International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 4, Issue 4, 2017, PP 81-89
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
DOI: http://dx.doi.org/10.20431/2349-4859.0404010
www.arcjournals.org

Reconnoitering and Instigating Fingerprints as Secure Biometric Technique

Pravjot Kaur[1], Dr. Gagandeep Jagdev[2]

[1]*Research Scholar (M.Phil), Dept. of Comp. Appl., Guru Kashi University, Talwandi Sabo (PB)*

[2]*Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib (PB)*

Corresponding Author:** ***Dr. Gagandeep Jagdev*, Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib (PB), India.*

Abstract: *It is now a known fact that passwords and tokens are highly susceptible to being stolen or lost. A weak password is the main reason for security and data breaches. Even strong passwords are not able to resist sophisticated hacker attacks. Resetting forgotten or lost passwords require time and hinder the employee productivity. So all this needs to be placed on a more secure technology like biometric.Biometric authentication is a practice of identifying or verifying individuals on the basis of their unique physiological or behavioral characteristics such as iris, gait, fingerprints, facial patterns, DNA, voice patterns, etc. The notion of identifying people on the basis of fingerprints can be traced back to thousands of years. However, it first appeared as an automated technology in the year 1970. The driving force behind the use of biometrics has been convenience besides security. Fingerprint authentication denotes the automated practice of verifying and matching fingerprints of two humans. Fingerprint identification is more popular than other biometric identifications because of its ease in the acquisition, the established use, and collections by immigration and law enforcement agencies and the multiple sources (ten fingers) accessible for collection. The research paper elaborates the key features of fingerprints and the working of Automatic Minutiae Detection algorithm. The paper also highlights the implementation of Matlab code concerning recognition of characteristics of fingerprints. The paper also compares the 2D fingerprint identification with 3D fingerprint identification.*

Keywords: *Automatic Minutiae Detection; biometrics; fingerprints, minutiae.*

Abbreviations: *AMD*

1. INTRODUCTION

The technology is bound to smart enough to fulfill the needs and necessity for higher levels of security. It is mandatory for any new innovation, creation, or development to be unsophisticated in order to be acceptable worldwide. This strong need for user friendly systems committed to protect one's privacy led to the development of technology what's called biometrics [1]. Biometrics involve identification of persons by their behavioral or physical characteristics. Physical characteristics comprises face, iris, fingerprints, and even palm geometry and behavioral characteristics involves signature, voice, and keystroke dynamics as shown in Fig. 1.

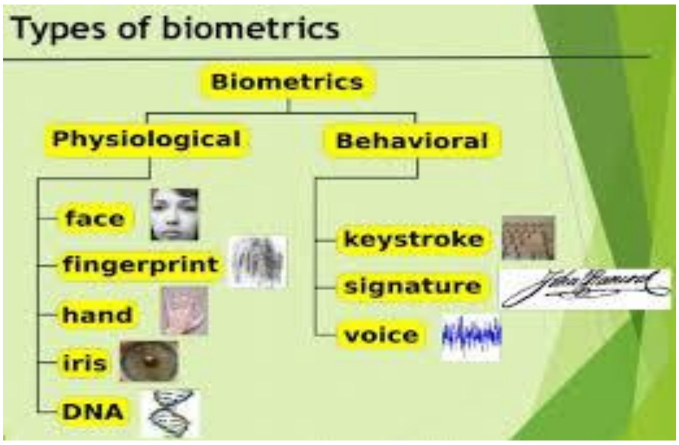


Fig1. *The figure shows two categories of biometrics*

Biometrics is the promising area of bioengineering. Biometrics modes involved in identification purposes have been found to be most convincing and interesting authentication technique. Biometrics authenticates one as one. The parts of human body act as permanent passwords. Biometrics offers unique advantages over traditional methods of identifying humans. Besides eliminating risks, biometrics offer a high level of convenience and security to both administrators and users. Table 1 below illustrates different biometric parameters which should be fulfilled by the technology to qualify as a secured biometric [2, 3].

Universality	Signifies that each person should have the biometric characteristic
Uniqueness	Signifies that biometric adopted should be such that it separates individuals from another
Permanence	Signifies that biometric should be such that it should resist factors like aging and other variance over time
Collectability	Signifies that biometric should be easily acquirable for measurement
Performance	Signifies that accuracy, speed, and robustness of biometric should be dependable
Acceptability	Signifies degree of approval of technology
Circumvention	Signifies ease of use of a substitute

Since fingerprints are inborn to individuals and can neither be stolen or lost, makes it reliable and precise. The easy accessibility and availability of low-cost fingerprint readers attached with easy incorporation capabilities have led to the widespread disposition of fingerprint biometrics in a variety of organizations. Verification and identification are two different concepts of recognizing individuals on the basis of their fingerprints. Verification refers to the practice of confirming that a person is indeed who he/she claims to be and accomplishes a one-to-one comparison of the individual's fingerprint sample with the already stored template for reference. On the other hand, identification performs the one-to-many comparison in order to confirm person's identity. In identification process, the individual's fingerprints are compared against all the reference templates stored on a file [4, 5]. A person is identified if his/her individual fingerprint image matches with any of the stored in the templates. Fig. 2 shows different human body parts qualifying as biometrics. Table 2below shows fingerprints compared to other biometric technologies in terms of accuracy, convenience, cost and size (1 being worst and 5 being the best). Fig. 3 shows the graphical representation of the data mentioned in Table 2.

Fig2. *The figure shows different human body parts acting as biometrics*

Table2. *The table shows the comparison of 5 different biometric techniques on 4 parameters*

Technology	Accuracy	Convenience	Cost	Size
Fingerprint	5	5	4	4
Voice	1	5	5	5

Face	2	3	4	3
Hand	3	3	2	2
Iris	5	2	3	3

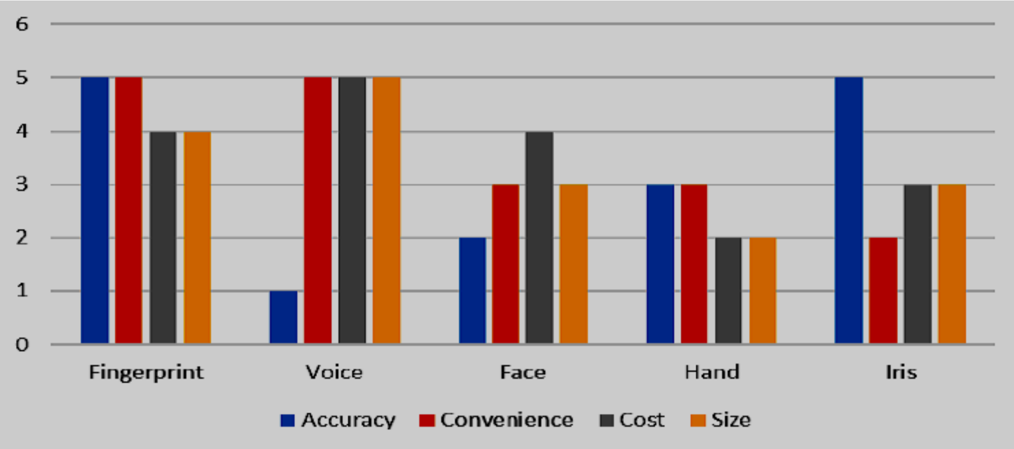


Fig3. *The figure shows the graphical representation of the data placed in Table 2*

2. Fingerprints Classification

During past, manual fingerprint classification systems were brought in practice to categorize fingerprints based on general ridge formations, which results in the filing of paper records in large collections based on ridge patterns and was independent of birth date, name, and other biographic data that an individual may misrepresent. The three prominent fingerprint classification systems are the Roscher system, the Vucetich system, and the Henry system. The Roscher system was established in Germany and along with Germany, was also implemented in Japan. The Vucetich System was brought up in Argentina and adopted throughout South America. The Henry system was developed in India and adopted in many English speaking countries. The Henry system comprises of three main fingerprint patterns: loop, whorl, and arch. Loops are mostly ulnar or radial, depending on the side of the hand to which tail points. Whorls can be classified as accidental whorls, double loop whorls, plain whorls, and central pocket loop whorls. Fig. 4 shows the different patterns of fingerprints possessed by humans [6].

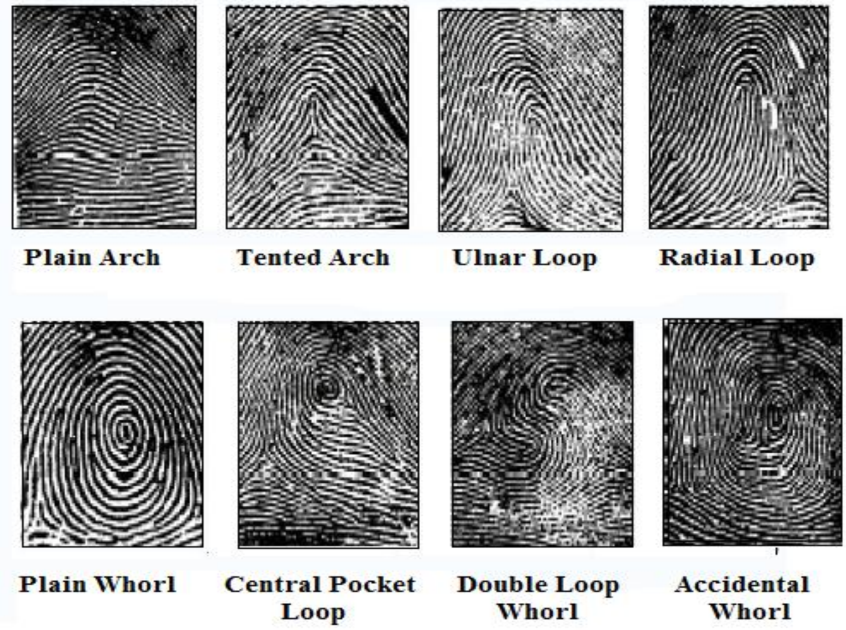


Fig4. *The figure depicts the different patterns available in fingerprints*

3. Working of Fingerprint Recognition Technique

This section details about the step-wise working on fingerprint recognition technique. Fig. 5 depicts the main modules involved in fingerprint recognition system [7, 8].

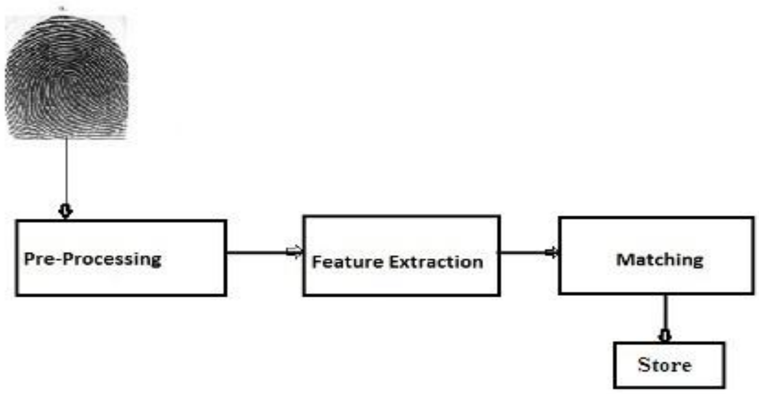


Fig5. *The figure shows the main modules of a fingerprint recognition system*

The main modules of a fingerprint verification system (Fig. 5) are:

- *Fingerprint sensing*

Firstly, the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation.

- *Preprocessing*

In this, the input fingerprint is enhanced and adapted to simplify the task of feature extraction.

- *Feature extraction*

In this step, the fingerprint is further processed to generate discriminative properties, also called feature vectors.

- *Matching*

In this step, the feature vector of the input fingerprint is compared against one or more existing templates. The templates of approved users of the biometric system, also called clients, are usually stored in a database. Clients can claim an identity and their fingerprints can be checked against stored fingerprints.

Fig. 6 and Fig. 7 depicts the working and algorithm of fingerprint recognition technique respectively.

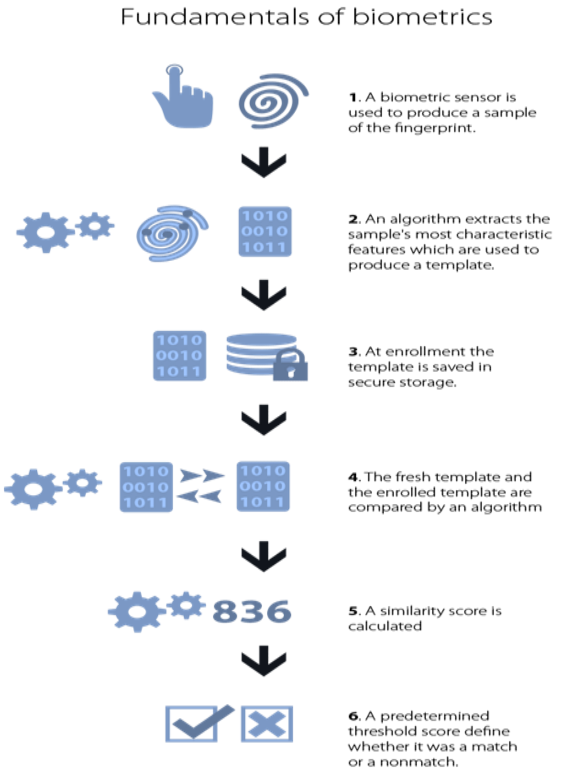

Fundamentals of biometrics
1. A biometric sensor is used to produce a sample of the fingerprint.
1010 0010 1011
2. An algorithm extracts the sample's most characteristic features which are used to produce a template.
3. At enrollment the template is saved in secure storage.
4. The fresh template and the enrolled template are compared by an algorithm
836
5. A similarity score is calculated
6. A predetermined threshold score define whether it was a match or a nonmatch.

Fig6. *The figure elaborates the fundamental working of fingerprint recognition technique*

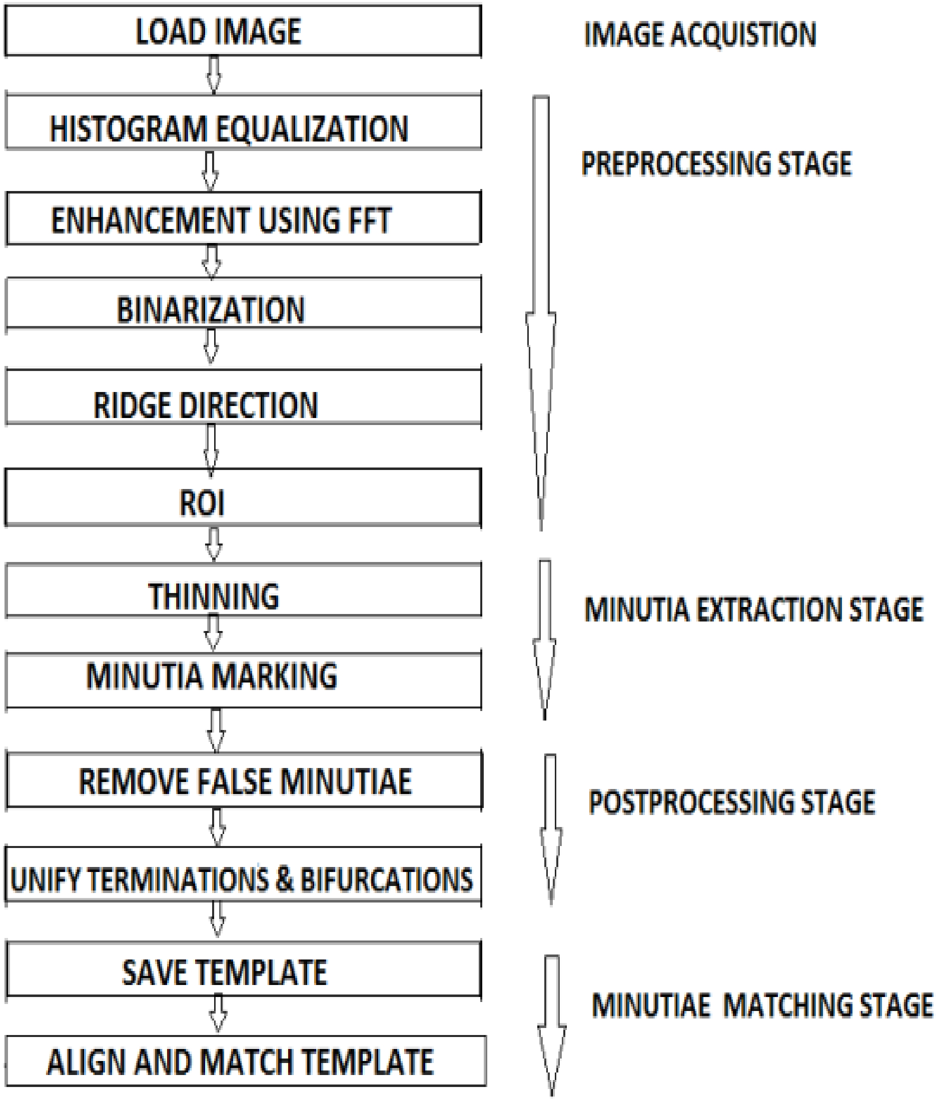


Fig7. *The figure shows the flowchart depicting working of Fingerprint Recognition technique*

4. Major Problems Encountered In Fingerprint Recognition

The primary problems concerned with this research work are mentioned as under [9, 10].

Quality of image

- One of the open issues in fingerprint verification is the lack of robustness against image quality degradation. The performance of a fingerprint recognition system is heavily affected by fingerprint image quality.
- Several factors determine the quality of a fingerprint image: skin conditions (e.g., dryness, wetness, dirtiness, temporary or permanent cuts and bruises), sensor conditions (e.g., dirtiness, noise, size), user cooperation, etc

Poor quality images result in spurious and missing features, thus degrading the performance of the overall system. Therefore, it is very important for a fingerprint recognition system to estimate the quality and validity of the captured fingerprint images.

Avoiding False Rejection

Any biometric method may present some rejection problem because they involve human and biological characteristics. That means that even a person whose fingerprint is already recorded may not be recognized. This is called "false rejection" and happens with any technology and manufacturer [11].

- This problem rarely occurs (below 0.1% of the cases), but it is important to keep this possibility in mind during the implementation, so you can plan on what to do if that happens. The individuals that present this kind of situation are the elderly and children up to 6 years old.
- Some chemical products may also provoke the temporary reduction of a fingerprint quality. In addition, some people don't have fingerprints on some periods of the year, due to biological conditions associated with weather or to their own organism.

However, many false rejections happen because of an error during the registration, with the capture of a partial fingerprint. That increases the possibility of a rejection, because the next time that fingerprint will be read, the captured image may be a different one, not registered yet. A correct registration is the best way of avoiding a false rejection [12, 13].

5. Contribution and Implementation

The research work makes use of Matlab as simulation tool for analyzing fingerprints and extracting minutiae points via writing appropriate codes. The snapshots below explain the working of designed project.

The image is given as an input from database (Fig. 8) and enhanced in order to recognize the terminal points and bifurcations (Fig. 9). Finally, a text file is generated (Fig. 10 and Fig. 11) with detailed reports illustrating different points having ridge ending and bifurcations.

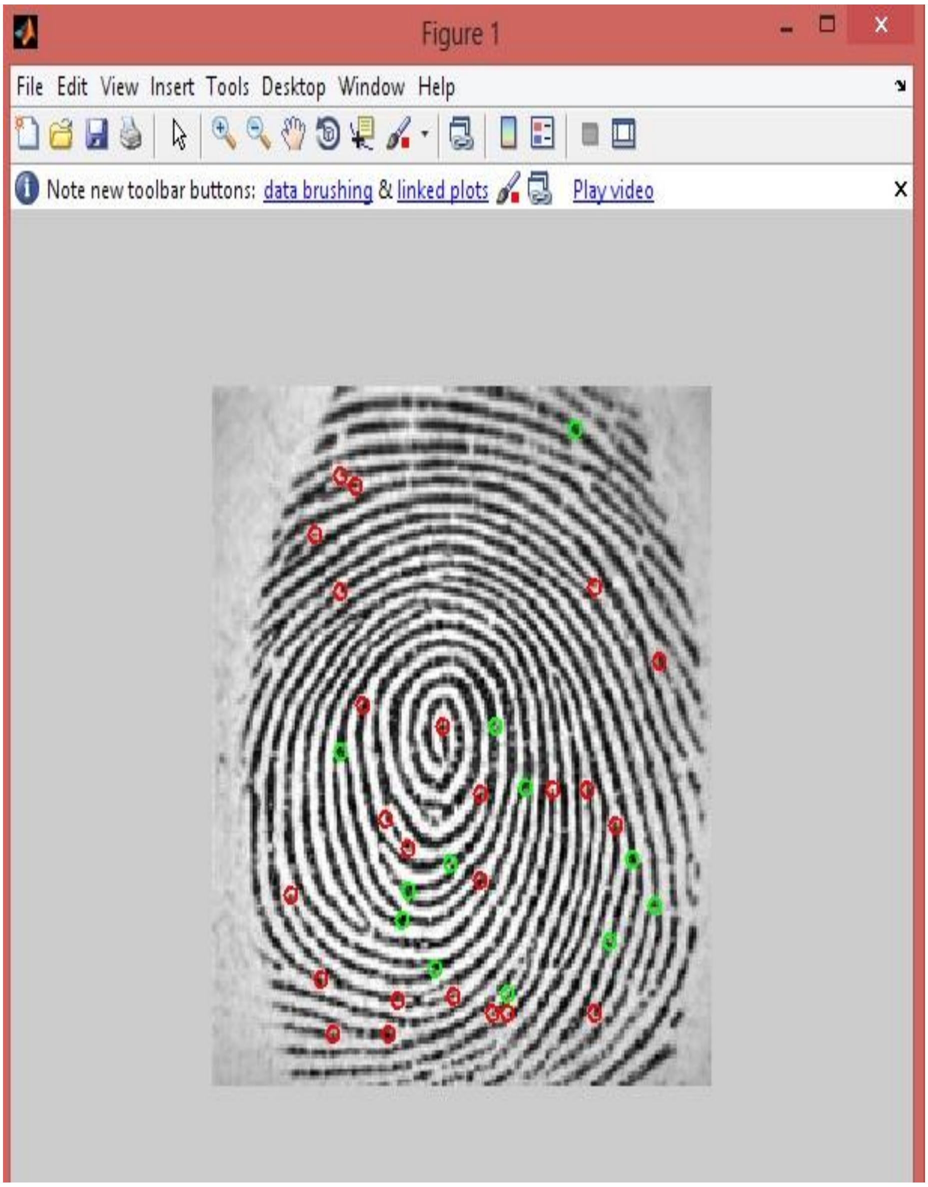


Figure 1
File Edit View Insert Tools Desktop Window Help
Note new toolbar buttons: data brushing & linked plots
Play video

Fig8. *Snapshot depicts a partially enhanced input image highlighting termination points (red colored) and bifurcations (green colored).*

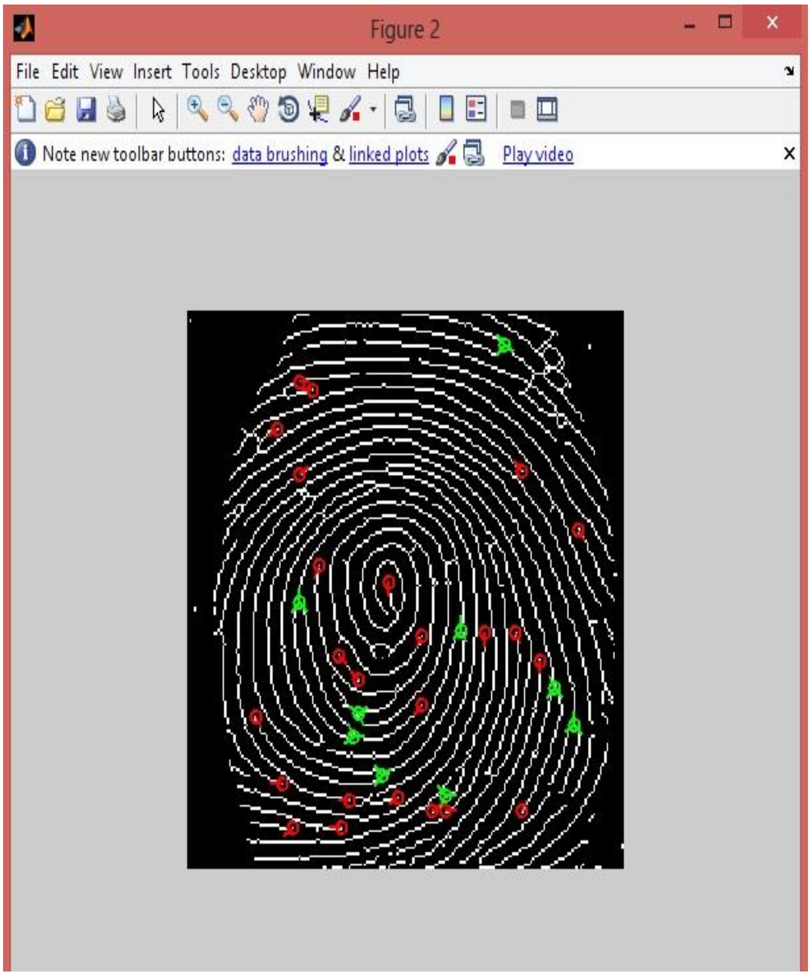
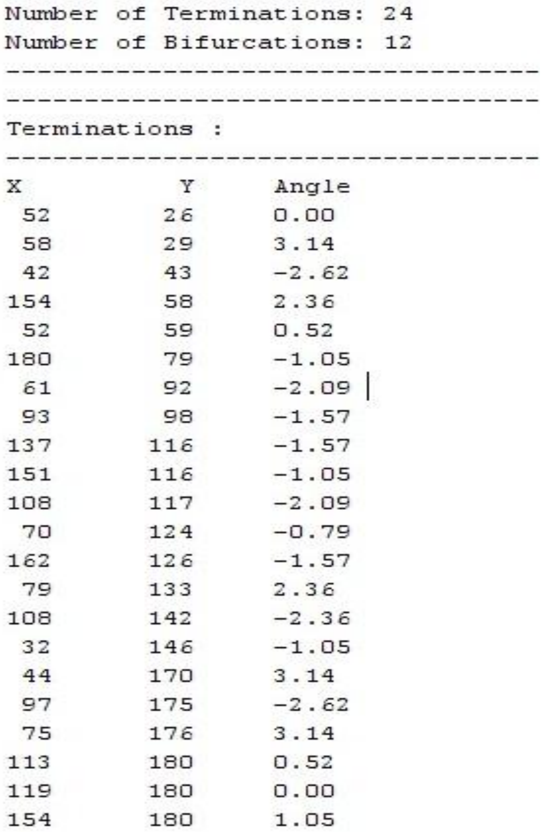


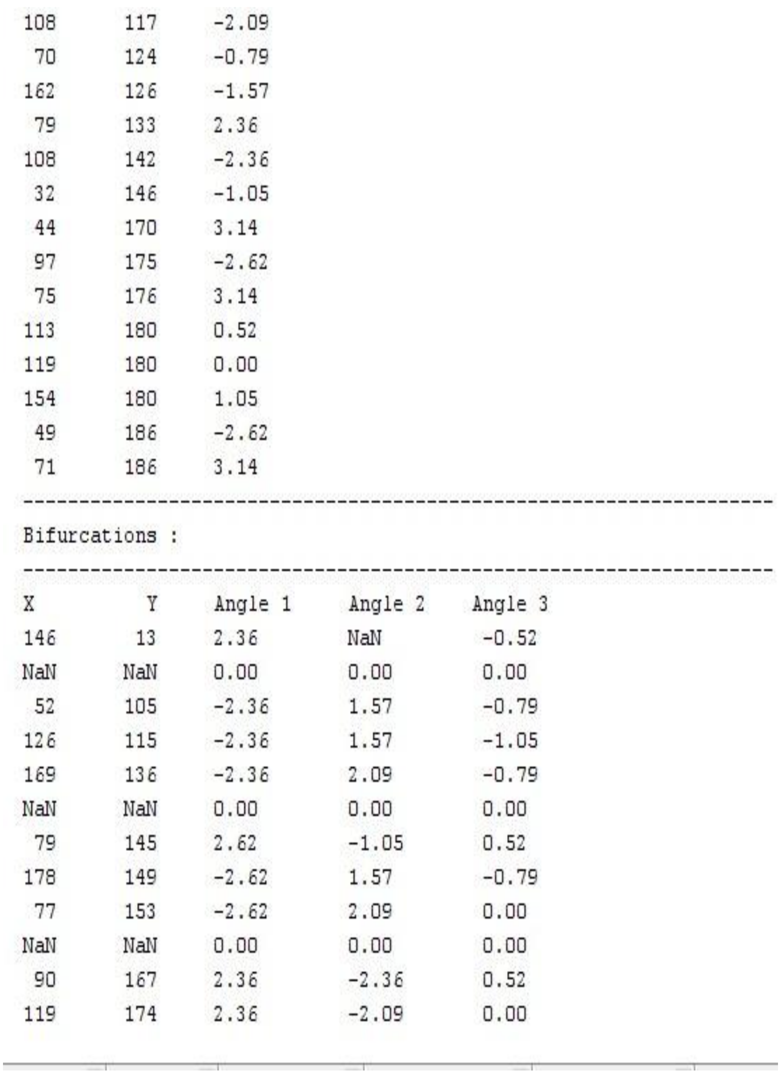
Figure 2
File Edit View Insert Tools Desktop Window Help
Note new toolbar buttons: data brushing & linked plots
Play video

Fig9. *Snapshot depicts a fully enhanced input image highlighting termination points (red colored) and bifurcations (green colored).*



```
Number of Terminations: 24
Number of Bifurcations: 12
-----------------------------------
-----------------------------------
Terminations :
-----------------------------------
X          Y      Angle
 52       26      0.00
 58       29      3.14
 42       43      -2.62
154       58      2.36
 52       59      0.52
180       79      -1.05
 61       92      -2.09
 93       98      -1.57
137      116      -1.57
151      116      -1.05
108      117      -2.09
 70      124      -0.79
162      126      -1.57
 79      133      2.36
108      142      -2.36
 32      146      -1.05
 44      170      3.14
 97      175      -2.62
 75      176      3.14
113      180      0.52
119      180      0.00
154      180      1.05
```

Fig10. *Snapshot depicts the text file generated highlighting termination points at different x-y axis.*



```
108      117     -2.09
 70      124     -0.79
162      126     -1.57
 79      133     2.36
108      142     -2.36
 32      146     -1.05
 44      170     3.14
 97      175     -2.62
 75      176     3.14
113      180     0.52
119      180     0.00
154      180     1.05
 49      186     -2.62
 71      186     3.14
---------------------------------------------------------------------
Bifurcations :
---------------------------------------------------------------------
X          Y     Angle 1      Angle 2    Angle 3
146       13     2.36         NaN         -0.52
NaN      NaN     0.00         0.00        0.00
 52      105     -2.36        1.57        -0.79
126      115     -2.36        1.57        -1.05
169      136     -2.36        2.09        -0.79
NaN      NaN     0.00         0.00        0.00
 79      145     2.62         -1.05       0.52
178      149     -2.62        1.57        -0.79
 77      153     -2.62        2.09        0.00
NaN      NaN     0.00         0.00        0.00
 90      167     2.36         -2.36       0.52
119      174     2.36         -2.09       0.00
```

Fig11. *Snapshot depicts the text file generated highlighting bifurcations at different x-y axis.*

6. Conclusion

With respect to traditional fingerprint recognition systems, which require the contact of the finger with the sensor, touch less biometric technologies present important advantages in terms of quality of the acquired samples, usability, acceptability, and robustness to environmental conditions. The research paper elaborated the characteristics associated with biometrics and prominently with fingerprints. The paper also discussed the implementation of fingerprint recognition technique and providing the number of bifurcations and terminals points as an output in a text file after pre-processing and enhancing the given input image.

References

[1] Subhas Barman et al., “Fingerprint-based crypto-biometric system for network security”, EURASIP Journal on Information Security, Springer Open Journal, 2015, DOI 10.1186/s13635-015-0020-1.

[2] Sally. H. Ismail et al., “Experimental Study of Minutiae Based Matching Algorithm for Fingerprint Recognition System”, IJCST, Volume - 4, Issue – 5, Sept - Oct 2016.

[3] Sangeeta Narwal et al., “Comparison between Minutiae based and Pattern Based Algorithm of Fingerprint Image”, MECS, March 2016, DOI: 10.5815/ijieeb. 2016. 02. 03.

[4] NaserZaeri, “Minutiae-Based Fingerprint Extraction and Recognition”, Intech Open Science, http://www.intechopen.com/books/biometrics.

[5] Gagandeep Jagdev et al., “Analyzing 2D & 3D Fingerprint Recognition Techniques as Secure Biometric”, International Journal of Scientific and Technical Advancements (IJSTA), ISSN: 2454-1532Vol. 2, Issue 4, pp – 119 – 124, 2016.

[6] Priyanka Sharma, Manavjeet Kaur, Classification in Pattern Recognition: A review, IJARCSSE, Volume 3, Issue 4, April 2013.

[7] M. D'Acuntoa , G. Pierib, M. Righib, and O. Salvettib, A Methodological Approach for Combining Super Resolution and Pattern Recognition to Image Identification1, Springer, Pattern Recognition and Image Analysis, Vol. 24, No. 2, pp. 209-217, 2014.

[8] Madhuri and Richa Mishra, Fingerprint Recognition using Robust Local Features, IJARCSSE, Volume 2, Issue 6, June 2012.

[9] Gagandeep Jagdev et al., "Drawbacks of 2D Fingerprint recognition systems makes way for 3D Fingerprint recognition systems", WECON 2015, Chandigarh, India.

[10] Neeraj Bhargava, Ritu Bhargava, Manish Mathuria, MinaxiCotia, Fingerprint Matching using Ridge-End and Bifurcation Points, International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012).

[11] Gagandeep Jagdev et al., "A Study on working of 2D fingerprint recognition system and how contactless 3D fingerprint recognition systems assures greater perfection in human identification", International Conference on Advanced Computing & Communication Technologies (ICACCT – 2014), Volume 2, ISBN: 978 – 93 – 84935 – 00-9, 15th November 2014, pp. 150 – 154, APIIT, Panipat, India.

[12] DibyenduNath, Saurav Ray, Sumit Kumar Ghosh, Fingerprint Recognition System: Design & Analysis.

[13] Ravi Subban and Dattatreya P. Mankame, A Study of Biometric Approach Using Fingerprint Recognition, Lecture Notes on Software Engineering, Vol. 1, No. 2, May 2013.

AUTHOR'S BIOGRAPHY

Dr. Gagandeep Jagdev, is a faculty member in Dept. of Computer Science, Punjabi University Guru Kashi College, Damdama Sahib (PB). His total teaching experience is above 11 years and has above 118 international and national publications in reputed journals and conferences to his credit. He is also a member of editorial board of several international peer-reviewed journals and has been active Technical Program Committee member of several international and national conferences conducted by renowned universities and academic institutions. His field of expertise is Big Data, ANN, Biometrics, RFID, Cloud Computing, Cryptography, and VANETS.

Citation: *Pravjot Kaur & Dr. Gagandeep Jagdev (2017). Reconnoitering and Instigating Fingerprints as Secure Biometric Technique, International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), 4(4), pp.81-89, DOI: http://dx.doi.org/10.20431/2349-4859.0404010*