International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Detection and Prevention of Fingerprint Altering / Spoofing Based on Pores (Level-3) with the Help of Multimodal Biometrics

Maneesh Kumar Sharma

M. Tech (CSE), Department of Computer Science and Engineering, Monad University, Pilakhua, HAPUR (U.P.), India
manumanish007@gmail.com, +91-9452137629

Abstract: ***The concept of spoofing focus on altering fingerprint, which become a serious issue concern of fingerprint recognition system. This project work brings a new approach to sense and detect fake fingers, based on the analysis of fingerprint pores and its extraction. Making fake fingerprint now days an open matter for identifying fingerprint systems. In this case submitting an artificial fingerprint clone from a genuine user. Present sensors provide an image which is then processed as a "true" fingerprint. this is so- called 3rd-level features, namely, pores, which are visible in high-resolution fingerprint image mostly 500/1000 ppi, have been used for matching. In this paper, we propose to analyze pores location for characterizing the "liveness" of fingerprints. There are several features identifying a fingerprint which is Level-1(pattern), Level-2 Minutia, Lvel-3(Pores and ridge counters). AFIS (Automated Fingerprint Identification System currently uses level 1 and level 2 features. The 3 level features allow you to scan 1000 ppi and extract all features along with pores and ridges using gabor and transform filters. It also uses the dual matching logic where we can user the combination of finger + face/iris to authenticate or prevent spoofing.***

Keywords: Pores Extraction, multomodel biometrics, spoofing detection, fusion algorithms, fake detection techniques

1. Introduction

Biometrics is known as an automated function of identifying and verifying a living human based on physiological and behavioral characteristics. The biometrics work upon Fingerprint, Facial, iris etc. A spoof is a counterfeit biometric that is used in an attempt to circumvent a biometric sensor. In the case of fingerprints, this can be as simple as a latent print on a sensor, reactivated by breathing on it, or as sinister as using a dismembered finger. Differentiating a genuine biometric trait presented from a live person versus some other source is called spoof detection. The act of sensing vitality ("liveness") signs such as pulse is one method of spoof detection. In some areas of research, the term liveness detection is synonymous with spoof detection. To face this problem, two major approaches can be im- plemented [2]. The first one is hardware-based` and adds to the sensor a device that is able to acquire an explicit vital- ity information like temperature, blood pulsation, electrical conductivity of the skin, etc. This method increases the cost of the overall system since it requires additional hardware. The second one is software-based and integrates a liveness detection algorithm into a standard fingerprint sensor.

Such option may use static features, extracted from one or multiple impressions of the same finger or dynamic features, obtained by processing two successive images, captured in a certain time interval.

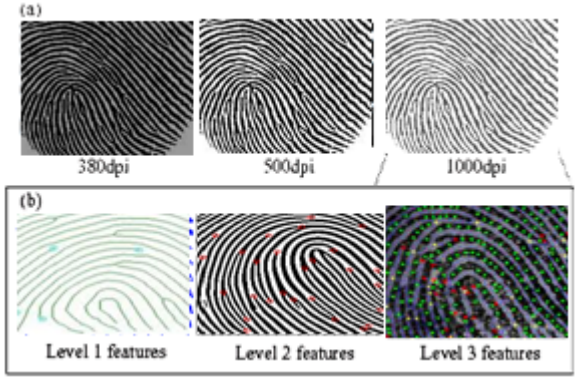

Figure 1: Fingerprint Features (a) A partial fingerprint image captured at various resolutions (380dpu, 500dpi, and 1000dpi) using indentix 200DFR and CrossMatch ID1000 sensors. (b) Features extraxted at different levels from the 1000dpi fingerprint in (a).

FBI has set the standard resolution to be 500 dpi for forensic application like IAFIS in order to reliably extract level 2 features. Spoof/alter detection method divided or categorized into three different purposes- A) Collect the data for biometric purpose, B) further process information already collected to generate discriminating information or collect additional biometric images over time, C) Using of more hardware and related software to detect the signals some years ago [2]. Different materials can be used to create a "mould" and others for the final replica [1]. When submitted to standard sensors, an image equivalent to that of a "live" finger is generated. Then, it is processed and matched with the client template, thus increasing the probability of deceiving the system.

This motivated several attempts to increase the ability of systems to "detect" physiological, "liveness" features: for example, by using additional hardware [2], or by image

processing and pattern classification methods [3-6]. Among others, the most effective approaches exploit the "pores perspiration" which is not present in "fake fingerprints" [3].

Worth noting, pores have been proposed as 3rd- level features for fingerprint matching [7-8]. They can be detected by high-resolution capture devices, but also by fingerprint sensors already present on the markets, as shown in datasets of Fingerprint Verification Competition [9]. As noticed in [3], the pores presence in live fingerprints determines the perspiration effect. However, no work pointed out that pores are difficult to be replicated in the fake fingerprint fabrication process. With the term "pores replication", we mean that the fake replica is also characterized by "small holes" correspondent to the pores position. Since pores size is less than 1 mm, it is very difficult to replicate pores by using liquid silicone rubber, or gelatin, or play-doh, i.e., commonly used materials for fake fingerprint [4]. Therefore, our claim is that a large number of pores can be easily detected in live fingerprint images whilst, on average, a much lower number of pores is present in fake fingerprint images. In other words, the pores distribution in fake and live fingerprints should be different.

In this paper we propose to analyze pores distribution in order to discriminate between fake and live fingerprint images. Experiments are carried out on a large data set of more than 14,000 fingerprint images. This is currently the largest data set for fingerprint liveness detection. The paper is organized as follows. Section 2 motivates and describes pores-based features for liveness detection. Section 3 reports experimental results and Section 4 concludes the paper.

2. Fabrication of Fake Finger

There are two ways when fabricating fake fingerprints. One is produced by cloning with a plasticine mold under personal agreement. The other is created by cloning from a residual fingerprint. Because fabricating fake fingerprint needs appropriate materials and appropriate processing. Its hard to make fake fingerprint. Especially fabricating fake fingerprint from a latent fingerprint is requiring a professional skill.
The material and procedure are two necessary factors when altering fake fingerprints. The common materials are paper, films and silicon. Gelatin and synthetic rubber are also used very often for fake fingerprint because they have physical and electrical properties very similar to human skin. Recently Prosthetic finger, clone of whole fingers, has appeared. Prosthetic fingers are expensive yet, but they are almost same [11].

Figure 2: Shows Fake Fingerprint using Rubber, Silicon, Prosthetic finger and Gelatin process.

3. Level 3 Feature Extractions and Pore

3.1 Detection

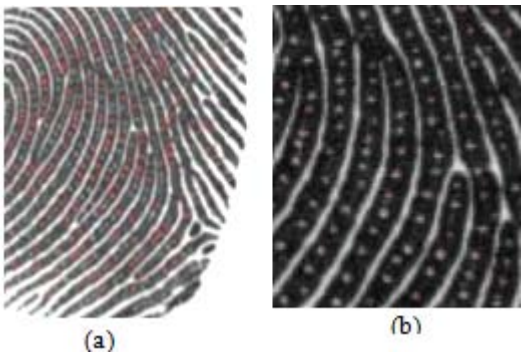

Figure 3: Fingerprint image (a) where pores can be easily noticed as small "holes" along ridges flow (as evident in the zoom (b))

Fig. 3 shows a "live" fingerprint image with related pores. Pores are defined as external openings of duct of sweat gland. Through pores, transpiration of aqueous fluid is allowed. Accordingly, the skin may appear as moist or dry, depending on the pores perspiration phenomenon [3, 7].

It is possible for several sensors, where resolution is more than 500 dpi, to display even fingerprint pores. In particular, the adopted sensor exhibits 500 dpi. Similarly, pores can be seen in several images of FVC data sets [9]. By considering that sensors providing 1000 dpi are already available, using pores for matching has been investigated [7-8].Since the size of pores is less than 1 mm, it is quite difficult to reproduce them during the fabrication process of fingerprint replica. Currently, state-of-the-art methods for fingerprint reproduction are classified in consensual and non-consensual [4]. Of course, the most effective method is the first one. It requires that the subject put his finger on a plasticine-like material, in order to create a mould. Then, a cast is provided by dripping over the mould materials like liquid-silicone rubber, gelatin, play-doh. If well done, this fabrication process leads to a replica where minutiae and texture are quite similar to that of the original, "alive" finger.

The skin on the palmar side of the finger tips contains dermatoglyphic patterns comprising the ridges and valleys commonly measured for fingerprint-based biometrics. Importantly, these patterns do not exist solely on the surface of the skin—many of the anatomical structures below the surface of the skin mimic the surface patterns.

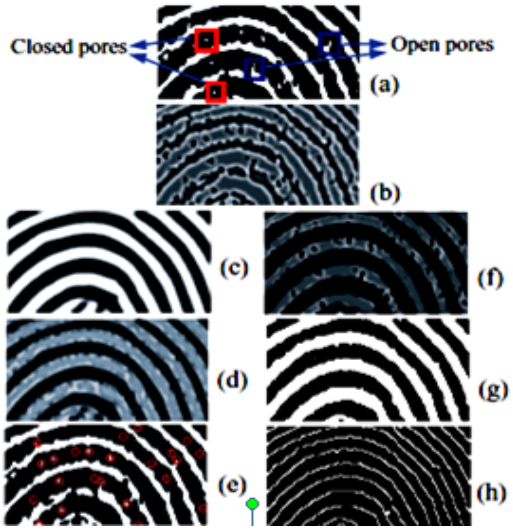

Figure 4: Level 3 feature extraction. (a) A partial finger print image at 100dpi. (b) wavelet response (s=1.32) o the image in (a). (c) Ridge enhancement of image in (a using Gabor filters. (d) Pore enhancement using a linear addition of (b) and (c). (e) Extracted pores (red Circles) after thresholding on (d). (f) Ridge enhancement using a linear subtraction of wavelet response (s=1.74) and (c). (g) Identified ridges after binarification on (f). (h) Extracted ridge contours after applying the filters on (g).

Based on the position on the ridges, pores are often divided into two categories: open and closed. A closed pore is entirely enclosed by a ridge, while an open pore intersects with the valley lying between two ridges (Figure 2(a)). A method to extract pores using skeletonized image was proposed for 2000dpi fingerprint images [6, 8]. Generally, if a point has 1 (or 3) neighbors in the skeletonized image, it is determined as an open (or close) pore. However, this method is very sensitive to noise and fails to work in cases when images are of poor quality or of lower resolution (1000dpi).Pore positions often give high negative frequency response as intensity values change abruptly from white to black. In order to capture this sudden change, we apply the Mexican hat wavelet transform to the original image

f(x, y) ∈ R2 to obtain the frequency response w:

$$w(s, a, b) = 1 \sqrt{s} \_ \_R2 f(x, y)\varphi(x - as, y - bs)dxdy, (1)$$

Where s is the scale factor (= 1.32) and (a, b) is the shifting parameter. Essentially, this wavelet is a band pass filter with scale s. After normalizing the filter response (0-255) using min-max rule, pore regions that typically have high negative frequency response are represented by small blobs with low intensities (Figure 2(b)).

4. Fake Detection Techniques

Two types of techniques for tracking Spoof fingers:

4.1 Hardware-based Methods

- **Odor Method:** A odor sensor (electronic nose) is used to sample the odor signal and an ad-hoc algorithm allow to discriminate the finger skin odor from that of other material such as latex, silicon or gelatin, usually employed to forge fake fingerprints.
- **Blood pressure detection:** Continuous noninvasive arterial blood pressure can be measured in finger arteries using an inflatable finger cuff (FINAP) with a special device and has proven to be feasible and reliable in adults.
- **Body temperature detection:** Temperature detection and regulation is of vital importance to any homoeothermic organism. In order to maintain temperature homeostasis it is necessary for the autonomic nervous system to monitor small fluctuations in core body temperature and initiate counter measures to prevent temperature fluctuations beyond a tightly controlled set point.
- **Pulsedetection:** The pulse sensor is noninvasive, easy to use, and made from items readily available. As a standalone, the pulse detector can be a way to introduce students into electrical engineering, spectrophotometry and to biomedical studies.

4.2 Software-based Methods

- **Analysis of perspiration pores:** The static features measure periodic variability in gray level along the ridges due to the presence of perspiration around the pores. The fake fingers fail to provide the static patterns due to the lack of active pore-emanated perspiration.
- **Shade changes between ridges and valleys:** equal height differences between ridges and valleys as a human finger. Optical sensors require the fingerprint capture platens be *shaded* from the.... dry fingers that have low contrast between the fingerprint ridge and valleys.
- **Comparison of fingerprint image sequence:**
A method for creating unique identifiers, called fingerprint sequences, for visually distinct locations by recovering statistically significant features in panoramic color images. Fingerprint sequences are expressive enough for mobile robot localization, as demonstrated using a minimum energy sequence-matching algorithm that is describe.
- **Observation of sweat pores :**
Sweating from a sweat gland could be continuously recorded using a technique in which ion-free sucrose solution was perfused onto a small region of the skin, and the secreted sweat detected by the change in electrical conductivity.

5. Experiment Result

5.1 The Set of Collecting Data

In this section when a person try to put a finger on any scanner platen area which is embedded with spoof technology , right now I am using Lumidigm V-Series v30X scanner to capture a time – series sequence of fingerprint scanned images at a particular frame rate.

For Example-:

While live scan surface when the SR (surface rate) is 20 fps (frame rate per second) and the capturing duration is 1.5 second, the sequence of image number is 30. The image sequence is used for detecting fake finger. One or more of them can be used for fingerprint authentication. Let {F1, F2… Fn} be the sequence of n images. For each image sequence, we use the last image to compute two features which are called static features. And we use all the images in sequence to compute three features which are called dynamic features.

According to my knowledge the FBI afis and other country AFIS using 500 dpi resolution image. So there is no database available in public or government sector of 1000 dpi resolution fingerprint. Then we make the database of 1000 dpi of slap fingerprint database around 500 different impression using Lumidigm J110 MSI sensor live scanner, each user gives 2 impression into 2 session interval of 2 days. Two different matching algorithms used for level 2 feature called Ridge/ minutia matcher. And level-3 feature are going to applied for this database. ROC(Receiver operating characteristic) curves for each individual matcher and the fusion algorithm are shown in figure 5. The number of genetic and imposter matches, respectively, are 3, 060 (500 × 6) and 83, 845 (500 x 509/2).

It is observed that matching results based on Level 3 features alone is very comparable to that of Level 2 features. Significant performance improvement (20%) is observed when the proposed Level 3 matcher is combined with Level 2 matchers using score-level fusion [11], as shown in Figure 4. This suggests that Level 3 features provide some discriminative information and should be used in combination with lower level features. It must be noted that the performance of both Level 2 and Level 3 matchers can be further improved if the images are captured in a more controlled environment. Currently, the high resolution optical sensor used in our experiment requires movement of the finger over a glass panel, resulting in partial distortion and smudginess in the captured images. In addition, the sensor is sensitive to skin condition and there is a large variance in image quality due to dryness or moisture (Figures 5(a-b)).

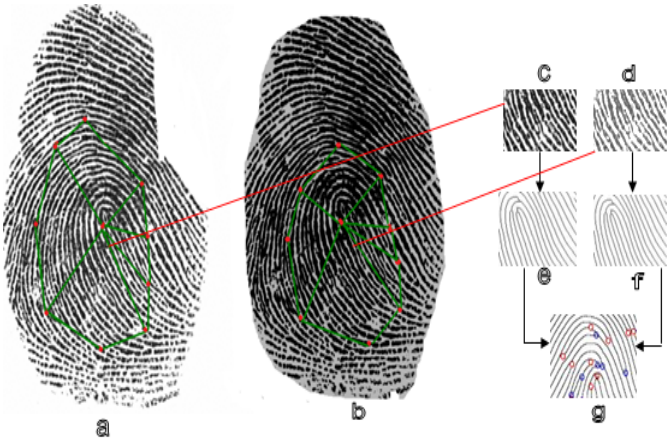

Figure 5: Matching features of Level 3: (a-b) the question and answer images with relative minutia overlaid. (c-d) Windows segmented from the temple and query. (e-f) Extracted Level-3 features from the segmented windows from the temple and query.(g) Level-3 matching using the modified ICP algorithm.

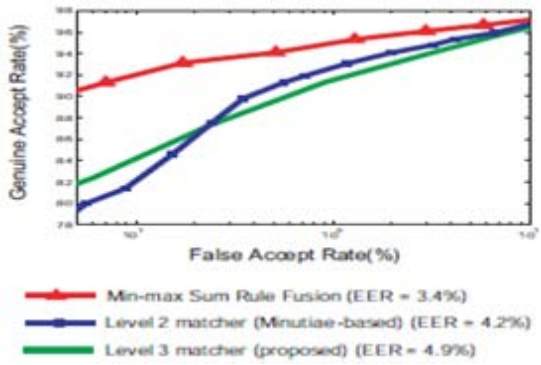

Figure 6: ROC curves for Level 2 and Level 3 matchers and the fusion algorithm based on using sum-rule and min-max normalization.

6. Prevent Fingerprint Spoofing Help of Multimodal Approach

A multimodal approach included the high and reliable techniques of authenticating genuine users. A multimodal include more than biometric sources to achieve the goals. Multimodal biometrics can include the physiological and behavioral biometrics, but mostly physiological is used for more reliable authentication. A physiological biometrics is more accurate comparison to other. Multimodal biometrics system uses multiple sensor or biometrics to overcome the limitation of unimodel biometrics system. For example – Fingerprint can be used with IRIS, palm, face or can be used as a combined.

Multimodal system contain both finger and iris feature in the database as a fusion algorithms.

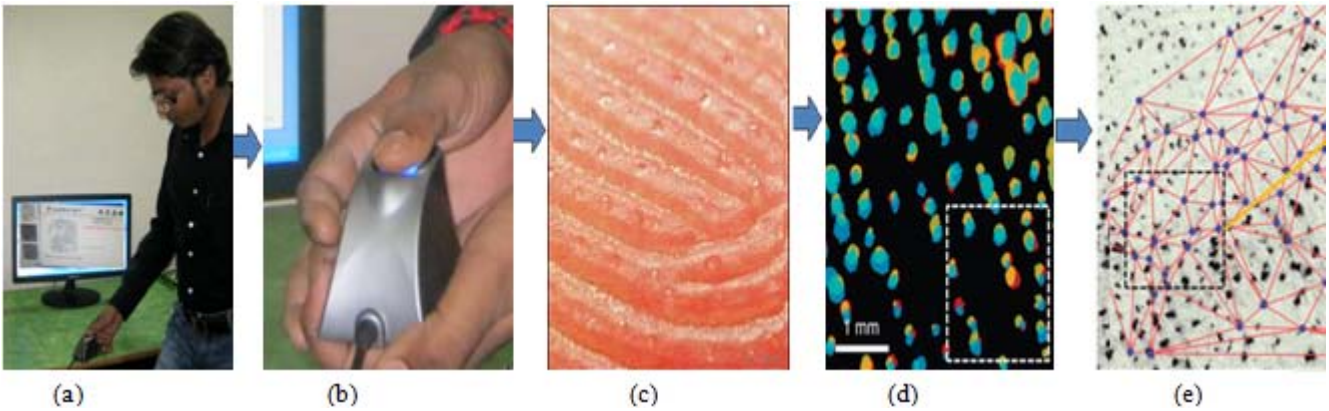

Figure 7: Experiment spoof detection work using Lumidigm vx30x Scanner. (a)- Ready to give impression with spoof detection algorithm using lumidigm GUI. (b)- Capturing impression (c)- A Ridge and valley showing pores structure. (d)- Pores pattern recognition with invert background. (f)- Connective pores path structure start with relative points.

Now if a user trying to give alter finger, same time it needs to give another biometrics source like face and iris. If both are failed to authenticate then system rejects the user. Multimodal biometrics makes the use of multiple source of information for personal authentication.

Noisy data, Intraclass Variation, Interclass Similarities, Non universality, Spoofing etc problems are imposed by unimodal biometric systems which tend to increase False Acceptance Rate [FAR] and False Rejection Rate [FRR], ultimately reflecting towards poor performance of the system.

Some of the limitations imposed by unimodal biometrics can be overcome by including multiple source of information for establishing identity of person. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a Verification or Identification system. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. Multimodal biometrics also address the problem of spoofing as it concern with multiple traits or modalities, it would be very difficult for an imposter to spoof or attack multiple traits of genuine user simultaneously [13].

Multimodal biometric system has the potential to be widely adopted in a very broad range of civilian applications as well as Criminal application:

Banking security such as ATM security, check cashing and credit card transactions,, AMBIS (Automatic Multibiometrics Identification System), information system security like access to databases via login privileges. A decision made by a multimodal biometric system is either a “genuine individual" type of decision or an “imposter" type of decision. In principle, Genuine Acceptance Rate [GAR], False Rejection Rate [FRR], False Acceptance Rate [FAR] and Equal Error Rate [ERR] is used to measure the accuracy of system. Generally multimodal biometrics operates in two phases i.e. Enrollment phase and authentication phase which are described as follows:

Enrollment phase: In enrollment phase, biometric traits of a user are captured and these are stored in the system database as a template for that user and which is further used for authentication phase.

Authentication phase: - In authentication phase, once again traits of a user captured and system uses this to either identify or verify a person. Identification is one to many matching which involves comparing captured data with templates corresponding to all users in database while verification is one to one matching which involves comparing captured data with template of claimed identity only.

Fusion Feature: Combination of multiple schemas applied in the recognition system is become more effective. In the feature level fusion, signals coming from different biometric traits are first processed and feature vectors are extracted separately from the each biometric trait. After that these feature vectors are combined to form a composite feature vector which is further used for classification. In case of feature level fusion some reduction technique must be used in order to select only useful features. Some of the researchers have applied fusion at feature level. Since features contain richer information of biometric trait than matching score or decision of matcher, fusion at feature level is expected to provide better recognition results but it has also observed that when features of different modalities are compatible with each other then fusion at feature level achieves more accuracy.

Figure 9 shows feature level fusion.

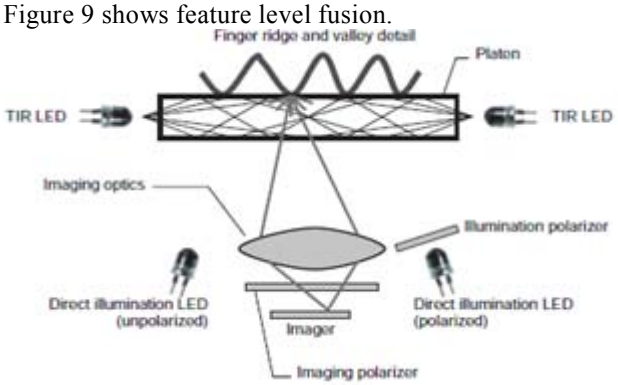

Figure 8: showing Lumidigm spoof MSI sensor showing TIR illumination

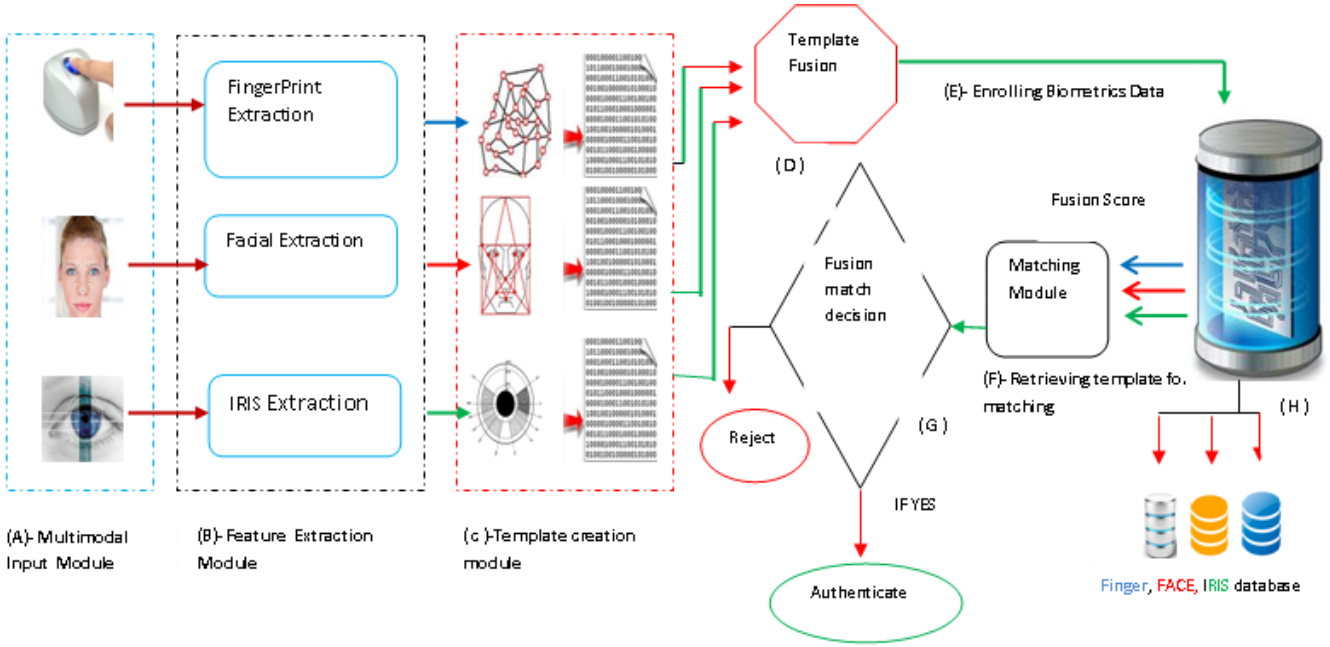

Figure 9: Showing Multimodal biometric system for accurate matching and preventing spoof detection using of fusion score matching algorithm. (A)- showing multimodal input system. (B)- Extraction module extract features of finger face, and iris. (C)- This module makes the template of finger, face and iris. (D)- Fusion algorithm fuses the template in single unit. (E)- According to query Template enroll in relevant database. (F)- Retrieving fused template for authenticating user. (G)- Decision module acknowledges whether user is valid and fusion algorithm check whether multimodal cumulative score is above matching threshold or not. If score is ok then system authenticate else rejected.

7. Conclusion

In this paper describes a way of detecting fake finger by using multiple static features like pores extraction, ridge and valley and taking help of multimodal biometrics such as face, iris. There are many multimodal biometric systems in existence for authentication of a person but still selection of appropriate modals, choice of optimal fusion level and redundancy in the extracted features are some challenges in designing multimodal biometric system that needs to be solved. Preventing spoofing for finger use more than one biometrice resources to identify someone. If user trying to alter finger the fusion algorithm return the cumulative score whether its match or not. Although biometric authentication devices can be susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such attacks.

8. Future Work

In this project we are discussing about altering fingerprint using Level 3 feature of pores extraction with the help of multimodal system. Although multimodal system is more accurate and reliable but if you don not want multimodal and only focus on fingerprint then there were several techniques to prevent spoofing, which is you can use ridge and valley, dots, scars, and also can be used thermal , pulse and vein detection algorithm. Because implementing multimodal is cost effective and can't be use by all person. Combination of IRIS and facial with fingerprint used in highly secured are like police, government security are, army, banks or some sensitive and important areas. So, its best that use of some other feature of fingerprint which we discussed above to track down spoofing of fingerprint.

References

[1] Neuro technology Inc., VeriFinger, http://www.neurotechnology. com/vf_sdk.html, 2011.
[2] Lumidigm. J-Series Multispectral Fingerprint Sensors. Albuquerque, NM. 2006.
[3] S. Parthasaradhi, R. Derakhshani, L. Hornak, and S. Schuckers, Time-series detection of perspiration as a vitality test in fingerprint devices, IEEE Trans. On SMC, Part C, 35 (3) 335-343. 2005.
[4] P. Coli, G.L. Marcialis, and F. Roli, Vitality detection from fingerprint images: a critical survey, IEEE/IAPR International Conference on Biometrics ICB 2007, Springer LNCS 4642, pp.722-731.
[5] Y. Chen, A.K. Jain, S. Dass, Fingerprint deformation for spoof detection, Biometric Symposium, 2005.
[6] P. Coli, G.L. Marcialis, and F. Roli, Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device, Int. Journal of Image and Graphics, 8 (4) 495-512, 2008.
[7] NIST Special Database 14, NIST Mated Fingerprint Card Pairs 2 (MFCP2), http://www.nist.gov/srd/nistsd14.htm. 2011.
[8] A. Roddy, and J.D. Stosz, Fingerprint features-statistical analysis and system performance estimates, Proc. IEEE, vol. 85 n. 9, pp. 1390-1421, 1997.
[9] http://bias.csr.unibo.it/fvc2004/
[10] A. Tidu, Fingerprint vitality assessment by pores detection, M.Sc. Thesis, G.L. Marcialis and F. Roli (Supervisors), University of Cagliari, April 2010.
[11] Fake Finger Detection Using the Fractional Fourier Transform, http://link.springer.com/chapter/10.1007/978-3- 642-04391-8_41#page-1

[12] J.D. Stosz and L.A. Alyea, "Automated system for fingerprint authentication using pores and ridge structure," Proc. of the SPIE Automatic Systems for the Identification and Inspection of Humans, Volume 2277, pp. 210-223, 1994.
[13] Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013 DOI : 10.5121/sipij.2013.4105 AN OVERVIEW OF MULTIMODAL BIOMETRICS
[14] Mishra, "Multimodal Biometrics it is: Need for Future System," International Journal of Computer Application, vol. 3, no. 4, pp. 28-33, June 2010.
[15] Pores and Ridges: High-Resolution Fingerprint Matching Using Level 3 Features Anil K. Jain, Fellow, IEEE, Yi Chen, Student Member, IEEE, and Meltem Demirkus, Student Member, IEEE

Author Profile

Maneesh Kumar Sharma was born in Mankapur (Gonda) U.P. India. He received the B.Sc degree from Awadh University Faizabad U.P., E-commerce diploma from NIIT Lucknow, MCA degree from Sikkim Manipal University, MCP, MCSA, MCSE Diploma from Microsoft, MBA (IT) Degree from Amity University Lucknow U.P. He is currently pursuing M.Tech(CSE) from Monad University Hapur U.P. Maneesh Sharma currently working as a Project Manager (R&D IT) since 2005 at SecureMantra Technologies Lucknow .U.P. and handling Criminal biometrics projects in more than 15 states in india. Totally involved in R&D of Fingerprint, Facial and IRIS based recognition system. In R&D center he is researching about different method of image processing, live scanners, spoof detection algorithms using hardware and software, and also monitoring and implementing multimodel biometric system, which is combination of fingerprint, facial and IRIS for Police Department (Crime Branch). The project which he is handling called AFIS (Automated fingerprint identification system), AMBIS (Automated multimodal biometric identification system).