Turkish Journal of Computer and Mathematics Education Vol.12 No.9 (2021),1577-1584

Research Article

Analysis of Finger Print Bank Algorithm based Fingerprint Matching Scheme

Gousiya Begum[1], Shirisha Kampati[2]

[1]Assistant Professor Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, INDIA
[2]Department of CSE Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, INDIA

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

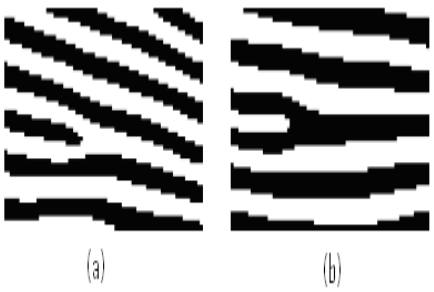
ABSTRACT: - Now-a-days it is an important need to preserve one's data/information securely without giving an option to attackers or intruders to steal it. For this case authentication are considered to be the most important feature, which allows everyone to individually prove their authentication to the system and once it is correct allow them to access the features of the system otherwise neglect or block them to proceed further. There are many authentication schemes available in the information technology and security industries such as Biometric Scheme, IRIS Matching Scheme, Face Recognition, Password Management Scheme and so on. The most popular, well-known and one of the best classical scheme is called Biometric Finger Print Matching Scheme, which allows the user to register the finger print into the system for training purpose and further at every time of accessing the features into the system it gathers the present (testing) finger print from the user and match it with the already registered finger print, once it matches with the trained sample, it allows the user to login into the system or else block the user to proceed further. The proposed Finger Print Bank Algorithm uses an efficient finger print matching principles to accurately match the correct finger print and gives a Boolean result to user to inform that to proceed further or not. The Finger Print Bank Algorithm uses efficient filtering schemes to filter the finger print to extract the internal and global core details of it as well as extracts the raw code of it and compares that with the already registered finger print. For all the entire proposed approach guarantees for the best result and accuracy in results.

KEYWORDS*:* Fingerprint, Biometric System, Finger Code, Filter Schemes, Finger Print Bank Algorithm.

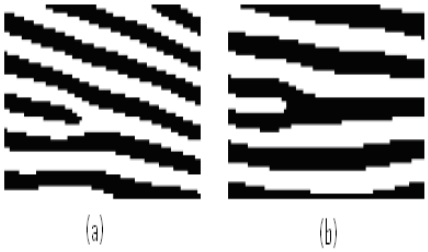
1. Introduction

Biometric-Matching Scheme is the study of interestingly perceiving people in light of at least one inherent physical or social characteristic. Finger Prints are the most generally utilized parameter for individual ID among all biometrics. Unique Finger-Print ID is regularly utilized in legal science to help criminal examinations and so forth. A unique Finger-Print is an extraordinary example of edges-and-valleys on the surface of a finger of a person. An edge is characterized as a solitary bended section as well as a valley is the area between two contiguous edges. Minutiae-Points are the neighbourhood edge discontinuities, which are of two sorts: edge-endings-and-bifurcations'. A decent quality picture has around '40-100' Minutiae-points [1][2]. It is these Minutiae-points which are utilized for deciding uniqueness of a unique Finger-Print. Mechanized Finger-Print acknowledgment and self confirmation frameworks [2][5] can be classified as check or ID frameworks.

The check procedure either acknowledges or rejects the client's character by coordinating against a current Finger-Print database. In distinguishing proof, the character of the client is set up utilizing Finger Prints. Since precise coordinating of Finger Prints depends to a great extent on edge structures, the nature of the Finger-Print picture is of basic significance. In any case, by and by, a unique Finger-Print picture may not generally be very much characterized because of components of commotion that degenerate the lucidity of the edge structures.



(a)



(b)

Fig.1. Minutiae-Point (a) Edges (b) Bifurcation' View

This debasement may happen because of varieties in skin and impression conditions, for example, scars, dampness, earth, and non-uniform contact with the Finger-Print catch gadget. Numerous calculations [3][4][5][6] have been proposed in the writing for minutia investigation and Finger-Print coordinating and arrangement for better Finger-Print check and distinguishing proof. As of late, methods [15][16][17][18] have been suggested that utilization different features separated from minutiae for unique Finger-Print acknowledgment. Chen-et-al [1][15] propose to recreate the unique Finger-Print's introduction field from minutiae and use it in the coordinating stage to enhance the framework's execution. Cao-et-al [16] have acquainted two novel features with manage non direct contortion in Finger Prints. These features are the finger arrangement bearing and the edge similarity.

Choi-et-al [7][8] proposed to join edge features like edge tally, edge length, edge ebb and flow course and edge compose together with details to expand the coordinating execution. Current logical investigations demonstrate that use of transformative calculations may enhance the execution of biometric frameworks fundamentally [9][10][19]. There are various occasions in the writing [20][21] where developmental calculations are utilized for coordinating details of a Finger-Print with that of a database of Finger-Print images. The consequences of every such strategy rely upon the nature of the information image. Hence, image improvement procedures are frequently utilized to diminish the commotion and to upgrade the meaning of edges against valleys so that no misleading minutiae are recognized.

Indeed, coordinating inert Finger Prints from wrongdoing scenes is troublesome in view of their low quality and the unique Finger-Print coordinating exactness is enhanced by consolidating physically checked details with naturally extricated ones [22]. A few strategies have been proposed for upgrade of Finger-Print pictures which depend on picture standardization and Gabor separating (Hong's-calculation) [1], Directional Fourier sifting [2][3], Binarization Method [2][4], improvement utilizing directional middle filter [2][5], Finger-Print picture upgrade utilizing sifting techniques [2][6], picture recovery in view of shading histogram and printed features [2][7] and numerous others [2][21]. The Hong's calculation inputs a Finger-Print picture and applies different strides for upgrade. A few other upgrade strategies exhibit in writing depend on fluffy rationale and neural systems [3][4].

Choo woo-et-al [4][10] exhibited a novel way to deal with upgrade include extraction for low quality unique Finger-Print pictures utilizing stochastic reverberation (SR). SR alludes to a marvel where a fitting measure of commotion added to the first flag can build the flag to-clamour proportion. Exploratory outcomes demonstrate that Gaussian clamor added to low quality unique Finger-Print pictures empowers the extraction of valuable features for biometric recognizable proof.

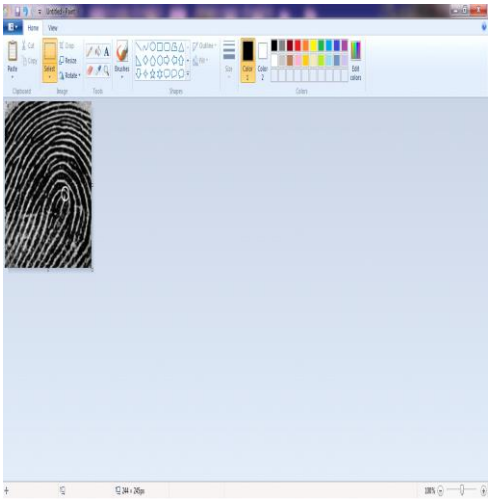


Fig.2 Ridge View and Centre Point Focused Perception

2. Problem summary

Even-though automatic-unique-finger-print recognition advances have quickly progressed amid the most recent forty years, there still exists a few testing researches issues, for instance, perceiving low-quality-fingerprints. Unique finger impression matcher is exceptionally delicate to image quality as saw in the FVC2006, where the coordinating precision of a similar calculation fluctuates altogether among various datasets because of variety in image quality. The distinction between the exactness's of plain, rolled and inert unique finger impression coordinating is significantly bigger as seen in innovation assessments directed by the National Institute of Standards and Technology (NIST). The outcome of low-quality fingerprints relies upon the sort of the finger-print recognition framework. A finger-print recognition framework can be named either a positive or negative framework. In a positive recognition framework, for example, physical access control frameworks, the client gathered be helpful and wishes to be distinguished. In an adverse recognition framework, for example, distinguishing people in watch records and identifying numerous enlistments under various names, the client of intrigue (e.g., offenders) assumed be uncooperative and does not wish to be recognized.

In a positive recognition framework, low quality will prompt bogus reject of honest to goodness clients and in this manner bring bother. The result of low quality for a negative recognition framework, in any case, is significantly more genuine, since malignant clients may intentionally lessen finger-print quality to keep unique finger impression framework from finding the genuine personality. Indeed, law authorization authorities have experienced various situations where lawbreakers endeavoured to maintain a strategic distance from ID by harming or precisely modifying their fingerprints. Consequently, it is particularly essential for negative finger-print recognition frameworks to identify low quality fingerprints and enhance their quality with the goal that the unique finger impression framework isn't imperilled by malignant clients. Corruption of unique finger impression quality can be photometric or geometrical. Photometric corruption can be caused by non-perfect skin conditions, filthy sensor surface, and complex image foundation (particularly in idle fingerprints).

Geometrical corruption is mostly caused by skin twisting. Photometric debasement has been generally considered and various quality assessment calculations and improvement calculations have been proposed. In actuality, geometrical corruption because of skin twisting has not yet gotten adequate consideration, in spite of the significance of this issue. This is the issue this paper endeavours to address. Note that, for a negative finger-print recognition framework, its security level is as feeble as the weakest point. In this way it is critical to create Distorted Finger-Print (DFP) discovery and correction calculations to fill the opening. Versatile bending is acquainted due with the inalienable adaptability of fingertips, contact-based finger-print procurement methodology, and an intentionally horizontal power or torque, and so forth. Skin contortion expands the intra-class varieties (distinction among fingerprints from a similar finger) and along these lines prompts false non-coordinates because of constrained capacity of existing unique finger impression matchers in perceiving extremely misshaped fingerprints.

3. Minutiae-extraction

An exact portrayal of the unique finger print image is basic to programmed finger-print recognizable proof frameworks, in light of the fact that most sent business vast scale frameworks are subject to include based matching (connection-based systems have issues as examined in the past area). Among all the finger-print features, minutia point features with relating introduction maps are one of a kind enough to segregate among fingerprints vigorously; the particulars include portrayal decreases the mind-boggling finger-print recognition issue to a point design coordinating issue.

Keeping in mind the end goal to accomplish high-exactness details with differed quality finger-print images, division calculation needs to isolate closer view from uproarious foundation which incorporates all edge-valley locales and not the foundation. Image upgrade calculation needs to keep the first edge stream design without changing the peculiarity, join broken edges, clean ancient rarities between pseudo-parallel edges, and not present false data. At last details identification calculation needs to find effectively and precisely the particulars focuses.

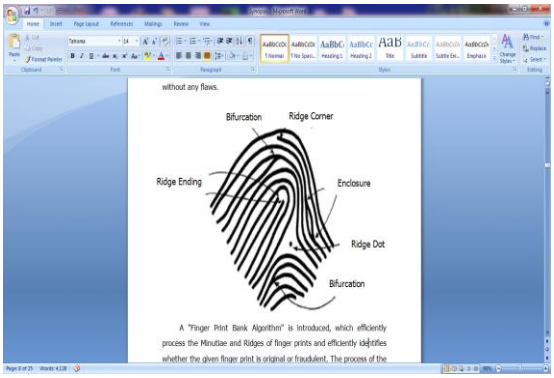


Fig.3 Types of Minutiae and Minutiae Markings

4. Literature survey

In the year of 2012, the authors "X. Si, J. Feng, and J. Zhou", proposed a paper titled "Detecting fingerprint distortion from a single image [21]", in that they described such as: versatile bending of grinding edge skin is one of the real difficulties in finger-print coordinating. Since existing unique mark coordinating frameworks can't coordinate truly misshaped fingerprints, crooks may intentionally mutilate their fingerprints to avoid recognizable proof. Existing twisting recognition procedures require accessibility of particular equipment or unique mark video, constraining their utilization in genuine applications. In this paper we direct an examination on unique mark mutilation and build up a calculation to identify finger-print bending from a solitary picture which is caught utilizing conventional finger impression detecting methods. The finder depends on investigating edge period and introduction data. Promising outcomes are acquired on an open space unique mark database containing contorted fingerprints.

In the year of 2015, the authors "L. M. Wein and M. Baveja", proposed a paper titled "Using fingerprint image quality to improve the identification performance of the U.S. visitor and immigrant status indicator technology program [22]", in that they described such as: inspired by the trouble of biometric frameworks to accurately coordinate fingerprints with poor picture quality, we figure and unravel an amusement theoretic definition of the distinguishing proof issue in two settings: U.S. visa candidates are checked against a rundown of visa holders to identify visa extortion, and guests entering the U.S. are checked against a watchlist of lawbreakers and suspected fear mongers. For three sorts of biometric methodologies, we unravel the amusement in which the U.S. Government picks the technique's ideal parameter esteems to amplify the location likelihood subject to a requirement on the mean biometric preparing time per lawful guest, and after that the psychological militant picks the picture quality to limit the identification likelihood. At current investigator staffing levels at ports of section, our model predicts that a quality-subordinate two-finger procedure accomplishes an identification likelihood of 0.733, contrasted with 0.526 under the quality-autonomous two-finger system that is right now actualized at the U.S. outskirt.

Expanding the staffing level of monitors offers just minor increments in the identification likelihood for these two systems. Utilizing in excess of two fingers to coordinate guests with poor picture quality permits a recognition likelihood of 0.949 under current staffing levels, however may require real changes to the current U.S. biometric program. The location probabilities amid visa application are around 11-22% littler than at ports of section for each of the three techniques, yet the same subjective ends hold.

In the year of 2012, the authors "S. Yoon, J. Feng, and A. K. Jain", proposed a paper titled "Altered fingerprints: Analysis and detection [23]", in that they described such as the far-reaching arrangement of Automated-Fingerprint-Identification-Systems "AFIS" in law authorization and fringe control applications has increased the requirement for guaranteeing that these frameworks are not bargained. While a few issues identified with unique mark framework security have been researched, including the utilization of phony fingerprints for disguising character, the issue of finger-print change or jumbling has gotten next to no consideration.

Unique mark obscurity alludes to the ponder adjustment of the unique mark design by a person to mask his character. A few instances of unique mark jumbling have been accounted for in the press. Unique mark picture quality evaluation programming (e.g., NFIQ) can't simply identify modified fingerprints since the certain picture quality because of adjustment may not change altogether. The principle commitments of this paper are: (a) gathering contextual analyses of occurrences where people were found to have modified their fingerprints for dodging AFIS, (b) researching the effect of unique mark modification on the exactness of a business unique mark

matcher, (c) ordering the changes into three noteworthy classes and recommending conceivable countermeasures, (d) building up a method to consequently identify adjusted fingerprints in light of investigating introduction field and details conveyance and (e) assessing the proposed strategy and the NFIQ calculation on a substantial database of changed fingerprints given by a law requirement office. Trial results demonstrate the plausibility of the proposed approach in recognizing adjusted fingerprints and feature the need to additionally seek after this issue.

5. Finger print bank algorithm

The unique finger print recognition [4][5][6] issue can be gathered into three sub-spaces: finger print enlistment, confirmation and finger-print distinguishing proof. Moreover, as unique in relation to the manual approach for finger-print recognition by specialists, the finger-print recognition here is eluded as FPBA (Finger Print Bank Algorithm), which is program-based. Confirmation is regularly utilized for constructive recognition, where the point is to keep numerous individuals from utilizing a similar personality. Unique finger print confirmation is to check the legitimacy of one individual by his/her unique finger print. There is balanced correlation for this situation. In the distinguishing proof mode, the framework perceives a person via looking through the layouts of the considerable number of clients in the database for a match. In this manner, the framework leads a one to numerous correlations with set up a person's character. Both check and distinguishing proof utilize certain methods for finger-print coordinating as demonstrated in the accompanying subsection. There are different finger-print-matching methods examined in past era are as per the following: (i) Minutiae Finding, (ii) Pattern Matching/Ridge Feature Extraction, (iii) Correlation Technique and (iv) Image Matching.

The proposed algorithm called "Finger Print Bank Algorithm" estimate the scanned finger prints differently as well as get the maximum benefits from all the quoted points above and make a better scheme compare to all. Similar to all other algorithms, the proposed algorithm also concentrates on minutiae and centre-point focusing or determination-based start-ups, but it does not put themselves with only these two substances. Apart from this two the proposed algorithm manipulates the variance of finger print first, there are many different types of finger prints are available in general, those are listed one-by-one as follows: Whorl-Type, Looping Type (both left and right loops) or comes under Tended-Arch-Based finger print.

Algorithm: Finger Print Bank Algorithm

Input: Scanned Finger Print Image
Output: Comparison Result with Accuracy Ratio
Step-1: Scan the User's Finger Print
Step-2: Image Pre-Processing
- Convert the scanned finger print into gray scale format
- Resize the pixels into 256X256 natures.

Step-3: Check for Orientation of the scanned finger print.
- Checks with the ridge's points based on X and Y.
- Estimate the centre-point of the scanned finger print.

Step-4: Identify the type of the finger print such as Whorl, Loop or Arch based.
Step-5: Matrix Coordination of the input or scanned finger print.
Step-6: 5X5 matrix separation, dividing the finger prints into blocks for estimate the centre-point of the finger print.
Step-7: Ridge category estimation such as: extracting the corners of the input or scanned finger print, divisions in the ridges, corner joining over ridges, delta-points for identifying the shapes of the joining-positions of ridges and extracting the core-nature of finger print.
Step-8: Applying filtering techniques to eliminate the noise level of the input.
Step-9: Extracting core features from the scanned finger print and from the registered or trained finger print.
- X(i,j) input finger print features, where i and j are the indexes of feature such as position, center-point level, vector distance and so on.
- Y(i,j) trained or registered finger print features, where i and j are the indexes of feature such as position, center-point level, vector distance and so on.

Step-10: Compare the resulting sets of X and Y.
- If (X(i,j) == Y(i,j))

Indicates the Finger prints are identical.
- Else

Finger prints are different
- End

Step-11: End

6. Experimental results

The following figure, Figure-4 shows the actual input of the fingerprint to analyse the minutiae and features in it.

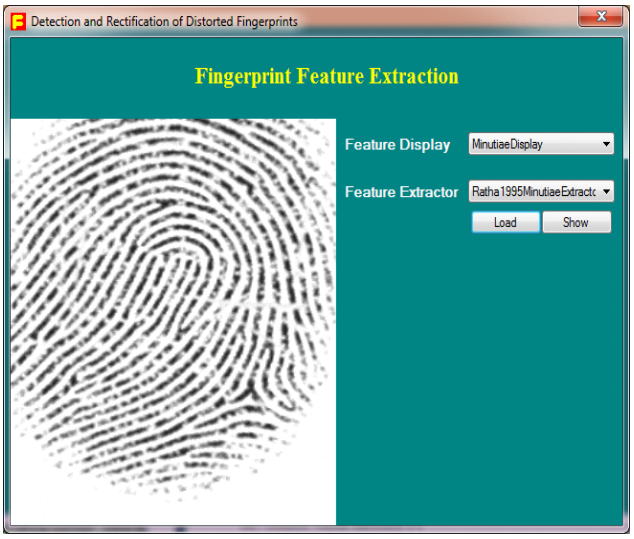


Fig.4 Input Finger-Print Image

The following figure, Figure-5 illustrates the minutiae point detection and marking over the input image for comparison with the existing finger-print.

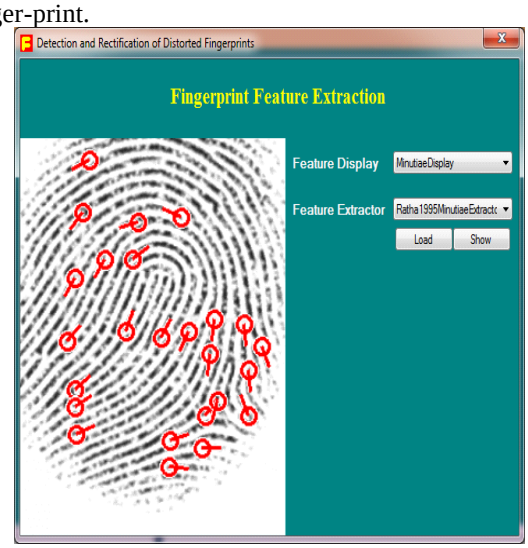


Fig.5 Minutiae Point identification over the input Finger-Print Image

The following figure, Figure-6 illustrates the image orientation analysis and standard correction of the input finger-print image.

Fig.6 Image Orientation Identification and Correction

The following figure, Figure-7 illustrates the minutiae-triplets view of the minutiae identified finger-print image.

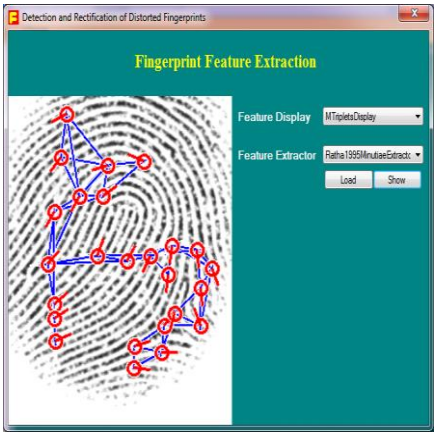


Fig.7 Minutiae-Triplets Point Marking

Recognizing twisted finger-print images is a noteworthy issue in finger-print identification frameworks. A few methods, for example, the details triplet's system, have been proposed for details coordinating/matching and ordering. The minutiae-triplets method anyway is to a great extent influenced by details contortions and impediments and subsequently can seldom create a steady list of capabilities.

7. Conclusion and future work

Image quality is connected straightforwardly to a definitive execution of programmed finger-print verification frameworks. Great quality finger-print images require just minor pre-processing and improvement for precise component identification calculation. This paper evaluated an expansive number of methods portrayed in the writing to separate particulars from finger-print images. The methodologies are recognized based on a few components like: the sort of information images they handle, that is, regardless of whether paired or dark scale, methods of Binarization and division included, in the case of diminishing is required or not and the measure of exertion required in the post handling stage, if exists. Yet, low quality finger-print images require pre-processing to build differentiate as well as diminish distinctive sorts of clamors as boisterous pixels additionally produce a considerable measure of deceptive particulars as they likewise get improved amid the pre-processing steps. Further, more accentuation is to be laid on characterizing the nearby criteria, keeping in mind the end goal to set up the legitimacy of a minutia point, which is especially helpful amid finger-print coordinating/matching and embracing more complex distinguishing proof models, for example broadening particulars definition by including trifurcations, islands, spans, goads and so forth. Likewise, the paper prompts the further investigation of the measurable hypothesis of finger-print particulars. Specifically, methodologies can be explored to decide the quantity of degrees of opportunity inside a finger impression populace which will give a sound comprehension of the measurable uniqueness of finger impression particulars. The work is further enhanced by means of apply the same logic in real-time/real-world working scenario with hardware units, which can provide ultimate support to

the present scenario to prove the practical logic and working case proof of the present scenario. For this kind of hardware and software association, we need a specialized programming algorithm in association with Finger Print Bank Algorithm (FPBA) called Intelligent Hardware Associated FPBA, which can provide efficient hardware and software associations to prove the designed approach is better compare with all other schemes in past.

References

A. L. Hong, Y. Wan, and A. K. Jain, "Fingerprint image enhancement: Algorithms and performance evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20(8), 1988, pp. 777–789.

B. M. K. Khan, "Fingerprint Biometric-based Self Authentication and Deniable Authentication Schemes for the Electronic World", IETE Technical Review, Volume 26, Issue 3, 2009.

C. A. K. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, 19(4), 1997, pp. 302–314.

D. A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, " An identity authentication system using fingerprints". Proc. IEEE, 85(9), 1997, pp.1365–1388.

E. A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching", Image Processing, IEEE Transactions on, 9(5), 2000, pp. 846–859.

F. M. Kaur, M. Singh, P.S. Sandhu, "Fingerprint Verification system using Minutiae Verification Technique", Proceedings of world Academy of Science, Engineering and Technology, vol. 36, 2008.

G. L. H. Thai and N. H. Tam, "Fingerprint recognition using standardized fingerprint model", IJSCI International Journal of Computer Science Issues, vol. 7, issue 3, no. 7, 2010, pp. 11-16.

H. R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint classification by directional image partitioning", Pattern Analysis and Machine Intelligence, IEEE Transactions on, 21(5), 2002, pp. 402–421.

I. R. Cappelli, D. Maio, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems. IEEE Transactions on Pattern Analysis and Machine Intelligence", 28(1), 2006, pp. 3–18.

J. S. Pankanti, S. Prabhakar, and A. K. Jain, "On the individuality of fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(8), 2002, pp. 1010–1025.

K. A. K. Jain, F. Patrick, A. Arun, "Handbook of Biometrics. Springer science and Business media", I edition, 2008 pp. 1-42.

L. S. Prabhakar, J. Wang, A. K. Jain, S. Pankanti, and R. Bolle, "Minutiae Verification and classification for fingerprint matching". Proc. 15th International Conference Pattern Recognition (ICPR) vol. 1, 2000, pp. 25–29.

M. B. Bir and T. Xuejun, "Fingerprint indexing based on novel features of minutiae triplets", IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(5), 2003, pp. 616–622.

N. Z. Chen and C. H. Kuo, "A topology-based matching algorithm for fingerprint authentication", in proc. IEEE International Carnahan Conference on Security Technology, 1991, pp. 84–87.

O. F. Chen, J. Zhou and C. Yang, "Reconstructing Orientation Field from Fingerprint Minutiae to Improve Minutiae Matching Accuracy", IEEE Transactions on Image Processing, vol. 18, no. 7, 2009, pp. 1665-1670.

P. K. Cao, X. Yang, X. Tao, P. Li, Y. Zang and J. Tian, "Combining features for distorted fingerprint matching", Journal of Network and Computer Applications, vol. 33, 2010, pp. 258-267.

Q. H. Choi, K. Choi and J. Kim, "Fingerprint Matching Incorporating Ridge Features With Minutiae", IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, 2011, pp. 338-345.

R. S. Kumar D. R., K. B. Raja, R. K. Chhotaray and S. Pattanaik, "DWT Based Fingerprint Recognition using Non Minutiae Features", IJSCI International Journal of Computer Science Issues, vol. 8, issue 2, no. 7, 2011, pp. 237-264.

S. N. Goranin and A. Cenys, "Evolutionary Algorithms Application Analysis in Biometric systems", Journal of Engineering Science and Technology Review vol. 3, no. 1, 2010, pp. 70-79.

T. T, V. Le, K. Y. Cheung and M. H. Nguyen, "A Fingerprint Recognizer Using Fuzzy Evolutionary Programming", In Proc. Hawaii International Conference on System Sciences, 2001.

U. X. Si, J. Feng, and J. Zhou, "Detecting fingerprint distortion from a single image" IEEE International Workshop on Information Forensics and Security (WIFS), 2012.

V. L. M. Wein and M. Baveja, "Using fingerprint image quality to improve the identification performance of the U.S. visitor and immigrant status indicator technology program", National Institute of Standards and Technology, 2015.

W. S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2012.