International Journal For Technological Research In Engineering
Volume 3, Issue 8, April-2016 *ISSN (Online): 2347 - 4718*

IMPLEMENTATION OF BIOMETRIC RECOGNITION SYSTEM FOR FINGERPRINT, IRIS AND FACE

Mohd. Sarfaraj Shaikh[1], Prof. Ashutosh Gupta[2]
[1]PG Student, [2]Assistant Professor, Electronics & Communication Department, RKDF College of Engineering, Bhopal, India

ABSTRACT: ***We have to make sure actual presence of a real legal feature in response to a fake reconstructed sample which is important problem in biometric authentication, which can be resolved with the development of new ,efficient and effective protection measures. In this process we apply a software detection method which is a fake which can be used in multiple biometric systems which help in detecting different types of fake access attempt. The main aim and objective of this system is that the biometric recognition security must be enhanced by improving livens assessment in a fast, which must be user friendly, which are not interfering and disturbing with the help of image quality assessment. The present approach has a very low complexity, which makes it suitable for real-time applications, using different sample of image quality features extracted from one image which is used to compare the difference between real and fake samples. The result which is obtained from general public sample datasets of iris, fingerprint and face, show that present method is competitive as compared with other state-of-the-art approach and the study of the general image quality of real biometric samples expose valuable information which help to make a difference between real and fake traits.***

I. INTRODUCTION

Biometrics technology is used to security problems, recognizes persons in a fast and reliable performance through the use of unique biological characteristics. The human characteristic which is used as a biometric characteristic are universal, distinctiveness, performance acceptability, collectability and permanence. Many unimodal biometrics systems has an inability to tolerate deformed data because of presence of noise, deformed data from the sensor device, unevenness of an individual's physical appearance and sample over time and distorted signal from environmental noise. Multimodal biometric is able to solve several of these limitations by combining information from multiple biometric sources. The computational demands, processing time and storage requirements of a multimodal biometric system are good as compare with unimodal system. In recent years the interest is in the evaluation of biometric systems security which has led to the creation of several and very diverse initiatives which allow to focused on this major field of research: As many research works which has been publish led to disclose and evaluate different biometric vulnerabilities [2], [3], the proposal of new protection methods [4], [5], associated books chapters [6], the explanation of standard in the area [7], [8], the devotion of specific tracks, signal processing conferences, organization of competitions which allow to focused on on vulnerability assessment [10],[11], gaining of specific datasets [12], [13], creation in the field of laboratories has allow evaluation in the field of biometric security[14], or extinction of various European Projects along with the biometric security topic as main research interest [15], [16]. All proposals highlight the importances which involved in the development of biometrics which provides improvement of the system security which can be applied practically in use. As we consider the different threats among all are called direct attacks have motivated the biometric community to study the vulnerabilities against this type of fake actions such as the iris [2], the face [13] and the fingerprint [17] and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artifact (face mask or ris printed iris image and gummy finger) or mimic the behavior of legal user to fraud access the biometric system. In the analog domain, these type of attack are performed and is done with regular protocol along with digital protection mechanism such as encryption, watermarking which are not such effective. The aforesaid works and other analogue studies, have shown the necessity to recommend and develop specific protection methods against this threat. Researchers have focused on the specific design that measures the biometric systems to detect fake samples and reject them and create an improving the robustness and security level of the systems. In addition with other anti- spoofing approaches like use of multi biometrics or special attention has been done on the liveness detection techniques to distinguish between real and fake behavior. Challengng problem in todays liveness assessment methods have to satisfy certain demanding requirements [21]:

- user friendly, people should not be unwilling to use it;
- Fast, results must be produced in a very reduced interval because sensor cannot be interact with the user for long period of time.
- It must be low cost,
- Besides to having a good fake detection rate, the protection scheme should not degrade the false rejection of the biometric system.

Liveness detection methods are classified into one of two types

- Hardware-based techniques, in which sensor add some specific device to detect the properties of a living trait such as blood pressure, particular reflection properties of eye and fingerprint sweat.

- Software-based techniques, in which fake feature is detected once the sample is acquired with a standard sensor because it allow to distinguish between real and fake traits which s extracted from biometric sample.

These two types of methods have some advantages and drawbacks over the other and, in general, a combination of both would be produce much better performance to increase the security of biometric systems. These two types of methods have some advantages and drawbacks over the other and, in general, a combination of both would be produce much better performance to increase the security of biometric systems. The hardware based schemes usually have higher fake detection rate, whereas software based technique are less intrusive and less expensive because implementation is transparent to the user. Software-based techniques usually be embedded in the feature extractor module which help to allow to detect other type of spoofing attacks. In some case, software based method protect system which produce reconstructed or synthetic samples. A lot of work has made in the field of spoofing detection due to this attacking methodologies become more and more complicated As a result, there are still big challenges to be faced in the detection of direct attacks. In this case it is not rare that proposed approach produce a high detecting type of spoofs but their efficiently drop when they present different type of synthetic trait.

II. PREVIOUS WORK

As biometric technology has been grown rapidly, pattern protection become vital for securing the integrity of biometric security system and stop the illegal access. One of the best solution to secure biometric identification and verification is cancellable biometric. A new technique for robust cancellable pattern algorithm which gain the benefit of multimodal biometric using feature level fusion. Templates can be cancelled by applying feature level fusion. For an iris image binary iris code is very compact representation. Iris code did not contain enough information for reconstruction of original iris it has been assumed for a long time. The present work proposes an algorithm to reconstruct iris images from binary pattern and evaluate the similarity between original image and reconstructed synthetic iris image. The performance of reconstruction technique is evaluate by approximation the probability of successfully matching of synthesized iris image against true image of database. The outcome indicate that the reconstructed image look like a real image. Result can successfully deceive a commercial matcher but a a human expert may not be easily deceived by them. In addition proposed method synthesize multiple iris images from a single iris code.

III. METHODOLOGY

Flow Chart:

The working of proposed approach which is described along with Figure 3.1as follows:

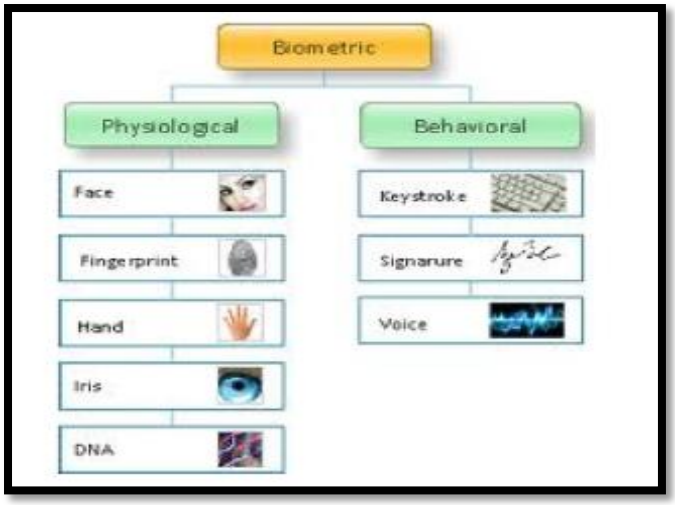


Fig-3.1 -Categories of biometric

Biometrics makes the use of biological terms that deals with data statistically. It verifies a person's uniqueness by analyzing his physical features or behaviors (e.g. face, fingerprint, voice, signature, keystroke rhythms). The systems record data from the user and compare it each time the user is claimed. A biometric system is a computer system that implements biometric recognition algorithms. A typical biometric system consists of sensing, feature extraction, and matching modules.

We can classify the biometric techniques into two classes:

- Physiological based techniques include facial analysis, fingerprint, hand geometry, retinal analysis, DNA and measure the physiological characteristics of a person.
- Behavior based techniques include signature, key stroke, voice, smell, sweat pores analysis and measure behavioral characteristics.
- Biometric recognition systems based on the above methods can work in two modes: identification mode, where the system identifies a person searching a large data base of enrolled for a match; and authentication mode where the system verifies a person's claimed identity from his earlier enrolled pattern.

Reasons for using Biometrics

Using biometrics for identifying human beings offers some reward like it can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys etc can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a huge number of passwords and personal identification numbers for computer accounts, bank ATMs, e-mail accounts, wireless phones, and web sites and so on. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less exclusive authentication for a variety of applications. The biometric authentication provides the ability to require more instances of authentication in such a quick and easy manner that users are

not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

IV. BLOCK DIAGRAM

A) Fingerprint-

The architecture of fingerprint based automatic identity authentication system of shown in fig. It consists of four components.

- user interface
- system database
- Enrollment module and
- Authentication module.

The user interfaces provides mechanism for user and input his fingerprint into the system. The system database consists of collection of record of fingerprint that has access to the system. Each record i.e. fingerprint in the database is in a minutiae pattern on a template form. Now the fingerprint image from a system database is taken out and now minutiae extraction algorithm is first applied to fingerprint image and minutiae pattern are extracted from the captured. A quality checking algorithm is used to ensure that the record in the system database only consist of fingerprint of good , in which significant number of genuine minutiae may be detected. If the fingerprint image is of poor quality, it is enhanced to improve the clarity of ridge/valley structure and mask out all region that cannot be reliably recovered. When the fingerprint image is fed in the user interface, it extracts the feature of fingerprint. It then enhanced the fingerprint image, after that masking is done to the input image. Now the minutiae pattern is extracted from the captured fingerprint image and fed to the matching algorithm which matches it against the person minutiae pattern which is stored in system database to establish the identity.

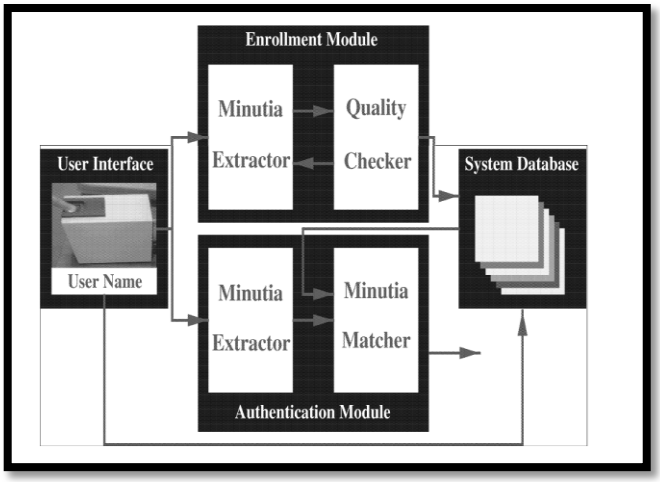


Fig. block diagram of fingerprint

B) IRIS

The iris images which are color images acquired from the database. So these are converted to gray level in order to save the computational cost and storage memory. Histogram Equalization was then applied to adjust the contrast of the image. The segmentation method detects the boundaries. The unique iris pattern from a digitized image of the eye is extracted and encoded into a biometric template (pattern,shape) using the image processing techniques. This can later be stored in the data base. The unique information in the iris is represented as objective mathematical representation. This is checked against templates for resemblances (similar).

When a person wishes to be authorized by an iris recognition system, their eye has to be first photographed, and a pattern is created for their iris region. The pattern is compared with the other templates in the knowledgebase. The comparison can be made till a matching pattern is found and the person is recognized, or no match is found and the person is overruled. There are five main steps for the iris recognition process.

The first step is the enrolment, where the eye image is captured. The next step is the segmentation of the iris from the other parts of 8 the eye image. Normalization is the third step, in which the iris pattern is scaled to a constant size. Iris is represented as iris code in the fourth step. The classification phase is the final step, where a matching technique is used to find out the similarity between the two iris codes. Below depicts the schematic for an Iris recognition system.

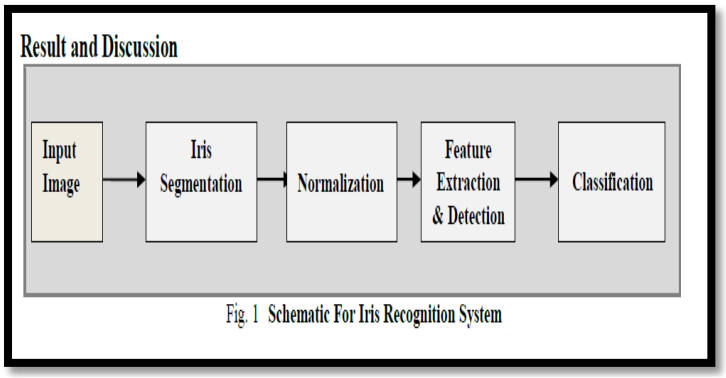


Fig-schematic for iris recognition

c) Face Detection

Face detection is a computer technology that identifies human faces in digital images. Face detection also refers to the psychological process by which humans locate and attend to faces in a visual scene. Face images can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person. Now the face image which is captured is taken into particular size of pixel which is of same size as that of database image pixel size. In this process we compare selected facial features from the image and a facial database. Face detection find the locations and sizes of all objects in an image. Firstly, the possible human eye regions are detected by testing all the valley regions in the gray-level image. Then the eyebrows, the iris, the nostril and the mouth corners are also detected step by step. The fitness value of each candidate is measured based on its projection on the eigen faces. After a number of iterations, all the face candidates with a high fitness value are selected for further verification.

We identify facial features by extracting landmarks, or features, from an image of the subject's face by analyzing the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features. Image which is present in the database has been extracted and this extracted trained image is now compared with the input test image considering various parameters such as the outline of the eye sockets, nose, and chin. After the processing is done we will find that whether the test image and trained image are same or not.

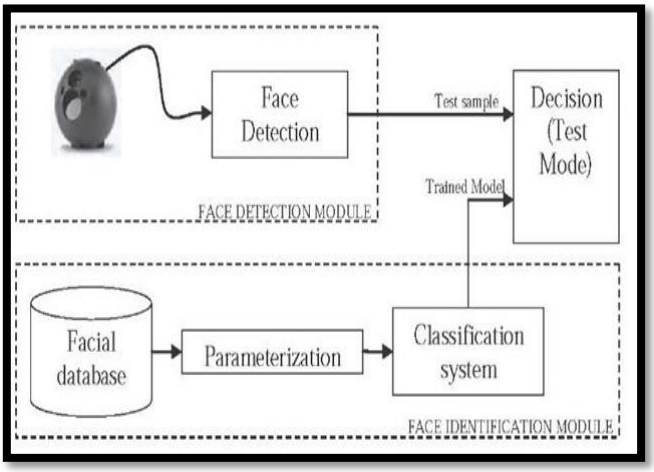
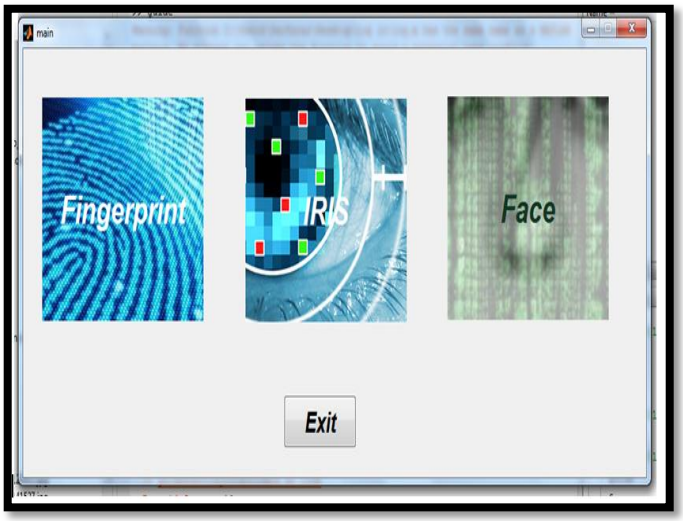


Fig-block diagram of face identification module

Summary:
The working of biometric of various techniques is described with the help of flow chart. It show that minutia method for fingerprint, Edge detection technique for iris and Eigen face for face detection has better and improved result. The next chapter is explained software platform required for implementation of this optimization approach.

V. EXPERIMENTAL RESULTS

a) Figure-1show login page of a project



b) When we select the fingerprint and the input is applied to it the following process takes place as show below in fig-2

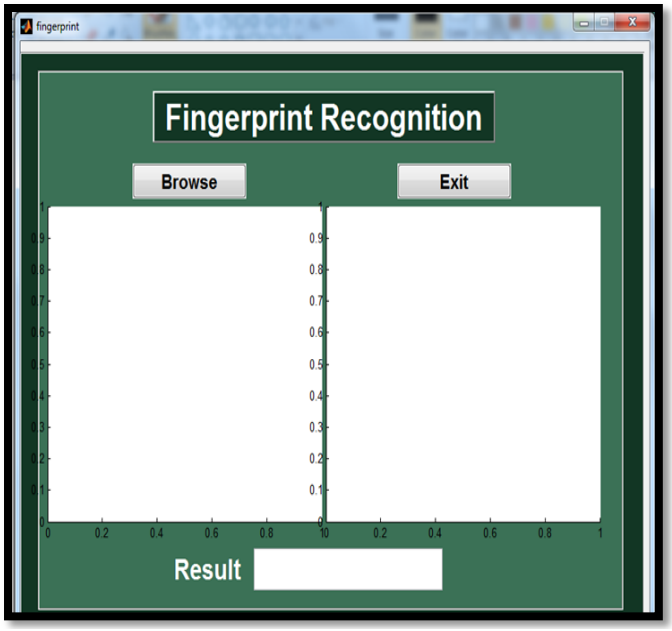


Fig-2 input to fingerprint

When input fingerprint is given then enhancement process takes place , masking is done, then it find the minutiae extraction if any present in it and finally it filter the false minutiae extraction. Now this extracted and enhanced image is compare with database image and find the similarity between input extracted image and database image. After the comparison is done it display the result whether the input applied fingerprint is match with database image or not.

Fig-3 show that input extracted image and database image are matched and it display authorized access.

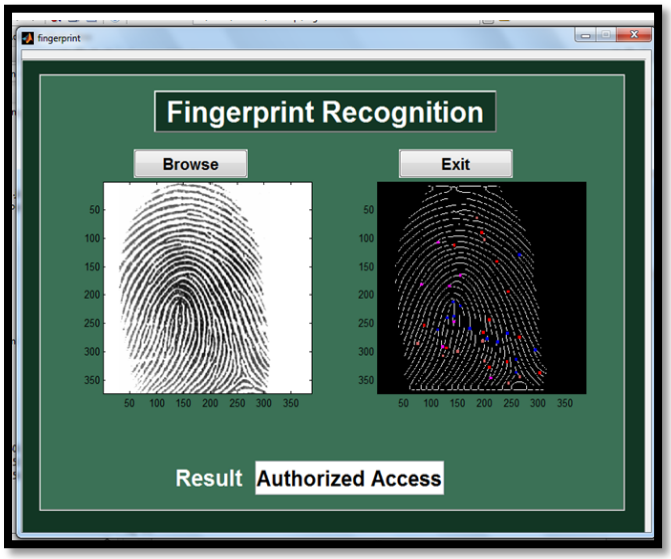


Fig-3 Input fingerprint matched

If the extracted and enhanced image is compare with database image and find that there is no similarity between input extracted image and database image.

Fig-4 below show that input extracted image and database image are not matched and it display unauthorized access.

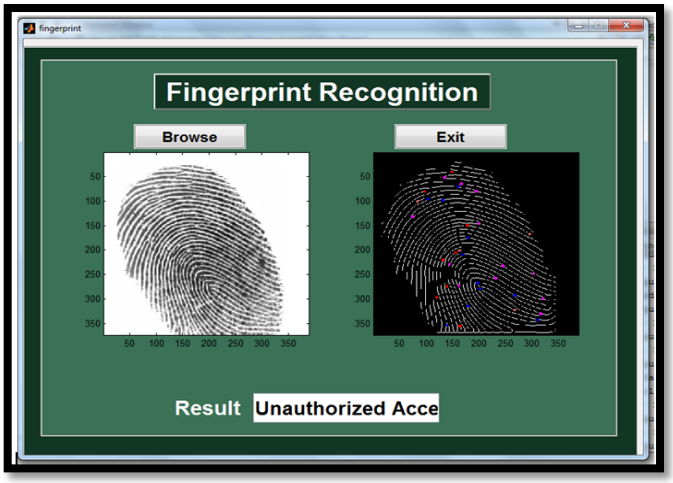


Fig-4 input finger print unmatched

c)When iris is applied in input stage then it compare database image with input image and the processing is done by converting t from rgb to gray color in which only white and black pixel is observed which mark the white and black point. During the comparison it show how much percentage of input iris is matched with database iris image

i) Fig fig-5show that input iris is matched with database iris image. So the applied image is known image.

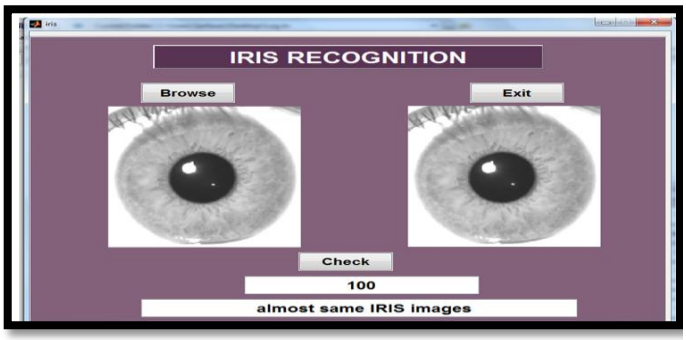


Fig -5 Input iris matched

ii)Fig-6 that if less percentage is match between input image and database image and input iris is not matched with database iris image then it display the result iris image is not match.

Iris input image will match with database image when it show the 85% matching.

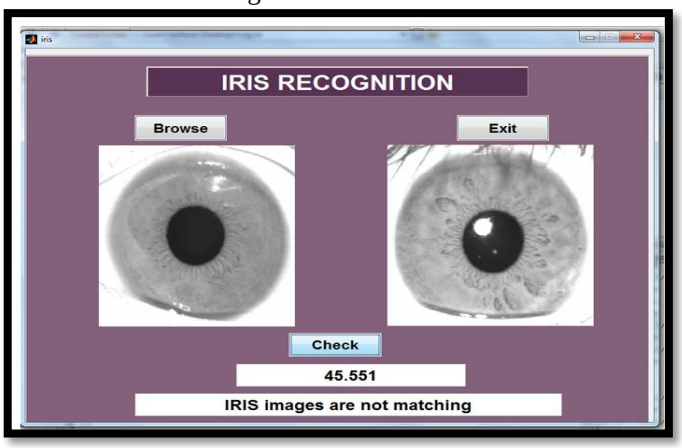


Fig -6 Input iris unmatched

d)In this process the train image is selected from train database and now the input image which is to be tested is applied to testing section. Now the test image is compare with all the database training image and the comparison is done considering the distance between two eyes, position of jaws, check bone shape, and width of the nose. Face recognition fig -7 below

Fig -7 Input to a face recognition

Cancellable biometrics

Biometrics which are cancelled are refer to systematically repeatable distortion and intentional of biometric features in order to protect responsive user-specific data. If we compromised with cancellable feature, the same biometrics is mapped to a new pattern and distortion characteristic are also changed.

Cancellable biometrics is one of the major categories for biometric template protection purpose besides biometric cryptosystem. Biometrics is a powerful tool and has been widely used in security system , biometric characteristics are unchallengeable resulting in permanent biometric even when a template is stolen. The biometric which was introduced can be cancelled and withdraw with the help of password and can be unique to every application. Cancelable biometrics want storage of the distinct version of the biometric pattern which provides high confidentiality level by allowing multiple pattern to be connected with the same biometric data.

Four objectives of designing a cancelable biometric scheme are as followed:

- Diversity: No same cancelable features can be used across various applications; therefore a large number of protected templates from same biometric feature is required.
- Reusability/Revocability: Straight forward revocation and reissue in the event of compromise.
- Non-inevitability: Non-inevitability of template computation to prevent recovery of original biometric data.

- Performance: The formulation should not deteriorate the recognition performance.

VI. CONCLUSION

Multi-Biometric is more challenging system but it is more secure than unibiometric system. Here we studied three biometric system i.e. face recognition, iris recognition and fingerprint. Multi-biometric system is used in various application. In future we will add one more biometric system to improve the system for making the system more secure. In fingerprint we used minutia matching method. For matching minutia points in fingerprint minutia matching method is being used. In iris the result show that proposed system is capable in order to make iris localization fast and accurately. The result also demonstrated that canny edge detection provides better efficiency and the higher detection rate and also the well suited execution speed. We used Eigen faces for face Recognition because it is simple, fast and work well under limitation condition. For face recognition we do not require ideal identification but just low error rate. It is better to give small set of likely matches rather than searching large database of faces. We can reduce this dimensionality by using Eigen face approach.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2,pp. 33-42, Mar./Apr. 2003.
[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.
[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027-1038, 2010.
[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113-129, Jan.2008.
[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega- Garcia,"A high performance fingerprint liveness detection method 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: Springer- Verlag, 2008,pp. 403-423.723
[7] ISO/IEC 19792:2009, Information Technology—Security Techniques—Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.
[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.
[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.
[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., "First international fingerprint liveness detection competition LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009, pp. 12-23.
[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., "Competition on countermeasures to 2D facial spoofing attacks," in Proc. IEEE IJCB, Oct. 2011, pp. 1-6.
[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems,"
[13] J. Telecommun. Syst., vol. 47, nos. 3-4, pp. 243-254, 2011. [13] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1-7.
[14] Biometrics Institute, London, U.K. (2011). Biometric Vulnerability Assessment Expert Group [Online].Available: http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert- group-bvaeg.html
[15] (2012). BEAT: Biometrices Evaluation and Testing [Online]. Available: http://www.beat-eu.org/
[16] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/
[17] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., vol. 31, no. 8, pp. 725-732, 2010.
[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366-375.
[19] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, 2012, pp. 3280-3283.
[20] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283-288.
[21] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York, NY, USA: Springer-Verlag, 2009.
[22] R. Cappelli, D.Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, p 1489-1503, Sep. 2007.
[23] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in Proc. IEEE ICIP, Oct. 2006, pp. 317-320.
[24] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imag., vol. 15, no. 4, pp. 041102-1-041102-17, 2006.
[25] M. C. Stamm and K. J. R. Liu, "Forensic detection

of image manipulation using statistical intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492-496, Sep. 2010.

[26] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," IEEE Trans. Image Process., vol. 12, no. 2, pp. 221-229, Feb. 2003.

[27] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111-119, Mar. 2006.

[28] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271-276.

[29] I. Avcibas, B. Sankur, and K. Sayood, "Statistical evaluation of image quality measures," J. Electron. Imag., vol. 11, no. 2, pp. 206-223, 2002.

[30] Huynh-Thu and M. Ghanbari, "Scope of validity of PSNR in image/video quality assessment," Electron. Lett., vol. 44, no. 13, pp. 800-801, 2008.

