

Fingerprint Verification System based on Active Forgery Techniques

Abbas H. Hassin Alasadi

Department of Computer Information System,
College of Information Technology,
Basra University, Iraq.

Roqaya Hamad Jaffar

Department of Computer Science, College of
Science, Basra University, Iraq.

ABSTRACT

The fingerprint is a powerfully applicable tool for person authentication in commercial business, civil, and forensic usage. Minutiae points and ridge patterns consider the main source of features that mostly used in recent fingerprint identification systems. In this paper, Scale Invariant Feature Transform (SIFT) is extensively used for representation and extraction of features. After that, RANSAC algorithm is used for determining the matching area exactly. Database of International Fingerprint Verification Competition (FVC2000 and FVC2002) has used in experimental results. Finally, the results have compared with other works. Empirically, the results of the proposed algorithm were acceptable and better.

General Terms

Biometrics, Pattern Recognition, and Image Processing.

Keywords

Fingerprint matching, Feature extraction, SIFT, RANSAC.

1. INTRODUCTION

Nowadays, many methods, such as iris, face, fingerprints, veins, hand geometry, voice, retina, handwriting recognition have implemented as biometrics authenticate identity system. Because it is suitable, unique, and low cost tool, the fingerprint is one of the widespread biometrics that increasingly utilizes [1]. The fingerprint is one of the tools that are used often for personal determining in both forensic application and civilian.

Because of the fingerprints database is huge size, the recognition process encounters a time problem for searching the person's distinctiveness inside the database. Consequently, the reducing the time of processing are main goal and challenges of any fingerprint systems. A reduction of processing of identification time can be performed by managing two factors, that is, "the process time of a single matching system" and "the number of matching system".

Methods of fingerprint recognition can be mainly classified as texture based or minutiae based which all depend on one of the features; i) minutiae, ii) correlation and iii) ridge features. [2,3,4,5, 6,7,8,9].

Consequently, using additional feature may be required for accuracy matching in a fingerprint image. More than 1400 pores may be found in one image of a fingerprint. According to [10], only 20 to 40 pores are required for fingerprint identification.

This paper proposes an approach for fingerprint matching using Scale Invariant Feature Transform (SIFT) describing fingerprint image features. In processing images, Lowe provided the SIFT algorithm [11] as a method for extraction of distinguished invariant features. It has profitably applied to

various problems of depended on feature matching, which involves processes such as recognizing objects, estimating poses, retrieving the image.

2. DATABASE

In this paper, database of International Fingerprint Verification Competition (FVC) FVC2000 and FVC2002 has used in experimental results. Images are collected by the Biometric System Lab (University of Bologna), the Pattern Recognition and Image Processing Laboratory of Michigan State University and the U.S. National Biometric Test Center (San Jose State University).

The database consists of four groups of images. Every group has 80 images, 8 images for every person. Fig.1 exhibits a sample of FVC2000 database. For more specific distinctive of these two databases are brief in Table 1 and Table 2.

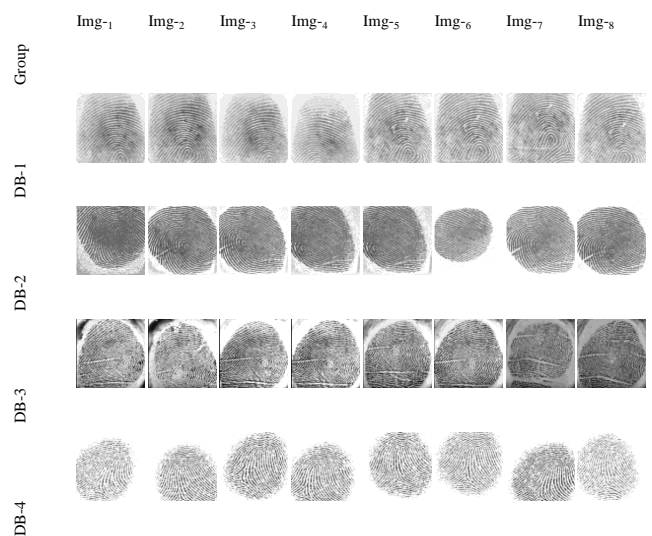


Fig 1: Samples of FVC2000 database.

Table 1. Description of FVC 2002 DB1 and DB2 databases [12].

	Sensor Type	Image Size	No. of images	Resolution
DB-1	Optical Sensor	388x374 (142K pixels)	10x8	500 dpi
DB-2	Optical Sensor	296x560 (162K pixels)	10x8	569 dpi

Table 2. Explanation of FVC 2000 DB1, DB2, DB3, and DB4 databases [12].

	Sensor Type	Image Size	No. of images	Resolution
DB-1	Low cost-Optical Sensor	300 x300	10x8	500 dpi
DB-2	Low Cost-Capacitive Sensor	256 x364	10x8	500 dpi
DB-3	Optical Sensor	448 x478	10x8	500 dpi
DB-4	Synthetic Generator	240 x320	10x8	About 500dpi

3. FINGERPRINT MATCHING SYSTEM (FPMS)

There are two stages of the phase proposed structure of fingerprint matching approach: the testing and training. Each stage has specific functions, so all functions have explained in detail as the following subsections. The testing phase and the training phase are the same, but, in the testing phase, the features do not put in the database just entered to matching system. Fig. 2 describes the block diagrams of the training and testing stages of FPMS respectively.

3.1 Preprocessing

In this paper, the data sets from FVC2000 and FVC2002 have collected. The database contain 740 images are captured in the TIF format, with different resolution and different size. Consequently, two steps of preprocessing are prepared. First step is converting the TIF format into JPG. Second is size normalization to 200x200 pixels. Furthermore, contrast and brightness both are corrected.

For reducing the time consuming, we merged the eight images for each person into one image with converting it into gray color.

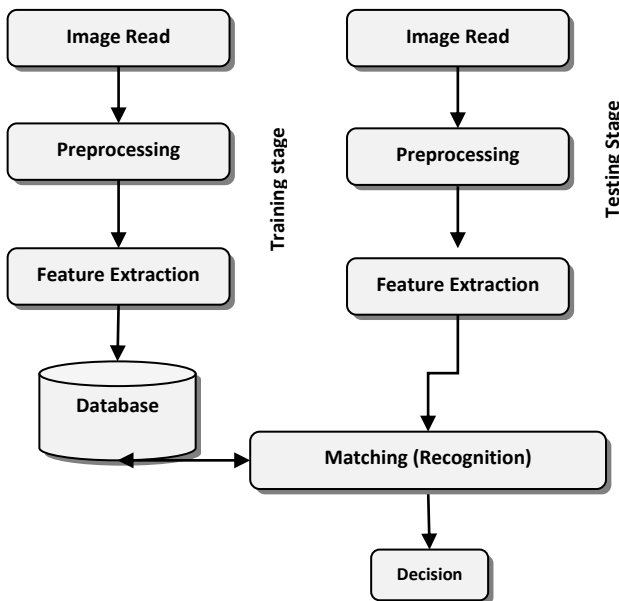


Fig 2: A block diagrams of the training and testing stages of FPMS.

3.2 Feature Extraction

Feature extraction is considered as a substantial step in fingerprint discrimination, whereas the preprocessor results have utilized as a guide for features extraction. However, SIFT algorithm was applied for all fingerprint images. The SIFT algorithm involves four major stages for detection and description of local features, or key points, in the image [11]

- Scale-space peak detection.

- Localization for Keypoints.
- Assignment for Orientation.
- Descriptor for each 6Keypoints.

4. BACKGROUND OF SIFT

To discover the regions in a fingerprint image and matching with other fingerprints, here an explanation in details for the suggested approach. Fig. 3 showing the main stages of SIFT-based approach including the preprocessed image of a given fingerprint.

4.1 Extraction of Image Keypoints, then Collecting Features

For finding possible identical fingerprints in the database, RGB type of images should be converted to grayscale type by standard color space conversion for the image. The first process is the extraction of Image Keypoints, then Collecting Features. The locations that transfer determined information of the image contents are called keypoints. Keypoints can be identified by a feature vector where a collection of image statistics comes from local neighborhoods of the keypoint. The required keypoints and favorable features for extraction must be located in a distinguish site of the image, moreover, computable and robust to geometrical transformations, lighting variations, noising, and degradation[13]. For any selected keypoints, a 128-dimensional features vector is produced by the histograms of local gradients of keypoint's neighborhoods.

4.2 Putative Keypoint Matching

Then, the best-bin-first method was used for matching the revealed SIFT keypoints according to their feature vectors. A matching was performed for each keypoint (at location x with feature f), with the nearest neighbor (location \tilde{x} , feature vector \tilde{f}) correspondent one by measuring Euclidean distance.

Usually, natural images are smooth so that the finest matching of a keypoint occurs within its nearest spatial contiguity. Searching was performed outside a 11×11 pixels region around the keypoint to prevent localization of searching to the nearest of the keypoint's neighbors. Furthermore, the only keypoints kept were the most distinguished similar while different keypoints could possible match together. Specifically, we require that for any other feature vector f' other than f and \tilde{f} , the distance between f and \tilde{f} has to be smaller than that of f and f' by at least a factor of ε , as $\| \tilde{f} - f \|_2 < \varepsilon \| f' - f \|_2$, where $\varepsilon(0;1)$ is a preset threshold controlling the distinctiveness of the matching. We use a default $\varepsilon = 0.5$ to provide a good trade-off between matching accuracy and ratio of outliers.

4.3 Evaluation of Transformed Affine Between Matched Keypoints

According to matching the supposed keypoints, the possible geometric distortions of the duplicated regions were evaluated. The distortion was modeled as a transformed affine of the pixel in order to generalize rotation, scaling, and shearing transforms available in image editing software.

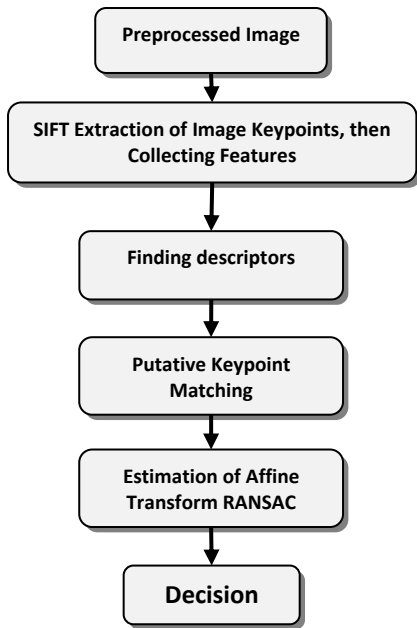


Fig 3: The main steps of SIFT based method

4.4 Estimation of Affine Transform by RANSAC

Affine transform parameters were evaluated by applying supposed matching of SIFT keypoints. The results obtained were inaccurate because of the wide extent of keypoints mismatching. Consequently, In purpose of reducing deceptive keypoints relations and obtaining correct transform parameters at the same time, a Random Sample Consensus (RANSAC) were used as a widely confirmed robust evaluating method [14].

5. EXPERIMENTAL RESULTS

Many published works used FVC2000 DB2, DB1, DB3, and DB4 databases in order to evaluate their algorithms performance; this paper depends on this database as well. Each database composed of images of 100 different fingers with eight impressions of 500-dpi resolution for every fingerprint.

1. Positive case : Fig. 4A computes the SIFT for the fingerprint and another image for eight fingerprints; firstly, we compute the keypoints for fingerprint which equals to 7547. Fig. 4B determines the descriptor that equals to 128×7547 . Thirdly, Fig. 4C computes the second neighbor matching between two images (2nn) that matches to 107 features. Finally, Fig. 4D computes the geometric transform (geo) which matches to 43 features.

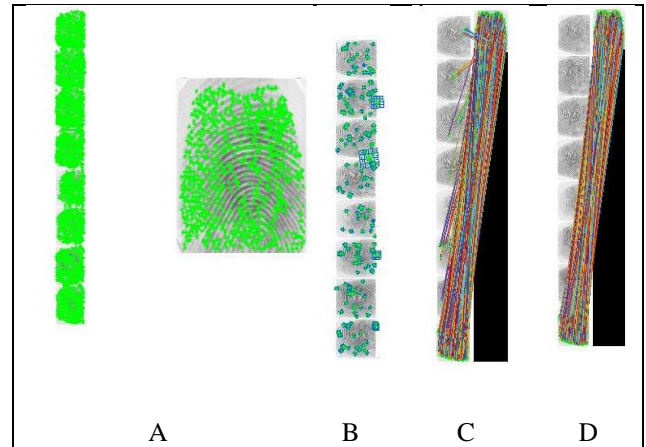


Fig 4: Experimental results as a positive case.

2. Negative case : Fig. 5A computes the SIFT for the fingerprint and another image for eight fingerprints; firstly, we computes the keypoints for fingerprint that equals to 8537. Secondly, Fig. 5B determines the descriptor, which equals to 128×8537 . Thirdly, Fig. 5C computes the second neighbor matching between two images (2nn) that matches to 2 features. Finally, Fig. 5D computes the geometric transform (geo) which matches to zero features. That is mean no matching.

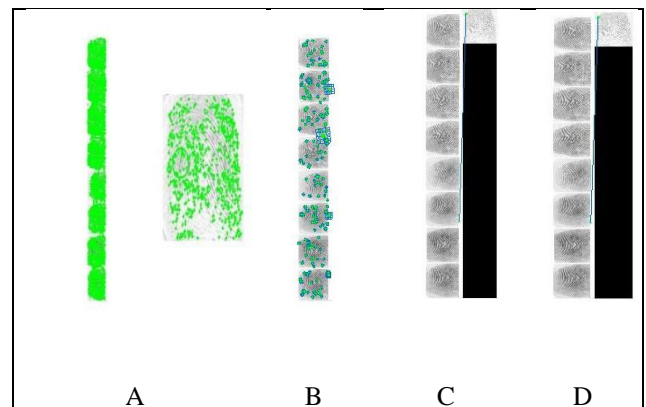


Fig 5: Experimental results as a negative case.

Lastly, for checking the performance of experimental result, we computes the whole fingerprint images in DB1 at once. Fig. six computes the SIFT for all fingerprints and another image for eight fingerprints; firstly, we compute the keypoints for fingerprint that equals to 49635. Secondly, it determines the descriptor, which equals to 128×49635 . Thirdly, it computes the second neighbour matching between two images (2nn) that matches to 995 features. Finally, it computes the geometric transform (geo) which matches to 620 features. There is a matching.

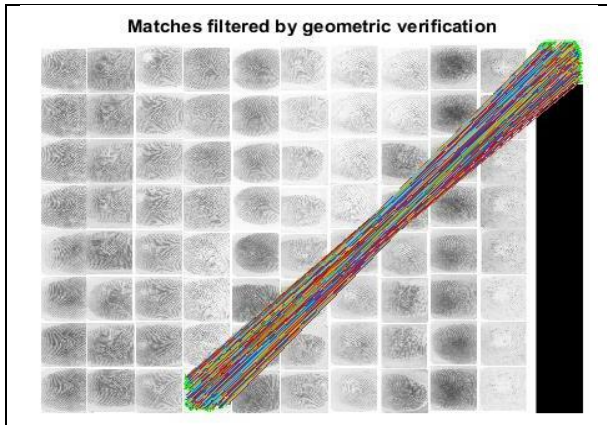


Fig. 6. Experimental results for all DB1 fingerprint images.

6. PERFORMANCE METHODS

Roc curve is a fundamental tool for diagnostic test evaluation. It is a graph, which is used for summarizing the efficiency of the classifier over every conceivable threshold. It's plotting the false positive ratio (FPR) and true positive ratio (TPR) against the false negative ratio (FNR) and true negative ratio (TNR) as user changes threshold to assign observations for a specific class [15].

In the proposed system, the efficiency can be classified into the following perspectives:

The sensitivity (TRUE POSITIVE) of a recognized test is the fraction of positive cases over the total of afflicted cases, which can be expressed by:

$$\text{Sensitivity} = \frac{\text{true positives}}{\text{true positives} + \text{false negatives}} \quad (1)$$

A test with a high value of sensitivity must have a minimal number of false negatives and is therefore useful in order to recognize the fingerprint.

The specificity (TRUE NEGATIVE) of a test is the fraction of healthy cases over the total of un-afflicted cases, which can be expressed by:

$$\text{Simplicity} = \frac{\text{true negatives}}{\text{true negatives} + \text{false positives}} \quad (2)$$

A test with a high value of specificity must have a minimal number of false positives and is therefore useful to exclude the wrong fingerprint.

There are other criteria that include those four perspectives, such as accuracy that is the measure of the global performance of the algorithm about the correct decisions and precision which corresponds to the fraction of relevant recognitions:

$$\text{Accuracy} = \frac{\text{true positives} + \text{true negatives}}{\text{true negatives} + \text{true positive} + \text{false positives} + \text{false negatives}} \quad (3)$$

$$\text{Precision} = \frac{\text{true positives}}{\text{true positive} + \text{false positives}} \quad (4)$$

Table 3 displays the performance measure, which applied on FVC2000 databases. Simultaneously, Table 4 displays the FVC2002 database.

Table 3. The performance measure, which applied on FVC2000 databases.

Criteria	DB-1	DB-2	DB-3	DB-4	ALL
Sensitivity	0.93	0.94	0.89	0.94	0.92
Accuracy	0.88	0.90	0.86	0.90	0.89
Precision	0.83	0.86	0.82	0.86	0.84
Simplicity	0.85	0.87	0.83	0.87	0.85

Table 4. The performance measure that applied on FVC2002 databases.

Criteria	DB-1	DB-2	ALL
Sensitivity	0.92	0.92	0.92
Accuracy	0.86	0.86	0.86
Precision	0.76	0.8	0.78
Simplicity	0.81	0.82	0.81

7. PROPOSED SYSTEM VS. RELATED WORK SYSTEM

The implementation of proposed system has illustrated by two types of features and compared with other related system as in Table 5.

Table 5. Proposed System vs. related work system.

Algorithm	EER (%)
Compensatory algorithm	0.378
FVC2002/ PA15	0.19
FVC2002 /PA27	0.33
Proposed Algorithm Fvc2002/Db1	0.21
Proposed Algorithm Fvc2002/Db2	0.20

8. CONCLUSION

In this paper, SIFT has been used for fingerprint feature extracting and verification. It is invariant according to picture scaling, rotation. Fingerprint matching is performed in two stages:

- i) Feature extract for matching and
- ii) Determining false fingerprint matches with estimation geometric translation.

Improving the performance of SIFT is done by reduction the image noise. Typically, pre-processing step start by converting the given image into grey level and then normalize all images into fixed sizes. As a feature extraction step, determine the key points that used in the SIFT operator. These key points are extraction by usability computing Gaussian and DoG pyramid. The key points of low contrast or are noxious placed alongside an area will below stand removed. The specialty is accomplished by way of the usage of a high dimensional vector. When the use of SIFT within fingerprint discrimination, the range regarding key points are extracted. Totally concerning the attribute regarding an image of a fingerprint. After computing SIFT keypoints and determine the descriptors has computed the matching steps. Particularly, we consider a comparison between the same fingerprints with the different impression. When we applied SIFT algorithm should be used other algorithms because the huge computation, which means that it is better to usage another procedure such as RANSAC algorithm to determine matching area exactly.

9. REFERENCES

- [1] Jain, Anil, Arun A. Ross, and Karthik Nandakumar. Introduction to biometrics. Springer Science & Business Media, 2011.

- [2] Stoianov, Alex, Colin Soutar, and Allan Graham. "High-speed fingerprint verification using an optical correlator." *Optical Engineering* 38.1 (1999): 99-107.
- [3] Bolle, Rudolf Maarten, et al. "Fingerprint representation using localized texture feature." U.S. Patent No. 8,180,121. 15 May 2012.
- [4] Jain, Anil K., Salil Prabhakar, and Shaoyun Chen. "Combining multiple matchers for a high security fingerprint verification system." *Pattern Recognition Letters* 20.11 (1999): 1371-1379.
- [5] Willis, Andrew John, and L. Myers. "A cost-effective fingerprint recognition system for use with low-quality prints and damaged fingertips." *Pattern recognition* 34.2 (2001): 255-270.
- [6] Jain, Anil K., et al. "Filterbank-based fingerprint matching." *IEEE transactions on Image Processing* 9.5 (2000): 846-859.
- [7] Cappelli, Raffaele, Matteo Ferrara, and Davide Maltoni. "Minutiae-based fingerprint matching." *Cross Disciplinary Biometric Systems*. Springer Berlin Heidelberg, 2012. 117-150.
- [8] Jain, Anil, Lin Hong, and Ruud Bolle. "On-line fingerprint verification." *IEEE transactions on pattern analysis and machine intelligence* 19.4 (1997): 302-314.
- [9] Maltoni, Davide, Raffaele Cappelli, and Didier Meuwly. "Automated Fingerprint Identification Systems: From Fingerprints to Fingermarks." *Handbook of Biometrics for Forensic Science*. Springer International Publishing, 2017. 37-61.
- [10] Mathur, Surbhi, et al. "Methodology for partial fingerprint enrollment and authentication on mobile devices." *Biometrics (ICB)*, 2016 International Conference on. IEEE, 2016.
- [11] D.G.Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *International Journal of Computer Vision*, 60(2), 91-110, 2004.
- [12] D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, FVC2002: Second Fingerprint Verification Competition, International Conference on Pattern Recognition, 811–814, 2002.
- [13] Beis, Jeffrey S., and David G. Lowe. "Shape indexing using approximate nearest-neighbour search in high-dimensional spaces." *Computer Vision and Pattern Recognition, 1997. Proceedings., 1997 IEEE Computer Society Conference on*. IEEE, 1997.
- [14] Fischler, Martin A., and Robert C. Bolles. "Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography." *Communications of the ACM* 24.6 (1981): 381-395.
- [15] Parikh, Chirag R., and Heather Thiessen-Philbrook. Key concepts and limitations of statistical methods for evaluating biomarkers of kidney disease. *Journal of the American Society of Nephrology*, 2014, 25(8):1621-1629