JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Image Processing Based on Verification for Secure Fingerprint

Jaishree Jain[1*], Heena Arora[2]

[1]Department of Computer Science and Engineering, Chandigarh University, Punjab, India &
Department of Computer Science and Engineering, Uttarakhand Technical University, Dehradun, India
[2]Department of Computer Sciences and Engineering, Student of Chandigarh University, Punjab, India

**Corresponding Author: jaishree3112@gmail.com, Tel.: +91-7055455947*

DOI: https://doi.org/10.26438/ijcse/v7i5.169174 | Available online at: www.ijcseonline.org

Accepted: 12/May/2019, Published: 31/May/2019

Abstract— In this paper, we have worked on digital fingerprint for secure and true verification of any human. The fingerprint fractionalization presents the extracted feature in characteristic polygon. It is accurate and secure method with the onion algorithms of computational geometry to detect the verification which are based on fingerprint over the cloud. This method is an alternative method, which used to minutiae extraction algorithm. We can compare proposed algorithm (Onion Algorithm of computational geometry) to commercial verification algorithm which works simultaneously with Ratha's algorithm. During the execution, the experiment result comes in positive verification of the digital Fingerprint in our proposed work. Low cost and super automated technique is the best advantage of the Biometric fingerprint recognition to verify the best match among multiple human fingerprints. We have also used texture feature in this paper.

Keywords— Computational Geometry, Encryption, Fingerprint, Onion layers, Verification of fingerprints

I. INTRODUCTION

Biometry, as the research is going on mathematical and statistical property in the area of behavioral human characteristics and its physiology, which are widely using in forensic and non-forensic organization with its application software to provide the more flexible security for the verification of authorized or unauthorized humans by the their fingerprint. We can also use remotely with the PC or other devices which works as Personal Computer. If the connected computer of the respective organizations gives the access by the server's owner to control the verification of human fingerprints via LAN, MAN, WAN. In the proposed work, we have worked on a finger print scanning technique, the unique and small marks of the fingerprint emphasize as minutiae. We can identify the Minutiae points where the ridge goes to end and also can be seen in the branches on the tips of any finger with the bifurcations [1, 2]. In the live-scan of fingerprint, it contains 30-40 minutiae. Finger scanning keeps protection from the environmental disturbance. Quality of the fingerprint affects while capturing the image process. If, scanner device surface is dirty and if any finger of human touch on scanner device then the fingerprint image records in the bad quality and that record goes into the garbage. Quality of the fingerprint also depends on the condition of the pressure at the time of taking fingerprints, skin sharpness, alignment and rotation of the finger. Further, such type of methods may be caused to attack by hackers when biometric features are transferred via Internet [3]. We have developed the method, which also find-out the position of finger print as rotation, alignment, reverse, which indicates the attacks to the fingerprint data so that fingerprint data can't be affected by the hackers. Our proposed method is based on Onion computational geometry algorithm. A novel process method used as main extract feature, which would be specified as unique for each human. The features of OACG determine by the pixels of fingerprint brightness, degree, edge, and minutiae points and ridges detection. Specific geometric area dominants the range of brightness value of the fingerprint. Biometrics fingerprint database can be stored securely in many of the applications, which make biometrics useful for the several types of organizations. For the security purpose, digital fingerprints database are used to take information of human in more protected way so that the efficiency and bandwidth of the system can be improved. Further, we have divided this paper in four sections i.e. Tool & Techniques is described in section II, Proposed Work in section III, Result in section IV and Conclusion in section V.

II. TOOLS & TECHNIQUES

A. Software Tools with their Function:

1. *Java Eclipse:* This is general basic software, which is used in this paper. This software has many functions that helps to

implement the advance software and in the research for the researchers. We have mentions some main functions are as follows:

- Frame creations
- Frame link to Database
- Connection of the link between Arduino Board and computer.

2. *Arduino software:* This software establishes the connection between the computer and finger print sensor R307.
3. *XAMMAP:* This is a DBMS software to store the data of the digital fingerprint record.

The thin driver converts JDBC calls directly into the specific database protocol. That is why it is known as thin driver. It's programming written in Java language. Steps of Thin Driver:-

- LOAD DRIVER CLASS
- CREATE CONNECTIONS
- LOADING JAR FILES

(a) Advantage:

- Process speed and outputs is better than the other drivers.
- It is not based on particular software for the client and the server.

(b) Disadvantage:

- The Driver is not independent for the Database.

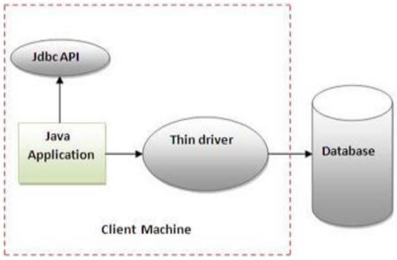

Fig. 1: Thin Driver

B. Hardware Tools with their Functions:

1. ARDUINO BOARD:

The Arduino Uno board is a microcontroller which based on the ATmega328. This hardware designed with 14 digital pins to give and take the input/outputs. It has 6 analog inputs with 16 MHz crystal oscillator, an ICSP header, power slot, and a reset button, etc. This microcontroller contains everything which is needed to support the computer and compatible with a USB cable to connect to the computer and power on with the AC or DC to get started by the battery. Its adapter converts Alternative current to Direct Current to get started. The Arduino device works differently with its older device version as it doesn't use the FTDI for connect to USB to serial port driver chip.

Fig. 2: Arduino Device

2. *R307:* This device contains finger print sensor that is used to take the images and store in the memory. The stored images, which the device has been taken finger print, it can be uploaded or distributed into the single or multiple databases by transferring.

Fig. 3: R307 fingerprint sensor to read and verify the fingerprints

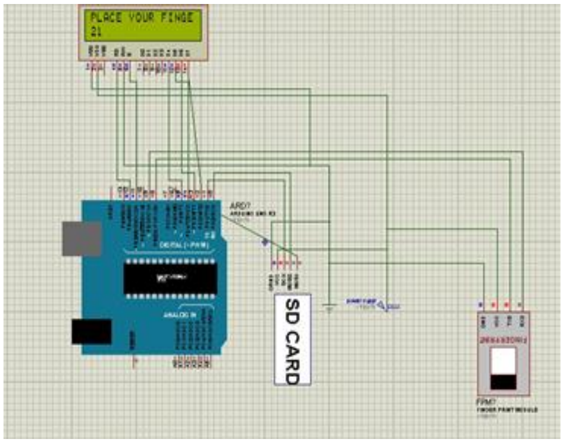

Fig. 4: Arduino Connectivity

III. PROPOSED WORK

In this paper, we have collected the fingerprint image and store the image in the database along with their information that is asked in the registration form that information is stored in the database and could be accessed and updated only by the authorised user only.

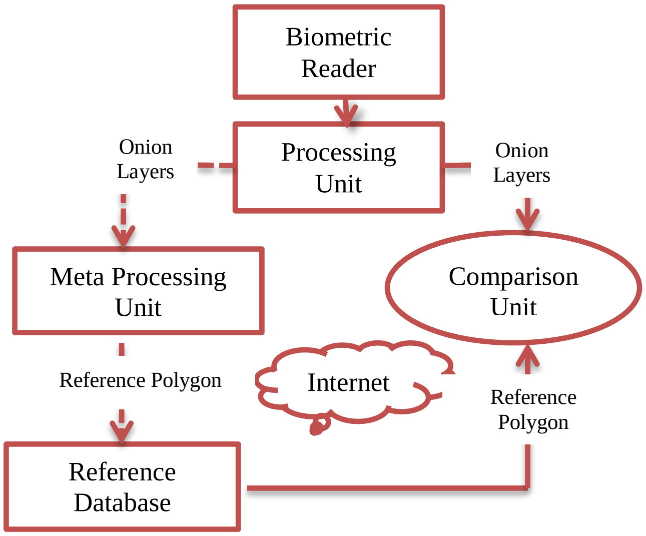

Fig. 5: Flow Chart

Fingerprint has tiny ridges and reflects or can be seen on the tip of each finger, which are based on whorls and valley patterns. There is 64 billion chance in the world that your fingerprint ridge may be matched exactly with someone else fingerprint. Scanner of the fingerprint is a device which having technology that verify the fingerprint for identify the an authenticate to make the authenticated human by their own individual fingerprints, which order and grant the access permission or deny access after the verification to its software application on a computer system.

2. The proposed method is defined in the following steps:

(1) *Pre-processing stage* — Fingerprint image as input make suitable for further processing by image enhancement techniques.

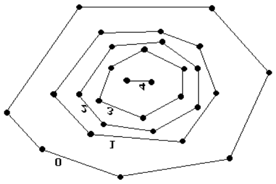

Fig. 6: Define the set of points of Onion Layers

(2) *Processing stage*— The fingerprint data comes after Ist Step, The set of data submit into specific segmentation with the usage of computational geometry algorithm.

(3) *Meta-processing stage* – The constructed and smallest onion layer (convex polygon) is insulated from the fingerprint in radius vector form, which will be referred to the referenced polygon and it stores in related database, for the subsequent verification.

(4) *Verification stage* — The constructed and smallest onion layer (convex polygon) is insulated from the fingerprint in radius vector form, which will be referred to the referenced polygon and it stores in related database, for the subsequent verification.

(5) *Evaluation & comparison of the algorithm* — Step 4 repeat with the use of C.V. algorithm that execute as Ratha's algorithm.

Fingerprint Image enhancement, Minutiae-based template synthesis, and use of METRIC gives more robust and fast identification method for verification. Value of FAR and FRR is also maintained [4].

3.1 CGA method for Pre-processing

In this process fingerprint image with the use of image extension file format like (.tif, .bmp, .jpeg, etc), is transformed into the matrix pixels. [5]. It synthesizes bright square of fingerprint image of the dark background. The value fetch from the output of an analog to digital transform. The matrix pixels of the fingerprint image identify in square appearance, where the image is described as P x P and n bit pixels [6,7]. Character P denotes the number of points along with its axes and n denotes and control the number of brightness values. In this said process n bit show the range of 2 n values and ranges from 0 to 2 n -1. Therefore, the digital fingerprint image denotes in the below compact matrix form:

$$f(x,y)=\begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,P-1) \\ f(1,0) & f(1,1) & \dots & f(1,P-1) \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ f(P-1,0) & f(P-1,1) & \dots & f(P-1,P-1) \end{bmatrix} \quad (1)$$

The coordinate vector of the above matrix is:

$$R = [f(x, y)] \qquad (2)$$

Thus, a vector 1 × P^2 of dimension has generated.

3.2 Processing stage

We have considered that the set of brightness values for each fingerprint image contains a convex subset, which has a specific position in relation to the original set. This position may be determined by using a combination of computational geometry algorithms, which is known as Onion Peeling Algorithms [8,9].

We consider the set of brightness values of a fingerprint image to be the vector R (eq.2). The algorithm starts with a finite set of points R = R0 in the plane and the following iterative process is considered.

Let R1 be the set

$$R0 = \partial H(R0) : R,$$

Minus all the points on the all boundaries of the hull of R. Define as:

$$R_{i+1} = R_i - \partial\, H(R_i)$$

The layers of the set is called hulls and the peeling process, which peeling away from the layers is called onion peeling for exact reasons. Any point of the onion image shows its own onion depth.

3.3 *Meta Processing stage*

In this case, it has depth 3 of the smallest convex layer carries related information. This position gives a geometrical interpretation of the fingerprint brightness [10, 11].

This feature may be characterized as unique to each fingerprint, because the following conditions ensure:

(i) The area of the layer can't intersect with another layer.

(ii) The depth of the smallest layers makes the variables. Onion layer is called a subset of the original fingerprint set the value R.

3.5 Verification stage

In this stage, the work has been done on the subset 'Rxy' against further subset 'Pxy', which come from the processing of further set P. This processing takes 3 levels (Fig. 2), where Subset 'Rxy' and subset 'Pxy' are correlated.

(i) The depths of the iterative procedure, from which the subsets were extracted, are compared.

(ii) The intersection between subset Pxy convex layer and one of set R onion layers is controlled.

Furthermore, it is considered that subset Pxy identifies set R as the parent onion layers when:

(i) The cross-correlation number of subset Rxy Pxy is approximately 1.

(ii) The intersection [12] between the convex layer of subset Pxy and one of the onion layers of set R is 0.

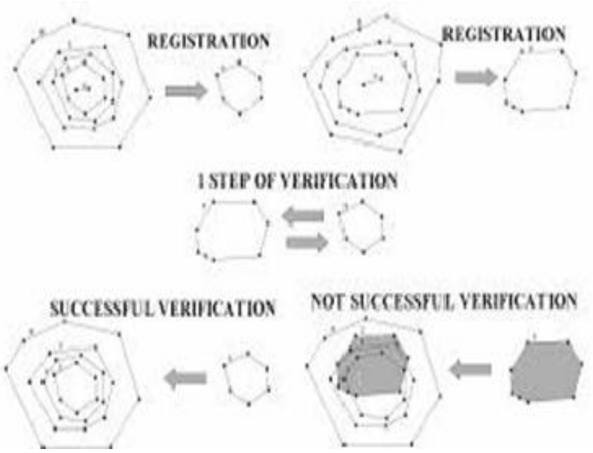

Fig. 7 Registration and Verification

3.6. Verification stage

Fingerprint verification has be taken with use of Ratha's algorithm, which is a technique [13,14] to specify the digital fingerprints into the many type of pre-specified as described above. Fingerprint verification can be seen with the process of coarse level matching of the fingerprints. An input fingerprint is used as the first match at a coarse level to one of the pre-specified types, which compared with the subset of the database and it contains only fingerprint data. We have implemented an algorithm to identify the classes of fingerprints into 5 classes as whorl, right loop, left loop, arch, and tented arch. We have used the algorithm to separate the number of ridges, which presents in four directions i.e. (1) 0 degree (2) 45 degree (3) 90 degree and (4) 135 degree to filter the central part of the fingerprint with the use of Gabor filter. This information is used to generate the fingerprint code [15, 16, 17].

IV. Experimental Results

In our experiment result, we have maintained the fingerprint record in .tiff format, which represent the matrix of the image in 255×255 pixels, which come by the converting quantization sampling process.

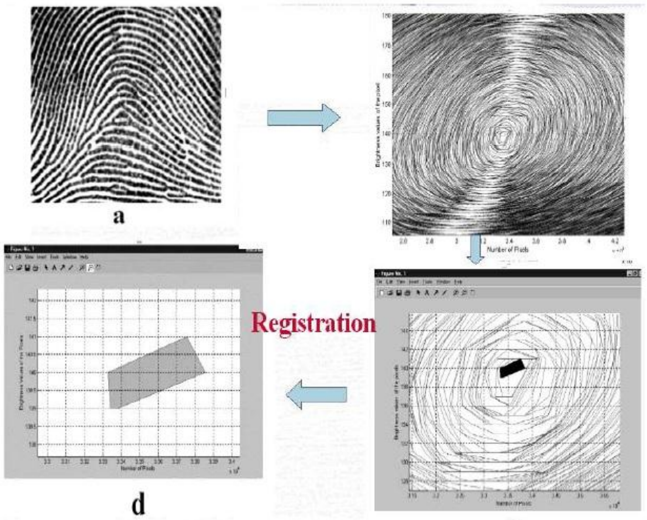

Fig. 8. Fingerprint in 4 frames for registration and the verification stages

Each pixel of the fingerprint has been used which consists of 8 bits, therefore n=8 and the brightness ranges from 0 to 255. The dimension is created in the compact matrix as f(x,y) of equation 1 is R and the vector of fingerprint is respectively. Vector R on the onion layers have been created according to the CG Algorithm. The variable number of layers as convex polygons extracted for every fingerprints in this case. We have created convex polygons in 944 layers of onion, which consisted and the number of vertices of the smallest internal layer are five. Further, the average of vector value is R. With the help of aforementioned verification conditions for the system, it can be decided, whether the polygon is identified correctly or not.

Table 1. Fingerprint Verification Scores, Ratha's vs. Onion Algorithms.

INDIVIDUALS	RATHA'S						ONION					
1	45	1	0	1	0	0	48	0	0	0	0	0
2	1	44	1	0	0	0	0	47	1	0	0	0
3	1	1	45	1	1	1	1	0	48	0	0	0
4	0	1	1	44	1	0	0	0	1	0	47	0
5	0	0	0	1	0	45	1	0	0	0	0	46

Table 1 describes the depth of the smallest referenced layer (polygon) is 966 in contrast to that of the tested vector that was 699 respectively. When negative corrections come at the time of the verification in this case, then the final decision depends of the system by considering the position and the sizes of characteristic polygons. In this experiment forty (40) indexed fingerprints belong to five individuals i.e. (5x8=40) and called A, B, C, D, E and tested.

V. CONCLUSION AND FUTURE SCOPE

In this paper, we focused and applied our method on Onion Algorithm of computational geometry method that will be used to secure and accurate fingerprint verification, which made our purpose successfully. Extraction feature is applied, which covers the specific area of the fingerprint. We observed and analyse that biometrics are not secured and hackers are using silicon imprints made by wax molds. However, the usage of biometric digital fingerprint trends is increasing to use in the private companies for taking digital attendance in lieu of signature or card machine and Indian government also using biometrics digital fingerprints to verify the originality of the live human and same to give the security, so that fake human can't use the identity of the other humans for crime. Finally, we get successful results to keep the security on biometric digital fingerprint to prevent from the hackers and hackers attack.

REFERENCES

[1] T. K. Thivakaran, S. V. V. N. C. Padira, A. S. Kumar, S. S. Reddy, "*Fusion Based Multimodel Biometric Authentication System using Ear and Fingerprint*", International Journal of Intelligent Engineering and Systems, Vol.**12**, No.**1**, pp. **62-73**,**2019**.

[2] D. Maio & Maltoni, "*Direct gray-scale minutiae detection in fingerprints*", IEEE Transactions on PAMI, Vol. **19**, No. **1**, pp. **27-40**, **1997**.

[3] A. K. Bhatia and H.Kaur,"*Security and Privacy in Biometrics: A Review*", International Journal of Scientific Research in Computer Science and Engineering, Vol.**1**, Issue **2**, pp. **33-35**, **2013**

[4] T. Poon & P. Banerjee, "*Contemporary Optical Image Processing With Matlab*", Hardcover: Elsevier Science Ltd, **2001**.

[5] R. Gonzales, R. Woods, "*Digital Image Processing*", Horton M., NJ: Prentice – Hall, Upper Sandle River, **2002**.

[6] S. Bhatnagar, N. Jain, R. Vyas, "*Minutia based Verification Technique for Fingerprint – A Evaluation Text*", Vol. **4**, No. **3**, pp. **191-194**, **2013**.

[7] F. Dhib, M. Machhout and A. Taoufik, "*Pre-Processing Image Algorithm For Fingerprint Recognition And Its Implementation on Dsp Tms320c6416*", International Journal of Software Engineering & Applications (IJSEA), Vol.**9**, pp. **65-79**, **2018**.

[8] I. Rahman, A. H. Razzaq and U. Ali, "*A Review on Fingerprints Recognition System*", Journal of Computer Science Systems Biology, Vol. **11**, Issue **5**, pp. **286-289**, **2018**.

[9] K. M. Sagayam, D. N. Ponraj, J. Winston, Y. J C, E. Jeba D, A. Clara, "*Authentication of Biometric System using Fingerprint Recognition with Euclidean Distance and Neural Network Classifier*", International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol. **8**, Issue-**4**, pp.**766-771**, **2019**.

[10] Dr. S. P. Angayarkanni, "*Fingerprint Reconstruction And Pattern Recognition Matching Using Deep Convolution Neural Network*", International Journal of Computer Engineering and Applications, Vol. **12**, Issue **7**, pp. **1-15**, **2018**.

[11] W. Yang., S. Wang, J. Hu, G. Zheng and C. Valli, "*Security and Accuracy of Fingerprint-Based Biometrics: A Review*", Symmetry, Vol. 11, pp. 1-19, **2019**.

[12] A. H. H. Alasadi, R. H. Jaffar, "*Fingerprint Verification System based on Active Forgery Techniques*", International Journal of Computer Applications, Vol. **180**, pp. **1-6**, **2018**.

[13] T. N. T. and H. LEE, "*High-Secure Fingerprint Authentication System Using Ring-LWE Cryptography*", IEEE Access, Vol. **7**, pp. **23379-23387**, **2019**.

[14] S. Khan, A. Waqas, M. A. Khan and A. W. Ahmad, "*A Camera-Based Fingerprint Registration and Verification Method*", IJCSNS International Journal of Computer Science and Network Security, Vol.**18** No.**11**, **2018.**

[15] S. KANCHANA, "*Fingerprint Based Biometric Authentication In Iot For Resolving Security Challenges*", International Journal of Research and Analytical Reviews, Vol. **5**, Issue **4**, pp. **1000-1003**, **2018**.

[16] I. McAteer, A. Ibrahim, G. Zheng, W. Yang and C. Valli, "*Integration of Biometrics and Steganography: A Comprehensive Review*", Technologies MPDI, Vol. **7**, No. **34**, pp. **1-22**, **2019**.

[17] P. Devi, "*Attacks on Cloud Data: A Big Security Issue*", Int. J. Sci. Res. in Network Security and Communication, Vol.**6** Issue **2**, pp. **15-18, 2018**.

Authors Profile

Jaishree Jain is an Assistant Professor in the department of AIT-Computer Science & Engineering, Chandigarh University, Punjab, INDIA. She has 8.10 years teaching experience in CSE/IT Department as an Assistant Professor since July 2010. She is a Ph.D. scholar of Uttarakhand Technical University, Dehradun, INDIA. She received the master’s degree in Software Engineering from MNNIT, Allahabad. Her research interests include Image Processing, Cloud Security, and Steganography. She had been published one patent in last year i.e. August 2018 and about 23 papers in UGC/International/National Journals & Conferences. She is a life time member of ISTE,ICSES, SCINAPSE and also the member of ECI (Engineering Council of India) as an Professional Engineer.

Heena Arora is an Assistant Professor in the department of AIT-Computer Science & Engineering, Chandigarh University, Punjab, INDIA. Her area of interest is in Big Data & Machine Learning. She has published several papers in her specialization field.