

Enhanced Security based Multibiometric System for Face Recognition using SIFT Algorithm and Fingerprint Recognition

Sonali R. Khobragade¹, Girish R. Talmale²P.G. Student, Department of Computer Engineering, GHRCE, Nagpur, India¹Assistant Professor, Department of Computer Science, GHRCE, Nagpur, India²

ABSTRACT:- In this modern era where technology plays an important role, persons can be recognized (for security reasons) depending upon their behavioral and physiological characteristics (for example fingerprint, face, iris, keystroke, signature, voice, etc.) such systems are known as biometric systems. In these kind of systems the security is still a question mark because of various intruders and attacks. A reliable and efficient countermeasure is needed in order to combat the endemic growth of fake access. In this paper, we present novel software and hardware based protection measure against fraudulent biometric system access attempt. Scale Invariant Feature Transform (SIFT) features are features extracted from images which helps in reliable matching between different views of the same object. The proposed system introduces a new approach to catch an unauthenticated person i.e multibiometric system with fake detection for enhancing security more.

KEYWORDS: biometrics, security, spoofing attack;

I.INTRODUCTION

The human being body is a complicated design, filled of each required intellect for recognition, authentication and verification; and it is forever on the edge to be understood in a larger coverage. It is a multifarious structure, a superb work of art, an indescribable appeal and so vibrantly immaculate that it holds An exact character to continue a mystery for each and every distinct of us. For hundreds of thousands of years we individual, have been trusting upon with venture in the expectation of exploring ourselves and our internal secret. Thus, the human body and its routine span have been discovered on a usual basis in order to exercise the routine for its own better intention and betterment

We human contain always use our ordinary instinct and the existing sensory organs contained by us to recognize and validate others around us, be that living being or non-livings. As the growth of Information technology and the digital world escalate, the improved level of counterfeit practices and the flourishing establishment of fraudulence, disbelieve and deception among us has sky rocket immensely; moreover, such actions have become normal survival instinct/techniques for several people. Thus, it is because of such group of participations in fraudulence, it has at present turn into an expected task for every single individual to correctly differentiate the human being as to confirm whether a person is truly and accurately herself/himself when one claims who she/he is. Hence, while ingoing the digitized world of verification and authentication, one is essentially introduced to biometrics.

Biometrics are automated methods which gives identity or authentication to uniqueness of a living individual based on a physiological or behavioral characteristics. In these technique basic traits of human being is compared with the existing data and then based on the matching identification of a human is traced. There are wide range of applications and solutions where biometrics technology used in security systems. It plays an important role to recognize individuals. in groups which are under surveillance. Such identifiers are measurable characteristics, distinctive and used to describe and label individuals. Identifiers can be classified as physiological versus behavioral characteristics. Physiological

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

characteristics: which are associated to the shape of the body Such as fingerprint, face recognition, DNA , palm veins, palm print, iris recognition, hand geometry, retina and odor/scent. Behavioral characteristics: which are associated with the model of behavior of the person, including but not limited to typing gait, rhythm, and voice. After analyzing the different threats, spoofing attacks or direct attacks have motivated the biometric community to study the weakness against this fake action in modalities such as the fingerprint, the face, the signature, the iris, or even the gait and multimodal approaches. The intruder i.e. a fake person uses some type of synthetically produced objects like gummy finger, face mask or a printed iris image or it tries to imitate the behavior of the real user like signature, gait, to get access on biometric system.

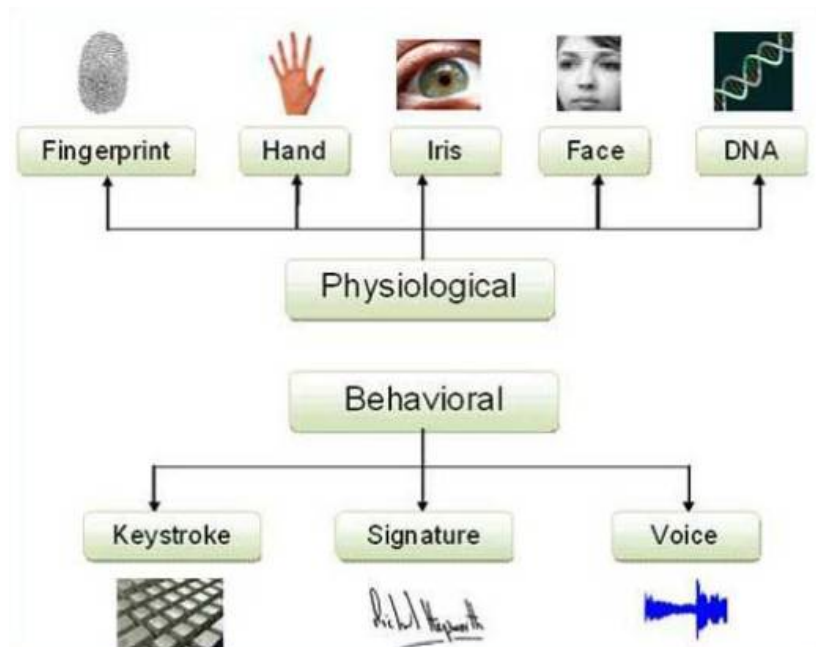


Fig 1:- Types of biometrics

II.RELATED WORK

Different researcher worked on biometric systems. Variety of approaches is developed in order to increase the security of a biometric system. But the biometric systems are still vulnerable to spoofing attacks.

Javier Galbally, Julian Fierrez, Fernando Alonso-Fernandez, Javier Ortega-Garcia [1] presented a software-based liveness detection approach where a novel fingerprint parameterization is used which is based on quality associated features. A highly challenging database is tested which comprised of 10,500 real and fake images gathered with five sensors of different technologies. To generate the gummy fingers large extent of direct attack scenarios in terms of materials and procedures carried out.

Nesrine Charfi, Hanene Trichili, Adel M. Alimi, Basel Solaiman [3] proposed a novel approach for personal verification i.e. combining palmprint and hand shape features extraction using the Scale Invariant Feature Transform (SIFT) algorithm. SIFT descriptors were extracted from hand and palmprint images. Likewise paper [2] Phalguni Gupta, Dakshina Ranjan Kisku, Jamuna Kanta Sing described about face recognition using SIFT algorithm.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Samarth Bharadwaj , Mayank Vatsa and Richa Singh [9] focused on a survey of the strengths, features, and worked on limitations of existing quality assessment methods in fingerprint, face and iris biometric and they found that Quality assessment of biometric readings plays an important role for the research in biometrics community. They made a clear distinction between the biometric quality and image quality of a biometric model to capture modality-specific perceptivity of quality assessment .

Vishal Moyal, Rohit Kuma [5] worked on quality assessment approach and suggested image information that measures the information which is present in the reference image and also how much features of this reference samples can be extracted from the distorted image.

Smita S. Mudholkar , Pradnya M. Shende, Milind V. Sarode [10] proposed a brief introduction about biometrics and the information regarding the intrusion detection system and finally proposed a method which is based on fingerprint recognition which allows us to detect more efficiently any abuse of the computer system that is running.

This research work is motivated from work done in [4][8]. Javier Galbally, Sébastien Marcel [4] in contrary to a fake self manufactured synthetic or restored sample the actual presence of a real authentic trait are focused here. A new software-based fake detection technique that can be used in multiple biometric systems to detect different types of fraudulent access attempts is presented.

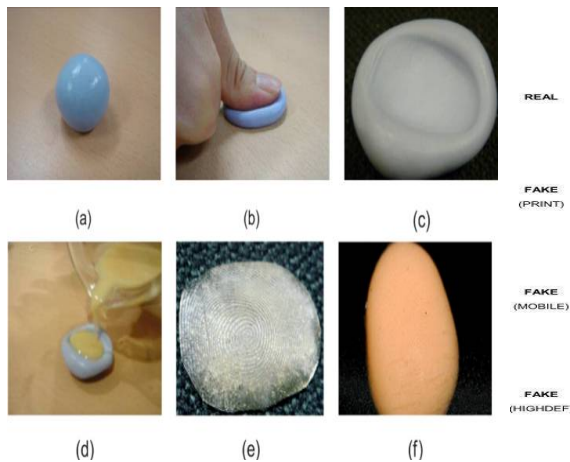


Fig 2:- Fake Fingerprints

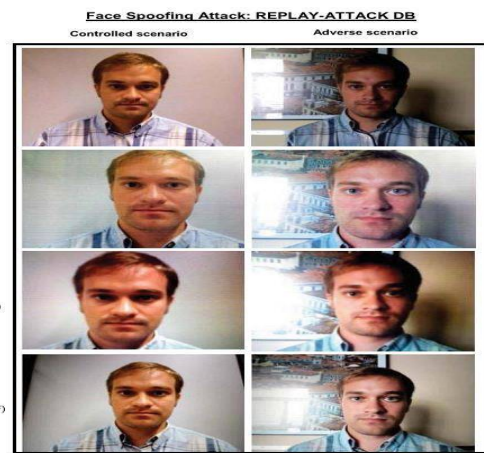


Fig 3:-Face Spoofing Attack

III. PROPOSED PLAN

In the field of biometric security Existing work has made several contributions to the state-of-the-art. For securing Biometric systems against various attacks in particular it has Shown the huge potential of image quality assessment, validation and proposal of a novel biometric protection method. The objective of designing a new system is to prevent the biometric system from an unauthenticated access i.e fake user and to fetch that person by sending an image of a fraudulent to any consultant person. As biometric technology is growing rapidly, to secure integrity of the biometric security system template protection plays a crucial role for preventing unauthorized access.

IV. WORKING METHODOLOGY

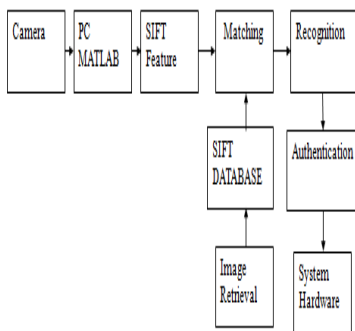


Fig 4:-Block diagram

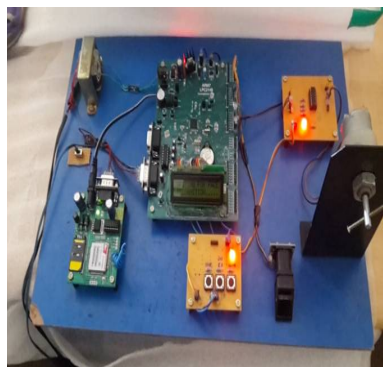


Fig 5:-System hardware

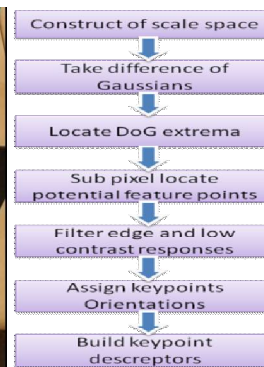


Fig 6:- Overview of SIFT algorithm

In this proposed work, database is used to store the facial images and the fingerprint images .we can add these images while enrolling the user. stored images are later used while authenticating the persons. Fingerprint feature extraction is prepared by means of minutia and image feature extraction is done by using SIFT algorithm . Fused value of fingerprint and face features are stored in the database. The next step is to test an image with the previously stored image that process is known as matching. Fingerprint recognition uses minutiae based matching and for face recognition SIFT descriptors are compared with the previously stored descriptors. If the system gives both the authentication then the user will be true user .Otherwise that person is considered as a fake one and his images will be taken then the designed system will store images of that fraudulent into database and with the help of GSM unauthentication message will be sent to the consultant person.

V. EXPERIMENTAL RESULTS

Figures shows the results of Enhanced Security based Multibiometric System. Figure 7,8,9 shows the graphical user interface ,extracted features of the user and the authentication provided to the real user .If the person is real one then

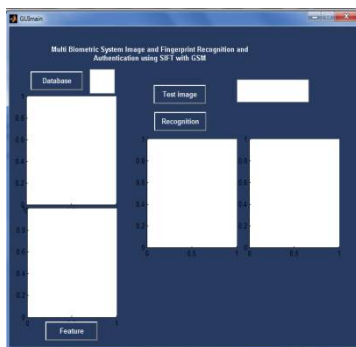
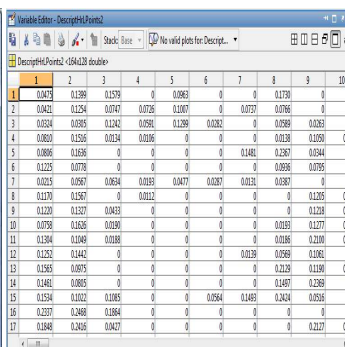


Fig 7:-GUI



	1	2	3	4	5	6	7	8	9	10
1	0.0475	0.1360	0.1579	0	0.0963	0	0	0.1730	0	
2	0.0421	0.1254	0.0747	0.0726	0.1007	0	0.0737	0.0766	0	
3	0.0624	0.0935	0.1242	0.0591	0.1299	0.0282	0	0.0269	0.0261	
4	0.0603	0.1526	0.0134	0.0196	0	0	0	0.0128	0.0101	0.0
5	0.0806	0.0166	0	0	0	0	0.1481	0.2267	0.0244	
6	0.1225	0.0770	0	0	0	0	0	0.0595	0.0195	
7	0.0123	0.0167	0.0634	0.0261	0.0471	0.0207	0.0124	0.0367	0	
8	0.1170	0.1567	0	0.0212	0	0	0	0	0.1295	0.0
9	0.1210	0.1527	0.0453	0	0	0	0	0	0.1228	0.0
10	0.0750	0.1626	0.0280	0	0	0	0	0.0163	0.1271	0.0
11	0.1304	0.1049	0.0188	0	0	0	0	0.0168	0.2100	0.0
12	0.1252	0.1442	0	0	0	0	0.0129	0.0569	0.1061	0.0
13	0.1365	0.0975	0	0	0	0	0.2129	0.1190	0.0	0.0
14	0.1461	0.0855	0	0	0	0	0.1457	0.2269		
15	0.1534	0.1022	0.1065	0	0.0564	0.1493	0.3424	0.0516		
16	0.1657	0.2490	0.1884	0	0	0	0	0		
17	0.1849	0.2426	0.0427	0	0	0	0	0	0.2127	0.0

Fig 8:-Feature Extraction

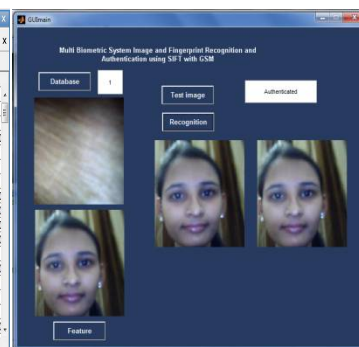


Fig 9:-Authentication

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

and then only he gets an access to the system and if the person is found to be fake he will get unauthentication and the proposed system will automatically generate one unauthentication SMS and send it to the consultant person.

VI. APPLICATIONS

1. Government applications such as Aadhaar card, social security, passport control, border control, welfare Disbursement, driver's license etc.
2. Commercial applications such as e-commerce, ATMs or credit cards, mobile phones, medical records management, physical access control etc.
3. Forensic applications such as criminal investigation, parenthood determination, terrorist identification etc.

VII. CONCLUSION

This paper presented an approach for enhancing security of the multibiometric systems as the system is equipped with the SIFT descriptor which improves the performance of image matching in the sense of achieving higher efficiency and This study provided a new approach to fetch the fraudulent persons. Proposed system will help us to diminish the crime rate and make the world more secure.

REFERENCES

- [1] Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, Javier Ortega-Garcia " A high performance fingerprint liveness detection method based on quality related features" *Future Generation Computer Systems*, Elsevier Journal, Volume 28 Issue 1, Pages 311-321, January, 2012
- [2] Dakshina Ranjan Kisku, Phalguni Gupta, Jamuna Kanta Sing "Face Recognition using SIFT Descriptor under Multiple Paradigms of Graph Similarity Constraints" *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 5, No. 4, pp. 1 – 18, October, 2010
- [3] Nesrine Charfi, Hanene Trichili, Adel M. Alimi, Basel Solaiman " Bimodal Biometric System based on SIFT Descriptors of Hand Images " 2014 IEEE International Conference on Systems, Man, and Cybernetics October 5-8, pp 4141-4145., 2014, San Diego, CA, USA
- [4] 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, No. 2, Page 710-724, February 2014.
- [5] Rohit Kuma , Vishal Moyal "Visual Image Quality Assessment Technique using FSIM" *International Journal of Computer Applications Technology and Research* Volume 2– Issue 3, pp 250 - 254, 2013
- [6] Pradnya M. Shende , Dr. Milind V. Sarode, Prof. Mangesh M. Ghonge " A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake Biometric" *International Journal of Computer Science Engineering and Technology (IJCSET) | |* Vol 4, Issue 4, pp 129-132 , April 2014.
- [7] Matthew A. Turk, Alex P. Pentland " Face recognition using eigenfaces." In Proceedings CVPR 91., IEEE Computer Society Conference on Computer Vision and Pattern Recognition , 1991
- [8] Anagha A. Shinde, Sachin D. Ruikar "Face Recognition using PCA and Eigen Face Approach " *International Journal of Computer Applications (0975 –8887)*, International Conference on Recent Trends in Engineering & Technology – 2013
- [9] 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, pp. 283–288, Sep. 2012