IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 3, March 2015.
www.ijiset.com
ISSN 2348 – 7968

Biometric Template Feature Extraction And Matching Using CANNY Edge Detection And SIFT Based Algorithm

V.Nandhini [1], S.Vijayalakshmi [2]

[1] Computer Science and Engineering,IFET College of Engineering, Villupuram, Tamil Nadu, India
[2] Computer Science and Engineering IFET College of Engineering, Villupuram, Tamil Nadu, India

Abstract

To ensure the actual presence of real image in contrast to a fake image is one of the significant problem in biometric authentication. Many biometrics methods have been developed and it is currently used in face, iris, fingerprint, palm print etc., in order to detect whether it is real or fake image and provide authentication to real image. But still there is lagging in providing perfect security and authentication to the biometric. The great challenge to biometrics is thus to improve recognition performance in terms of both accuracy and efficiency and it greatly resistant to deceptive practices. The finger-bone X-ray images and skull front view are the promising biometric pattern for personal identification in terms of its security and authentication. By using biometric template feature extraction and matching techniques it can be efficiently distinguish the real X-ray samples from fake X-ray samples and provide authentication to real X-ray sample.

Keywords: biometric authentication, finger-bone X-ray, skull front view, feature extraction, matching.

1. INTRODUCTION

The biometric is the study of physical or behavioural characteristics which help us to identify the person [5]. The biometric systems offer several advantages over traditional authentication systems . The Use of password and pin identification number are traditional methods which are providing security but it is easy vulnerable to attacks and it can be easily stolen. The password system suffers from many drawbacks and it is unable to absolutely identify the user. Simplistic passwords can be easily predictable by computer hacker using tools such as password cracker and login spoofing. Once the intruder has found the password, the system cannot able to recognize the true identity of the user and the intruder has total access to associated resource . Making the password more complicated sounds good but end users tend to forget difficult string of password. User behaviour can actually bypass password security by failing to choose password cleverly, to remember the password, to change the password repeatedly and to the extreme, to keep the password at secure place. The Biometric security systems will verify a persons identity by scanning fingerprints, irises or faces [6]. Authentication with biometrics system requires comparing a registered or enrolled biometric sample against a newly captured biometric sample . Though biometrics has been improve security, biometric systems are also have vulnerabilities such as being spoofed by fake fingers or, in the worst case, dismembered fingers. Spoofing attacks are one of the main threats to the security of biometric systems. They are carried out by submitting a counterfeited biometric to the sensor. Spoofing attacks have a great practical relevance because they do not require advanced technical skills and, therefore, the possible amount of attackers was large. It has been shown throughout the history of automated personal recognition that the spoofing attacks can be carried out against many types of biometrics system such as face ,palm and iris[7] . To deal with spoofing attacks, several “liveness” detection methods have been proposed. Liveness detection are helpful to recognition of human physiological activities as the liveness indicator to prevent spoofing attack, it is becoming a very energetic topic in field of fingerprint recognition and iris [7][8] . But there is a problem in liveness detection that are seen in a two class classification problem where an input fingerprint image has to be allocated into two classes: real or fake. Biometric identifiers currently available or under development include fingerprint, face recognition, palm print, retinal scan, iris pattern, signature, and voice pattern but still there is an problem to identify the real image from the fake image. In order to avoid there attack the finger X-ray and skull front view are taken and it is reside inside the body and it cannot be attacked.

ISSN 2348 – 7968

2 LITERATURE REVIEW

In any security systems, the user authentication is the basic requirement. Most of the researchers made their efforts to design such systems and contributed to the security related applications. The literatures available for these are summarized below;

In [1] a author proposed the BIOFACE which incorporating several facial biometric techniques . It includes the well established Eigenfaces and also the Tomofaces techniques, which implement face recognition based on facial appearance and diminuendos, respectively. Both methods are based on the space dimensionality reduction and the enrollment which requires the projection of several confident face samples to the reduced space. Instead, BIOFACE also performs face recognition based on there matching with the Scale Invariant Feature Transform (SIFT) features. BIOFACE extracts a facial soft biometric shape, which consists of a bag of facial soft biometric characters such as skin, hair, size, location and eye color. The fast and efficient detection of the facial soft biometrics is performed at the pre-processing step, and working for the search for the facial recognition module. In [2] the various threats that can be encountered by a biometric system. They specially focus on attacks designed to prompt information about the original biometric data of an individual from the stored template. A template represents a set of salient features that summarizes the biometric data of an individual person . Due to its compressed nature, it is commonly assumed that the template cannot be used to elicit complete information about the original biometric signal. In [3] Liveness detection is based on the principle that additional information can be stored and data obtained by a standard verification system, and these additional data can be used to verify the biometric measure is authenticated. The Fingerprint Liveness Detection Competition goal is to compare both software-based and hardware-based fingerprint liveness detection methodologies and is open to all academic and industrial institutions. software-based systems, is used to check whether presented fingerprint originates from a live person or an artificial finger.

In [4] a typical biometric authentication system which consists of two phases. During the enrolment phase, a user scans there biometric data, and then features are extracted from the data and a template is created for the data and it is stored in database . During the authentication phase, a user who claims should scans her biometric data again, and then the same feature extraction algorithm is applied and check for the result whether it compared with the stored template. If they are sufficiently similar according to some similarity measure, the matching algorithm outputs the result as yes, which indicates that the user is authentic, or a no when the user is not authentic.

3 PROPOSED SYSTEMS

The finger-bone x-ray images and skull front view is a promising biometric pattern for personal identification in terms of its security and X-ray image and skull front view are stored in the convenience. In the proposed system template generator will extract the feature of the finger bone database. When any user enter in to the system the captured X-ray image of the user are extracted and compare with the database using template matching and provide authentication to the real X-ray image. In these Biometric authentication system four modules are used they are Image acquisition, Filtering process, Feature extraction, Template/similarity matching.

3.1 IMAGE ACQUISITION

In Image acquisition module the finger bone X-ray image and skull front view image are taken using the scanner. This finger bone X-ray image and skull front view will act as the input to the system.

3.2 FILTERING

In this module we need to filter the input image using median filter, this filter will remove any unwanted salt and pepper noise in input image and give the noise free image.

3.3 FEATURE EXTRACTION

After removing the noise the edge of the image are detected using canny edge detection. The Canny edge detection algorithm is known to many as the optimal edge detector. The purpose of edge detection algorithm is to expressively reduce the amount of data in an image, while protecting the structural properties of the data for further image processing. In the feature extraction module the biometric image feature are extracted from the X-ray image during user enrolment and compare with the authenticated X-ray image.The SIFT algorithm is used for skull feature extraction.

3.4 TEMPLATE/SIMILARITY

The template/Similarity matching module compares the feature set extracted during authentication with the enrolled X-ray image.

ISSN 2348 – 7968

Structural similarity is measured in this module to see whether the input image and user image matches or not. If the similarity index in 1 or close to 1, then it means the images matches.The greater advantage of using the finger bone and skull X-ray are it is hidden inside the body and is mostly invisible to human eyes, so it become difficult to copy or steal the X-ray.

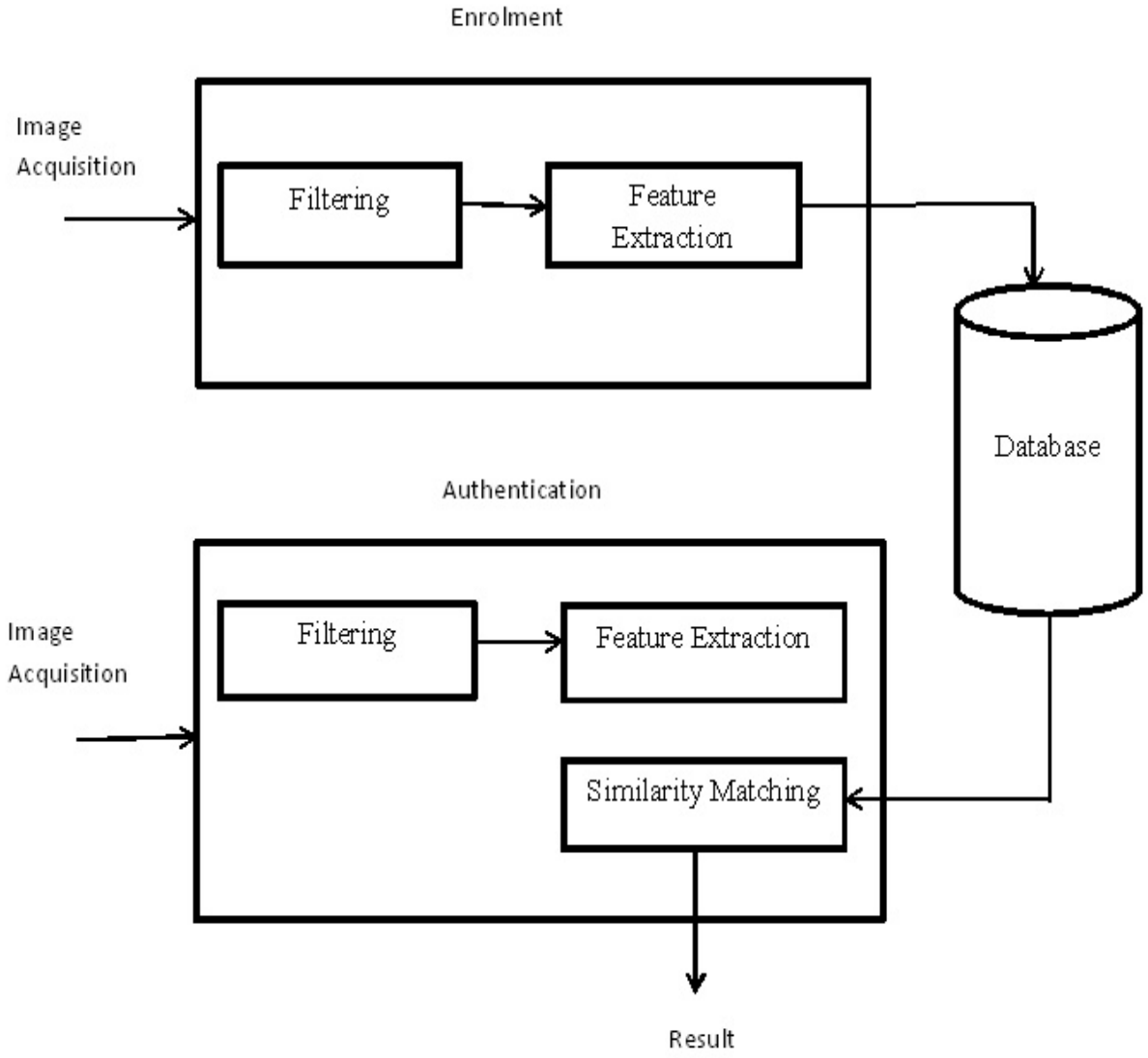
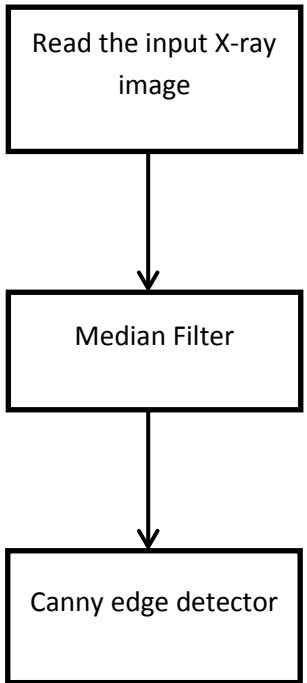


Fig 3.1 Block diagram of the proposed system

4 SYSTEM FLOW OF PROPOSED SYSTEM

In our proposed system the input image such as finger bone Xray image and skull front view are taken as the input. The input image is filter by the median filter and noise free image is taken for the next step. After the removal of the noise the edge of the X-ray image are taken by using canny edge detection. The feature of the X-ray image are taken and stored in the database.If the new user enrolled in the system the x-ray image of the new user and compared with the stored template.



ISSN 2348 – 7968

Fig 4.1:Sytem flow of proposed system

5 MEDIAN FILTER

Median filtering is a nonlinear method used to remove noise from X-ray images. It is widely used and it is very effective at removing noise and it will preserving the X-ray edges. The median filter works by moving through the X-ray image pixel by pixel and replacing each value with the median value of its neighbouring pixels. The pattern of neighbours is called the "window", which slides, pixel by pixel over the entire image 2 pixel, over the entire image. The median is calculated by first sorting all the pixel values from the window into ascending order, and then replacing the pixel being considered with the middle (median) pixel value.

6 CANNY EDGE DETECTOR

Canny Edge detection algorithm is used to identifying points in a digital image at which the X-ray image brightness changes sharply or, more formally, has discontinuities[15]. The canny edge detector is an edge detection operator that uses a multi-stage algorithm to detect a wide range of edges in the X-images.
The algorithm runs in 5 separate steps:
1. Smoothing
2. Finding gradients
3. Non-maximum suppression
4. Double thresholding
5. Edge tracking by hysteresis

Fig 6.1 Noise removed X-ray

ISSN 2348 – 7968

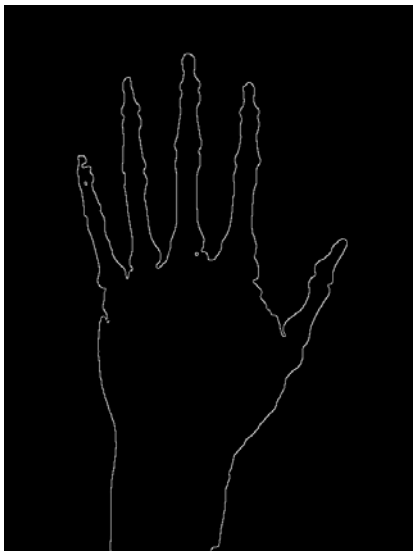


Fig 6.2 Canny edge detector

7 SCALE-INVARIANT FEATURE TRANSFORM

Scale-invariant feature transform (or SIFT) is an algorithm in computer vision to detect and describe local features in images. Sift keypoints of objects are first extracted from a set of reference images and stored in a database for authentication purpose [14]. An object is recognized in a new image by individually comparing each feature from the new image to the database and finding candidate matching features based on euclidean distance of the feature vectors. From the full set of matches the subdivisions of the keypoints that agree on the object and its location, size, scale, and orientation in the new image are identified to filter out good matches.

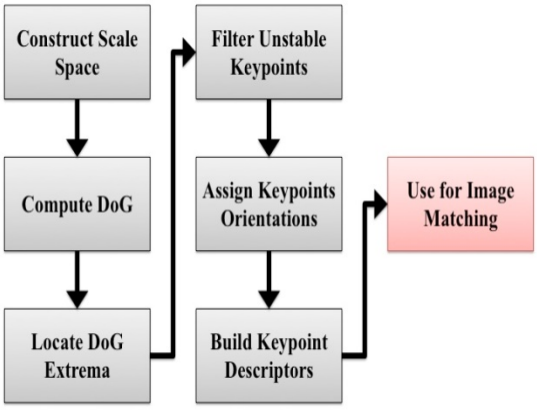
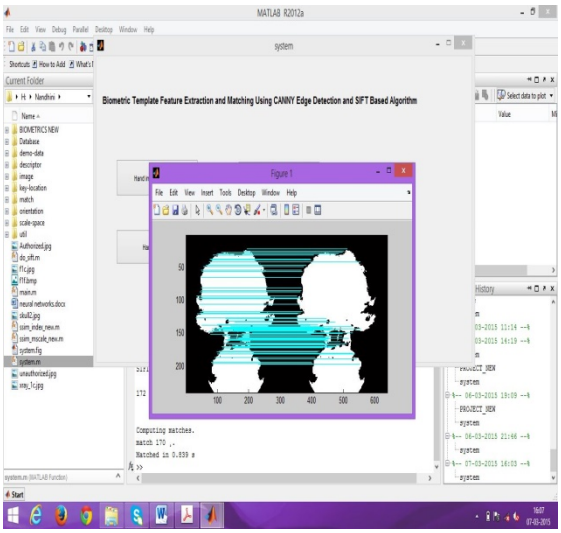


Fig 7.1 SIFT algorithm steps

8 EXPERIMENTAL RESULT



In the above experimental result we are matching the real and fake skull front view using SIFT based algorithm and finding the matching of these two skull and its time taken to find these matching.

9 CONCLUSION

The study of the liabilities of biometric systems against different types of attacks has been a very active field of research in recent years . This interest has leads to big developments in the field of safety-enhancing technologies for biometric-based applications system. However, in spite of this clear improvement, the development of efficient protection methods against known threats has recognized to be a challenging task. In order to impove the authentication and to proved security the finger bone xray and skull fornt view are taken inorder to replace the finger and face regonition system.In order to overcome spoofing attack in the biometric sytem these system has been proposed. The proposed method is able to consistently perform at a high level for different biometric system and also it is able to adapt to different types of attacks providing for all of them a high level of protection .

10 REFERENCES

[1]. Mourad Ouaret, Antitza Dantcheva, Rui Min, Lionel Daniel, Jean-Luc Dugelay “BIOFACE, a Biometric Face demonstrator”,2010

[2] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,”*EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 113–129, Jan. 2008.

ISSN 2348 – 7968

[3]. Luca Ghiani, Valerio Mura, Simona Tocco, Gian Luca Marcialis, Fabio Roli, David Yambay, Stephanie Schuckers "LivDet 2013 Fingerprint Liveness Detection Competition 2013"
[4]. Yagiz Sutcu, Qiming Li, Nasir Memon "Secure Biometric Templates from Fingerprint-Face Features"

[5]. Joseph Lewis, University of Maryland, BowiemState University, "Biometrics for secure Identity Verification: Trends and Developments"mJanuary 2002.

[6]. A. K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics:mPersonal Identification in Networked Society*. Kluwer*m*Academic Publishers, 1999.

[7]. T. Van der Putte and J. Keuning, "Biometrical fingerprint recognition:mdon't get your fingers burned," in *Proc. IFIP*, 2000, pp. 289–303.
[8]. J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez, "Fakemfingertip generation from a minutiae template," in *Proc. ICPR*, 2008.
[9]. 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.
[10]. Biometrics Institute, London, U.K. (2011). *Biometric VulnerabilitymAssessment Expert Group* [Online].
Available:http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup-mbvaeg.html
[11]. (2012). *BEAT: Biometrices Evaluation and Testing* [Online]. Available: http://www.beat-eu.org/
[12]. (2010). *Trusted Biometrics Under Spoofing Attacks (TABULA RASA* [Online]. Available: http://www.tabularasa-euproject.org/
[13]. Lifan Yao , Hao Feng , Yiqun Zhu , Zhiguo Jiang, Danpei Zhao, Wenquan Feng "An Architecture of Optimised SIFT Feature Detection for an FPGA Implementation of an Image Matcher"
[14]. Prateek Verma* ,Yogesh Bahendwar, Amrita Sahu, Maheedhar Dubey "Feature Extraction Algorithm of Fingerprint Recognition " 2012
[15]. Rashmi , Mukesh Kumar, and Rohini Saxena "Algorithm And Technique On Various Edge Detection: A Survey" 2013.