of wavelet transformed face image are used as face feature descriptor. It is used to reduce image dimension before statistical reduction techniques as PCA and LDA.

Image quality based adaptive face recognition investigates the use of image quality measure using the techniques such as universal quality index, image quality based adaptive normalization, fusion global LQ and region LQ indexes. The intensity component of the famous universal quality index given to provided a quantitative quality value to an image. This measure is called the LQ index that measures its luminance and it was used to develop global and region quality-based adaptive illumination normalization procedures.
The inspection that the wavelet-based multi-stream recognition scheme that was developed previously has no objective means of selecting fusion parameters. This has led in developing of a new adaptive approach to face recognition [2].

The performance of the IQA-based protection method has been tested on a face spoofing database: the REPLAY-ATTACK DB which is available from the IDIAP Research Institute. The recordings were carried out under two different conditions: controlled and adverse. Images from 3 different sources were taken viz. Printer, Mobile and High Definition Camera. Access attempts were noted in two modes depending on the strategy followed to hold the attack replay device (paper, mobile phone or tablet): i) hand-based and ii) fixed-support. This makes the DB a benchmark for testing anti-spoofing techniques in face-based systems. Some inequalities between the real and fake images can be observed after images getting translated to proper feature space. This is because the biometric traits have their own optical qualities like refraction and absorption. The properties of image quality are different in real and fake accesses. The proposed method is able to -

Consistently perform at a high level for different biometric traits, adapt to different types of attacks providing protection, generalize well to different databases, acquisition conditions and attack scenarios, the error rates achieved by the proposed protection scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested in the framework of different independent competitions, presents some other very attractive features such as: it is simple, fast, non-intrusive, user-friendly and cheap, all of them very desirable properties in a practical protection system [1].

There are different reasons for data uncertainty such as inaccurate measurement and sampling errors. Methods of processing such data include data mining, data clustering and uncertain data management. The original training samples were broken to create virtual training samples and proposed a scheme of selecting and exploiting useful training samples from BTSS to represent and classify a test sample. This scheme is helpful for eliminating the improper training samples which have side effect on classification of the test sample, and thus can improve the recognition accuracy. The experiment results with right choice of the number of useful training samples which is beneficial for better recognition. We will deal with the problem of mechanically selecting the most appropriate number of useful training samples for the test sample in the future [3].

A new approach is offered to prevent image attacks, which is categorized as a method in the first group. A fake detection approach is proposed which can be applied to detect image attacks by new techniques, building access control solutions for different consumer electronics without using additional tools or user interactions. Background motion index (BMI) gives the amount of motion in the background region compared with the foreground region. It indicates motion occurrence in the background compared with that in the foreground region. We assume that the location of the image is correctly determined by the face detector. The performance of the system can be improved by more refined object detection approach. For future research, a cheap and accurate method of foreground-object extraction will be studied to improve the performance of the system to build various access-control solutions for consumer electronics [4].

The study of face recognition describes the large scale analysis by using different demographics such as age,gender,ethinicity or we can called it as race. For all these demographics there are six different types of algorithm for the face recognition depending upon the three systems i.e. the first one is the three commercial off the shelf(COTS) face recognition system, the second one is the face recognition algorithm that do not utilize training data and the third one is the trainable face recognition algorithm. There are number of face images provided by the face databases for the studies of demographics such as age,gender,ethinicity.The first algorithm i.e. Commercial Face Recognition Algorithm describes about the neurology,pittpatetc.The second algorithm i.e. Non Trainable Face Recognition Algorithm describes the local binary patterns and the Gabor features. The third algorithm i.e. Trainable Face Recognition Algorithm describes the spectrally sampled structural subspace features which is also called as 4SF.The analysis of having the similar demographic characteristics have difficult such as having black colour,twins.The training data set algorithm is efficient way to improve the design of face recognition algorithm[5].

IV. PROPOSED SYSTEM

In this context, the present work has made several contributions to the state-of-the-art in the field of biometric security. It has shown the high potential of image quality assessment for securing biometric systems against a variety of attacks. The proposal has been accepted and validation of a new biometric protection method is used. The reproducible evaluation on multiple biometric traits based on publicly available databases is very essential to use. The comparative results with other previously proposed protection solutions are better. The present research also opens new possibilities for future work, including extension of the considered 25-feature set with new image quality measures; ii) further evaluation on other image-based modalities (e.g., palm print, hand geometry, vein);iii)inclusion of temporal information for those cases in which it is available (e.g., systems working with face videos); iv) use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB); v) analysis of the features individual relevance. Also since we are going to use machine learning for training the system to recognize the real and fake for that we will be using Naive Bayes classifier algorithm to classify the training data and form rules so at to give added information to the system and making it more generic.

The following fig shows the block diagram of the proposed system.

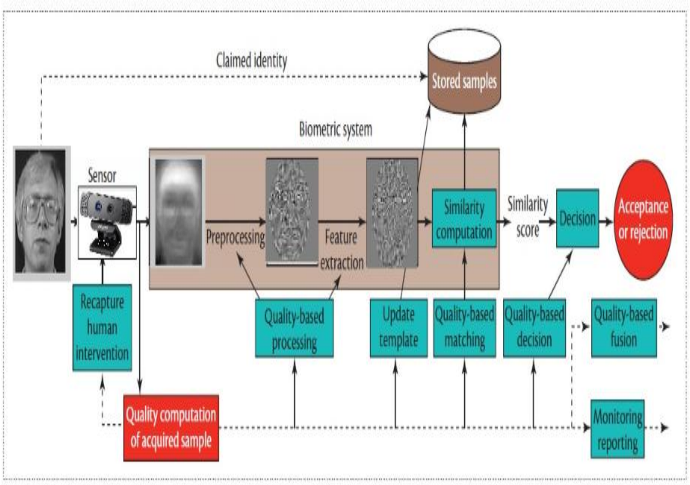

Figure 2: Block Diagram of Proposed System.

The main goal of our proposed system is to improve the quality of an facial image and by making the use of biometric technique recognize the actual facial image weather it is the fake or real.
The block diagram shows above features i.e quality assessment and recognition of face.

The block diagram describes

a) Recapture Human Intervention

The biometric system block does the identification of an image and the remaining part does the quality measurement. In the given fig the recapture of the loop.

b) Quality Based Processing

Exacted the features from the valid region only means that only useful face is used means avoiding the unnecessary region of our body. Define the conditional execution of the facial image for the performance degradation means that check whether the any lighting condition
or image resolution affects on the image quality or not. Fix the rating or raking of the feature extraction which is based on the local regions only.

c) Update Template

In the template updating the database maintenance is very important. In this the storage of different samples is require which may be variation of different poses of an face .And during the system operation the updating of the stored samples to achieve the better quality.

d) Quality Based Matching:

We can apply the different algorithms for the quality based mathching.e.g: Baysian Algorithm.

e) Quality Based Decision

In the quality based decision the difference between the real facial image quality or actual real time facial image quality is measured and valid decision is taken.

f) Quality Based Fusion

The quality based fusion includes selection of the data sources which is use for the matching purpose depending upon the soft biometric trait. The soft biometric trait includes age, height, gender, color etc.

g) Monitoring and Measuring

In this we can know the problems related to the poor quality and we can take the corrective actions depending upon which problems has occurred and which problems are going to be occurred. The monitoring and measuring includes the applications, terminal or site, capturing device, subject, template which is stored ,biometric input. The application includes the environmental setups, various scanners which may affect on the signal quality. The capture device includes the appearance of the specific image and impact due the various acquisition purposes. Terminal or site includes the operational and environmental conditions. Subject is used for better training of the new user. By making the use of stored template we can identify how the database quality varies in the creation of new template and updating of an old template. Biometric input includes if the particular system uses the different biometric traits then the assessment should improve the combination of those traits.

V. CONCLUSION

In this context, the present work has made several contributions to the state-of-the-art in the field of biometric security, in particular: i) it has shown the high potential of image quality assessment for securing biometric systems against a variety of attacks; ii) proposal and validation of a new biometric protection method; iii) reproducible evaluation on multiple biometric traits based on publicly available databases; iv) comparative results with other previously proposed protection solutions. The present research also opens new possibilities for future work, including: i) extension of the considered 25-feature set with new image quality measures; ii) further evaluation on other image-based modalities (e.g., palmprint, hand geometry, vein); iii) inclusion of temporal information for those cases in which it is violable (e.g., systems working with face videos); iv) use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB); v) analysis of the features individual relevance.

REFERENCES

[1]. Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez," Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition" Ieee Transactions On Image Processing, Vol.23,

[2]. No.2, February 2014.

[3]. Harin Sellahewa and Sabah A. Jassim "Image Quality Based Adaptive Face Recognition", Ieee Transactions On Instrumentation And Measurement, Vol. 59, No. 4, April 2010.

[4]. Yong Xu, Member, IEEE, Xiaozhao Fang, Xuelong Li, Fellow, IEEE, Jiang Yang, Member, IE Jane You, Hong Liu, and Shaohua Teng "Data Uncertainty in Face Recognition",Ieee Transactions On Cybernetics.

[5]. Younghwan Kim, Jang-Hee Yoo, Member, IEEE, and Kyoungho Choi, Member, IEEE "A Motion and Similarity-Based Fake Detection Method for Biometric Face Recognition Systems",IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.

[6]. Brendan F. Klare, Member, Ieee, Mark J. Burge, Senior Member, Ieee, Joshua C. Klontz,Richard W. Vorder Bruegge, Member, Ieee, And Anil K. Jain, Fellow, Ieee "Face Recognition Performance: Role Of Demographic Information" Ieee Transactions On Information Forensics And Security, Vol. 7, No. 6, December 2012.