

# Efficient Fingerprint Matching Algorithm for Reduced False Similarity Contribution In Forensics and Partial Finger Prints

Waqas Ellahi, Kashif Sardar<sup>1</sup>, Mohsin Raza<sup>2</sup>, Nauman Aslam<sup>3</sup>, Wajih Ullah Baig,

<sup>1</sup>*Center for Advanced Studies in Engineering (CASE), Islamabad, Pakistan*

<sup>2</sup>*Department of Math, Physics and Electrical Engineering, Northumbria University, Newcastle, UK*

<sup>3</sup>*Department of Computer Science and Digital Technologies Northumbria University, UK*

**Abstract:** Minutiae based matching algorithms use both local and global matching techniques for a better discrimination of scores. However, these algorithms inherently produce high false matching scores for partial fingerprint identification. This paper introduces a novel mechanism to reduce false matching scores without degrading true matching scores by evaluating minutiae points that reside in over-lapping fingerprint area. The main contributions of the paper are 1) introduction of new and faster algorithm that replaces the GrahamScan algorithm to find a point inside a convex hull 2) reduction of false match scores. The performance of the proposed algorithm is evaluated using FVC-2002 and other databases. FingerjetFx is used for feature extraction. The evaluated results show that the proposed algorithm offers improved accuracy along with over 300 percent improvement in computational efficiency.

**Keywords:** Fingerprint Recognition; Minutiae; Convex Hull; Point slope formula; Equal Error Rate (EER), optimization.

## 1. Introduction

In the past few decades, biometric authentication systems have been widely adopted (1). These systems have evolved over the years and more secure identification and authentication systems have been developed (2) and (3). Presently, a much broader range of modalities are in use for biometric user authentication. Some of the systems have been perfected for years and are marketed to offer improved security, protection of the valuables and authorized access.

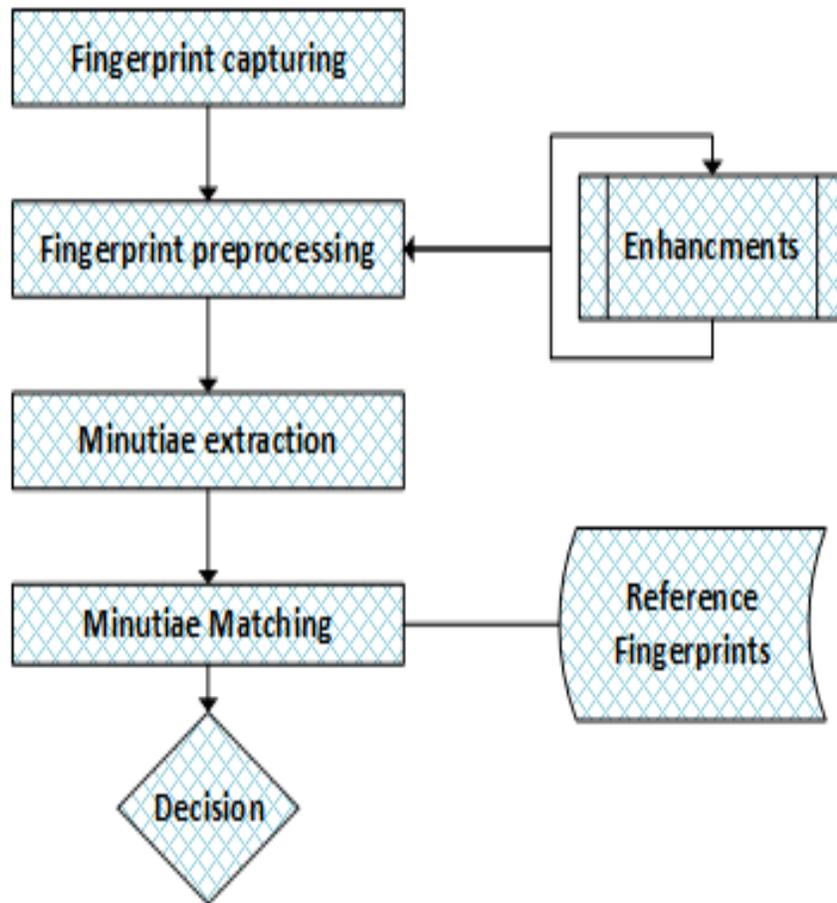


Figure 1 General minutiae based fingerprints identification system

The available biometrics can widely be divided in two categories: behavioral (4) and physiological (5, 6). Behavioral modalities require a particular activity to be performed by the user, used for the identification and authentication purposes. The performed activity is segmented into several markers and key movement patterns, allowing the sensors and the authentication system to formulate distinguishable attributes of a user. These accumulated key markers and attributes from an activity are used for identification of the user based on the similarity in the earlier and presently collected attributes. Walking pattern identification can be considered as one of the examples of behavioral biometrics. The physiological, on the other hand, considers one of the hard-coded attributes of the user for the identification purposes. These biometrics may include fingerprint, iris, DNA which naturally bear unique features that can be used to distinguish one person from the other (7).

Both, behavioral (signature, voice, walking style) and physiological (DNA, palm, facial, iris, fingerprint) biometrics are widely used. The primary objectives for using these biometrics can either be verification or identification. For the identification purposes, fingerprint identification is one of the most widely used and accepted solution (8). Due to the higher accuracy, cost efficiency, ease of use, small storage requirements and well developed algorithms, fingerprint identification systems are widely in place.

Minutiae based finger print matching includes minutiae points for representation of fingerprint image (9). Each minutiae point is usually represented in the form of triplet $(x, y, \theta)$ , quadruple $(x, y, \theta, q)$ , or quintuplet $(x, y, \theta, q, t)$ , where  $(x, y)$  provides spatial location,  $\theta$  is the orientation angle of the ridge,  $q$  is the quality of minutiae and  $t$  is the type of minutiae.  $t$  is either ending or bifurcation and it provides useful information primarily used for classification in large data sets.

In (1) and (13) authors present a general minutia based fingerprints identification system where the block diagram of fingerprint recognition is presented in Figure 1. The identification system initially captures the image through scanning device, then some enhancements (Gabor or FFT based) are applied (11) and (12). Image may also go through segmentation, orientation and/or thinning, followed by extraction of minutiae. Finally matching with reference fingerprints in database, the results are evaluated, based on which final decision (matched/ not matched) is provided. High matching score usually means both fingerprints are from the same finger, while low matching score means different fingerprints (14). However, the threshold for deciding match and mismatch is selected based on the sensitivity of the application and the cost paid for the false positive and the false negative. In sensitive systems, where the fingerprint based authentication system is used to control access to a highly secure facility, false positive (A person is authorized by the biometric system to visit the facility when actually was not authorized to do so) has very high penalty compared to false negative and hence the decision is more tilted towards the strict criteria for matching the fingerprint. Whereas to facilitate the users by giving more acceptable thresholds is quite common in fingerprint based attendance system used for a regular office.

The accuracy of minutiae based matching algorithm is usually affected by two known problems, inter-class and intra-class variations. *Inter-class variation* is the difference between fingerprints

not belonging to same finger, while *intra-class variation* is difference between fingerprints belonging to same finger. The causes of intra-class variation are (15):

1. Transformation (caused by placing same finger at different location on scanning surface)
2. Stretching (caused by difference in pressure while capturing the image)
3. Dry/oily skin condition
4. Existing residual on scanner and
5. Error while extracting features(minutiae)

Minutiae based matching algorithms have been extensively studied and used. Majority of the existing algorithms perform well on good quality fingerprints but their performance is adversely affected on poor quality and forensic fingerprints. Despite of the known issue the minutiae based matching algorithms are still heavily used but accuracy of matching score based on similarity is still a big challenge. Furthermore, despite the extensive research in this field, there are no set rules to reduce the contribution of false similarities from matching score.

Matching score based on contribution does not usually indicate whether matching fingerprints are from same or different fingers. The situation is further complicated by adding extensive image enhancement techniques and incorporation of filters which not only increase the computational complexity of the algorithms but also limit the scope of the algorithm to be run on larger databases. Another problem that is found to be dominant in most of the fingerprint identification algorithms is the observed inaccuracy in identification of partial and forensic fingerprints (30), (33). Since the accuracy of majority of the algorithms is dependent on the matching score, their lack of consideration for partial fingerprints and its effect on matching score leads to much higher error rates and poor identification accuracy. Due counter some of the listed problems, different methods have been presented over the years for evaluating suitable matching scores.

There are three common ways of calculating minutiae similarity based matching score: local minutiae based similarity score (16), (17), (18) (19); global minutiae based similarity score (20), (22), (23); and combination of both local and global minutiae based similarity scores (also referred as hybrid) (24), (25). Local minutiae based similarity scores measure similarity per minutiae pair during minutiae comparison and this information is used in final score computation.

In global minutiae based similarity, final score is computed using total matched minutiae pair, number of minutiae in each set of fingerprints and minutia in common area in both fingerprints. Hybrid uses both local and global minutiae based similarity for final score computation.

When partial fingerprints are compared with full fingerprints, a case of false contribution usually arises, which affects the final matching score. Therefore, an optimal final matching score for full fingerprints and partial fingerprints is needed.

This paper explores different existing algorithms to evaluate similarity based final score. It also proposes Point Slope Formula (PSF) based technique to compute final score by reducing the contribution of false similarities. The Proposed scheme specifically targets the partial fingerprint cases. The proposed scheme not only manages to reduce the overall complexity of the algorithm, it also manages to provide higher accuracy for partial fingerprints. This paper also presents a novel common area mask expansion which allows to improve the accuracy by considering borderline minutiae using optimal expansion window.

The rest of the paper is organized as follows. Section 2 presents the literature review. Section 3 covers the details of proposed algorithm. In Section 4, performance of proposed algorithm is presented. Finally, the conclusion and future directives are presented in section 5.

## **2. Materials & Methods**

### **2.1. Literature Review**

In the past decade, various minutiae based matching algorithms are presented. The general minutiae based matching algorithms (22) usually have following stages

1. Calculation of transformation parameters.
2. Alignment of templates.
3. Determination of final results.

The transformation parameters provide displacement and angular disposition measurements. Based on these parameters the two minutiae templates are aligned. Once the templates are aligned the final results are evaluated based on the mathematical notations. Due to the significance of the

final results, some noteworthy contributions in the literature are presented as under (the description of the variables used in selected notations are presented in Table 1)

In (22) , authors present a mechanism for evaluation of similarity between two minutiae sets. In this paper the mathematical formula used for evaluation of similarity is presented in Equation 1.

$$S_{L1} = N_M^2 / (N_Q \times N_R) \quad (1)$$

Equation 1 was further improved by Bazen and Gerez (27), and is presented in Equation 2.

$$S_{L2} = 2N_M / (N_Q \times N_R) \quad (2)$$

Although the suggested modifications offered improved results yet, the reliability of the scores suffer when dealing with images of different sizes (22) . Another variant of Equation 1 as proposed by (20) is presented in Equation 3.

$$S_{L3} = N_M / \max(N_Q \times N_R) \quad (3)$$

In Equations 1, 2 and 3, in case of partial fingerprints, the false similarity contribution is also included in the computation of final matching score, as the denominator factor in those equations contain the contribution from all the minutiae instead of the common minutiae. To remedy these false similarity contributions, the changes proposed by (20, 21) are as follows:

$$S_{L4} = N_M / N_{QO} + N_{RO} \quad (4)$$

Although Equation 4 works well in case of partial fingerprints but it also increases scores in impostors' cases. Changes proposed in (8) are represented in Equation 5 however, it leads to same problems as reported in Equation 4.

$$S_{L5} = N_M^2 / N_{QO} \times N_{RO} \quad (5)$$

The traditional way of computing score as in Equations 1, 2 and 3 performs very well at detecting impostors, because impostors usually have low matching score, but in case of partial fingerprints

these equations also include false similarity contribution as well. While Equations 4 and 5 perform well in partial cases, however it increases the scores for impostors' cases.

The algorithm proposed by (28) addresses both, the issue of partial cases and high score in impostors' cases. This algorithm uses convex hull based common area finding technique, where as an initial step  $N_Q$ ,  $N_R$ ,  $N_{QO}$ ,  $N_{RO}$  and  $N_{MO}$ , as indicated in Table 1 are evaluated. Afterwards, proportion of paired query minutiae is calculated using Equation 6.

$$T_{MQ} = N_{MO}/N_Q \quad (6)$$

Whereas total proportion of paired reference minutiae is calculated using Equation 7.

$$T_{MR} = N_{MO}/N_R \quad (7)$$

Finally, the similarity based matching score is calculated using Equation (8).

$$S_c = \frac{2N_M}{N_{QO} + N_{RO}} \times (T_{MQ} + T_{MR}) \quad (8)$$

The second term in Equation 8 is the remedy for false similarity problem.

Table 1 Evaluated information between two minutiae sets

Measurement	Symbol
Number of matched minutiae	$N_M$
Number of minutiae points in query template	$N_Q$
Number of minutiae points in reference template	$N_R$
Number of query template minutiae points inside the overlapped region	$N_{QO}$
Number of reference template minutiae points inside the overlapped region	$N_{RO}$
Number of matched minutiae pairs	$N_{MO}$

Convex hull is the most frequently used technique for finding common area between two images (28). To find the common area between the reference image and query image following steps are performed.

1. Minutiae list of query image is transformed with respect to minutiae of reference image. As in Figure 2 reference image is presented in Figure 2a query image is presented in Figure 2b

and transformation of query image minutiae with respect to Figure 2a is presented in Figure 2c.

2. Convex hull of reference image and transformed query is created as shown in Figures 2a and 2c.
3. Mask of reference image and transformed query image is created as shown in Figures 3a and 3b.
4. Both the masks presented in Figures 3a and 3b are multiplied to get common area mask as in Figure 3c.
5. Finally, by using the common area mask, minutiae are shortlisted for true similarity contribution depicted in Figures 4a and 4b.

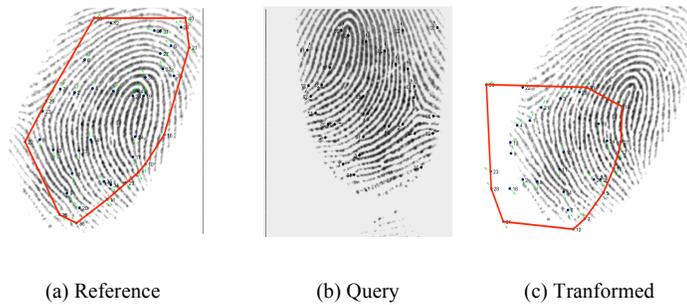


Figure 2 Transformation

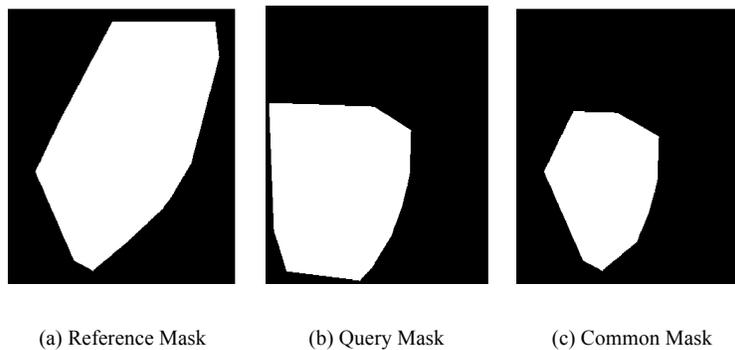


Figure 3 Masks Creation

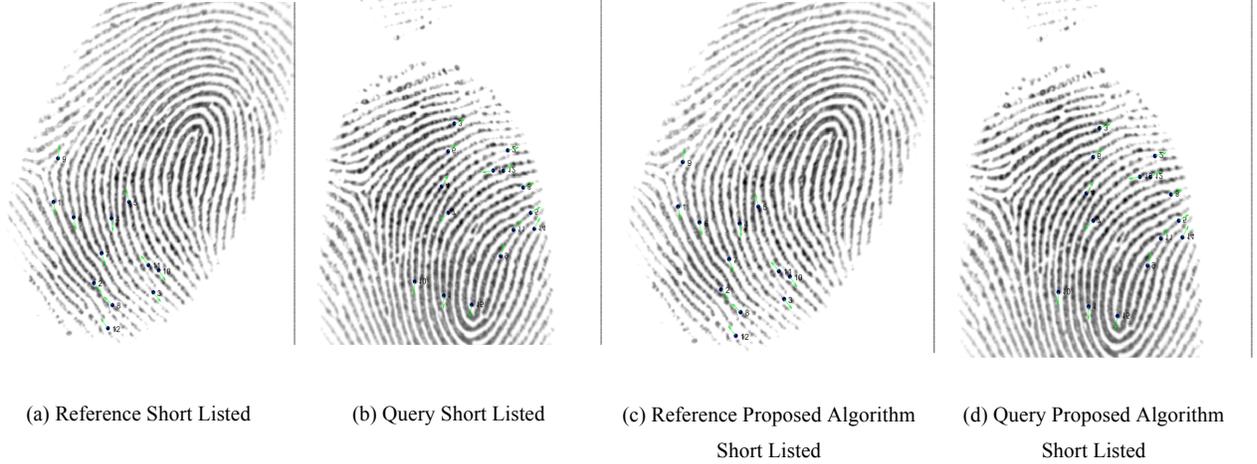


Figure 4 Short Listed Minutiae

## 2.2. Proposed Algorithm

The proposed algorithm checks whether a minutia point exists inside convex polygon or not based on PSF. It emphasizes the slope of the line and a point on the line (that is not the y-intercept). The graphical demonstration for the proposed algorithm is presented in Figure 5. Here  $m_1, m_2$  and  $m_3$  are the minutiae points and  $p_1, p_2$  and  $p_3$  are the points to be determined if they exist inside the polygon formed by  $m_1, m_2$  and  $m_3$ . Initially the slope between  $(m_1, m_2)$ ,  $(m_1, m_3)$  and  $(m_2, m_3)$  is computed using point slope formula. Then  $P_a$  and  $P_b$  are calculated using these slopes. Based on values of  $P_a$  and  $P_b$  final decision for the points  $(p_1, p_2$  and  $p_3)$  is made on following criteria

1. If  $P_a$  and  $P_b$  are on the same side of  $p_i$  then  $p_i$  is outside the polygon.
2. If  $P_a$  and  $P_b$  are on the different side of  $p_i$  then  $p_i$  is inside the polygon.

In Figure 5  $p_1, p_2$  are outside the polygon as  $P_a$  and  $P_b$  are on the same side in both cases, while  $p_3$  is inside the polygon as  $P_a$  and  $P_b$  are on the different sides of it.

The execution of the proposed algorithm on reference and query minutiae list is as follows.

1. The list of points denoted by  $b$  in Algorithm I is the minutiae list and  $(x_q, y_q)$  is the point to be determined if exists inside or outside of the polygon formed by the points in  $b$  in each iteration.  $m$  is the slope of line between  $(x_i, y_i)$  and  $(x_{i+1}, y_{i+1})$  in the list  $b$ . The point  $(x, y_q)$ , which lies on a line between  $(x_i, y_i)$  and  $(x_{i+1}, y_{i+1})$  is calculated and stored in  $X$ .

- By Iterating on list  $X$  the proposed algorithm checks whether at least two point from list  $X$  exists on the different sides of  $(x_q, y_q)$  or not.

The complete pseudo code of proposed scheme is presented in Algorithm I.

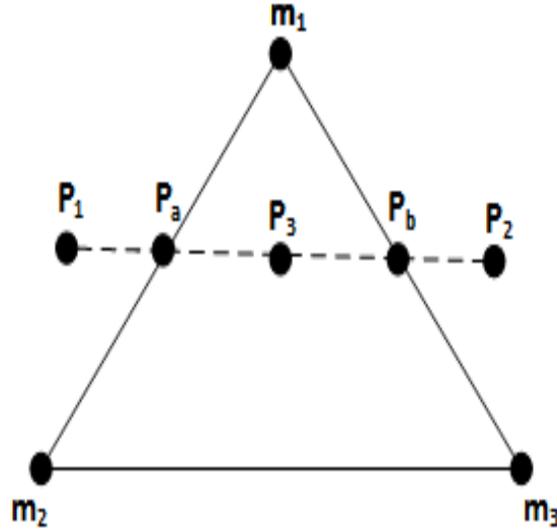


Figure 5 Demonstration of algorithm

The significance of our proposed algorithm is expansion of common area mask presented in Figure 4c, by simply setting an omega ( $\Omega$ ) value. This will expand the number of pixels according to  $\Omega$  value.

The proposed algorithm gives the shortlisted minutiae for true similarity contribution depicted in Figures 7a and 7b. Due to addition of that  $\Omega$  value in the algorithm, the number of minutiae in common area are higher than convex hull based technique.

The proposed algorithm is also evaluated with different omega ( $\Omega$ ) values. It has been observed that when the value of omega is zero the convex hull effect is minified to zero and all minutiae's are contributing to final score, while the optimal value, respective to least error is 16, as seen in graph in Figure 6.

ExistInConvexHull (*singleminutiae, listofminutiae*);

**Input** : Minutia  $a$  to check if exist inside list  $b$

**Output**: exist or not exist inside list  $b$

```
for  $i \leftarrow 1$  to  $size(b)$  do
    if  $a.y$  is between  $b_i.y$  and  $b_{i+1}.y$  then
        compute slope between  $b_i$  and  $b_{i+1}$ ;
        find the x coordinate of  $a.y$  that lies on line
        between  $b_i$  and  $b_{i+1}$ ;
        store the x value in a list  $X$  ;
    end
end
flagRight = 0;
flagLeft = 0;
for  $j \leftarrow 1$  to  $size(X)$  do
    if  $X[j] - \Omega$  is less than  $a$  then
        | flagLeft = 1;
    end
    if  $X[j] + \Omega$  is greater than  $a.x$  then
        | flagRight = 1;
    end
end
if flagLeft = 1 and flagRight = 1 then
    | exist inside;
else
    | not exist inside;
end
```

Algorithm I Proposed Method

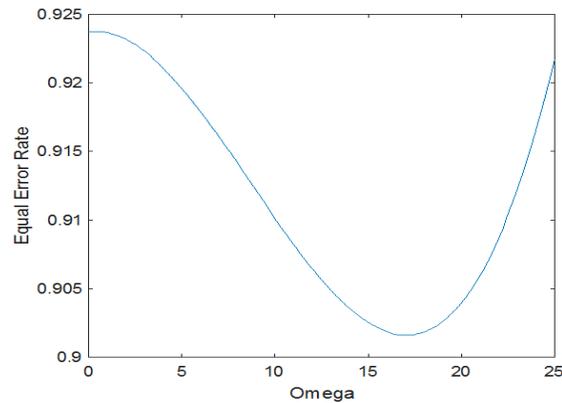


Figure 6 Omega Value and Equal Error Rate

### 3. Results

For the evaluation purposes the proposed algorithm is implemented using MATLAB where the performance of algorithm is verified using FVC-onGoing databases.

FVC-onGoing (34) is online competition for the evaluation of fingerprint recognition algorithms. FVC provides sequestered datasets, used for performance evaluation of proposed idea. Four different databases are used from FVC with following properties in each dataset

1. DB1: optical sensor "V300" by CrossMatch
2. DB2: optical sensor "U.are.U 4000" by Digital Persona
3. DB3: thermal sweeping sensor "FingerChip FCD4B14CB" by Atmel
4. DB4: synthetic fingerprint generation

Each dataset has four sub-datasets each containing 800 images. Hence, the performance of the proposed algorithm is evaluated using 24 distinct datasets.

FVC-2002 DB1\_A database (contains 800 fingerprints, 100 fingerprints subject with each having 8 impressions). The Equal Error Rate (EER) is used as a performance measure for the proposed method. The EER indicates the point where the False Accept Rate and False Rejection Rate are equal. To calculate the EER, genuine and imposter matching is performed. For feature extraction well known FingerJetFX (35) is used.

The performance of the proposed scheme is evaluated in comparison to simple matcher and convex hull algorithm. The results of matching speed as presented in Table 2, suggest nearly four times improvement in the matching speed, along with a reduction in EER in comparison with the convex hull.

Table 2 Result Comparison

Algorithms	<u>FVC 2002-DB</u>				Matching Speed (Sec)
	DB-1	DB-2	DB-3	DB-4	
Simple Matcher	1.1026	1.002	6.4538	3.7337	-
With Convex Hull	0.9237	0.9356	6.7051	3.6341	0.0483
Proposed Techniques	0.8962	0.8862	6.4329	3.6024	0.0101

## 4. Discussion

The computational cost of convex hull based technique is finding two convex hull with time complexity  $2n \log n$ , creating common mask and finally checking the point exist inside or not, while in our proposed method without any convex hull computation and mask creation, it can be decided if a point is inside a common area or not. The proposed scheme offers notable improvement in the computational efficiency and provides comparable accuracy.

### REFERENCES

1. Pahuja G, Nagabhushan T-N (2015) Biometric authentication & identification through behavioral biometrics: A survey. International Conference on Cognitive Computing and Information Processing(CCIP): Noida, pp. 1-7.
2. Sousedik C, Busch C (2014) Presentation attack detection methods for fingerprint recognition systems: a survey. IET Biometrics: vol. 3, no. 4, pp. 219-233.
3. Noor A, Manivanan N, Balachandran W (2012) Transformation invariant algorithm for automatic fingerprint recognition. Electronics Letters: vol. 48, no. 14, pp. 834-835.
4. Li Y, Xie M, Bian J (2016) SEGAUTH: A segment-based approach to behavioral biometric authentication. IEEE Conference on Communications and Network Security (CNS): Philadelphia, PA, pp. 1-9.
5. Miao F, Bao S-D, Li Y (2013) Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security. IET Information Security: vol. 7, no. 2, pp. 87-96.
6. Al-Shamma S-D, Al-Noaemi M-C (2010) Heart sound as a physiological biometric signature. 5th Cairo International Biomedical Engineering Conference: Cairo, pp. 232-235.
7. Physiological vs Behavioral Biometrics (2016) Available at: <http://encyclopedia.jrank.org/articles/pages/6678/Physiological-vs-Behavior-biometrics.html#ixzz4g35x6Ge4>
8. Jain A, Lin H, Sharath P (2000) Biometric identification. Communications of the ACM: 43.2, pp. 90-98.
9. Cappelli R, Matteo F, Davide M (2012) Minutiae-based fingerprint matching. Cross Disciplinary Biometric Systems, Springer Berlin Heidelberg: pp. 117-150.
10. Haddada L-R, Trimech I-H, Ben-Amara N-E (2016) A biometric watermarking approach of fingerprint images by DLDA Gabor face features without altering minutiae. International Image Processing, Applications and Systems (IPAS): Hammamet, pp. 1-6.

11. Chavan S, Mundada P, Pal D (2015) Fingerprint authentication using Gabor filter based matching algorithm. International Conference on Technologies for Sustainable Development (ICTSD): Mumbai, pp. 1-6.
12. Jain A, Hong L (1997) On-line fingerprint verification. IEEE Transactions on Pattern Analysis and Machine Intelligence: Vol. 19, No.4, pp. 302-314.
13. Jain A, Ross A, Prabhakar S (2001) Fingerprint Matching using Minutiae and Texture Features. International Conference on Image Processing (ICIP): Thessaloniki, Greece, pp.282-285.
14. Venkataramani K, Keskinöz M, Kumar K-V (2005) Soft information fusion of correlation filter output planes using support vector machines for improved fingerprint verification performance. Proc. SPIE Conference on Biometric Technology for Human Identification.
15. Velraj (2009) Handbook of Fingerprint Recognition volume 02, Maltoni D, Maio D, Jain A-K, Prabhakar S (Springer).
16. Conti V, Vitello G, Sorbello F, Vitabile S (2013) An advanced technique for user identification using partial fingerprint. Complex Intelligent and Software Intensive Systems (CISIS) Seventh IEEE International Conf. on: pages 236-242.
17. Jia J, Cai L, Lu P, Lu X (2007) Fingerprint matching based on weighting method and the svm. Neurocomputing: pp. 849-858.
18. Cao K et al (2012) A novel ant colony optimization algorithm for largedistorted fingerprint matching. Pattern Recognition: pp:151-161.
19. Jain A-K, Feng J (2011) Latent fingerprint matching. IEEE Trans. Pattern Analysis and Machine Intelligence: pp. 88-100.
20. Ravi J, Raja K-B, Venugopal K-R (2009) Fingerprint recognition using minutiae score matching. International Journal of Engineering Science and Technology: pp. 35-42.
21. Lee D, Choi K, Kim J, A (2002) Robust fingerprint matching algorithm using local alignment. In Proc. 16th International Conf. on Pattern Recognition: volume 3.
22. Jea T-Y, Govindaraju V (2005) A minutiae-based partial fingerprint recognition system. Pattern Recognition Letters: pp. 1672-1684
23. Lumini A, Nanni L (2008) Advanced methods for two-class pattern recognition problem formulation for minutiae-based fingerprint verification. Pattern Recognition Letters: pp. 142-148.
24. Lui Y, Li D, Isshiki T, Kunieda H (2010) A novel similarity measurement for minutiae-based fingerprint verification. Biometrics Theory Applications and Systems (BTAS) 2010 Fourth IEEE International Conference on: pages 1-6.

25. Feng J (2008) Combining minutiae descriptors for fingerprint matching. Pattern Recognition: pp. 342-352.
26. Wang C-W, Li J-W (2002) Fingerprint Identification Using Point Pattern Matching. Journal of Chongqing University: (Natural Science Edition), Vol. 25, No.6.
27. Bazen A, Gerez S (2003) Fingerprint matching by thin-plate spline modeling of elastic deformations. Pattern Recognition:pp. 1859-1867.
28. Khanyile N-P, De-Kock A, Mathekga M-E, Similarity score computation for minutiae-based fingerprint recognition. IEEE International Joint Conference on Biometrics: Clearwater, FL, pp. 1-8.
29. Bazen A-M et al. (2000) A correlation-based fingerprint verification system. Proc. Workshop on Circuits Systems and Signal Processing (ProRISC 2000)
30. Cao K et al. (2010) Combing features for distorted fingerprint matching. Journal of Network and Computer Applications: pp.258-267.
31. Hatano Tet al (2002) A fingerprint verification algorithm using the differential matching rate. 16th Interantional Conf. on Pattern Recognition: volume 3 pp. 799-802.
32. Mansukhani P, Govindaraju V. Exploring similarity measures for biometric databases. 5th Interantional Conference on Audio-And Video-Based Biometric Person Authentication: pp. 832-840.
33. Campisi P, Carter R, Crooks C, Govindaraju V (2010) IEEE Certified Biometric Professional (CBP) Learning System: Module 4: Biometric Standards. USA 2010.
34. FVC-onGoing: on-line evaluation of fingerprint recognition algorithms, (2017) available at: <https://biolab.csr.unibo.it/FVConGoing/UI/Form/Home.aspx>.
35. FingerjetFx database (2017). available at: <https://github.com/FingerJetFXOSE/FingerJetFX>