SPIE Defense and Security Symposium, Orlando, Florida, 2008

Fingerprint Verification Using SIFT Features

Unsang Park*[a], Sharath Pankanti[a], A. K. Jain[b]
[a]IBM T. J. Watson Research Center, Hawthorne, NY, USA 10532;
[b]Dept. of Computer Science & Engineering, Michigan State Univ., East Lansing, MI, USA 48824

ABSTRACT

Fingerprints are being extensively used for person identification in a number of commercial, civil, and forensic applications. Most of the current fingerprint verification systems utilize features that are based on minutiae points and ridge patterns. While minutiae based fingerprint verification systems have shown fairly high accuracies, further improvements in their performance are needed for acceptable performance, especially in applications involving very large scale databases. In an effort to extend the existing technology for fingerprint verification, we propose a new representation and matching scheme for fingerprint using Scale Invariant Feature Transformation (SIFT). We extract characteristic SIFT feature points in scale space and perform matching based on the texture information around the feature points using the SIFT operator. A systematic strategy of applying SIFT to fingerprint images is proposed. Using a public domain fingerprint database (FVC 2002), we demonstrate that the proposed approach complements the minutiae based fingerprint representation. Further, the combination of SIFT and conventional minutiae based system achieves significantly better performance than either of the individual schemes.

Keywords: Fingerprint verification, SIFT, Minutiae points, Characteristic points

1. INTRODUCTION

When the Home Ministry Office, UK formally conceded in 1893 that no two individuals have the same fingerprints, it set in motion a chain of events that culminated in widespread use of fingerprint pattern recognition systems, called AFIS (Automatic Fingerprint Identification Systems) that are being used by law enforcement agencies world wide for over 40 years [1,9]. In fact these fingerprint matching systems are so spectacularly successful in nailing down perpetrators that the term fingerprint has become synonymous with the uniqueness/inherent characteristic itself (e.g., “DNA fingerprinting”). This success has spurred on an ever widening spiral of its applications beyond its original forensic domain. Forensic fingerprint recognition systems graduated to a second generation fingerprint matching technology geared for civilian applications such as deterring welfare disbursement fraud. These second generation “civilian” large scale fingerprint matching systems typically operate completely automatically and are being deployed in significantly more mainstream applications dealing with a larger cross-section of society. It now appears that we are poised for witnessing development of a third generation ubiquitous large scale fingerprint recognition systems that will involve *all* of us. The magnitude of identity theft and security threats has reached an unprecedented epidemic proportion threatening to destroy the very core fabric of our society. The question that is being asked of biometric technologies in general and of fingerprints in particular is that whether these technologies can work all the time, everywhere, and in all contexts for reliable person identification and authentication.

One of the design criteria for building such completely automatic, and reliable fingerprint verification systems is that the underlying sensing, representation, and matching technologies must also be very robust and it is essential that these individual components degrade their performance gracefully in the presence of unwanted “noise”, atypical fingerprint impressions, and unusual or adverse imaging situations. One way to address these requirements of robust performance is to adopt robust representation schemes that capture the discriminatory information in fingerprint impressions.

The most popular method for fingerprint representation is based on local landmarks called minutiae. This scheme evolved from an intuitive system design tailored for forensic experts who visually match the fingerprints. The minutiae-based systems first locate the points, often referred to as minutiae points, in fingerprint image where the fingerprint ridges either terminate or bifurcate and then match minutiae relative placement in a given finger and the stored template. A good quality fingerprint contains between 25 and 80 minutiae depending on sensor resolution and finger placement on the sensor. It is well known that it is difficult to automatically and reliably extract minutiae based representations from poor quality fingerprint impressions arising from very dry fingers or from fingers mutilated by scars, scratches due to accidents, injuries, or profession-related (e.g., electrician, mason, musician) work. Also, there is anecdotal evidence that a fraction of the population may have fingers that have relatively small number of minutiae thereby making fingerprint-based identification more vulnerable to failures for the corresponding individuals.

There are three typical categories of fingerprint verification methods: i) minutiae, ii) correlation, and iii) ridge features. However, considering the types of information used, a method can be broadly categorized as minutiae based or texture based. While the minutiae based fingerprint verification systems have shown high accuracy [10,11,14,5], they ignore the rich information in ridge patterns which can be useful to improve the matching accuracy. Most of the texture based matchers use the entire fingerprint image or local texture around minutiae points [2,3,8,6]. Using local texture is more desirable because the global texture will be more sensitive to non-linear and non-repeatable deformation of fingerprint images. When the local texture is collected based on the minutiae points, the texture based fingerprint representation is again limited and its performance depends upon the reliability of extracted minutiae points. It is not obvious how one could capture the rich discriminatory texture information in the fingerprints that is not critically dependent on finding minutiae points [3] or core points [8].

For the purpose of extending characteristic feature points of fingerprint beyond minutiae points, we adopt Scale Invariant Feature Transformation (SIFT) [4]. SIFT extracts repeatable characteristic feature points from an image and generates descriptors representing the texture around the feature points. In our work, we demonstrate the utility of SIFT representation for fingerprint-based identification. Since the SIFT feature points have already demonstrated their efficacy in other generic object recognition problems, it is expected that this representation is also stable and reliable for many of the matching problems related to the fingerprint domain. Further, since SIFT feature points are based on texture analysis of the entire scale space, it is hoped that these feature points will be robust to the fingerprint quality and deformation variation.

The rest of this paper is composed as follows. Section 2 describes the SIFT algorithm. Section 3 describes our fingerprint matching scheme using SIFT, section 4 describes experimental results, and section 5 provides conclusions and future work.

2. SCALE INVARIANT FEATURE TRANSFORMATION

Scale Invariant Feature Transformation (SIFT) [4] was originally developed for general purpose object recognition. SIFT detects stable feature points in an image and performs matching based on the descriptor representing each feature point. A brief description of the SIFT operator is provided below.

2.1 Scale Space Construction

A scale space is constructed by applying a variable scale Gaussian operator on an input image. Difference of Gaussian (DOG) images are obtained by subtracting subsequent scales in each octave. The set of Gaussian-smoothed images and DOG images are called an octave. A set of such octaves is constructed by successively down sampling the original image. A typical number of scales and octaves for SIFT operation is 5 and 6, respectively. Fig. 1 shows 4 successive octaves with 5 scales and the corresponding difference images.

2.2 Local Extrema

Local extrema are detected by observing each image point in DOG space. A point is decided as a local minimum or maximum when its value is smaller or larger than all its surrounding neighboring points by a certain amount.

2.3 Stable Local Extrema

A local extrema is observed if its derivative in scale space is stable and if it is on an apparent edge. More detailed description of this process can be found in the original paper by Lowe [4]. If an extremum is decided as unstable or is placed on an edge, it is removed because it can not be reliably detected again with small variation of viewpoint or lighting changes.

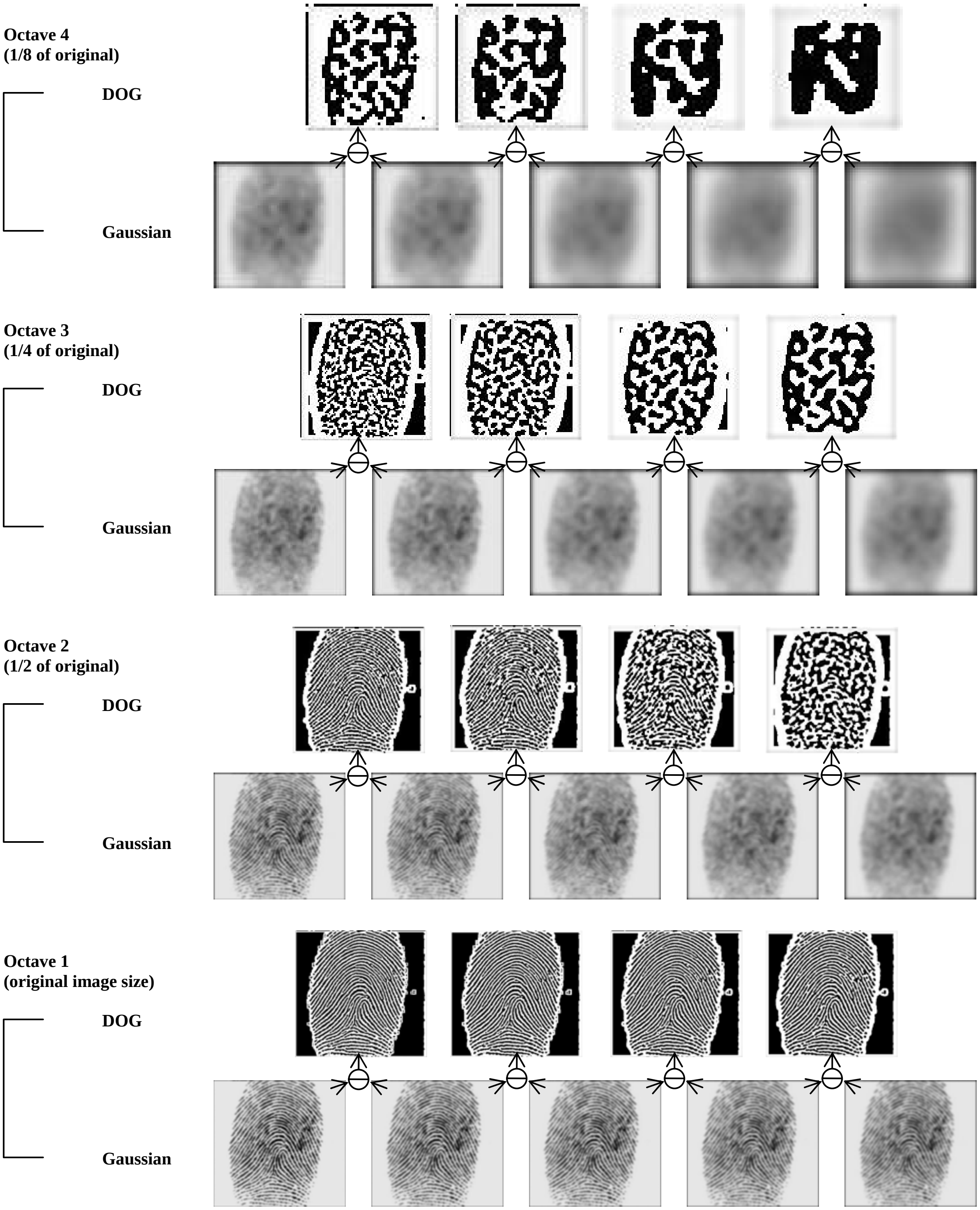


Figure 1. Scale space construction for SIFT operation.

2.4 Assigning Descriptor

A 16x16 window is used to generate a histogram of gradient orientation around each local extremum. To make the descriptor orientation invariant, all gradient orientations are rotated with respect to the major orientation of the local extremum.

2.5 Example Figure

Matching is performed by comparing each local extrema based on the associated descriptors. Suppose we want to match two images I_1 and I_2. Given a feature point p_{11} in I_1, its closest point p_{21}, second closest point p_{22}, and their distances d_1 and d_2 are calculated from feature points in I_2. When the ratio d_1/d_2 is sufficiently small, p_{11} is considered to match with p_{21}. The matching score between two images can be decided based on the number of matching points and their geometric configuration.

3. SIFT ON FINGERPRINT IMAGES

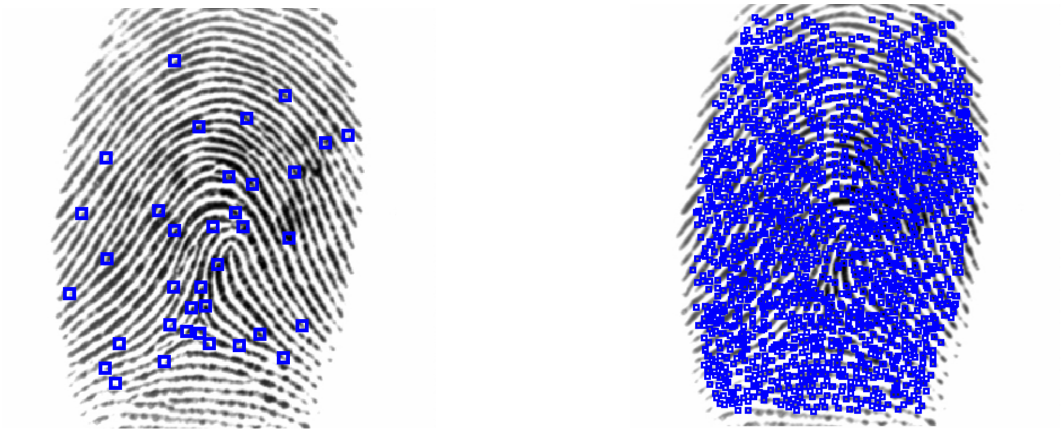
3.1 Characteristic feature points in fingerprints

Minutiae points are strictly defined by the ridge ending and bifurcation points. Therefore, the number of minutiae points appearing in a fingerprint image is limited to a small number (<100). However, SIFT points are only limited by the condition of local minima or maxima in a given scale space, resulting in a large number of feature points. The number of SIFT feature points are affected by a set of parameters such as the number of octaves and scales. Typical fingerprints may contain up to a few thousand SIFT feature points. Fig. 2 shows an example of minutiae points and SIFT feature points on the same fingerprint image. There are only 36 minutiae points, but the number of SIFT feature points is observed to be 2,020. The SIFT parameter values we used are the number of octaves = 4, number of scales = 5, width of Gaussian kernel = 3, and the initial value of the standard deviation of the Gaussian kernel = 1.8.

3.2 Fingerprint verification using SIFT

3.2.1 Preprocessing

Even though SIFT was originally developed for general purpose object recognition and does not require image pre processing, we have performed a few preprocessing steps on fingerprint images to obtain better matching performance. The preprocessing is performed in two steps: i) adjusting the graylevel distribution, and (ii) removing noisy SIFT feature points. When the fingerprint images show similar texture, the performance is expected to be improved because SIFT utilizes texture information both for extracting feature points and matching. For the same reason, noisy SIFT feature points are removed to obtain better matching performance. First, to overcome some apparent differences in gray level



(a) 36 minutiae points

(b) 2020 SIFT feature points

Figure 2. Minutiae and SIFT feature points extracted from the same image (a) minutiae points (b) SIFT feature points.

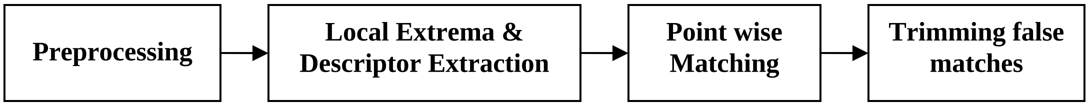
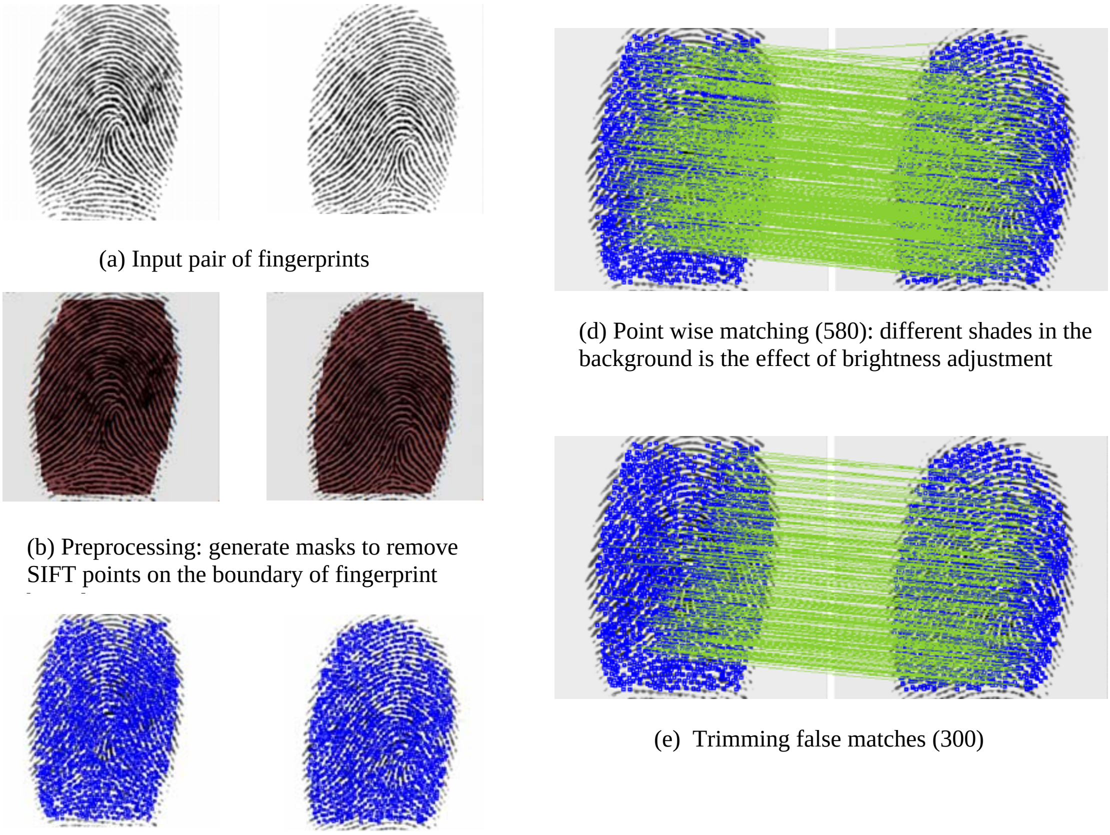


Figure 3. Flow chart of fingerprint matching using SIFT operator.



(a) Input pair of fingerprints

(b) Preprocessing: generate masks to remove SIFT points on the boundary of fingerprint

(c) Local Extrema & Descriptor Extraction

(d) Point wise matching (580): different shades in the background is the effect of brightness adjustment

(e) Trimming false matches (300)

Figure 4. Description of fingerprint matching process using SIFT operator.

distributions, we measure the image intensity in the central area of fingerprint and adjust the histogram. Second, the boundary area of a fingerprint always causes some feature points to be detected because they are local extrema. However, the boundary region is different for every fingerprint impression even for the same finger. Therefore, feature points on the fingerprint boundary usually result in false matches. We construct a binary mask that includes only the inner part of a fingerprint and use it to prevent any noisy feature points from being detected on the boundary. Example binary masks are shown in green color in Fig. 4 (b).

3.2.2 Point wise Matching

The first step in matching is to directly compare each feature point based on the descriptor using Euclidean distance metric. The point wise matching process is described in Sec. 2.5.

3.2.3 Trimming False Matches

The point wise matching generates some erroneous matching points which increase the false accept rate. Therefore, it is necessary to remove spurious matching points using geometric constraints. The typical geometric variations appearing in fingerprint images are limited to small rotations and translations. Therefore, when we place two fingerprint images side by side and draw matching lines as shown in Fig. 4 (d), all true matches appear as parallel lines with similar lengths. Based on this observation, we select a value of majority orientation and length and keep the matching pairs that have the majority orientation and length. This reduces the number of matching points as shown in Figs. 4 (d) and (e).

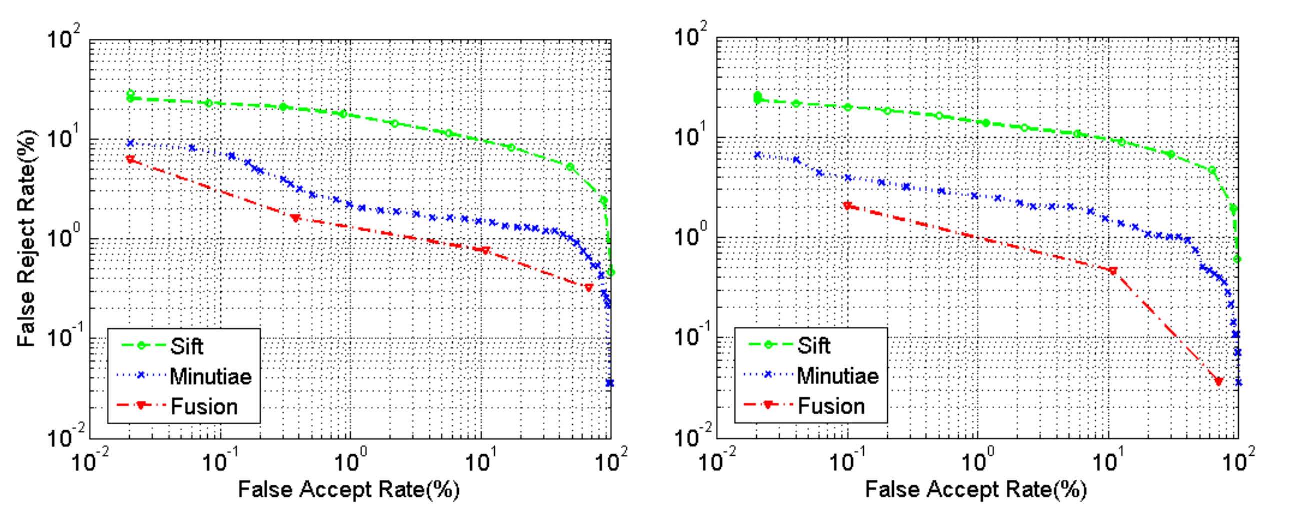
4. EXPERIMENTAL RESULTS

4.1 Database

The performance of the proposed SIFT based fingerprint verification has been evaluated on FVC2002 DB1 and DB2 fingerprint databases [7]. Both the databases contain images of 100 different fingers with 8 impressions for each finger. More detailed characteristics of these two databases are summarized in Table 1. The same set of parameters described in Sec. 3.1 are used for both the databases.

Table. 1. Description of FVC 2002 DB1 and DB2 databases

	Sensor Type	Image Size	Number of images	Resolution
DB1	Optical Sensor	388x374 (142K pixels)	100x8	500 dpi
DB2	Optical Sensor	296x560 (162K pixels)	100x8	569 dpi



(a) DB 1

(a) DB 2

Figure 5. Performance of minutiae and SIFT matchers and their fusion result.

4.2 Fingerprint matching

We have performed all pair genuine matchings and a subset of all possible imposter matchings following the guideline of FVC 2002. As a result, the number of genuine matchings is 2,800 and the number of imposter matchings is 4,950. Fig. 5 shows the performance of SIFT matching using DET curve. By trimming out false matches using geometric constraints, the EER of SIFT matcher is almost reduced by about 50% for both the databases. We also performed a fusion of the SIFT and minutiae based matchers [15]. Fig. 5 shows the performance of minutiae and the fusion using weighted sum-rule with min-max normalization. The weights are empirically chosen as 0.92 for SIFT and 0.08 for minutiae for both databases. The fusion of matchers resulted in better performance than either of the two matchers. Table 2 summarizes the equal error rates (EER) computed from Fig. 5. Fig. 6 shows example matching pairs where minutiae matcher failed but SIFT succeeded in matching them correctly.

Table. 2. EER of SIFT, Minutiae, and Fusion matchers

	SIFT	**Minutiae**	**SIFT + Minutiae**
DB1	8.44 %	1.79 %	0.99 %
DB2	10.76 %	2.13 %	1.07 %

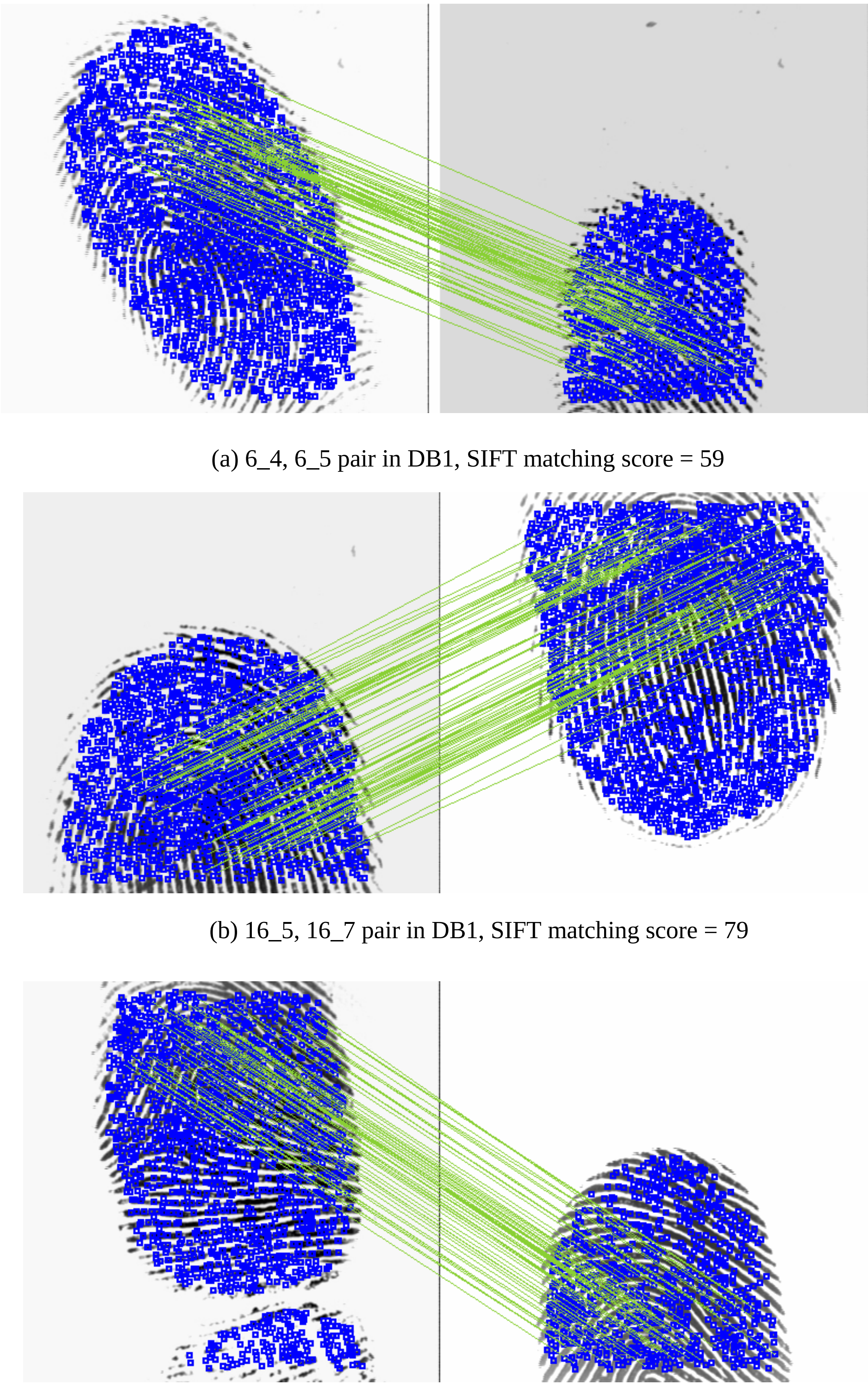
5. CONCLUSIONS AND FUTURE WORK

We have shown that the SIFT operator can be used for fingerprint feature extraction and matching. Even though there have been a few studies using SIFT for face verification [12,13], there have been no prior studies on fingerprint matching using SIFT. We performed fingerprint matching in two steps: i) point-wise match and ii) trimming false matches with geometric constraints. The fusion with a minutiae based matcher shows significant performance improvement on two public domain databases. We believe the performance improvement due to fusion is possible because the sources of information used in minutiae and SIFT based matchers are significantly different. SIFT shows a good possibility of extending minutiae based or minutiae related fingerprint representations. It is possible to further improve the performance of SIFT if proper preprocessing is performed on the input image that can reduce the noise in the images. The typical preprocessing in minutiae based technique involves connecting broken ridges and extracting skeletons of the ridge pattern, which removes all the texture information that is used in the SIFT operator. A proper preprocessing for the SIFT operator would require reducing noise in such a way as to preserve the inherent texture information. The average matching speed of the SIFT matcher, including feature extraction, is ~4 seconds on a 3.2GHz Pentium 4 PC.

Our future work will concentrate on improving the performance of SIFT by developing a proper preprocessing step, better representation of each feature point, and better matching schemes. A good combination of SIFT operator with other texture or minutiae based operations will also be developed to improve the performance.

ACKNOWLEDGMENTS

The minutiae based matching scores and minutiae points of the fingerprint images in FVC 2002 databases were provided by Karthik Nandakumar and Abhishek Nagar at Michigan State University. This research has been supported by ARO grant W911NF-06-1-0418.



(a) 6_4, 6_5 pair in DB1, SIFT matching score = 59

(b) 16_5, 16_7 pair in DB1, SIFT matching score = 79

(c) 17_2, 17_5 pair in DB1, SIFT matching score = 63

Figure 6. Example genuine pairs where minutiae matcher failed, but SIFT successfully matched given the threshold values corresponding to the EER. These pairs remained as correct matches after the fusion.

REFERENCES

1. A. K. Jain, P. Flynn, and A. Ross (eds.), *Handbook of Biometrics*, Springer, 2007.
2. D. Roberge, C. Soutar, and B. V. Kumar, High-speed fingerprint verification using an optical correlator, in *Proceedings SPIE*, vol. 3386, 242-252, 1998.
3. S. Chikkerur, S. Pankanti, A. Jea, N. Ratha, and R. Bolle, Fingerprint Representation Using Localized Texture Features, *International Conference on Pattern Recognition*, 521-524, 2006
4. D. Lowe, Distinctive image features from scale-invariant key points, *International Journal of Computer Vision*, 60(2), 91-110, 2004.
5. A. K. Jain, S. Prabhakar, and S. Chen, Combining Multiple Matchers for a High Security Fingerprint Verification System, *Pattern Recognition Letters*, 20(11–13), 1371–1379, 1999.
6. A. J. Willis and L. Myers, A Cost-Effective Fingerprint Recognition System for Use with Low-Quality prints and Damaged Fingertips, *Pattern Recognition*, 34(2), 255–270, 2001.
7. D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, FVC2002: Second Fingerprint Verification Competition, *International Conference on Pattern Recognition*, 811–814, 2002.
8. A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, Filterbank-based Fingerprint Matching, *IEEE Transactions on Image Processing,* 9(5), 846-859, 2000.
9. A. K. Jain, L. Hong, and S. Pankanti, Biometric identification. *Comm. ACM*, 91–98, 2000.
10. F. Pernus, S. Kovacic, and L. Gyergyek, Minutiae-based fingerprint recognition, *Proceedings of the Fifth international Conference on Pattern Recognition*, 1380-1382, 1980.
11. A. K. Jain, L. Hong, and R. Bolle, On-line fingerprint verification, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, 302-314, 1997.
12. M. Bicego, A. Lagorio, E. Grosso, and M. Tistarelli, On the Use of SIFT Features for Face Authentication, *Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, 35, 2006.
13. D. R. Kisku, A. Rattani, E. Grosso, and M. Tistarelli, Face Identification by SIFT-based Complete Graph Topology, *Automatic Identification Advanced Technologies*, 63-68, 2007.
14. N. K. Ratha, K. Karu, S. Chen, and A. K. Jain, A Real-Time Matching System for Large Fingerprint Databases, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 18(8), 799–813, 1996.
15. A. K. Jain, K. Nandakumar and A. Ross, Score Normalization in Multimodal Biometric Systems, *Pattern Recognition*, 38(12), 2270-2285, 2005.