Biometrics using Knuckle Print

Rakesh Bendre, Shraddha Das, Akshay Kulapurath
Dept.- Computer Engineering.
K.C. College of Engineering & Management studies & Research.
Thane, Maharashtra.

***Abstract*—Identification and Verification methods used in today's world are passwords which can be easily cracked and smartcards which can be stolen. Biometrics is an useful tool in recognizing an individual based on the characteristics and behaviour. In this paper a new biometrics methodology Finger Knuckle Print has been used. In this paper the key points from the Finger Knuckle Print are extracted using Scale Invariant Feature Transformation and clustered using K-means algorithm. The centroid of K-means is stored in the database which is then compared with the query using X-OR operation.**

***Keywords*—Biometrics, FKP, SIFT, Feature extraction, K-Means.**

I. INTRODUCTION

Biometrics is a useful and unique tool based on anatomic and behavioral characteristics of human beings like eye, retina,fingerprint,hand measurement and iris.Anatomical characteristics used for security are mainly fingerprint,iris,face and behavioral characters are voice,signature etc.Presently used systems like passwords are easily cracked by dictionary attacks and smartcards are stolen thus,this breaches the security and we are unable to findout the authorised user [3][6]. So the solution to this problem is biometrics which is unique for every person.In this paper a new biometric identifier named Finger Knuckle Print is shown.

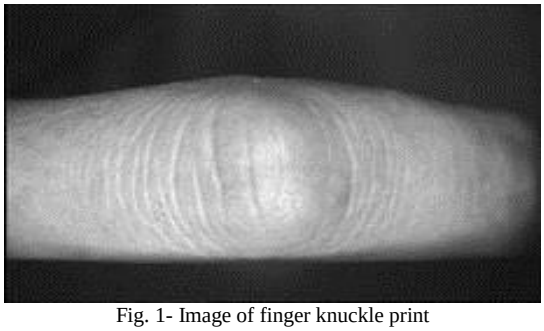


Fig. 1- Image of finger knuckle print

The Finger Knuckle Print recognition system consists of data acquisition, ROI extraction, extraction of feature, coding and matching [11].

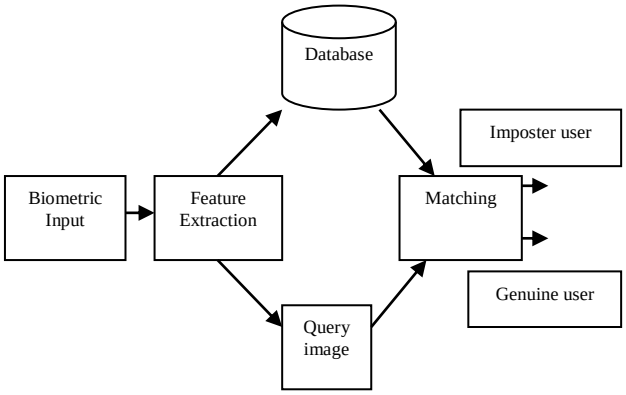


Fig. 2- General Biometric Recognition Process.

II. STRUCTURE OF PROPOSED WORK

This paper uses the SIFT and K-Means algorithm. Firstly a Finger knuckle print is taken as a biometric input. Then histogram equalization is applied to the FKP and Scale invariant feature transformation is used to extract the key points which is then clustered using K-Means algorithm [8] [3]. The centroid is calculated which is then converted into bits and stored in the database. Then the bit values from query image are matched with the bit values in database using XOR operation. The whole process is divided into 2 parts, Enrollment and Verification. Enrollment consists of the generation of bits from the biometric input and verification consists of the generation of bits from query image and matching [8].

III. FEATURE EXTRACTION OF FINGER KNUCKLE PRINT

In this paper to extract the features of FKP Histogram equalization and SIFT is used. Histogram equalization is used to enhance the visualization effect of image by increasing the pixel size.

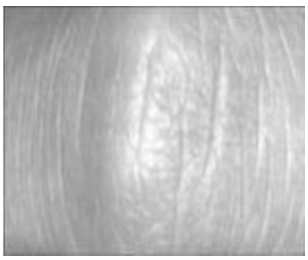


Fig. 3(a) - Input image of FKP

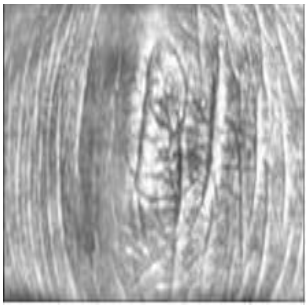


Fig. 3(b) - Histogram equalization

Scale Invariant Feature Transformation (SIFT) is used to extract the key points. SIFT is used for detection and extraction of local features of image [3].

IV. EQUATIONS

To detect the point locations in knuckle following equations have been used,

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

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

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

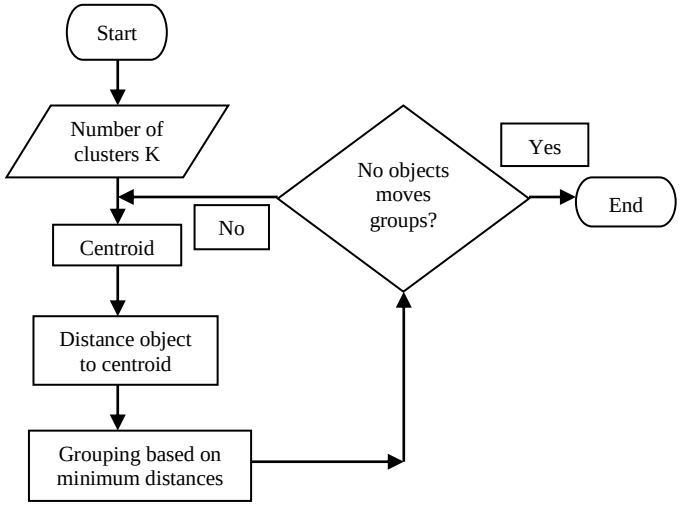
$$G(x,y,\sigma) = \frac{1}{2\pi\sigma^2} e^{-(x^2+y^2)/2\sigma^2} \quad (3)$$

Hence to represent image $L(x,y,\sigma)$,$D(x,y,\sigma)$, $I(x,y)$ & $G(x,y,\sigma)$ equations are used from (1)&(2) whereas the Gaussian function can be calculated by (3)[3].

V. ALGORITHM

The algorithm used is the K-Means Algorithm. The K-means is a clustering algorithm to classify or to group the different objects based on attributes or features into K number of groups[12].

The K-means algorithm is given in this way: Firstly, specify k, the number of cluster to be generated. Then choose the k points at random as the cluster centers. Assign each instances to its closet cluster. Then calculate the centroid for each cluster, and use it as a new cluster center. Reassign all instances to the closet cluster center. When no elements is moving from one cluster to another when the same process is done, the final clusters are obtained [8].



VI. TABLE

The methodology that is used from other papers is been explained in the below table.

Name of the paper	Methodology used
Mutimodal Biometrics Recognation Using Sift and K-means Algorithm	Extraction of features from FKP & are clustered using K-means algorithm.
Human Identification Using Finger and Iris Images	Finger knuckle print is used as biometrics.
Finger-knuckle-print: A new biometric identifier.	SIFT algorithm and histogram analysis is used.
Biometrics: Access control & Authorization on Finger-Knuckle Print Identification	Authorization and access control of user identity is maintained.
BI-Modal Palm Print and Knuckle Print Recognition .	Finger knuckle print is used as biometrics.

This is about the various methods or techniques used from different papers which is used in this paper.

VII. LITERATURE SURVEY

In this paper experiments are conducted using the finger knuckle print database Polytechnic University. The cropped image of Finger Knuckle Print is stored in the database. Their are four sub databases named left index FKP, left middle FKP, Right index FKP and Right middle FKP.12 images of 165 fingers each is stored in sub database. There are 660 folders of 7920 FKP images. Histogram equalization is used to enhance the FKP image [2][7].

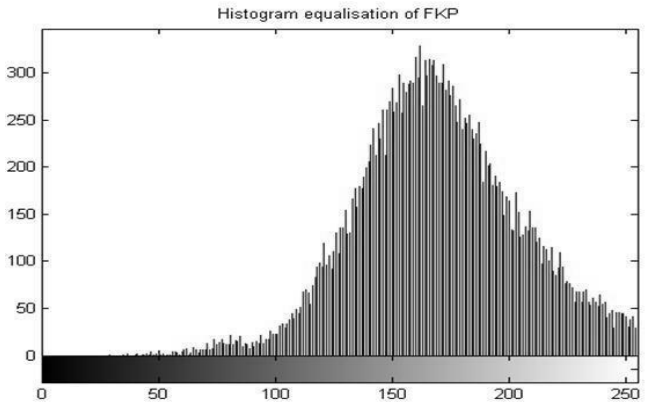


Fig. 4 - Histogram equalization of FKP.

The fig. 3 (a) and fig. 3 (b) shows the output of key point localization and key point's extraction. The centroid value is found by grouping the key points into 8 clusters. The centroid is converted into 128 binary bits, which are used to store and compare the values in enrollment and verification phase. Fig. 4 shows the K-means clustering biometric finger print key [8][9].

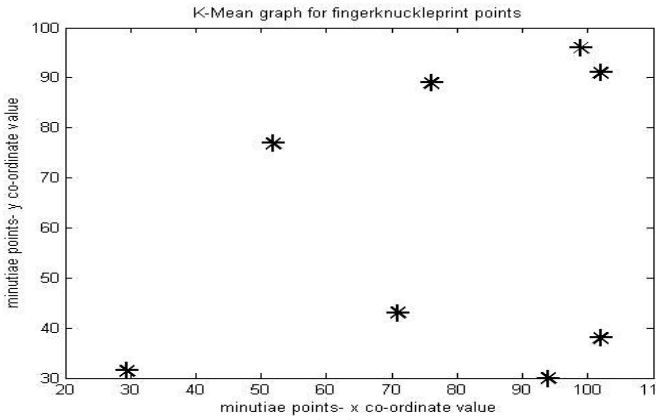


Fig. 5- K-mean clustering for finger knuckle print joints.

```
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. 6(1)- Generation of 128 binary bits of FKP.

The value of centroid is converted into 128 binary bits. Simulation is performed by 10 images of each database subset. For example, the image of finger knuckle print is used to take an enrollment output shown in fig.5, which is stored in database [4]. The same process is repeated for the verification process and then matching is performed where 128 bits stored is compared with 128 bits of query image using XOR operation.Fig.6.shows the result for genuine user.

```
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. 6(2) - Result of XOR operation

.

Table 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

VIII. CONCLUSION

The Paper used the method recognition system based on the Finger knuckle print bit generation using K-Means algorithm. According to this work, the authentication is done by generating bits value. By applying few methods, results are obtained. Such system can be used in security systems

IX. ACKNOWLEDGMENT

Our heartly thanks to Principle sir, Mrs. Amarja (H.O.D, Computer Engg, K.C College of Engg.) , Mrs. Sonal Balpande & Mr. Hari Rajai for providing support to us for this paper and providing with proper feedback.

X. REFERENCE

[1] A hierarchical classification method for figure knuckle print recognition.
[2] BI- Modal palm print and knuckle print recognition.
[3] An efficient figure knuckle print based recognition system using SIFT and SURF matching scores.
[4] Finger knuckle print recognition based on local and global feature sets.
[5] Finger knuckle surface biometrics.
[6] Secure biometrics finger knuckle print.
[7] Quality assessment of knuckle print biometrics images.
[8] Multimodal biometrics recognition using sift and k-means algorithm.
[9] Biometrics: Access control & Authorization on Finger knuckle print identification.
[10] Shape based hand recognition.
[11] Peg-free hand geometry verification system.
[12] Human identification using finger and its iris images.
[13] Personal identification on using finger knuckle print based on local binary pattern.
[14] Contactless finger knuckle identification using smartphones.
[15] Finger knuckle print: A new biometrics identifier.