Fake Biometric Detection

M. Goudhaman (gouth74@gmail.com)
S.Bagiravan (bagiravanselvam@gmail.com)
S.Dhinesh Kumar (sdhineshkumar2001@gmail.com)
N.Jai Kumar (jaikumar090909@gmail.com)

Department Of Computer Science and Engineering

Jeppiaar Engineering College , Chennai , India

---***---

Abstract - This paper presents fusion of three biometric traits, i.e., iris, face and palm, at matching score level architecture using weighted sum of score technique. The features are extracted from the pre-processed images of iris, face and palm. These features of a query image are compared with those of a database image to obtain matching scores. The individual scores generated after matching are passed to the fusion module. This module consists of three major steps i.e., Pre-Processing, DWT Segmentation and Image fusion. The final fusion is then used to declare the person as Authenticate or Un-Authenticate.

Key Words **:** Discrete Wavelet Transform (DWT),Local Binary Pattern (LBP),Average Absolute Deviation (AAD), Joint Photographic Experts Group (JPEG).

1. INTRODUCTION:

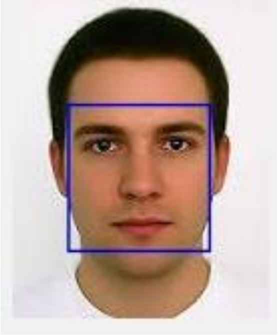
The identification of objects in an image. This process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures. The clever bit is to interpret collections of these shapes as single objects, e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skill full programming and lots of processing power to approach human performance.
Manipulating data in the form of an image through several possible.
The **iris** (plural: **irises** or **irises**) is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil and thus the amount of light reaching the retina. The colour of the iris is often referred to as "eye colour" .Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris(Figure:1).The automated method of iris recognition is relatively young, existing in patent only since in 1994.The human iris, an annular region located around the pupil and covered by the cornea, can provide independent and unique information of a person. Palm print Image Database (or CASIA-Palm print for short) contains 5,502 palm print images captured from 312 subjects. For each subject, we collect palm print images from both left and right palms. All palm print images are 8 bit gray-level JPEG files by our self-developed face recognition device. In our device, there are no pegs to restrict postures and positions of palms. Subjects are required to put his face into the device and lay it on a uniform-coloured background. The device supplies an evenly distributed illumination and captures palm print images using a CMOS camera fixed on the top of the device and palm. It takes the biological features of a person. Palm Recognition System has high acceptability, immutability, refers to the persistence of the palm over time, and individuality, and refers to the uniqueness of ridge details across individuals. The palms created by that friction ridge structure. A palm in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of the term, palms are the traces of an impression from the friction ridges of any part of a human hand.

2. BODY OF SCOPE:

When a new iris, finger and face image are presented as an input, the code matrix of the images is found out. Using the feature values, the pattern matching is performed. Based on this value, the class to which the new image belongs to is calculated. The recognition performance of iris feature alone using wavelet packet transform.

I. Facial Recognition

A **facial recognition system** is a computer application capable of identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database.



II. Iris recognition

Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.

Retinal scanning is a different, ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition. Iris recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual.[1] Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false match rates.

Several hundred million persons in several countries around the world have been enrolled in iris recognition systems for convenience purposes such as passport-free automated border-crossings and some national ID programs. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches, is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

III. Palm recognition

Palm recognition or **palm authentication** refers to the automated method of verifying a match between two human palms. Palms are one of many forms of biometrics used to identify individuals and verify their identity.

3. PROJECT REQUIREMENTS:

i. Software Requirements:

Operating system : Above Windows 7
Professional Tool : MATLAB 7.5 and above versions

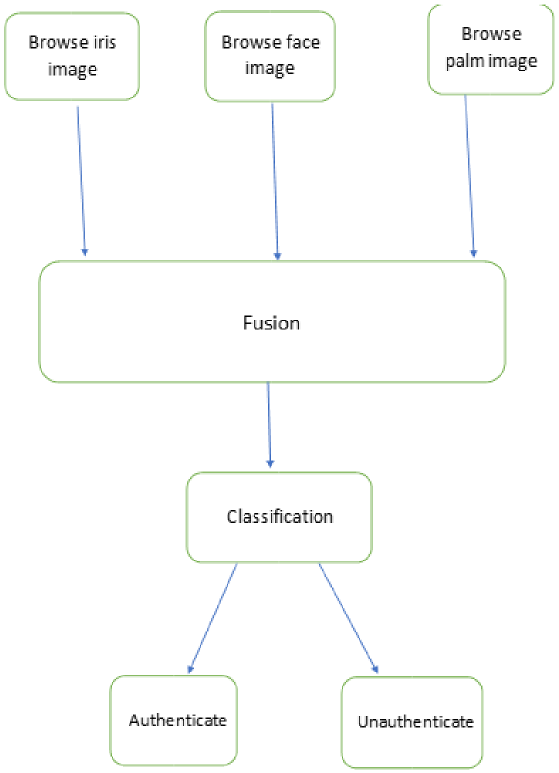
ii. Hardware Requirements:

PROCESSOR : INTEL i5
RAM : 8 GB
PROCESSOR : 2.4 GHZ
MAIN MEMORY : 8GB RAM
PROCESSING SPEED : 600 MHZ
HARD DISK DRIVE : 1TB
KEYBOARD :104 KEYS

4. DESIGN ARCHITECTURE:

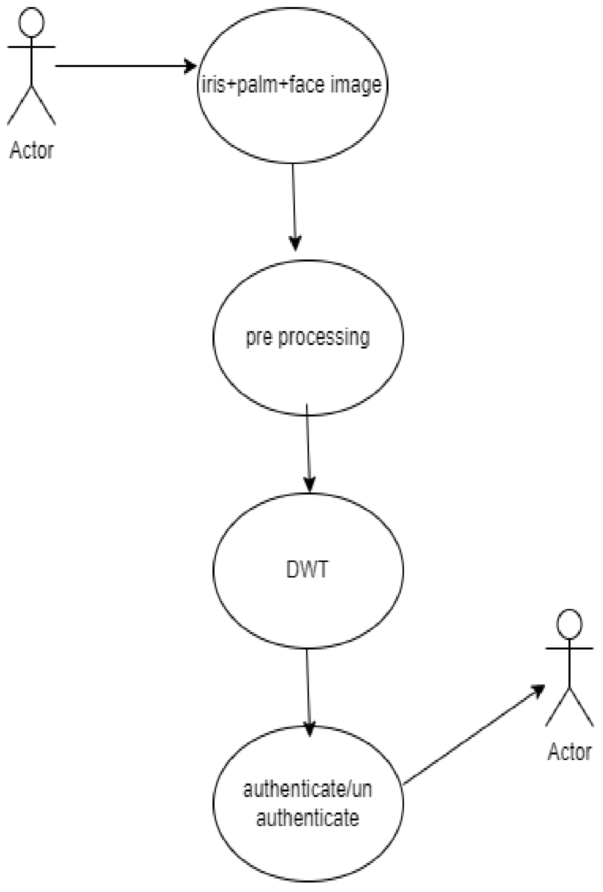
i. SYSTEM ARCHITECTURE:

A system architecture is the conceptual model that defines the structure, behavior, and more views of a system



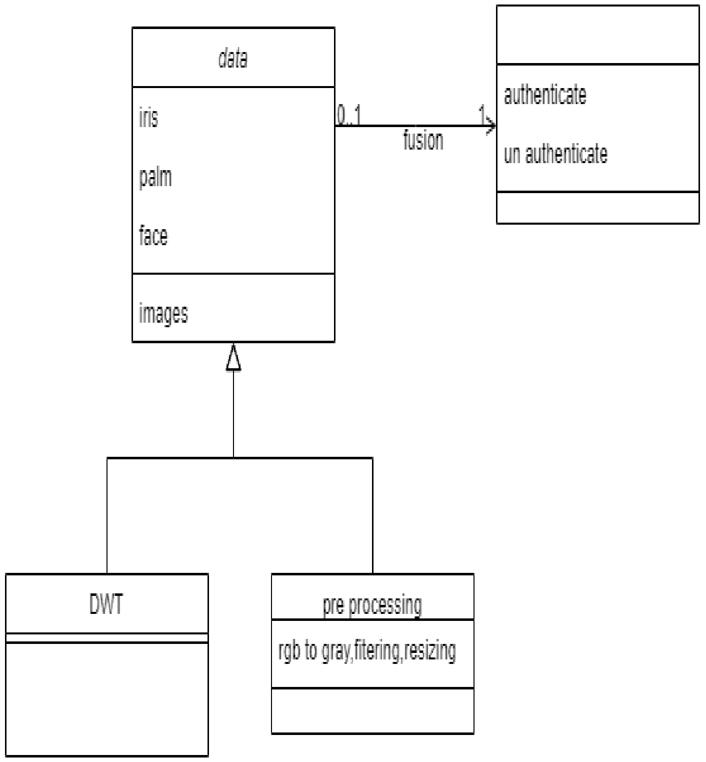
ii. USECASE DIAGRAM:

A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various use cases and different types of users the system has and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses. A use case diagram is a graphical depiction of a user's possible interactions with a system. A use case diagram shows various use cases and different types of users the system has and will often be accompanied by other types of diagrams as well. The use cases are represented by either circles or ellipses.



iii. CLASS DIAGRAM:

In software engineering, a class diagram in the Unified Modeling Language is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations, and the relationships among objects.



5. PROPOSED METHOD:

In recent years, biometric personal identification is in growing state of world, not only that it is the hot cake of both academician and industry. Traditional methods for personal identification are based on what a person possesses (Identity card, physical keyed, etc.) or what a person knows (a secret password) any how these methods have some pitfalls. ID cards may be forged, keys may be lost, and password may be forgotten. Thus Biometrics – Based human authentication systems are becoming more important as government and corporations worldwide deploy them in such schemes as access and border control, driving license registration, and national ID card schemes. The iris has unique features and is complex enough to be used as a biometric signature. It means that the probability of finding two people with identical iris patters is almost zero. According to Flom and Safir the probability of existence of two similar irises on distinct persons is 1 in 1072. The DWT is used for iris recognition The iris is well protected internal organ of the eye, located behind the cornea and the aqueous humor, but in front of the lens. The human iris begins to from during the third month of gestation. The structure is complete by the eight month of gestation, but pigmentation continues into the first year after birth.

6. CONCLUSIONS:

We have proposed a new PAD method based on the combination of local dense-SIFT image descriptors and three different feature encoding approaches (i.e., FV, VLAD, and BOW). The detection performance evaluation conducted over most publicly available

LivDet databases showed the soundness of our best fingerprint representation (i.e., FV) in more complex and realistic scenarios where unknown and known attack presentation attempts are carried out.Specifically, the FV approach yielded an average BPCER100 of 1.28% for known-scenarios, 8.69% for the unknown material scenarios, and 11% and 24% for the unknown capture device and cross-database scenarios, respectively, thereby achieving the top state-of-the-art results. In addition, a fusion between three encodings through a weighted sum approach showed an improvement of the baselines at most cases, thereby resulting in a BPCER100 in range of 1.98% - 17% in the presence of unknown PAI species.

7. FUTURE SCOPE:

As future work lines, we will improve the computational cost of the FV encodings in order to obtain the best trade-off between detection accuracy and computational efficiency. In order to tackle the fingerprint image quality limitation provided by Digital Persona, we will evaluate other texture descriptors in combination with FV. In addition, we will evaluate a new generative model in order to remove the GMM constraints on the input data distribution.

REFERENCES:

[1] 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.

[2] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[3] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

[4] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[5] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al.,

"First international palm liveness detection competition— LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009, pp. 12–23.

[6] 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.

[7] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz,

"Evaluation of direct attacks to palm verification systems," J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.

[8] 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.

[9] Biometrics Institute, London, U.K. (2011). Biometric Vulnerability Assessment Expert Group [Online]. Available: http://www. biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup-bvaeg.html

[10] (2012). BEAT: Biometrices Evaluation and Testing [Online].

[11] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available:http://www.tabularasa-euproject.org/

[12] 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.

[13] 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.

[14] 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.

[15] 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.