

Analysis and Classification of Altered Fingerprints Using FSDCA

¹R. Josphineleela and ²M. Ramakrishnan

¹Sathyabama University, Chennai, India

²Department of Information Technology, Velammal Engineering College,
Chennai, India

Abstract: In this study, researchers are analyzing the altered fingerprints and detecting fingerprints using the FSDCA. There are three types of altered fingerprints that are obliteration, distortion and imitations. Recent problem in the pattern recognition are alteration because of this alteration the criminals can easily evade from their identification. To overcome this problem we have proposed this method.

Key words: FSDCA, altered fingerprint, obliteration, distortion, imitations

INTRODUCTION

The problem of fingerprint obfuscation for the following reasons, fingerprint based biometric system are much more widespread for large scale identification than any other biometric modality. It is relatively easy to alter ones fingerprint using chemical and abrasives compared to say one's iris or face where a more elaborate surgical procedure may be mutilated fingerprints are being routinely encountered by law enforcement and immigration officials in several countries, thereby underscoring the urgency of finding a solution to this problem.

Types of altered fingerprints: There are three types of altered fingerprints obliteration, distortion and imitation.

Obliteration: Obliteration fingerprints can be obliterated by abrading, cutting, burning and transplanting applying strong chemicals and transplanting smooth skin. Skin disease asleprosy and side of a cancer drug can also obliterated fingerprints.

Distortion: Distorted fingerprints are unnatural ridge patterns by removing portions of skin from fingerprint and either grafting them back in different positions and they have unusual ridge patterns which are not found in natural fingerprints.

Imitation: Imitation fingerprints can still preserve fingerprints-like pattern after an elaborate procedure of fingerprint alteration. Portion of skin is removed from the fingerprint in Fig. 1 the three types of altered fingerprints are discussed with their orientation and it is discussed by Cappelli *et al.* (2007).

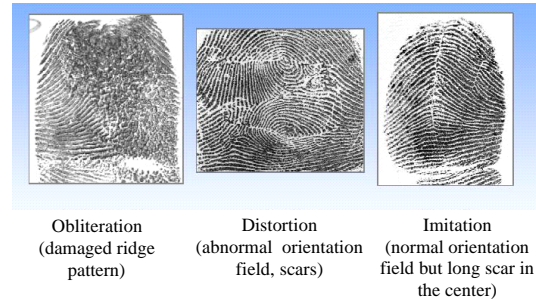


Fig. 1: Types of altered fingerprints

THE RESEARCH METHOD

Fingerprints are used to identify objects, compare objects remotely and test an object for changes. Since, fingerprints are smaller, they are very useful as stand-ins for remote objects. The primary purpose of fingerprint alteration is to evade identification using techniques that vary from abrading, cutting, accidents, etc. In this study, researchers propose classification method FSDCA (Fuzzy-System Design Classification Algorithm) for identifying criminals by purposely altering their fingerprints. Gray level co-occurrence matrix for Altered fingerprint classification consists of pre-processing, feature extraction, classification.

Motivation: The motivation behind the research is growing need to identify a person for security. The fingerprint is one of the popular biometric methods used to authenticate human being. The proposed enhancement method provides reliable and better result for classification of altered fingerprints.

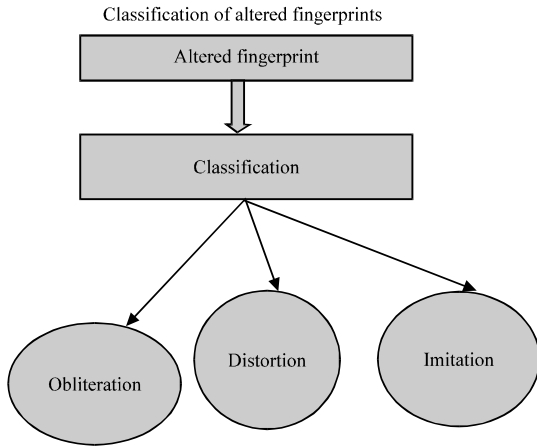


Fig. 2: System structure

Contribution: In this study, researchers used FSDCA algorithm for classifying the altered fingerprint into three types of fingerprints (obliteration, distortion and imitations) with the help of JAVA codes. The system structure is given in the Fig. 2. In Fig. 2 altered fingerprint is given as an input to the algorithm and the image is classified using the FSDCA algorithm. Pre-processing consists of normalization, segmentation, binarization and thinning.

PRE-PROCESSING

The fingerprint image gets corrupted due to irregularities and non-uniformity in the impression taken and due to variations in the skin and the presence of the scars, humidity, dirt, etc. To overcome these problems to reduce noise and enhance the definition of ridges against valleys, various techniques are applied as following.

Normalization: Image normalization is the next step in fingerprint enhancement process. Normalization is a process of standardizing the intensity values in an image so that these intensity values lie within a certain desired range. It can be done by adjusting the range of grey-level values in the image. Let $G(i, j)$ denotes the grey-level value at pixel (i, j) and $N(i, j)$ represent the normalized grey-level value at pixel (i, j) :

$$N(i, j) = \begin{cases} M_0 + \sqrt{\frac{V_0(G(i, j) - M)^2}{V}}, & \text{if } I(i, j) > M \\ M_0 - \sqrt{\frac{V_0(G(i, j) - M)^2}{V}}, & \text{otherwise} \end{cases}$$

where, M_0 and V_0 the estimated mean and variance of $I(i, j)$, respectively. Where Fig. 3 contains the three types



Fig. 3: a) A good quality fingerprint image; b) A poor quality fingerprint and c) A noisy fingerprint image

of fingerprints that figures are taken as an input of the normalization. In Fig. 3a is a good quality image, b is a poor quality image and c is a noisy image.

Segmentation: Image segmentation separates the foreground regions and the background regions in the image. The foreground regions refer to the clear fingerprint area which contains the ridges and valleys. This is the area of interest. The background regions refer to the regions which are outside the borders of the main fingerprint area which does not contain any important or valid fingerprint information. The extraction of noisy and false minutiae can be done by applying minutiae extraction algorithm to the background regions of the image.

Thus, segmentation is a process by which researchers can discard these background regions which results in more reliable extraction of minutiae points. Researchers are going to use a method based on variance thresholding. The background regions exhibit a very low grey-scale variance value whereas the foreground regions have a very high variance. Firstly, the image is divided into blocks and the grey-scale variance is calculated for each block in the image. If the variance is less than the global threshold then the block is assigned to be part of background region or else it is part of foreground. The grey-level variance for a block of size $S \times S$ can be calculated as:

$$Var(k) = \frac{1}{S^2} \sum_{i=0}^{S-1} \sum_{j=0}^{S-1} (G(i, j) - M(k))^2$$

Where:

- Var (k) = The grey-level variance for the block k
- G (i, j) = The grey-level value at pixel (i, j)
- M (k) = The mean grey-level value for the corresponding block k

Binarization: Most minutiae extraction algorithms operate on basically binary images where there are only two levels

of interest: the black pixels represent ridges and the white pixels represent valleys. Binarization converts a grey level image into a binary image. This helps in improving the contrast between the ridges and valleys in a fingerprint image and consequently facilitates the extraction of minutiae. One very useful property of the Gabor filter is that it contains a component of zero which indicates that the resulting filtered image has a zero mean pixel value. Hence, binarization of the image can be done by using a global threshold of zero. Binarization involves examining the grey-level value of every pixel in the enhanced image and if the grey-level value is greater than the predefined global threshold then the pixel value is set to value one; else, it is set to zero. The outcome of binarization is a binary image which contains two levels of information, the background valleys and the foreground ridges.

Fingerprint ridge thinning: Thinning is the process of reducing the thickness of each line of patterns to just a single pixel width. The requirements of a good thinning algorithm with respect to a fingerprint are:

- The thinned fingerprint image obtained should be of single pixel width with no discontinuities
- Each ridge should be thinned to its centre pixel
- Noise and singular pixels should be eliminated
- No further removal of pixels should be possible after completion of thinning process

In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3×3). And finally removes all those marked pixels after several scans. But it is tested that such an iterative, parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans. A one in all method to extract thinned ridges from gray-level fingerprint images directly. Their method traces along the ridges having maximum gray intensity value. The advancement of each trace step still has large computation complexity although it does not require the movement of pixel by pixel as in other thinning algorithms.

Enhanced thinning: Ridge thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. Ideally, the width of the skeleton should be strictly one pixel. However, this is not always true. There are still some locations where the skeleton has a two-pixel width at some erroneous pixel locations. An erroneous pixel is defined as the one with more than two 4-connected neighbors. The existence of erroneous pixels may:

- Destroy the integrity of spurious bridges and spurs
- Exchange the type of minutiae points
- Miss detect true bifurcations

Therefore, before minutiae extraction, there is a need to develop a validation algorithm to eliminate the erroneous pixels while preserving the skeleton connectivity at the fork regions. For this purpose an enhanced thinning algorithm is bid out.

Enhanced thinning algorithm:

Step 1: Scanning the skeleton of fingerprint image row by row from top-left to bottom-right. Check if the pixel is 1.

Step 2: Count its four connected neighbors.

Step 3: If the sum is greater than two, mark it as an erroneous pixel.

Step 4: Remove the erroneous pixel.

Step 5: Repeat steps 1-4 until whole of the image is scanned and the erroneous pixels are removed.

Sample input and output image of this process is shown in the Fig. 4 and this process is implemented using JAVA which is described in the Fig. 5.

Feature extraction: Researchers compute CM for the fixed d and $\theta = 0, 45, 90$ and 135 and statistical features

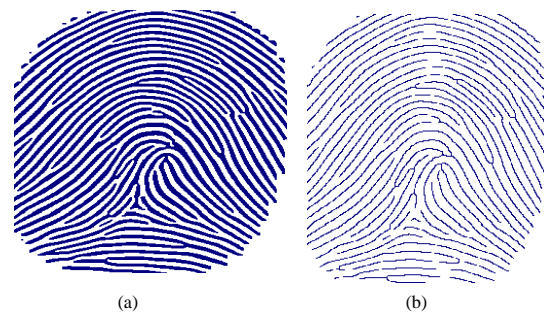


Fig. 4: a) Fingerprint ridge thinning; b) enhanced thinning

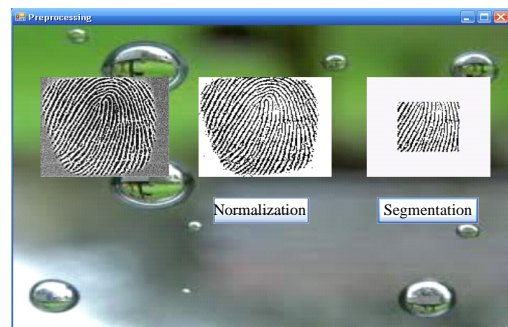


Fig. 5: Result of pre-processing

(Shi *et al.*, 2007) so researchers have (Huckemann *et al.*, 2008) co-occurrence matrices. Based on each computed CM, 12 features that can successfully characterize the statistical behavior of a co-occurrence matrix are extracted. In order to estimate the Orientation Method (Huckemann *et al.*, 2008) has been proposed. They are as follows.

Maximum probability:

$$f_1 = \text{Ma}_{i,j} p(i, j) \tag{1}$$

Contrast:

$$f_2 = \sum_i \sum_j (i - j) 2p(i, j) \tag{2}$$

Entropy:

$$f_3 = \sum_i \sum_j \frac{p(i, j)}{\log p(i, j)} \tag{3}$$

Angular second moment:

$$f_4 = \sum_i \sum_j p(i, j) \tag{4}$$

Homogeneity:

$$f_5 = \sum_i \sum_j \frac{p(i, j)}{1 + |i - j|} \tag{5}$$

Dissimilarity:

$$f_6 = \sum_i \sum_j |i - j| p(i, j) \tag{6}$$

Mean:

$$f_7 = \sum_i \sum_j \frac{p(i, j)}{m \times n} \tag{7}$$

where, m and n are the rows and columns in p, respectively.

Correlation:

$$f_8 = \sum_i \sum_j \frac{(i - \mu_x)(j - \mu_y)p(i, j)}{s_x s_y} \tag{8}$$

Where:

μ_x, μ_y = The means

σ_x, σ_y = The standard deviations of ρ_x, ρ_y , respectively

If researchers define $s = \sum \sum p(i, j)$, researchers can extract 4 other feature as follows:

$$f_9 = \frac{\sum_i \sum_j \frac{p(i, j)}{j^2}}{s} \tag{9}$$

$$f_{10} = \frac{\sum_i \sum_j j^2 p(i, j)}{s} \tag{10}$$

$$f_{11} = \frac{\sum_i \left(\sum_j p(i, j)^2 \right)}{s} \tag{11}$$

$$f_{12} = \frac{\sum_j \left(\sum_i p(i, j)^2 \right)}{s} \tag{12}$$

Classification of altered fingerprints using FSDCA (Fuzzy System Design Classification Algorithm):

Fuzzy if then rules represents fuzzy associative memory in which knowledge is stored systems are capable of representing diverse (Nandakumar *et al.*, 2007).

Inference rules in fuzzy logic:

- Two Objects are equal if and only if all properties applied to them are equivalent:

$$\forall x, y (x = y) \Leftrightarrow (\forall p (p(x) \Leftrightarrow p(y)))$$

- Two functions are equal if and only if they have same value for all arguments:

$$\forall f, g (f = g) \Leftrightarrow (\forall x (f(x) = g(x)))$$

Algorithm

Input: Altered fingerprints.

Output: Any one type of altered fingerprints obliteration, distortion and imitations.

Step 1: Image is given as an input to the preprocessing. In preprocessing the image is denoised.

Step 2: From the denoising image the features are extracted and that are stored in the matrix.

Step 3: Making the inference rules related to the problem and comparing the features with the given input image if any one rule is matched with an input.

Step 4: Finally the result is reached.

EXPERIMENTAL RESULTS

To test the proposed approach, two databases are used one is collected from the hospital that is used for testing (DB1 and DB2) and another database contains

Table 1: Results the altered fingerprint classification algorithm on the real database

Type	Imitations	Disortions	Obliterations	Normal	Un known
Number of Images	65	32	75	220	8 (not in proper impression)

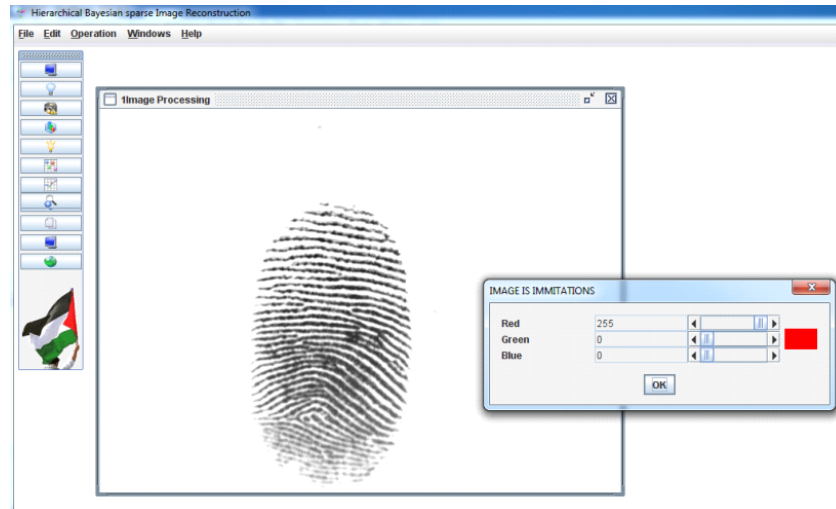


Fig. 6: Sample result of classification

the three images (obliteration, distortion and immitations). DB1 database contains 500 images that are classified using the FSDCA algorithm for the experitments, the first 100 images of fingerprints are used for training and the remaining 400 images were used for testing the result of the tested images are given in the Table 1 and the sample result of the image is shown in the Fig. 6 for fignerprint matching the many software (Huckemann *et al.*, 2008; Jain and Feng, 2011; Wang and Hu, 2011) and hardware (Xu *et al.*, 2009) solutions have been proposed.

CONCLUSION

Researchers have proposed algorithm FSDCA for the altered fingerprint classification. The altered fingerprin features are extracted in the matrixa and that can well characterize the regular texture of fingerprint images. The obtained better result for altered fingerprints.

REFERENCES

Cappelli, R., A. Lumini, D. Maio and D. Maltoni, 2007. Fingerprint image reconstruction from standard templates. *IEEE Trans. Pattern Anal. Machine Intell.*, 29: 1489-1503.

Huckemann, S., T. Hotz and A. Munk, 2008. Global models for theorientation field of fingerprints: An approach based on quadratic differentials. *Pattern Anal. Machine Intell. IEEE Trans.*, 30: 1507-1519.

Jain, A.K. and J. Feng, 2011. Latent fingerprint matching. *Pattern Anal. Machine Intell. IEEE Trans.*, 33: 88-100.

Nandakumar, K., A.K. Jain and S. Pankanti, 2007. Fingerprint-based fuzzy vault: Implementation and performance. *Inform. Forensics Security IEEE Trans.*, 2: 744-757.

Shi, P., J. Tian, Q. Su and X. Yang, 2007. A novel fingerprint matching algorithm based on minutiae and global statistical features. *Proceedings of the 1st IEEE International Conference on Biometrics: Theory, Applications and Systems, September 27-29, 2007, Crystal City, VA.*, pp: 1-6.

Wang, Y. and J. Hu, 2011. Global ridge orientation modelling for partial fingerprint identification. *IEEE Trans. Pattern Anal. Machine Intell.*, 33: 72-87.

Xu, H., R.N.J. Veldhuis, A.M. Bazen, T.A.M. Kevenaer, T.A.H.M. Akkermans and B. Gokberk, 2009. Fingerprint verification using spectral minutiae representations. *Inform. Forensics Security IEEE Trans.*, 4: 397-409.