A Novel Approach for Fingerprint Verification Using SIKP

Srinivasa Kumar Devireddy, NageswaraRao Thota ,Iyyanki V. Muralikrishna,Tiruveedhula V. Rao

Nalanda Institute of Engineering & Technology, Sattenapalli Mandal,Guntur Dt., A.P., India.

Summary
Fingerprint based verification systems have gained immense popularity due to the high level of uniqueness attributed to fingerprints and the availability of compact fingerprint sensors that can be easily embedded into a wide variety of devices requiring user authentication. 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 key points. We extract characteristic of Scale invariant key points in scale space and perform matching based on the texture information around the feature points using the Scale invariant key points operator. A systematic strategy of applying Scale invariant key points to fingerprint images is proposed. We have used a public domain fingerprint database (FVC 2002). We demonstrate that this approach complements the minutiae based fingerprint representation. Further, the combination of Scale invariant key points and conventional minutiae based system achieves significantly better performance than either of the individual schemes.

Key words:
Fingerprint verification, Scale invariant key points, Minutiae points, Characteristic points

1. Introduction

Biometric recognition refers to automatic authentication of a person based on his/her physiological or behavioral characteristics. Biometric recognition offers many advantages over traditional PIN number or password and token-based (e.g., ID cards) approaches; for example, a biometric trait cannot be easily transferred, forgotten or lost, the rightful owner of the biometric template can be easily identified, and it is difficult to duplicate a biometric trait. Some well known examples of traits used in biometric recognition are fingerprint, iris, face, signature, voice, hand geometry, retina, DNA, gait, keystroke dynamics and ear structure shown in figure 1. A number of commercial recognition systems based on these traits have been deployed and are currently in use. Biometric technology has now become a viable and more reliable alternative to traditional authentication systems. With increasing applications involving human-computer interactions, there is a growing need for fast authentication techniques that are reliable and secure. Biometric recognition is well positioned to meet the increasing demand for secure and robust systems.

There are several requirements that need to be met by a particular biometric trait when being considered for use in an authentication system. These requirements are: (i) universality, which means that each individual should possess the trait, (ii) distinctiveness, which means that the trait for two different persons should be sufficiently different to distinguish between them, (iii) perma¬nence, which means that the trait characteristics should not change, or change minimally, over time, and (iv) collectability, which means that the trait can be measured quantitatively. However, for prac¬tical biometric systems, there are other considerations that are important, namely,

(i) whether the performance and authentication rates of the system are at acceptable levels, measured in terms of speed, recognition accuracy and robustness, in different operational environments,

(ii) whether the biometric trait will be widely accepted by the public for use in their daily lives, and

(iii) whether the system based on the trait can be easily attacked or spoofed. The main requirements of a practi¬cal biometric system are that it should have acceptable recognition performance rates, recognition speed and cost. In addition, it should protect the user from privacy intrusions and be robust with respect to various spoofing attacks.

Among all the biometric traits used for authentication, fingerprint-based recognition has the longest history (almost 100 years) and has been successfully adopted not only in forensic applica¬tions, but in an increasing number of civilian applications.

Manuscript received July 5, 2008.
Manuscript revised July 20, 2008.

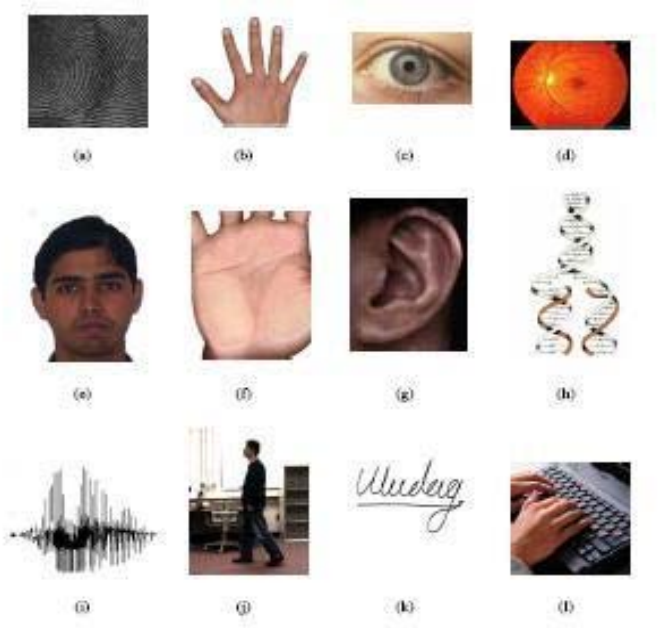


Fig. 1 Some examples of biometric traits: (a) Fingerprint; (b) Hand-geometry; (c) Iris; (d) Retina; (e) Face; (f) Palm print; (g) Ear structure; (h) DNA; (i) Voice; (j) Gait; (k) Signature and (l) Keystroke dynamics.

It is well known that no two individuals have the same fingerprints. Automatic Fingerprint

Identification Systems (AFIS) that are being used by law enforcement agencies world wide for over 40 years [1,9]. 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 [5,10,11,14], 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 [2,3,6,8].

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 key points (SIKP)[4]. SIKP 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 Scale invariant key points for fingerprint-based identification. Since the SIKP 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 these 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.

2. Scale Invariant Key Points (SIKP)

SIKP[4] was originally developed for general purpose object recognition. This detects stable feature points in an image and performs matching based on the descriptor representing each feature point. A brief description of this operator is provided below.

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. 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. 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 extrema 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. 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.

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. Scale Invariant Key Points on Fingerprint Images

3.1 Characteristic feature points in finger prints

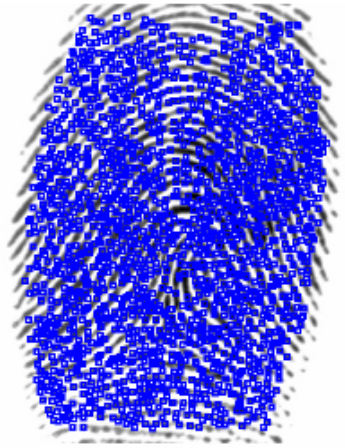
Minutiae points are strictly defined by the ridge ending and bifurcation points. Therefore, the number of minutiae points appearing in a fingerprint image is limited to a small number (<100). However, SIKP points are only limited by the condition of local minima or maxima in a given scale space, resulting in a large number of feature points. The number of SIKP characteristic 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 SIKP characteristic feature points. Figure 2 shows an example of minutiae points and SIKP characteristic feature points on the same fingerprint image. There are only 36 minutiae points, but the number of Scale Invariant Key Points are observed to be 2,020. The SIKP 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 SIKP

3.2.1 Preprocessing

Even though SIKP 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 gray level distribution and (ii) removing noisy SIKP feature points. When the fingerprint images show similar texture, the performance is expected to be improved because SIKP utilizes texture information both for extracting feature points and matching. For the same reason, noisy SIKP feature points are removed to obtain better matching performance. First, to overcome some apparent differences in gray level 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.

(a) 36 minutiae points



(b) 2020 Scale invariant key points

Fig. 2 Minutiae and SIKP extracted from the same image

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 Figure 4 (b).

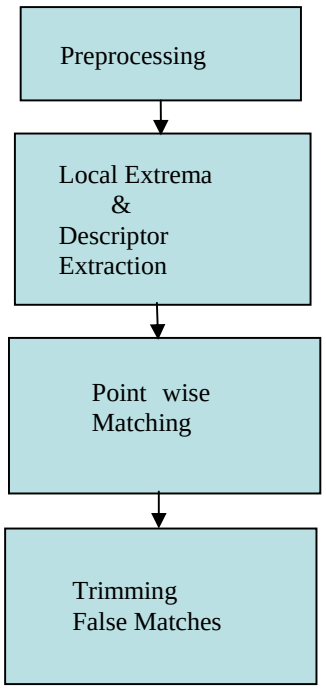
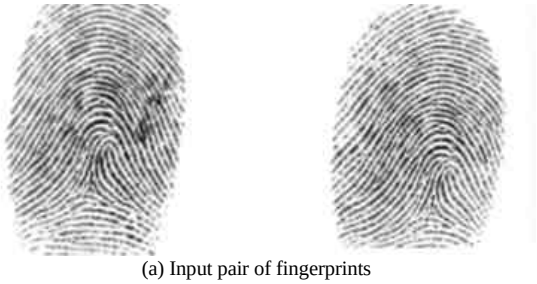


Fig. 3 Flow chart of fingerprint matching using SIKP operator

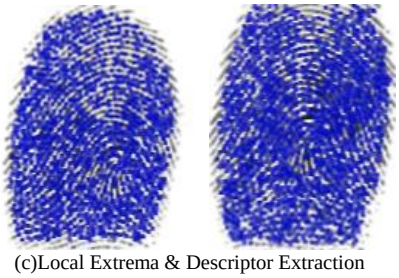
3.2.2 Point wise Matching

The first step in matching is to directly compare each feature point based on the descriptor using Euclidean distance metric. The point wise matching is performed by comparing each local extrema based on the associated descriptors. Suppose we want to match two images I1 and I2. Given a feature point p11 in I1, its closest point p21, second closest point p22, and their distances d1 and d2 are calculated from feature points in I2. When the ratio d1/d2 is sufficiently small, p11 is considered to match with p21. The matching score between two images can be decided based on the number of matching points and their geometric configuration.

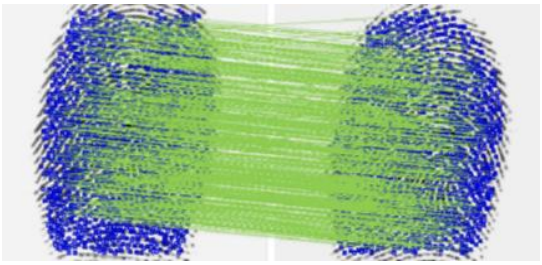


(a) Input pair of fingerprints

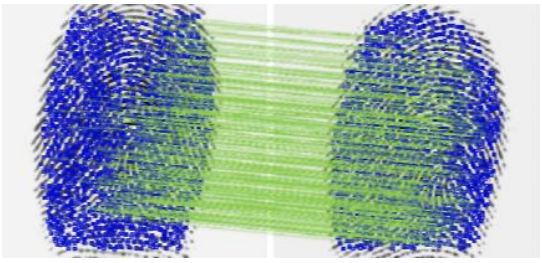
(b) Preprocessing



(c)Local Extrema & Descriptor Extraction



(d) Point wise matching



(e) Trimming false matches

Fig. 4 Description of fingerprint matching process using SIKP operator.

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 Figure 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 Figures 4 (d) and (e).

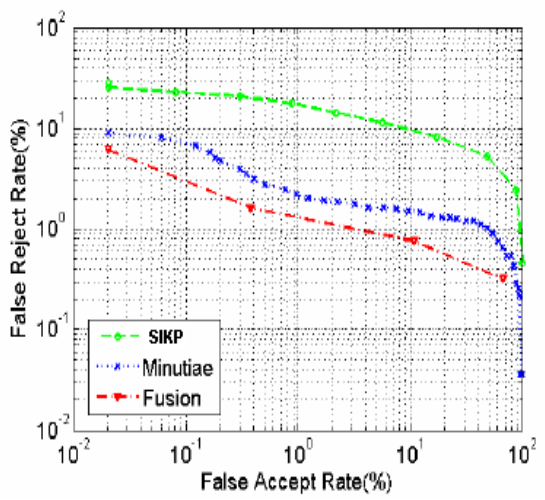
4. Experimental Results

4.1 Database

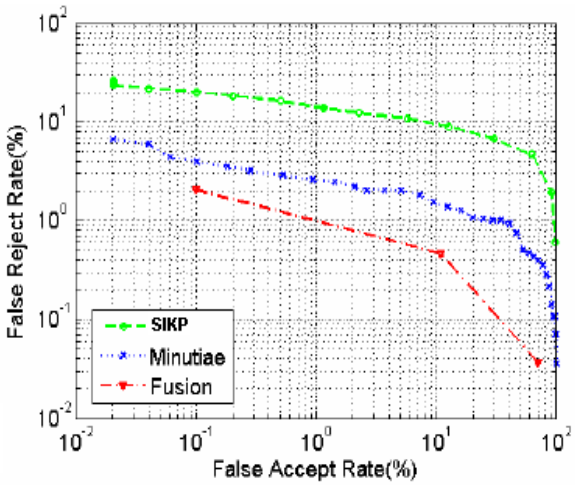
The performance of the proposed Scale invariant key points based fingerprint verification has been evaluated on FVC2002 DB1 and DB2 public domain fingerprint databases [7]. Both the databases contain images of 100 different fingers with 8 impressions for each finger. More detailed characteristics of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

Table 1: Description of FVC 2002 DB1 and DB2 databases

Data base	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) DB1



(b) DB2

Fig. 5 Performance of minutiae and SIKP 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 a public domain fingerprint database. As a result, the number of genuine matchings is 2,800 and the number of imposter matchings is 4,950. Figure 5 shows the performance of SIKP matching using DET curve. By trimming out false matches using geometric constraints, the EER of SIKP matcher is almost reduced by about 50% for both the databases. Figure 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 SIKP 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 Figure 5.

Table 2: Equal Error Rates of SIKP, Minutiae, and Fusion matchers

Database	SIKP	Minutiae	SIKP + Minutiae
DB1	8.44 %	1.79 %	0.99 %
DB2	10.76 %	2.13 %	1.07 %

5. Conclusions

We have shown that the SIKP operator can be used for fingerprint feature extraction and matching. We have 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 SIKP based matchers are significantly different. SIKP shows a good possibility of extending minutiae based or minutiae related fingerprint representations. It is possible to further improve the performance of SIKP 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 SIKP operator.

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 SIKP 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 SIKP-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.

Srinivasa Kumar Devireddy received the B.E. degree in Computer Science & Engineering from Karnataka University, Dharwad in 1992 and M.S. degree in Software Systems from Birla Institute of Technology and Science, Pilani in 1995. He is currently working as a faculty member in the department of Computer Science & Engineering, Nalanda Institute of Engineering & Technology, Guntur. He is a member of IEEE. His research interests are in the areas of Biometrics, Image Processing and Content Based Image Retrieval.

Nageswara Rao Thota received his M.Sc.(Mathematics) degree from Acharya Nagarjuna University, Guntur in 1997, M.Phil degree from Madhrai Kamaraj University, Madhrai, Tamilnadu in 2000 and M.Tech Computer Science & Engineering degree from Acharya Nagarjuna University in 2008. He is currently working as a faculty member in the department of Basic Engineering Sciences, Nalanda Institute of Engineering & Technology, Guntur. His research interests are in the areas of Image Processing and Content Based Image Retrieval.

Dr.MURALI KRISHNA I.V. did his M.Tech from Indian Institue of Technology(IIT), Madras and Ph.D. from Indian Institute of science (I.I.Sc.), Bangalore. He is working as a Professor in the Center for Spatial Information Technology, Jawaharlal Nehru Technological University, Hyderabad. At present he is the Director of Research and Development wing of Jawaharlal Nehru Technological University, Hyderabad. Guided many Ph.D. students in completion of their research work. He is having over 30 years of experience in teaching and research in the field of Information Technology. He was adjusted with the award of the Best Teacher for the year 2004-2005 by the Government of Andhra Pradesh, India.

Dr.Tiruveedhula Venkateswara Rao did his B.E. E.C.E. in 1977 form Andhra University, Visakhapatnam, M.E. Computer Science in 1979 from P.S.G.College of Technology, Coimbatore and Ph.D. in Computer Engineering in 1992 from Wayne state University, Detroit, USA. He worked as a senior faculty member in both USA and INDIA. At present working as Professor and Principal of Khammam Institute of Technology, Khammam. Guided many research scholars for the award of Ph.D. He is having so many international publications to his credit.