Implementation and Evaluation of SIFT Descriptors based Finger-Knuckle-Print Authentication System

E. S. Shameem Sulthana[1*] and S. Kanmani[2]

[1]Bharathiar University, Coimbatore, India; shammumunch@yahoo.com
[2]Department of IT, Pondicherry Engineering College, Pondicherry, India; kanmani@pec.edu

Abstract

Finger-Knuckle-Print (FKP) uses feature detection and matching techniques in its hard core design. It works similar for almost every authentication system. The Scale Invariant Feature Transform (SIFT) is the most reliable feature extraction technique that is used in authentication systems on FKP. The feature descriptors detected by SIFT claim to be capable of distinguishing each and every image in the dataset from one another with the cost involved in its operations. In SIFT based FKP authentication systems, the storage and computational cost will directly depend on the size of the feature descriptors used. Such matching process will directly match these feature descriptors to find an exact match and the descriptors were directly stored in storage media as templates. Hence there is a necessity for storing all the feature descriptors of the enrolled FKP images for future references. The size of these feature descriptors data will be greater than the original FKP image dataset and the performance of the system will rapidly decrease with respect to the increase in enrollment in the database. The proposed work address these issues with FKP based authentication system using SIFT for efficient computation and cost compared with the existing work and proven to be secure and tough resistant for authentication system.

Keywords: Authentication, Feature Description, Matching, Recognition, Scale Invariance

1. Introduction

Biometrics is a study of methods for recognizing individuals lays foundation on one or more inherent substantial characteristics such as finger print, iris, hand geometry and palm print or behavioral traits such as speech, gait. Among them, the most popular and commonly applied biometric systems use hand as a medium as it is easy to use and be implemented lively. The outer surfaces of finger joints have even more obvious line features within smaller area that motivated Lin Zhang et al.[6–10] to propose a new biometric technique – the Finger-Knuckle-Print (FKP), which refers to the image of the outer surface of the finger phalangeal joint. During the last decade, this hand-based biometric system using the features of FKP has been evolved and now competing with other biometric recognition systems.

1.1 Feature Descriptors

Local features are used in several computer vision tasks like object categorization, content-based image retrieval and image recognition. Local features are points, blobs or regions in images that are extracted using feature detector (local). These features are distinctive and yet invariant for many kinds of geometric and photometric transformation, in advance and provide further attention as promising performance[6]. Local feature representation of image is widely is used FKP based authentication systems.

1.1.1 Scale Invariant Feature Detectors

The following are some of the basic scale invariant feature detectors based on the review literature[7,8].

Harris detector: It finds feature points at a fixed scale.

Harris Laplace detector: It uses the scale-adapted Harris function to localize points in scale-space. It then selects the feature points for which the Laplacian-of-Gaussian attains a maximum over scale.

Hessian Laplace: It localizes feature points in space at the local maxima of the Hessian determinant and in scale at the local maxima of the Laplacian-of-Gaussian.

*Author for correspondence

Harris/Hessian Affine detector: It does an affine adaptation of the Harris/Hessian Laplace using the second moment matrix to detect the feature points.

Maximally Stable Extrema Regions detector: It finds regions such that pixels inside the MSER have either higher (bright extrema regions) or lower (dark extrema regions) intensity than all the pixels on its outer boundary.

Uniform Detector (unif): It selects some feature points uniformly on the edge maps by rejection sampling.

All the local feature detectors perform similarly like Harris Affine/Harris Laplace detector performing equal in most cases[9].

1.1.2 Scale and Rotation Invariant Feature Detectors

There are some scales and rotation invariant feature detectors or descriptors. The following feature descriptors can be used for rotation and scale invariant matching applications.

1.1.3 Scale Invariant Feature Transform (SIFT)

SIFT transforms image data into scale-invariant coordinates relative to local features[23–25]. These scale-invariant coordinates are represented by feature descriptors.

1.1.4 The Speeded Up Robust Features (SURF)

SURF is a robust local feature detector, which was presented by Herbert Bay et al. in 2006[13], and compared with SIFT it is claimed to be more vigorous besides dissimilar image transformation.

1.1.5 Binary Robust Independent Elementary Features (BRIEF)

This method uses binary strings as an efficient feature point descriptor and claims to be highly discriminative even when using relatively few bits and can be compute during simple intensity difference tests.

1.1.6 Maximally Stable Extrema Regions (MSER)

This feature detector was proposed by Matas et al.[14] to find correspondences between image elements from two images with different viewpoints.

1.1.7 Local Energy based Shape Histogram (LESH)

LESH[15] is an image descriptor for accessing actual shape with energy model feature. In this work, we will use SIFT method to design a FKP authentication system and validate the performance of the feature detection algorithms in terms of computational and storage cost.

1.2 Problem Specification

If the sizes of the feature descriptors which are used to index or understand an image are smaller than that of the original image, then it will not create any issues with storage and processing. But biometric recognition systems deals with huge volumes of images along with its data. If the size of the detected feature descriptors is higher than that of the size of original data, then, certainly it will cause problems related to computational and storage cost as well as accuracy.

Feature detection and matching are fundamental aspects of any biometrics based identification system and all other computer vision related applications in general[5]. In one of the earlier works of Lowe[16], he proposed a new method called "scale invariant feature transform (SIFT)"to find distinctive invariant features from images that can be used to perform better matching between similar images. In another work Bay[13] proposed a yet another fast, scale and rotation invariant detector and descriptor called "Speeded-Up Robust Features (SURF)".

Zhang et al. proposed a new kind of biometric identifier, called Finger-Knuckle-Print (FKP) an alternate for personal identity authentication. In those works[1–5], they used different techniques for Feature Detection and matching. Morales et. al.[17], used SIFT based algorithm for FKP based authentication system. Choras et. al.[18] used SURF based algorithm in their design of a FKP based authentication system. SIFT and SURF features are in the design of FKP based authentication system and the authors claim that they achieved 100% accuracy[19]. In general, most of the previous SIFT and SURF based FKP based authentication systems claim that they have achieved greater than 98% accuracy. But the storage costs and computations costs involved in handling such big feature descriptors were not addressed clearly in these previous works. The storage and computational costs are most important things of typical authentication system and these two things only will decide the portability of the biometrics system in to a low cost and compact hardware which are generally used in day to day use (such as a small, standalone fingerprint attendance system). This work address the issues related with storage and computational costs involved in SIFT based FKP Authentication system.

2. The Evaluated Feature

2.1 Descriptor Detection Algorithms

This section briefly explains the steps involved in the SIFT algorithm. From these steps one can understand the processing time involved in finding the feature descriptors. A detailed explanation was given by Lowe[16] and Bay[13].

2.1.1 Scale Invariant Feature Transform (SIFT)

1. Scale-space extreme detection

The invariant detected location of an images were subjected to change in scales that are searched with the same features deployed in all potential scales, using a constant function of scale is well-known as scale space. The invariant scale implementation uses gauss function efficiently to scan the likely points based on scale and orientation[16].

As explained in the above diagram, the octave scale space[7,20] construct the primary images that are subjected to Gaussian approach and produce set of image space by depreciating the images that has different gauss.

$$f^{\theta}(x,y) = \sum_{j=1}^{M} K_j(\theta) f^{\theta j}(x,y) \qquad (1)$$

The equation (1) creates interpolation functions with high and low pass sub filters for an image. Hence the Scale space formulae is represented as

$$L(x,y,\sigma) = G(x,y,\sigma) * I(x,y) \qquad (2)$$

and G and I represents Gaussian and Interpolation function representing image filters.

$$D(x,y,\sigma) = (G(x,y,k\sigma) - G(x,y,\sigma)) * I(x,y) \qquad (3)$$

$$= (L(x,y,k\sigma) - L(x,y,\sigma)) \qquad (4)$$

The Gaussian image represented by

$$G = k*\sigma \qquad (5)$$

The 2 factor is applied to all images by down trialing and repeating the process result in different gauss which are executed by further comparing of pixel range of its 26 corresponding neighbors with the said region. The region covers both the current and adjacent scales[16, 20].

2. Key point localization

The brief model explaining the entrant location was made fit to determine the position and scale. Key points are chosen based on procedures of their stability.

In order to detect the local maxima and minima, each sample point is compared to its eight neighbors in the current image and nine neighbors in the scale above and below which is shown in Figure 2. The image is simply chosen if it is bigger compared with its neighbors of smaller size. This test occupies less constraints by the following first few checks using the eqn. 6
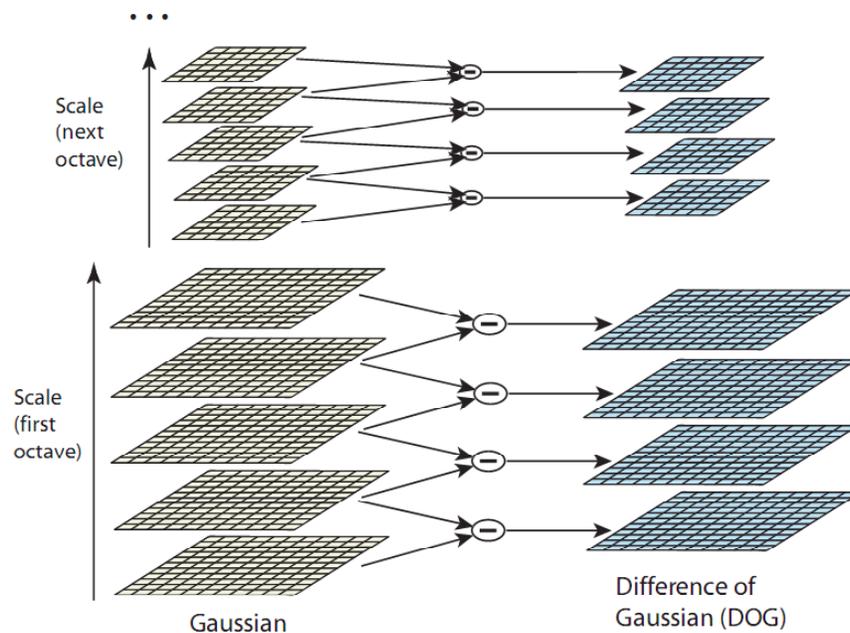
Figure 1. Operations within same octaves (samescale)[7].
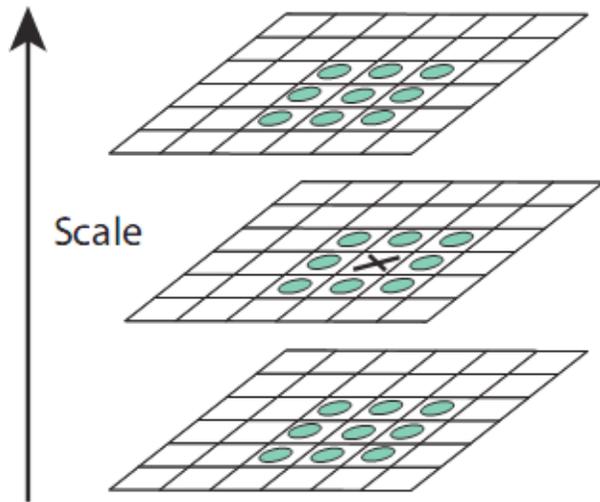
Figure 2. Operations between different octaves (different scale)[16].

$$m(x,y) = \sqrt[2]{(L(x+1,y)-[L(x+1,y)])^2 + (L(x,y+1)-[L(x,y-1)])^2} \quad (6)$$

a. Improving key point localization

To set the location range the key point and its corresponding neighbor pixel value is calculated results in complete data set in terms of location, scale and proportion of primary curvatures. The low contrast points are discarded that have low contrasts (sensitive to noise) which are poorly localized along an edge.

b. Eliminating edge responses

For stability, it is not sufficient to reject key points with small difference. The noise in the different gauss function has prominent focus on edges, even if the present position of edge is found insufficient and the weak defined peak of different gauss function makes prominentcurvature on the edges and few partial impacts in its perpendicular axis.

3. Orientation Assignment

The invariance of the image accessed using input point descriptor relates to its orientation based on image. The invariance achieved it so produce the results that are different as change in image direction (rotational). The downside of this approach will get rid of the images, which are outfit using invariance consistency. The input key points are also balanced with location gradient of the particular images. The operations on the image data is done with direction, degree and its position based on its attribute with invariance transformations.

4. Key Point Descriptor

The previous operations have assigned an image position, size, and direction to every key point. These parameters require resident image invariance of two dimensional coordinates that describes an image area followed by resident image area with its description. The area that is extremely distinctive yet is as invariant as possible to continue variations, such as transform in illumination or 3D viewpoint.

The resident image grades are measured using scaling features that are around the region of every point focused towards it. The illustrated figures show the gradient measures of all levels.

The image gradient and its orientation measures are created using key point descriptor[16]. It is done by focusing image sample points that are fixed to a region and its position (posterior end). The Gaussian difference of an image represented using covered loops and the data samples were taken with histogram measures deputed with a region and its sub region. The orientation of image magnitudes represented as arrow mark indicated with in the sub region. The sub region of samples 4×4 projected on the right side and continued with the sample range by the multiples of 2's starting from 2×2 till 16×16. The Figure 7 shows the histogram samples that are equal in length and magnitude. It shows the square matrix array of 2×2 histogram were achieved as our experiments below shows that the best results are achieved as 2 multiples with 8 bin orientation leads to 16×16. Hence the resultant set achieves the experiment result of 128 sets sample featuring and its vector for each key point.

Finally, the feature vector is modified to reduce the effects of illumination transforms. The procedure initialized by normalization the vectors by multiplying the pixel value with 2 bins. The resultant set overrules the difference of modification that affects vector normalization. The pixel difference was calculated by adding a constant
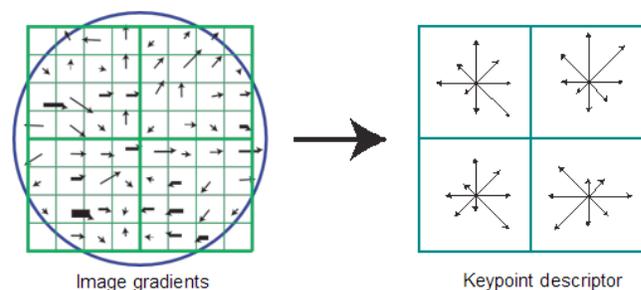
Figure 3. The Key point Descriptor[16].

value to every pixel and such component will distinguish from noise and will never affect the pixel value as stated by Lowe[21].

Therefore, the descriptor is invariant to affine changes in illumination. Even though the cost of extracting the image feature measure was done by cascade filter approach, by which only the initial set pixel value is deputed for the valuable operation that pass the initial test. It is obvious that the above mentioned operation will consume considerable time since the operation is repeated in several scales of different image frames.

3. The Implementation of Sift Based FKP Authentication Systems

The proposed FKP recognition system focus on SIFT feature descriptor detection algorithms and uses the standard FKP dataset[22] for the experiments.

3.1 About the Dataset Used

FKP database[22] used in this work was established as a standard database for FKP based recognition systems, by the Hong Kong Polytechnic University. The Biometric Research Centre (UGC/CRC) at The Hong Kong Polytechnic University has developed a real time FKP confine device, and has used it to make a large-scale FKP database.

An FKP image was composed with 165 members with the split of 125 and 40 male and females respectively out of which the age group is set as 20–30 for 75% of the total member size and rest under the age group of 30–50. The data set is collected from FKP database zip file available[23]. We collected samples in two separate sessions by collecting 6 images for each of the left index finger, the left middle finger, the right index finger, and the right middle finger from the subject.

The resultant 48 images (6×8) collected and accumulate the database with 7,920 images with 660 different fingers with different time interval taken at the average of 25 days. The maximum interval is set to 96 (in terms of days) and minimum interval is set to 14 (in terms of days) for the evaluation process.

3.2 Naming Convention

The original captured images as well as the ROI images were available for research. Each folder is named as "nnn_fingertype". "nnn" represents the uniqueness of the person. In each folder, the first 6 images (01~06) were captured in the first session and the latter 6 images (07~12) were captured in the second session. The file names in each folder of original captured images were named as nn_.jpg and the ROI images were named as nn_ROY.jpg where nn represents the serial number of the images (1–12) of one person.

3.3 Implementation Process

For implementing SIFT based FKP authentication system, we used VLFeat open source library for computer vision algorithms. We used Matlab version of vlfeat-0.9.16. It is a cross-platform open source collection of vision algorithms with a special focus on visual features and clustering. For better performance, binary versions of these libraries were used in both the design.

The following diagrams shows the basic steps involved in enrolling and authentication process in a typical FKP authentication system.

3.4 Metrics Considered for Evaluation

To evaluate the performance of the SIFT based FKP authentication system, we considered the following metrics:

3.4.1 Time Required for Feature Extraction

This is the time taken for enrolling and preparing the template database from the given set of FKP images of the users.

3.4.2 Time Required for feature descriptor Matching/Authentication

This is the time taken for matching/authenticating the input feature descriptors by matching it with overall template feature vectors of the dataset. This is the process of finding a feature template based on the highest matching score.

3.4.3 The Measures of Accuracy of the System

The biometric recognition application systems measures the utility component explained with two values[19] False Acceptance Rate and False Rejection Rate. The value of the FAR measure, which is the part of the amount of instances of different feature pairs of the traits found do match to the total number of equal attempts, and the value

of the number of instance of feature pairs not to match FRR criterion out of total attempt made. It is obvious that the system can be adjusted between values that depend on applications. The further evaluation is done with the threshold value achieved with FAR and FRR and the value makes one application better than other.

In biometrics systems, the threshold is estimated using a Receiver Operating Characteristic (ROC)[11,12] curve plotted in a graph for exemplify the achieved result of the classifier system with varying threshold value. The result projects the comparison of true vs. false positive rate, at various threshold settings. Accuracy can also be measured in terms of Area Under the ROC Curve (AUC). We considered ERR as the main quality metric for measuring the utility of the system because, often, most of the previous reference works used this metric.

4. Results and Discussion

The following three images show the feature points detected by SIFT algorithm. If we carefully notice these images, we can say that the SIFT was capable of detecting feature points uniformly throughout the image. Each detector descriptor points will have a magnitude and orientation. In the following figure, the magnitude is represented by green circle and the orientation is shown as a radius line from center. The center is marked with a blue + symbol.

The following image shows the matching patterns of SIFT descriptors. Each descriptor point in left is matched

Figure 5. The Authentication/matching Process.

Figure 6. The Images show features detected by SIFT.
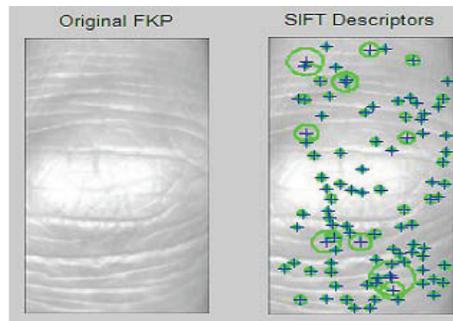
(a) 001_left middle/01ROI.jpg
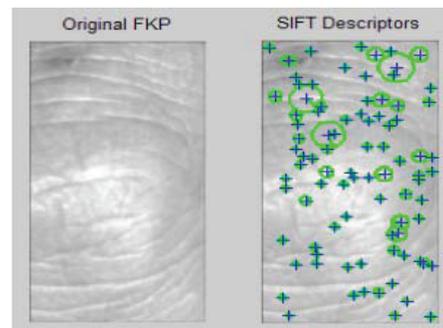
(b) 005_left middle/07ROI.jpg

Figure 4. The Enrolling Process.

with the matching point in right. the match is denoted by connecting the centers through a blueline.

The following figure shows the ROC curve of the SIFT based authentication system. SIFT provided EER of 0.65% and the accuracy measured in terms of AUC (area under curve) was 99.87%.

The following table shows the comparison of ERR.

In our implementation of SIFT, Feature vector of 128 values is computed from the local image region around the key-point as Key-point descriptor.

The following table shows the storage space consumed by the SIFT based descriptor feature data sets.

In fact, SIFT consumed much space than the original FKP image size.

4.1 Enrollment

In the following table, we present the Feature extraction performance of SIFT with respect to different number of images. This operation is usually done during enrolling the users in to the database.

4.2 Authentication/Matching

In the following table, we present the authentication/feature matching performance of SIFT feature descriptors with respect to different number of images and images/person.

If we use 8 images per person for enrollment, then for searching database of 165 to find a match of input image
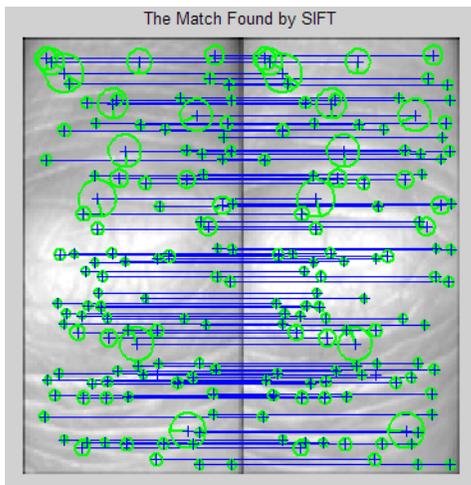
Figure 7. Match Found by SIFT.
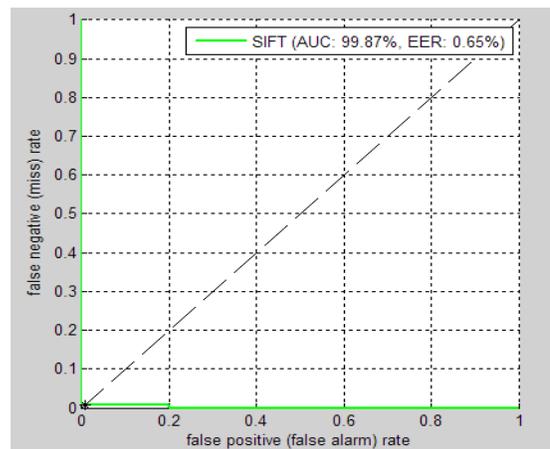
Figure 8. The ROC curve.

Table 1. The Comparison of ERR

Method	EER
OE-SIFT[18]	0.85
Non Enhanced SIFT[19]	2.69
Non Enhanced SURF[19]	1.90
Our Implementation of SIFT	0.65

Table 2. Comparison of the storage costs

No. Images	Database Storage Size on Disk (Mega Bytes)
165*6 (990)	10.9
165*12(1980)	22
165*24(3960)	43.8
165*48(7920)	87.5

Table 3. Comparison of the Processing Cost for Enrollment

No. Images	Time Taken For Feature Extraction (sec)
165*6(990)	45
165*12(1980)	92
165*24(3960)	183
165*48(7920)	364

Table 4. Comparison of the Processing Cost for Authentication/Matching

Image Template per Person	Total Training Images	Total Test Images	Time Taken For Matching (sec)
2	330	165	76.6
4	660	165	152.5
6	990	165	230.2
8	1320	165	307.7

it is taking around 1.8 second (307.7/165) for SIFT based FKP authentication system.

It means, for authenticating one person by matching his FKP features with a template of 165x8 size feature database, approximately 1.8 seconds needed. So obviously, this 1.8 second will grow rapidly if we increase the enrollment in the database. For example, if we need to enroll 1000 sets of FKP feature descriptors (1000×8) of persons, then it may take around 10 seconds to authenticate a person using that huge template set.

5. Conclusion

We have successfully implemented a FKP based authentication system using SIFT feature descriptors and evaluated its performance using a standard FKP database. The performance of SIFT and ERR equals proposed works[19, 24, 25]. But, our evaluations shows that the performance in term of storage cost and computational cost involved in SIFT based system needs improvement.

SIFT was a proven candidate algorithm for machine vision related applications in which , generally the detected feature vectors of one scene will be compared with some set of trained feature vectors to recognize different objects in that scene. But, for in real time authentication system, the differences between the training feature descriptors will be less. There will be lot of feature descriptors in a template database to match.

Even SIFT is efficient and much accurate feature detector/descriptor algorithms, but it consume much processing time as well as storage space. This will be a major obstacle in porting SIFT based FKP authentication systems to low cost dedicated hardware. Future works should address the ways to reduce the storage and computational costs in applying SIFT based FKP authentication systems.

We realized that the main cause of computation overhead is the representation of feature descriptors which consume much space even higher to that of original FKP image. There are techniques for reducing the size of the feature descriptors by using some abstract representation of the same. There are feature extraction techniques and dimensionality reduction techniques that can be used to reduce the size of the feature descriptors and hence reduce the storage and computational cost during matching or authentication phase. The achievable task in continuation of both the phases even develop a hybrid classification model using statistical and machine learning techniques that can dramatically reduce the computational costs involved in every phase especially validation phase that leads to more improved results in terms of EER. Future works may address these issues to develop much faster and accurate FKP based authentication system.

6. References

1. Zhang L, Zhang L, Zhang D. Finger-knuckle-print: a new biometric identifier. 2009 16th IEEE International Conference on Image Processing (ICIP). 2009 Nov 7–10; Cairo. 1981–84.
2. Zhang L, Zhang L, Zhang D. Finger-knuckle-print verification based on band-limited phase-only correlation [Lecture Notes]. Computer Analysis of Images and Patterns. 2009; 141–8.
3. Zhang L, Zhang L, Zhang D, Zhu HL. Online finger-knuckle-print verification for personal authentication. Pattern Recognition. 2010 Jul; 43(7):2560–71.
4. Zhang L, Zhang L, Zhang D. Monogeniccode: a novel fast feature coding algorithm with applications to finger-knuckle-print recognition. 2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB). 2010 Aug 22; Istanbul. 1–4.
5. Zhang L, Zhang L, Zhang D, Zhu H. Ensemble of local and global information for finger-knuckle-print recognition. Pattern Recognition. 2011; 44(9):1990–98.
6. Li J, Allinson NM. A comprehensive review of current local features for computer vision. Neurocomputing; 2008 Jun; 71(10–12):1771–87.

7. Mikolajczyk K, Schmid C. Scale and affine invariant interest point detectors. Int J Comput Vis Image Process. 2004; 60(1):63–86.

8. Available from: http://www.learningace.com/doc/1129401/a4a8e726324f2711b5daf203fa38cd1f/maji-presentation

9. Maji S. A Comparison of Feature Descriptors, Scientific Literature Digital Library, CiteSeerX. doi:10.1.1.141.4980. Available from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.141.4980

10. Merendáz, ACN, Thompson CAF, Assis JT. Local image descriptors invari ant to scale and rotation. Available from: http://www.sbmac.org.br/eventos/cnmac/xxx_cnmac/PDF/281.pdf

11. Kelly H. Zou's bibliography of ROC literature and articles. Available from: http://pel.caltech.edu/wiki/doku.php?id=fdr.

12. Available from: http: // en.cyclopaedia. net / wiki / ROC-Curve

13. Bay H, Ess A, Tuytelaars T, Van Gool L. Speeded-Up Robust Features (SURF). Comput Vis Image Underst. 2008; 110:346–359.

14. Matas J, Chum O, Urban M, Pajdla T. Robust wide baseline stereo from maximally stable extremal regions. Proceedings of British Machine Vision Conference; 2002. p. 384–96.

15. Zakir U, Zafar I, Edirisinghe EA. Road Sign Detection and Recognition by using Local Energy based Shape Histogram (LESH). Int J Image Process. 2010; 4(6):411–419.

16. Lowe DG. Distinctive image features from scale-invariant keypoints. Int J Comput Vis Image Process. 2004; 60(2):91–110.

17. Morales A, Travieso CM, Ferrer MA, Alonso JB. Improved finger-knuckle-print authentication based on orientation enhancement. Electron Lett. 2011; 47(6):380–81. doi:10.1049/el.2011.0156.

18. Choras M, Kozik R. Knuckle biometrics based on texture features. 2010 International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics (ETCHB). 2010; 1–5.

19. Badrinath GS, Nigam A, Gupta P. An efficient finger-knuckle-print based recognition system fusing SIFT and SURF matching scores. ICICS'11 Proceedings of the 13th International Conference on Information and Communications Security; 2011. p. 374–87.

20. Wahed M, El-tawel Gh.S, El-karim AG. Automatic image registration technique of remote sensing images. Int J Adv Comput Sci Appl. 2013; 4(2):177–87.

21. Lowe DG. Distinctive image features from scale-invariant keypoints. Int J Comput Vision. 2004; 60(2):91–110.

22. The Hong Kong Polytechnic University (PolyU) Finger-Knuckle-Print Database. Available from: http://www4.comp.polyu.edu.hk/~biometrics/FKP.htm

23. Available from: http://www4.comp.polyu.edu.hk/~biometrics/FKP.htm, FKP Database.zip

24. Blanco JL, Gonzalez J, Ferna´ndez-Madrigal JA. An Experimental Comparison of Image Feature Detectors and Descriptors applied to Grid Map Matching [Technical Report]; 2010 Apr 28.

25. Meraoumia A, Chitroub S, Bouridane A. On-line finger-knuckle-print identification using Gaussian mixture models & discrete cosine transform. International Conference on Electronics and Oil: From Theory to Applications-ICEO2013; 2013 Mar 5–6. Institutional Depot at the University Kasdi Merbah Ouargla UKMO-Algeria.

26. Norona C. Non-distributed object recognition potential on the android platform [Term Project Final Report]. COT5930 - Digital Image Processing Fall; 2010. Available from: http://static2.docstoccdn.com/docs/75108470/cnorona1_cot5930_projfinalreport.