Assessment of Image Quality in Face, Fingerprint, Iris, Palm print and Knuckle point for Detection of Fake Biometrics

Arya J L
M.Tech, Applid Electronic and Instrumentation
Department of ECE
Younus College of engineering and technology
Kollam, Kerala

Safuvan T
Assistant Professor
Department of ECE
Younus College of engineering and technology
,Kollam, Kerala

***Abstract*—Biometric system is a computer system, which identifies a person based on there behavioural and physiological triat . In this paper, different physiological characteristics of a person is combined to detect different attacks,so obtaining a high accuracy. Typical biometric system consist of sensing, feature extraction and matching modules. Nowadays, several attacks are detected by using fake biometrics. A new software based fake detetion method,that can be used in multiple biometric systems for detecting various types of fraudulent access attempts are presented in this paper.There are several techniques which can be measured automatically evaluated by a computer program,so that they are classified as univariate and bivariate measures. Liveness detection method is introduced in a fast,user friendly and non intrusive manner through the use of certain univariate measures and 25 bivariate measures a extracted from one image to distinguish between legitimate and impostor samples. The proposed method is highly competitive compared to other existing approaches.**

Keywords-Image quality assessment,biometrics,attacks,security.

I. INTRODUCTION

Biometrics is the science and technology of measuring and statistically analyzing human body characteristics such as fingerprints,eye retinas and irises,voice patterns,facial patterns and hand measurements mainly for authentication purposes. In fake biometrics,real images captured from a printed paper and fingerprint captured from a dummy finger of human identification characteristics are used to create the fake identities. Invader produces the fake sample for authentication by capturing the original identities of the genuine users. Biometric system is more secure as it have several methods to detect the fake users. Nowadays, numerous and diverse initiatives are created for ensuring the security of the biometric system. These initiatives exactly features the importance given by all parties involved in the development of the security of the systems for bringing the rapidly emerging technology into practical use. Direct or spoofing attacks encourages the study against different fraudulent attempts.in these attacks,in these attacks, Invader may produce synthetically produced artifact (eg:gummy finger,printed iris image or face mask)or or imitate the behaviour of the genuine user (eg:gait,signature) to access the biometric sytem fraudulently. Usual digital protection mechanisms are not effective as the attacks are performed in the analog domain and the interaction with the device is done by using regular protocol.

Biometric system is more secure than other security methods like password, PIN or card and key ,because each person have their unique characteristics identification..Multibiometric systems which is more secure than single biometric system recognizes personel authentication by using multiple source of information .Fake and real samples may contain predictable different quality acquisitions like colour, luminance level,general artifacts,quantity of informations and quality of sharpness etc. Iris images captured from a printed paper are likely to be fuzzy and face images captured from a mobile device will be under discovered. Image quality assessment is considered as a major topic in image processing area.large range of distortions are produced in digital images during storage,achievement,compression,processing,transmission,and reproduction. Subjective visual quality assessment and objective visual quality assessment are two divisions of general image quality assessment. .

Fig.1. Fake Iris

These studies are very essential to propose and develop specific protection methods against this threat.various techniques are developed which enables biometric system to

detect fake samples and reject them, thus improving the robustness and security level of the system.

II. LIVENESS DETECTION METHODS

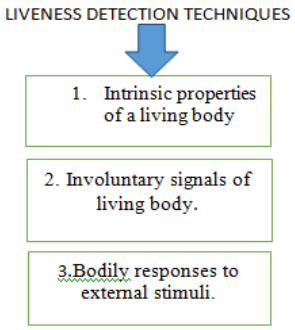


Fig.2. Liveness detection

Liveness detection methods are classified into two types generally.(i)*software based* techniques in this type,fake character is detected once the sample has been acquired with a normal sensor.(ii)*hardware based* techniques ,which adds some particular device to the sensor for detecting actual properties of a living character.

Different physiological and behavioural properties of human are used to differentiate between real and fake character. Certain challenging requirements are to be satisfied by the liveness assessment methods ,which is considered as a difficult engineering problem.(i) Non-invasive,which requires excessive contact with the user. (ii)User friendly,people should not hesitant to use it.(iii) Fast,results have to be produced in a very short interval of time.(iv)Low cost,large use cannot be expected if the cost is high.(v)Performance,in addition to good fake detection rate, False rejection is also necessary. Each of these methods have certain advantages and disadvantages. A combination of both would be the most advantageous protection approach to increase the security of the systems.

Hardware based schemes presents very high fake detection rate,but software based techniques are generally less expensive and less intrusive. Software based techniques are capable of detecting various illegal break-in attempts,as it is embedded in the feature extraction module.

III. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

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 the normal operation scenario for which the sensor was designed.*"

Quality differences between real and fake samples may include : degree of sharpness,colour,and luminance levels,local artifacts,amount of information found in both type of images (entropy),structural distortions or natural appearance.iris images captured from a printed paper are seen to be unclear or out of focus due to trembling,while,face images captured from a mobile device may be over or under-exposed.Fingerprint images captured from a gummy finger shows local gaining artifacts like spots and patches.unnaturally produced image is directly injected to the communication channel before the feature extractor in case of ultimate attack. Different quality measures are having diverse and sensitivity additional to additive noise ,while others such as the spectral phase error are extra sensitive to blur;whilegradient related features responds to distortions concentrated around edges and textures. Large range of IQMs exploits complimentary image quality properties which detects quality differences between real and fake samples expected to be found in many attack attempts . the main concept behind this is the presence of 'quality differences' theory between real and fake samples.

IV. COMPARISON RATE MEASURES

five important inter-related measures that govern the performance of general biometric system are .

(i)Penetration rate : it can be defined as the average ratio of the number of finger prints in a class to the total number of samples in a database. Lower penetration rate implies faster searching, for eg; fingerprints.

If q_i represents the ratio of number of finger prints in class to the total number of samples in database and p_i is the class occurrence probability ,the penetration rate is calculated by $\sum p_i q_i$

(ii)Bin error rate : probability that a search for the matching template in the database will be unsuccessful because the sample and template were erroneously placed in different "bins".

(iii)Single comparison false-non match rate : probability that a truly matching template will be missed.

(iv)Single comparison false match rate: Probability that an impostor template will be incorrectly matched to a sample.

(v) Comparison rate: (sample template comparison per unit time) of the hardware ,perhaps averaged over a time period long enough to include system availability considered.

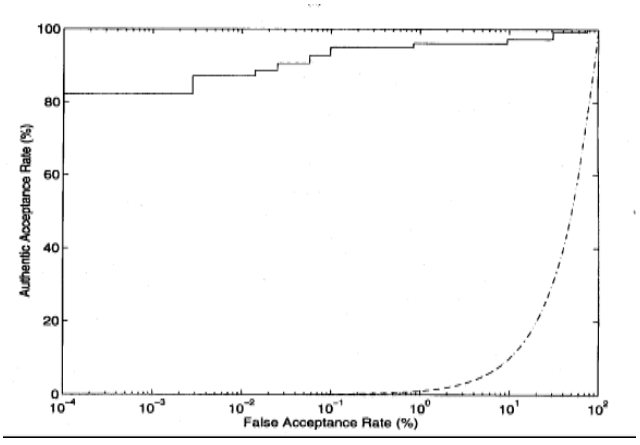


Fig.3. Comparison rate measure.

V. MULTI-BIOMETRIC SYSTEM

Most real-life biometrics systems are unimodal biometric system,which performs person recognition based on single source of biometric information . Multibiometric systems are very difficult to hack as one cannot obtain two features of same individuals. Multibiometric overcomes noisy sensor data, non-universality and spoof attacks .These are fusion of two or more unimodal biometric systems, which are expected to be more reliable due to the presence of multiple pieces of evidence. This paper presents a multibiometric recognition system using fingerprint ,iris ,face, knuckle point, and palm print., preprocessing extracts region of interest from each biometric image and feature vectors are collected from each biometrics separately. Matching scores for each biometric samples are extracted from corresponding templates. A unique matching score is obtained by combining the three different matching scores , based on which final decision is made.

A. Iris identification system

Iris recognition is one of the most accurate biometric technology, commercially in use today,where false-match and false non-match errors are very small, which implies a very high accuracy.

Iris identification system consist of 3 stages: (1) Iris analysis, involves iris localization and iris normalization .(2) feature extraction and encoding .(3) recognition stage involves identification and verification ..

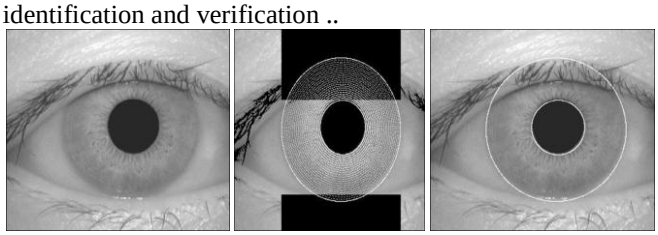
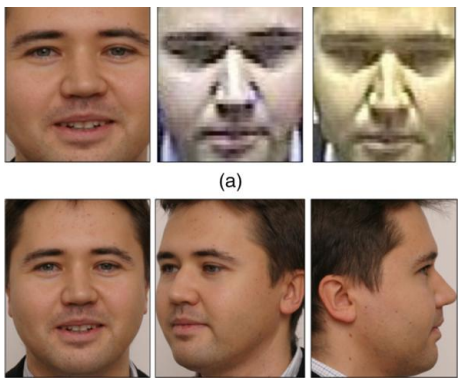


Fig. 4. A Sample of iris image with the corresponding segmented and normalized image

B. Face recognition system

It identifies or varifies a person from a digital image or a video frame from a video source automatically.some ac recognition algorithms identify facial features by extracting land marks from an image of subject's .



(a)

Fig.4. image quality vs biometric quality a)poor quality b)poor biometric quality

Relative position,,size and shape of the eyes,nose, checkbones and jaw are analyzed by algorithm and these features can be used to search for other images with matching features.

C. Fingure print recognition system

Fingerprint analysis ,also known as dactylography , in US,is the science of using fingerprints for recognizing an individual.Palms and soles contains distinguishing epidermal patterns ,identical twins even have contradictory fingerprint patterns.

There are three basic categories of finger print: visible print,like those made in oil,ink or blood. Latent prints are not seen under normal conditions. Powders and chemicals such as iodine,digital imaging,dye strains and fumes are used for collecting prints. Lasers can also be used.

Fig. 5. Fingerprint Sample

D. Palmprint identification system

Personal verification based on palm print has quickly entered biometric family due to its easiness in the acquisition ,high class acceptance and reliability. Besides an unique information available as an fingerprint has far more amount of details in terms of principal lines,wrinkles and creases.

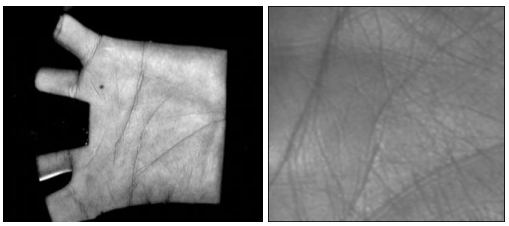


Fig.6. A sample of palm print image and corresponding region of interest

E Finger knuckle print identification system

In biometrics , lots of promising results are generated by the usage of finger-knuckle images for personal identification Finger-knuckle of the human hand are characterized by the creases which differs from person to person.

In the proposed technique, a preprocessed image is used and the features are extracted from the finger knuckle image. LDA is performed to extract only the significant features from the finger knuckle image.

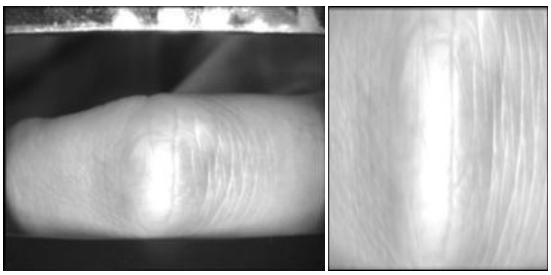


Fig.7. Knuckle point image and corresponding region of interest

VI. SECURITY PROTECTION METHOD

Real and fake are the two samples to which the input biometric sample has to be assigned. A set of discriminent features is introduced ,which permits to build an appropriate classifier which gives the image 'realism'.system needs only one input to hold its generality and simplicity.It does not require pre processing steps as the method operates on the whole image without searching any triat-specifying properties,which minimizes computational load. Linear Discriminent Analysis and Quadratic Discriminent Analysis classifiers are used for classifying the image into real and fake samples. IQMs are derived from the initial feature selection criteria. These four selection crierias are

Performance: Image quality measuures showing good performance are only considered.

Complimentarity. IQMs based on complimentary properties of the image can be used for generating attack detection system.

Complexity. For preventing high computational load,low complexity features are preferred.

Speed. Users should not kept wait for a response from the recognition system,which assures a user-friendly non-intrusive application .

VII. RESULTS AND DISCUSSION

Performance of biometric recognition system is measured by False Acceptance Rate(FAR) and False Rejection Rate(FRR) or Genuine Acceptance Rate(GAR).Proposed system have high GAR,corresponding low False Acceptance Rate,False Rejection Rate and Total Error Rate

$$FAR\% = \frac{false\ acceptance\ numbers}{no\ of\ impostor\ \ samples} \times 100\%$$

$$FRR\% = \frac{false\ rejection\ \ numbers}{no\ of\ client\ \ tests} \times 100\%$$

$$GAR(\%)=100- FRR(\%)$$

These rates are very important while considering its performance.

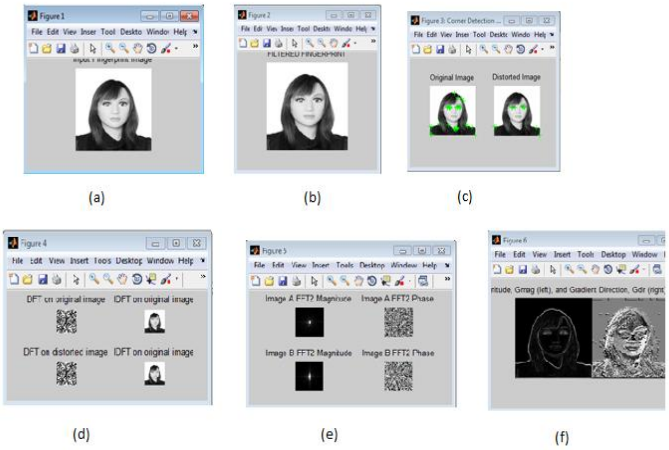


Fig.8. a) Input fingerprint image b) Filtered fingerprint c) corner detection result d) DFT and IDFT of original and distorted image e) FFT phase of image f) Gmag and Gdir using sobel method

In this experiment, two triats of an individual are combined to form a single image .by doing this kind of an experiment, it is ensured that it will be difficult for an impostor to attack the system.

First set of experiments are based on testing the physiological triats like fingerprint, face and iris of an individual .most most importantly,the original input image is filtered and the features are extracted from the region of interest. Images can be classified into two classes, say real and fake. Based on the univariate and bivariate measures,images are classified with high accuracy.

Fig7 shows the fingerprint recognition output, where the fingerprint sample is loaded, filtered, and feature vectors are extracted and classified with suitable accuracy.

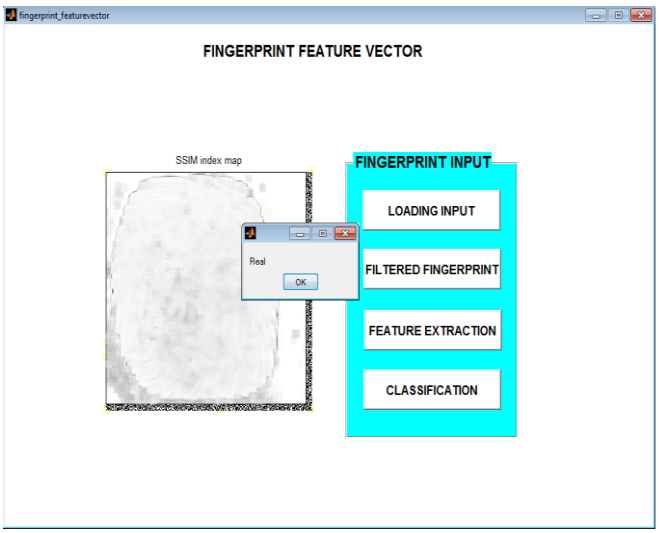


Fig.9. Finger print feature vector extraction and classification

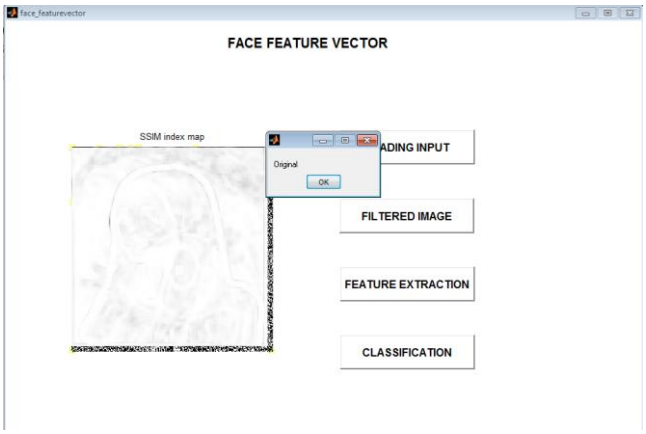


Fig 10. Face feature vector output using combination of face and iris input

VIII . CONCLUSION

In recent years, several security enhancing technologies are developed to study the vulnerabilities of biometric system against different types of attacks . it became a challenging task to develop efficient protection method , against known threat.

Real and fake samples of the same triat seen to be very similar and even the human eye may find it difficult to make a distinction between them. So that these images are translated into a proper feature space for obtaining disparities between the real and fake images. Ie, biometric triats as 3D objects have optical qualities , which other synthetically produced artifact do not posess. Inorder to obtain the 'quality difference' hypothesis , general image quality assessment is employed, which considers a feature space of various univariate and bivariate features,which is combined withsimple classifiers to detect real and fake attempts. Multiple biometric modalities like fingerprint, face,iris, palmprint and knuckle print are used along with the usage of fusion of two biometric modalities.

Conclusions obtained from the result are presented as follows:- i) It proposes high level of different biometric triats ii) Able to adapt to different types of attacks. iii) Generalization to different databases ,acquisition conditions and attack scenarios iv) Error rates are very low compared to other approaches.v) Proposed method is simple, fast, non – intrusive, user friendly and cheap besides its competitive performance ,and its 'multi-biometric' and 'multi-attack' characteristics.

Several contributions have been made by the present work to the field of biometric security, in particular :

i) Biometric systems are secured against a vereity ofattacks because of the high potential in image quality assessment.

.ii) new biometric detection method are proposed and validated.

iii) evaluation of multiple biometric triats based on publicly available databases are reproducible.

iv)it shows comparative results with other previously proposed protection solutions

REFERENCES

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

[2] International Journal of Computer Applications Technology and Research Volume 2– Issue 3, 250 - 254, 2013 www.ijcat.com 250 Visual Quality Assessment Technique using FSIM Rohit Kumar Csvtu bhilai Sscet bhilai India, Vishal Moyal Csvtu bhilai Sscet bhilai India.

[3] Image Quality Assessment Technique using FSIM Rohit Kumar Csvtu bhilai Sscet bhilai India, Vishal Moyal Csvtu bhilai Sscet bhilai India.

[4] A. Ross," An Introduction to Multibiometrics",appeared in proc.of the 15th European Signal Processing (EUSIPCO), September 2007.

[5] A. Ross, K. Nandakumar, and A. K. Jain. Handbook of Multibiometrics. Springer, New York, USA, 1st edition, 2006

[6] A. Ross, and A. K. Jain, "Information Fusion in Biometrics". Pattern Recognition Letters, 2003

[7] M. Faundez-Zanuy, "Data fusion in biometrics". IEEE Aerospace.

[8] X. Wang, J. Yang, X. Teng, W. Xia and B. Jensen, "Feature selection based on rough sets and particle swarm optimization". Pattern Recognition Letters, vol. 28. pp. 459–471. (2007).

[9] O. M. Aly, T. A. Mohamed, G. I. Salama, H. M. Onsi, "An Adaptive Multimodal Biometrics System using PSO". International Journal of Advanced Computer Science and Applications, vol. 4, no. 7, 2013.

,

.

-