ISSN: 0976-9102(ONLINE)
DOI: 10.21917/ijivp.2013.0083

FINGER KNUCKLE PRINT RECOGNITION WITH SIFT AND K-MEANS ALGORITHM

A. Muthukumar[1] and S. Kannan[2]
[1]*Department of Electronics and Communication Engineering, Kalasalingam University, India*
E-mail: muthuece.eng@gmail.com
[2]*Department of Electrical and Electronics Engineering, Kalasalingam University, India*
E-mail: kannaneeeps@gmail.com

Abstract
In general, the identification and verification are done by passwords, pin number, etc., which is easily cracked by others. Biometrics is a powerful and unique tool based on the anatomical and behavioral characteristics of the human beings in order to prove their authentication. This paper proposes a novel recognition methodology of biometrics named as Finger Knuckle print (FKP). Hence this paper has focused on the extraction of features of Finger knuckle print using Scale Invariant Feature Transform (SIFT), and the key points are derived from FKP are clustered using K-Means Algorithm. The centroid of K-Means is stored in the database which is compared with the query FKP K-Means centroid value to prove the recognition and authentication. The comparison is based on the XOR operation. Hence this paper provides a novel recognition method to provide authentication. Results are performed on the PolyU FKP database to check the proposed FKP recognition method.

Keywords:
Biometric, SIFT Algorithm, Feature Extraction, K-Means Algorithm

1. INTRODUCTION

Biometrics is defined as the measure of human body characteristics such as fingerprint, eye, retina, voice pattern, Iris and Hand measurement. It is a powerful and unique tool based on the anatomic and behavioral characteristics of the human beings. Most anatomical characteristics used for security application are fingerprint, Iris, face and palm print [4][5][6]. Apart from anatomical characteristics, behavioral characters like voice, signature, and gait moments are also used to recognize the user. Most biometric systems that are presently used in real time applications, typically uses a single biometric characteristic to authenticate a user. So authentication leads major part in the secured way of communication. Currently, passwords and smartcards are used as the authentication tool for verifying the authorized user. However, passwords are easily cracked by dictionary attacks, as well as the smart cards are stoles by anybody, and then we cannot check who the authorized user is. So the biometrics is an only remedy for the problems. This paper discusses about the new biometric identifier named as finger knuckle print shown in Fig.1. Many researchers are going on this new emerging biometric because, which is an also unique characteristic like fingerprint, Iris, etc. in order to prove the genuine user. The Finger Knuckle print recognition system contains data acquisition, ROI extraction, feature extraction, coding, and matching process [3] [12]. The features of FKP are extracted using the Gabor filtering with the cropped region of interest. The Gabor filter features are matched for recognize the user which was explained by Zhang, et.al [3] [12]. The average values of global and local orientation features of finger back surface or FKP was analyzed and matched with Fourier transform and Gabor filter respectively [2].

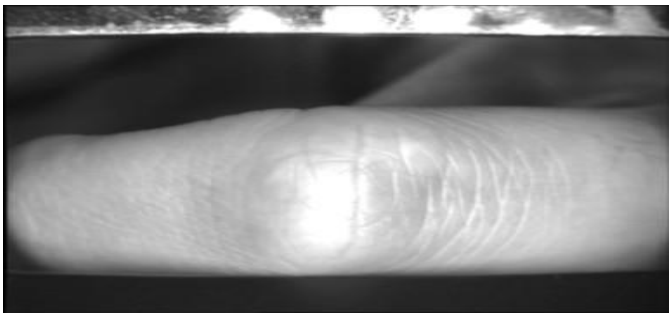

Fig.1. An Image of Finger Knuckle Print

Zhang, et.al proposed the score level fusion with FKP was performed with the phase congruency, local feature and local phase features [1]. David G.Lowe proposed a novel approach to extract the Invariant Features as key points used for object recognition using Hough transform [14]. The local information of FKP was accessed using Scale Invariant Feature Transform (SIFT) and Speed up Robust Features (SURF) [8] [14] [18]. The SIFT algorithm is used to get the key points using the scaling and invariant features which were matched to prove the user authentication [8] [14]. Ajay et.al, proposed a new method of triangulation, which is used to authenticate the hand vein images of finger knuckle surface of all fingers [9] [13].

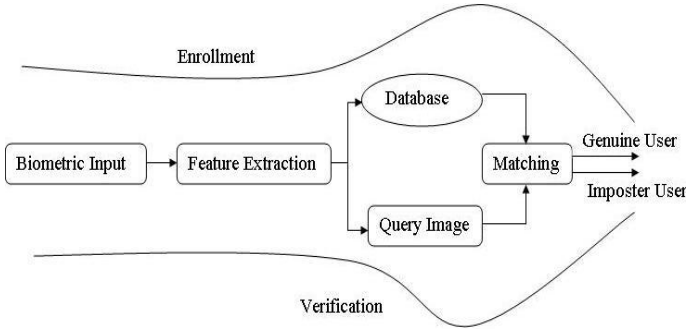

Fig.2. General Biometric Recognition Process

The fingerprint recognition was done with image segmentation and K-Means clustering and by Gongping Yang et.al [10]. Orthogonal linear discriminant analysis was also used to recognize the FKP along with Gabor filter with its key points [17]. The general recognition process was shown in Fig.2, which consists of two- phase, i.e., enrollment phase and verification phase. The first extracted features of any biometrics are stored in the database is known as enrollment phase and the same features are matched with the database using the query input is known as

verification phase. Above all the papers are explained that key points as key features are used to match the FKP image with its database for its recognition. This paper proposes an innovative of extracting the features of FKP using SIFT algorithm after the histogram process. Afterwards the key points extracted from the SIFT are clustered into groups with the K-Means algorithm, which is then converted into bits. The bit values are stored in the database, and these bits are used to match the authenticate user through the XOR operation process. The rest of this paper is arranged as follows. Section 2 describes about structure of the proposed work. Section 3 gives the details of the feature extraction of FKP. Section 4 discusses about the clustering process using K-Means Algorithm. Section 5 explains about the enrollment and verification phase. The experimental results and the analysis are discussed in section 6. Finally, section 7 provides the conclusion.

2. STRUCTURE OF PROPOSED WORK

Biometrics is a technique used to provide unique individual characteristics of a human being. The clustering is a method, which will give centroid value of the group which reduces the number of points of a system. So this paper proposes a new technique named as biometric clustering system to merge the above two process to provide authentication for individuals. This paper proposes a novel method to combine the SIFT algorithm with clustering to find the output values of knuckle print in the bit format. This paper also consists of two process i.e. enrollment and verification phase.

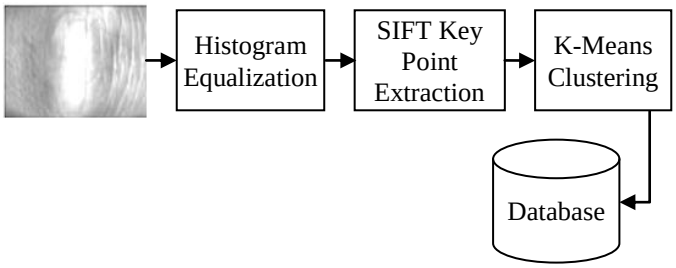

Fig.3. Finger Knuckle Print –Enrollment Phase

The enrollment process is shown in Fig.3. In this phase, the key points are extracted from the finger knuckle print using histogram and scale invariant feature transform. The key points are placed on the graph and clustered together to find the centroid value using K-Means algorithm. Then the centroid value is converted to binary values which is stored in the database.

The next phase of this paper is the verification phase which is shown in Fig.4. First step of the verification phase is same as enrollment phase to find the binary values with SIFT and K-means algorithm. The value found out from the query input is compared with values in the database. The comparison is done by XOR operation i.e. all the outputs of the compared values are zero, then the user is authenticated, otherwise the user is not a genuine user.

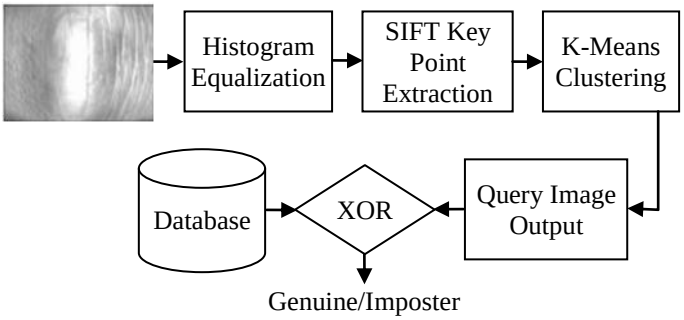

Fig.4. Finger Knuckle Print –Verification Phase

3. FEATURE EXTRACTION OF FINGER KNUCKLE PRINT

Finger Knuckle print is emerging tool of biometrics. The FKP is consisted of a number of curvatures. The paper proposes a feature extraction of FKP using SIFT algorithm [14]. The process of feature extraction is shown in Fig.3 and Fig.4 as first two steps i.e. Histogram equalization and SIFT key point extraction. Each valid key point is been characterized by two parameters: x-coordinate and y-coordinate. The first process of feature extraction is histogram equalization, which is used to enhance the input image of FKP in order to acquire the spatial characters correctly. Histogram equalization is used to enhance the visualization effect by increasing the pixel size which is shown in Fig.5(b).

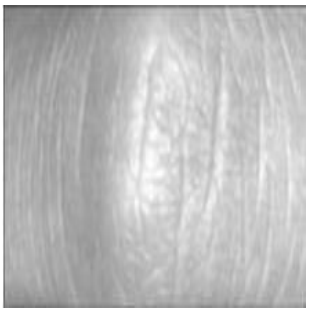

Fig.5(a). Input image of FKP

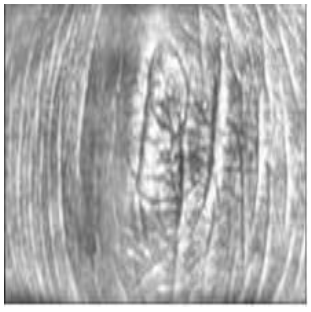

Fig.5(b). Histogram Equalization

The next step of feature extraction to extract the key points from finger knuckle print using the scale invariant feature transform (SIFT) [14]. The SIFT algorithm is mainly used for image matching purpose. Scale invariant feature transform is used for detection and extracting local features of an image. The first step of SIFT process is to find the difference of Gaussian function convoluted with the finger knuckle print

image to detect the key point locations which is invariant to scale change. The difference of Gaussian is calculated by Eq.(1) and Eq.(2).

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (1)$$

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

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \quad (2)$$

In the above equation $I(x, y)$, $G(x, y, \sigma)$, $L(x, y, \sigma)$, and $D(x, y, \sigma)$ are represents the image, Gaussian function, scale-space of image and Difference of Gaussian function respectively. The Gaussian function is calculated by using Eq.(3).

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \quad (3)$$

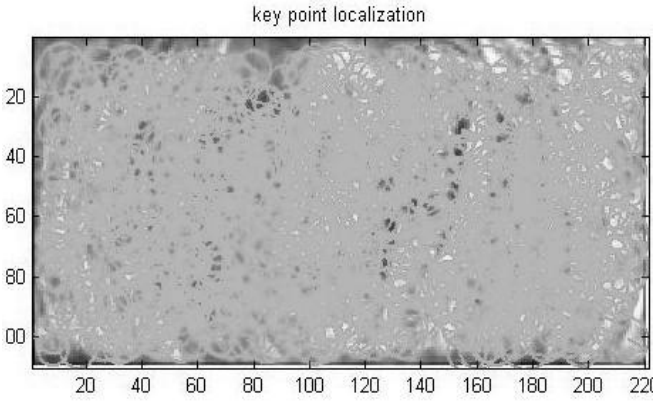

Fig.6(a). Key Point Localization of FKP

The next step is to detect the local maxima and minima of $D(x, y, \sigma)$ by comparing the each pixel value of FKP image with the neighbor pixel values. They are selected, if the pixel value is higher or lower related with the neighbor pixels.

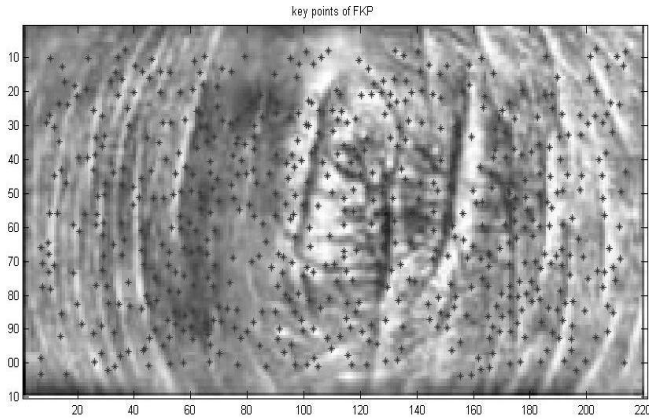

Fig.6(b). Key Points of FKP

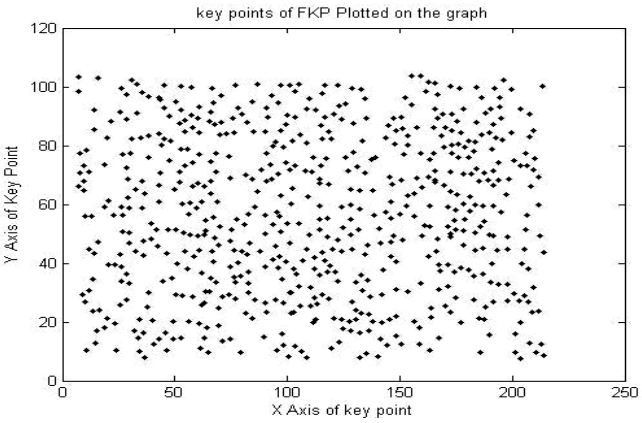

Fig.6(c). Key Point of FKP are plotted on the graph

These localized key points are shown in Fig.6(a). These selected values are named as key points. To eliminate the low contrast points along the edge of the image, Taylor's expansion method is used. After applying the Taylor expansion, stable key points are selected and located by eliminating the low intensity pixel key points. The orientations of key points are assigned for the selected key points. The key points taken from the finger knuckle print is shown in Fig.6(b).The key points selected are scale invariant points. The selected key points co-ordinates are plotted in a graph which is shown in Fig.6(c).

4. K-MEANS CLUSTERING

Clustering is the process of grouping a non-linear set of objects. This approach can assign the database of *n*-objects into *k*-number of clusters ($k < n$). The main concept of this K-Means approach is every object in the database must contain in any of the clusters or group, then every cluster must contain a minimum of one object. Then each cluster can be used to find a mean vector; according to this approach, it comes under the category of the centroid model.

In this paper, K-Means clustering is used to find the set of genuine key points, which is converted into binary bits and stored in the database in enrollment phase. The process of fingerprint K-Means clustering is shown in Fig.7 [11].

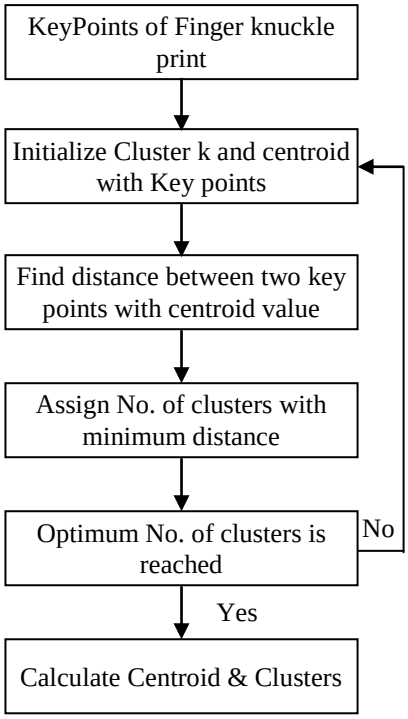

Fig.7. Finger knuckle print K-Means Clustering Process Flow

The key points are taken from the feature extraction process are clustered using this algorithm. Consider the key points are given as the input data vectors' $M = (m_1, \ldots, m_n)$. K-Means algorithm starts by initializing the first co- ordinates values as the centroid and defined the numbers of clusters to be split. According to our problem, this paper proposes the eight number of clusters to be defined, and to these objects are assigned to an each cluster initially. Then according to the initial centroid value, calculate distance between centroid and minutiae points using Euclidean distance Eq.(4). The minimum distance is retained in the updated distance matrix.

$$\| c_i - m_k \|^2 = \sum_{j=1}^{r} [c_i(j) - m_k(j)]^2 + \sum_{j=r+1}^{p} [c_i(j) - m_k(j)]^2 \quad (4)$$

The key points were grouped into new clusters until an optimum cluster reached. The optimum cluster value is reached, there after there are no possible movements for the minutiae points to move on the next cluster. At optimum level, centroid value is also calculated. The Centroid and key point binary value is calculated from the key points using this algorithm.

5. ENROLLMENT AND VERIFICATION PHASE

The paper consists of two phases named as enrollment phase and verification phase. The enrollment phase is first process of this Finger knuckle print recognition system. Here the input images used for this paper are downloaded from Hong Kong Polytechnic University. The steps of enrollment phase are as follows,

- The first step is to the enhance input image of finger knuckle print by histogram equalization method.
- The next step is to extract the key points from the enhanced finger knuckle print using SIFT algorithm.
- After extracting the key points are mapped on the map, and their points are clustered using K-Means algorithm.
- The centroid values calculated from k-means clustering are converted into128 bit binary values, which are stored in the database.

The next phase is verification phase. The steps of this phase are as follows,

- The first step is to enhance the query image of finger knuckle print by histogram equalization method.
- The next step is to extract the key points from the enhanced query finger knuckle print using SIFT algorithm.
- After extracting the key points are mapped on the map, and their points are clustered using K-Means algorithm.
- The centroid values calculated from k-means clustering are converted into 128 bits of binary values, which are compared with the stored 128 bits of binary values of finger knuckle print with XOR operation.
- Here, if the both values are same, the result is zero, else values are different, and the result is one. Finally, the result is zero means the user is genuine otherwise the user is imposter one.

6. EXPERIMENTAL RESULTS AND ANALYSIS

Experiments in this paper are conducted using the finger knuckle print database from FKPROI of Hong Kong Polytechnic University [7]. This database contains Finger Knuckle Print images with its region of interest alone by cropping the outer surface image. This database consists of four sub databases; they are left index FKP, left middle FKP, right index FKP, and right middle FKP. Each sub database consists of 165 fingers of 12 images each. Totally, database consists of 660 folders of 7920 FKP images. The finger knuckle print image is enhanced with histogram equalization, which is shown in Fig.5(b) and Fig.8.

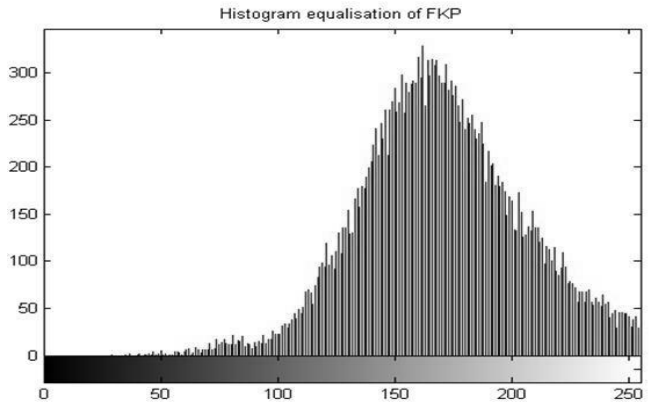

Fig.8. Histogram equalization of FKP

The output of finger knuckle print key point localization and key point's extractions are shown in Fig.6(a) and Fig.6(b). The key point values of finger knuckle print are grouped into eight clusters, and its centroid value is found, which is converted into 128 binary bits, which are used to store and compare the values

in enrollment and verification phase. The centroid value of k-Mean clustering biometric finger print key is shown in the Fig.9.

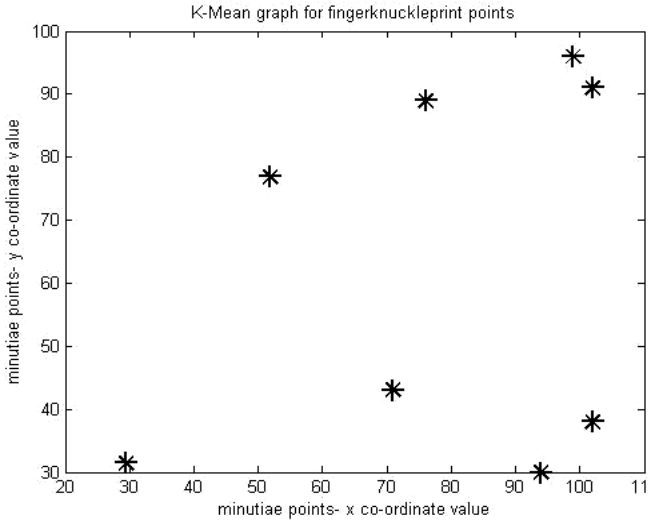

Fig.9. K-Mean Clustering graph for finger Knuckle print points

```
K =
Columns 1 through 14
  0   0   1   1   0   1   0   0   0   1   0   0   1   1
Columns 15 through 28
  0   1   0   0   0   1   1   1   0   1   0   0   0   1
Columns 29 through 42
  1   1   1   1   0   1   0   0   0   1   1   1   0   0
Columns 43 through 56
  1   0   1   0   1   1   0   1   0   0   1   1   0   0
Columns 57 through 70
  0   1   0   1   1   0   0   1   0   1   0   1   1   1
Columns 71 through 84
  1   0   0   0   0   1   1   1   1   0   0   1   1   0
Columns 85 through 98
  0   0   1   1   0   1   1   0   0   0   0   0   0   1
Columns 99 through 112
  1   0   0   1   1   0   0   0   1   0   0   1   1   0
Columns 113 through 126
  0   1   1   0   0   1   1   0   0   1   0   1   1   0
Columns 127 through 128
  1   1
```

Fig.10. Generation of 128 binary bits of FKP

The centroid value is converted into binary value of 128 bits, which is shown in Fig.10. For this paper, simulation is performed by 10 images of each database subset. For example, an enrollment output was taken from an image of finger knuckle print is shown in Fig.10, which is stored in the database. In verification process is above same process is repeated and finally, the 128 bits stored is compared with 128 bits of query image with XOR operation. The result for genuine user is shown in Fig.11.

```
Columns 1 through 14
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 15 through 28
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 29 through 42
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 43 through 56
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 57 through 70
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 71 through 84
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 85 through 98
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 99 through 112
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 113 through 126
  0   0   0   0   0   0   0   0   0   0   0   0   0   0
Columns 127 through 128
  0   0
```

Fig.11. Comparison result using XOR operation

Table.1. Parameters used for enrollment and verification phase

Parameter	Size
No. of Key Points	430-545 points
K-Means Clustering	8 clusters
Processing format	Hex Decimal, Binary
Finger Knuckle Print key Point value	128 bits
XOR comparison value	128 bits

Table.1. consists of all parameters which are used in this paper to perform the all steps. In order to define the accuracy of the biometric systems, many parameters are available, and in this paper; Genuine Acceptance rate (*GAR*) and False Rejection Rate (*FRR*) are considered. The *GAR* and *FRR* are calculated by Eq.(5) and Eq.(6),

$$GAR = \frac{No.\ of\ \ Genuine\ attempts\ accepted}{Total\ \ No.\ of\ \ genuine\ attempts} \quad (5)$$

$$FRR = \frac{No.\ of\ \ Genuine\ attempts\ rejected}{Total\ \ No.\ of\ \ Genuine\ attempts} \quad (6)$$

Table.2. Comparison for Proposed approach

Algorithm	GAR (%)	FRR
SIFT[8]	98	0.02
Comp Code[12]	96.5	0.035
ImComp Code & Mag Code[3]	97	0.03
LGIC[2]	99.14	0.0096
SIFT with K-Means Algorithm(Proposed)	99.4	0.006

The number of key points is high; the Genuine Acceptance Rate (*GAR*) is high but False Rejection Rate (*FRR*) is low. If this is not happened, FRR is high, and then system will not be valid one. According to this proposed approach, the *GAR* is increased with more key points and with the maximum cluster size.

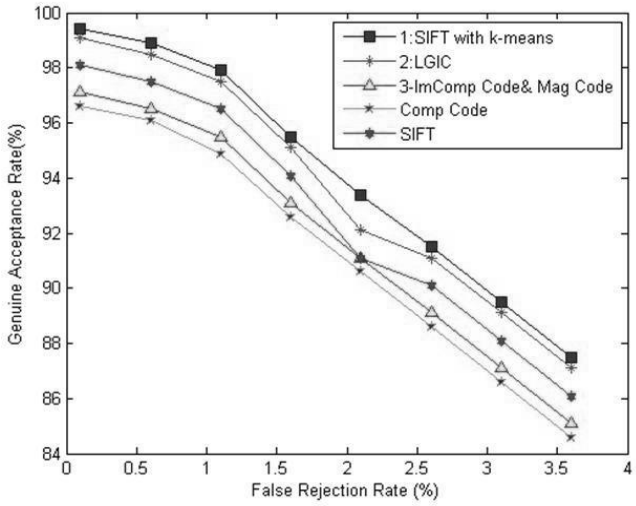

Fig.12. ROC curves of Proposed System compared with existing system

The comparison of proposed approach with the existing approach was tabulated in Table.2 and also shown in the ROC graph on Fig.12. The overall performance of this proposed approach was 99.4%.

7. CONCLUSION

This paper presented a new method of recognition system based on the finger knuckle print bit generation using K-Means algorithm. According to this work, the authentication is done by generating 128 bits value. For efficient matching, bit matching scheme proposed in this paper. To analysis their performance of this system, FKP database of 7920 ROI images are utilized. This type of system matches the data very effectively. In the future, we will extend this work to multibiometrics bit generation with the fusion values.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the management of Kalasalingam University, Krishnankoil, Tamil Nadu, India, for the facilities provided to carry out this research work.

REFERENCES

[1] Lin Zhang, Lei Zhang, David Zhang and Zhenhua Guo, "Phase congruency induced local features for finger-knuckle-print recognition", *Pattern Recognition*, Vol. 45, No. 7, pp. 2522–2531, 2012.

[2] Lin Zhang, Lei Zhang, David Zhang and Hailong Zhu, "Ensemble of local and global information for finger–knuckle-print recognition", *Pattern Recognition*, Vol. 44, No. 9, pp. 1990–1998, 2011.

[3] Lin Zhang, Lei Zhang, David Zhang and Hailong Zhu, "Online finger-knuckle-print verification for personal authentication", *Pattern Recognition*, Vol. 43, No. 7, pp. 2560–2571, 2010.

[4] Anil K. Jain and Sharath Pankanti, "Fingerprint-Based Fuzzy Vault: Implementation and Performance", *IEEE Transactions on Information Forensics and Security*, Vol. 2, No. 4, pp. 744-747, 2007.

[5] L. Hong, A.K. Jain and R. Bolle, "On-line fingerprint verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 19, No. 4, pp. 302–314, 1997.

[6] Kumar and A. Passi, "Comparison and combination of iris matchers for reliable personal authentication", *Pattern Recognition*, Vol. 23, No. 3, pp.1016–1026, 2010.

[7] Poly U FKP, Database: http://www.comp.polyu.edu.hk/~biometrics/FKP.htm.

[8] G.S Badrinath, Aditya Nigam and Phalguni Gupta, "An Efficient Finger-knuckle-print based Recognition System Fusing SIFT and SURF Matching Scores" , *Proceedings of 13th International Conference on Information and Communications Security*, pp. 374-387, 2011

[9] Ajay Kumar and Yingbo Zhou, "Personal Identification using Finger Knuckle Orientation Features", *Electronics Letters* , Vol. 45, No. 20, pp. 1023-1025, 2009.

[10] Gong ping Yang, Guang-Tong Zhou, Yilong Yin and Xiukun Yang, "K-Means based Fingerprint Segmentation with Sensor Interoperability", *EURASIP Journal on Advances in Signal Processing*, Vol. 2010, Article ID: 729378, pp. 12, 2010.

[11] Manhua Liu, Xudong Jiang and Alex Chichung Kot, "Efficient fingerprint search based on database clustering", *Pattern Recognition*, Vol. 40, No. 6, pp.1793–1803, 2007.

[12] Lin Zhang, Lei Zhang and David Zhang, "Finger-knuckle-print: A new biometric identifier", *Proceedings of the 16th IEEE International Conference on Image Processing*, pp. 1961–1964, 2009.

[13] Ajay Kumar and K. Venkata Prathyusha, "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape", *IEEE Transactions on Image Processing*, Vol. 18, No. 9, pp. 2127-2136, 2009.

[14] David G. Lowe, "Distinctive image features from scale-invariant keypoints", *International Journal of Computer Vision*, Vol. 60, No. 2, pp. 91–110, 2004.

[15] Ajay Kumar and David Zhang, "Improving Biometric Authentication Performance from the User Quality", *IEEE Transactions on Instrumentation and Measurement*, Vol. 59, No. 3, pp. 730-735, 2010.

[16] Miguel A. Ferrer, Carlos M. Travieso and Jesus B. Alonso, "Using Hand Knuckle Texture for Biometric Identifications", *IEEE Aerospace and Electronic Systems Magazine*, Vol. 21, No. 6, pp. 23-27, 2006.

[17] Yang Wankou, Sun Changyin and Sun Zhongxi, "Finger-Knuckle-Print Recognition Using Gabor Feature and OLDA", *Proceedings of the 30th Chinese Control Conference*, pp. 2975-2978, 2011.

[18] Zhu Le-qing, "Finger knuckle print recognition based on SURF algorithm", *Eighth International Conference on Fuzzy Systems and Knowledge Discovery*, Vol. 3, pp. 1879-1883, 2011.