Generation of private 512-bit Security Key using Human Palmprint

Rohit Khokher[1], Ram Chandra Singh[2], Saiyam Diwan[3], Rahul Kumar[4]
[1,3,4]*Vidya College of Engineering, Meerut- 250005 (UP), India*
[1,3,4]*Department of Computer Science & Engineering, Vidya College of Engineering, Meerut- 250005 (UP), India*
[2]*Department of Computer Science & Engineering, Sharda University, G. Noida (UP), India*
Email : khokherrohit@gmail.com

***Abstract* - This paper proposes an algorithm for authentication of an individual using palm prints. Biometrics is physiological characteristics of human beings, unique for every individual that are usually time invariant & easy to acquire. Palmprint is one of the physiological biometrics due to its stable & unique characteristics. The physical dimensions of a human palm contains information that is capable of authenticating the identity of an individual. In this study algorithm is proposed to compute 512-bit security key using figure length of fingers of an individual. The performance of a key is assessed on 1280 keys stored in a database. Simulation results shows false accept rate (FAR) is 25%,false reject rate (FRR) as18.75%, genuine acceptance rate (GAR) 81.25%, half total error rate (HTER) 21.87% and accuracy 78.12%.**

Keywords- Biometrics, palm prints, image pre-processing, median filter, masking, orientation, edge detection, security key, matching.

I. INTRODUCTION

Automatic personal authentication is a significant component of security systems with many technological challenges. The traditional methods of identification which includes passwords or tokens are not much reliable, but identifying individuals based on his or her unique physical characteristics is much reliable technique. A number of researchers have started the interaction between biometrics and cryptography, two potentially complimentary security technologies. Biometrics [1-6] guarantees the identification of individuals based on measuring the personal unique features with a high degree of assurance while cryptography assures a high degree of trust in the transactions of information through the communication networks. Any human physiological and behavioral characteristic can be used as a biometric characteristic as long as it satisfies the requirements of universality, distinctiveness, permanence, collectability, performance, acceptability and circumvention [7]. Few biometric traits that are used to authenticate or identify individuals are Fingerprints, Iris, ECG, Retina, Gait, Footprint, Speech, Face, DNA, etc. Palmprint is also one of the physiological characteristics that can be used to distinguish between individuals. Palmprint can be characterized by the geometry of few principal lines (heart, head and life lines) and the presence of several wrinkles and ridges in the palm.

Several studies on personal-recognition system have been developed using palm as a single feature. Zhang, et al.[8] developed an online identification system by implementing Gabor filter to obtain palm print feature information. Duta, et al.[9] separated set of feature points along the main line of palms and calculates a score that fits between a set of related features of the two hands. Li, et al. [10] used Fourier transformation to obtain the features of the palm. Wu, et al. [11] formed a line vector features (LVF) using the gradient magnitude and orientation of points on the main line of the palm to extract the palm print features. Jain and Duta [12] employed deformable hand shape matching to verify user.

The complete process of the study is shown in the figure 1.1. The sensor is used to obtain the palmprint images. In this study database is taken from www.coep.org.in [13] College of Engineering, Pune. During preprocessing of an image several operations like masking, filtering and normalization was applied on images. In this study an algorithm has been developed that find length of fingers as a feature of palm and use these lengths as an input of an algorithm to compute 512-bit security key. This key is stored as a template in database and matching is done to find that whether a user is legitimate user or an imposter user. In section 2 of the paper enhancement processes have been defined on an input image. The section 3 shows the working of developed algorithm to extract feature & computation of 512-bit security key. The section 4 shows the results. At last section 5 concludes the paper followed by the references.

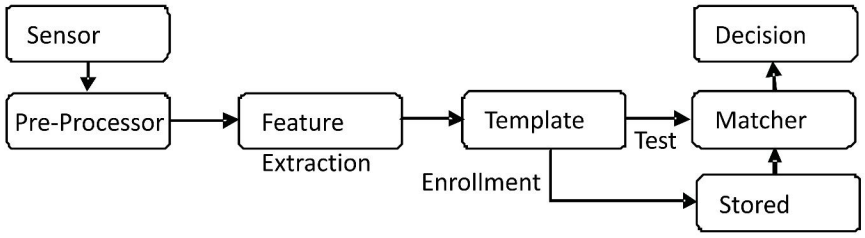

Figure 1.1 Process of Biometric Authentication

II. ENHANCEMENT OF IMAGE

The database obtained from www.coep.org.in, College of Engineering, Pune[13] contains the palm images of 160 individuals. For each individual palm images were captured 8 times i.e. 8 prints of every individual. All the prints are of right hand palm. The images obtained from the database are raw images that need to be pre-processed before gaining any information from them. The images contains noises like dust particles, light reflections or irregular backgrounds due to which accurate feature extraction cannot be done. Therefore the enhancement technique was applied to enhance palmprint impressions for feature extraction.Preprocessing of images involves processes orientation, normalization, masking, filtering and edge detection.

2.1. Orientation

Orientation is required to make the palm print images aligned in the same fashion so that a generalized algorithm can be applied over the whole database altogether. Orientation is done to rotate palm print images that aligned at some angle. Figure 2.1 shows the oriented image O(x,y,z) obtained from the original input image I(x,y,z). In MATLAB orientation process can be done by using "imrotate()" inbuilt function.

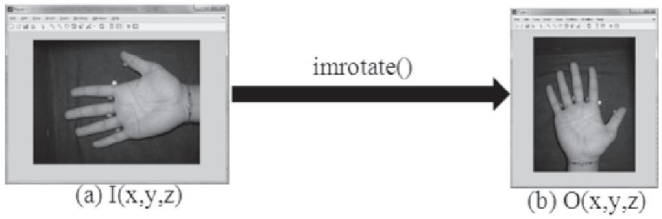

Figure 2.1 Orientation of image

2.2. Masking

Masking is a process to extract an object from an image, the object is masked using a masking matrix that assigns a value 1(white) to the object to be masked and 0(black) to the rest of the image. Thus a 2-bit black & white image is obtained that clearly shows the masked object. In this study the red layer of the oriented image was masked i.e. Or(x,y) (extracted as O(x,y,1)) using a pre-defined function "makeMask()"

in MATLAB. The makeMask() function takes as its input the background image, the original input image and the tolerance value and gives the 2-bit masked image as M(x,y). Figure 2.2 shows the masked image M(x,y).

Figure 2. 2Masking of Image

2.3. Filtering

Filtering is an image enhancement technique that is used to remove unwanted information from the image that had occurred as noise which may be due to dust particles, light reflections or irregular backgrounds. Many noise removal filters are available that removes the noise based on frequency or statistical information of the image. In this study several filters were used to remove the noise from the masked image that is shown in figure 2.3. The resultant image given by median filter is better in comparison to other filter because it is best known for removing "salt and pepper" type of noise which exists in the most of the masked image M(x,y) obtained after masking. The default mask matrix in median filter is of 3x3 in size but in this study it has been increased to 17x17 sized matrix. Figure 2.3 gives the masking matrix.

Figure 2.3. Comparative results of different filters.

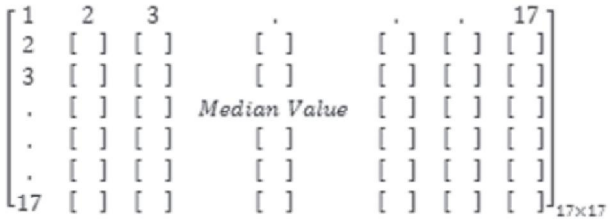

Figure 2.4. Median Filter Matrix.

This filter is also known as order-statistical filter as it takes the middle value from the set of sorted values that comes in a mask at a time. Thus irregular or sudden changes in the pixel values which represents noise is cleared. In this study an inbuilt function "medfilt2()" of MATLAB is used to filter the Masked image M(x,y). This function takes as input the masked image M(x,y) and the size of the matrix (17×17) and gives as output the filtered image F(x,y). Figure 2.5 shows the filtered image.

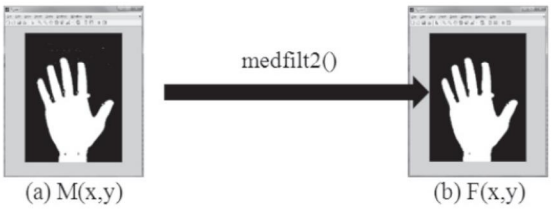

Figure 2.5. Filtering using median filter.

2.4. Normalization

The process of normalization is done over a filtered image F(x,y) to make it fit to a standard which may be in respect of its dimensions or frequency. Normalization is done so that operations can be applied over it irrespective of any environmental disturbances like empty spaces, irrelevant color layers,etc. In this process the filtered image F(x,y) is normalized by removing empty regions from the left, right, top and the bottom of the image and the normalized image N(x,y) is obtained. In this study normalization helps to estimate the correct length of the palm and the fingers irrespective of the area of the palm visible which differs from one image to the other. Figure 2.6 shows the normalized image N(x,y) obtained from the filtered image F(x,y).

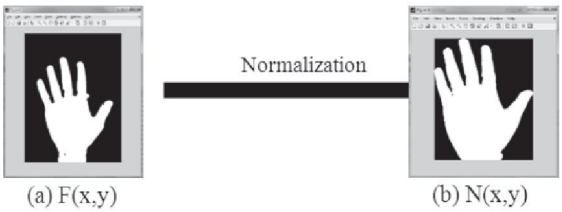

Figure 2.6. Normalization

2.5. Edge Detection

The final and the most important technique used for image enhancement is the edge detection. Edge detection is the name for a set of mathematical methods which aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed edges[14]. In this study the edges of the normalized image N(x,y) was obtained using an inbuilt function "edge()" in MATLAB. The function takes as input the normalized image N(x,y) and gives the output image E(x,y) that has a single pixel thick edge of the input palm. Figure 2.7 shows the detected edge of the palm.

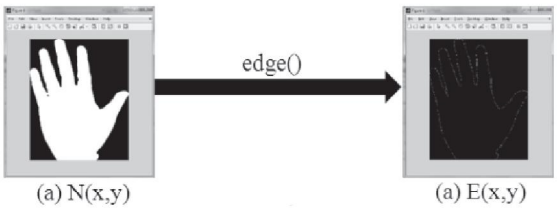

Fig. 2.7. Edge Detection

III. ALGORITHM TO EXTRACT FEATURE

The final image obtained after image enhancement techniques is E(x,y) that contains the fine edge of the palm print which was given as an input image to feature extraction algorithm. In this study an algorithm has been developed that is used to compute the length of four fingers l1, l2, l3 & l4 and to compute 512-bit security key using length of fingers.

The following steps are involved in a 512-bit security key generation algorithm

1. Start
2. Lfind() function is made to calculate length of fingers
3. Skfind() function is made to find the security key from length of 4 fingers
4. Stop

The function Lfind() includes following steps :

Step1: Obtain the set of points a[1...n] from the image edged E(x,y) such that their neighborhood pixels in the y-coordinate are of the same frequency.

Step 2: Cluster the set points in a[1...n] such that they are away from each other by a threshold value i.e. 20 pixels, so that only tip of the fingers are obtained as a1[1...m].

Step 3:Replace a by a1 and repeat the process of clustering until only 4 values are not obtained in the set of points under a1[1...m].

Step 4: The respective positions of these 4 values gives the length of fingers as l1, l2, l3 & l4 and shown in figure 3.1.

Step 5: The lengths calculated is further used to generate the 512-bit key which is later used for matching of the Palmprint images.

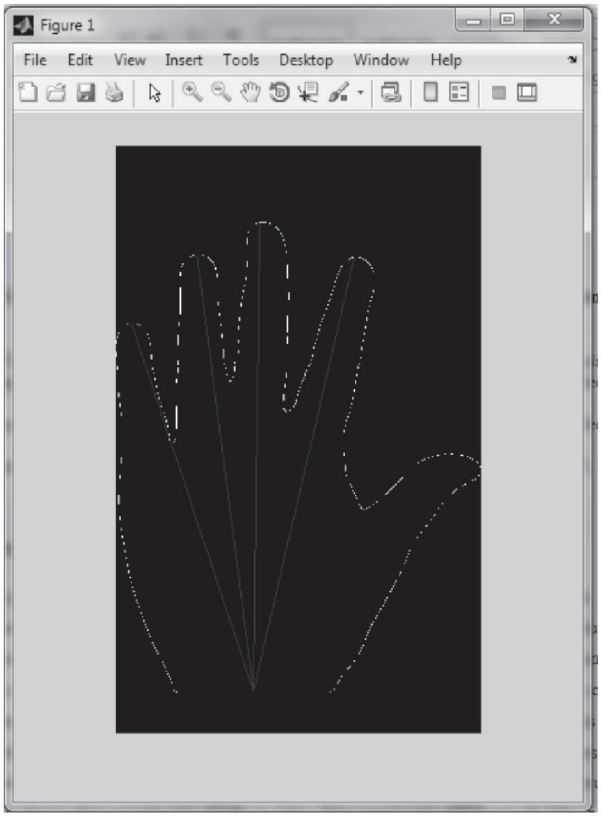

Figure 3.1. Length of 4 fingers.

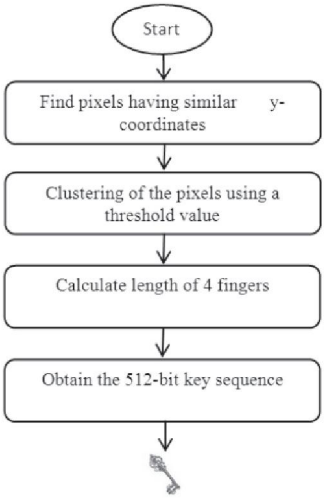

Figure 3.2. Flow chart to calculate length of fingers using Lfind() function.

The function Skfind() includes the following steps :

The encrypted key is obtained by using 3 mathematical operators mod, logarithmic & exponential. Finger lengths are taken as the parameters for computing the 512-bit security key.

Step1: Take the acquired lengths of four fingers i.e. l1, l2, l3 & l4

Step 2: Compute the mod value of each finger length with the palm length (PL)

M1=PL mod L1,M2=PL mod L2, M3=PL mod L3, M4=PL mod L4;

Step 3: To generate key the exponential value is computed for each mod values.

K1= exp(M1) , K2= exp(M2) , K3= exp(M3) , K4= exp(M4) ;

K[4]={K1,K2,K3,K4};

KEY= mean(K[4]);

Step 4: The key KEY is converted into binary form using "de2bi()" in MATLAB and stored in system as template.

Step 5: The stored key KEY is used for matching/comparison of the palm prints which are enrolled into the system in the future.

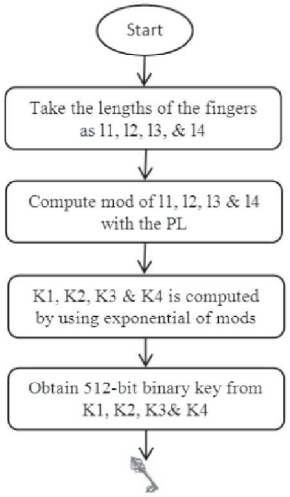

Figure 3.3. Flow chart to generate 512-bit binary key using Skfind() function.

This example clearly illustrates how the 512-bit security key is computed and how the 512-bit security key generation algorithm works. The same process was followed to generate the 512-bit security keys and were stored as templates in the database.

Example :

Step 1: Take the length of the fingers as l1=1112, l2=1053, l3=1047& l4=914

Step 2: Compute the mod of each finger length with palm length, where palm length=1112

Palm Length=max (l1, l2, l3, l4)

M1=0

M2=59

M3=65

M4=198

Step 3: 4 different keys are obtained by taking the exponential values of the 4 mod values.

K1=1

K2=4.20121040379051e+25

K3=1.69488924441033e+28

K4=9.77929206569632e+85

Step 4: Mean value of the K[4] is computed which is the required key for an individual's palm.

KEY=2.4448e+85

Step 5: The final key is stored in the database which is converted into binary value of 512 bit.

KEY =

0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0100111010110100111101001010110110111000010110000100000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000011000101000010
1100001110010001010110110110010011010100000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000

Step 6: This stored key is used for matching/comparison to find the legitimate and the imposter user.

IV. RESULT ANALYSIS

The performance of biometric security key generated by a system can be evaluated on the basis of biometric authentication parameters such as false accept rate, false reject rate, genuine accept rate, half total error rate, accuracy, etc. [15-17].

False Accept Rate (FAR) is the percentage of faulty recognized users, it is a measurement that explains the percentage of faulty recognized individuals.

$$\text{FAR} = \frac{\text{No. of false acceptance found}}{\text{Total No. of Comparisons}} \times 100$$

In this study out of 10176 comparisons 2544 were wrongly accepted. Hence, FAR computed is 25%.

False Reject Rate (FRR) is a statistic used to measure biometric performance when operating in the verification task and it usually calculated as the percentage of times the system produces a false reject. The FRR is calculated as,

$$\text{FRR} = \frac{\text{No. of false rejections found}}{\text{Total No. of Comparisons}} \times 100$$

In this study out of 1120 comparisons 210 wererejected when they were the legitimate user. Hence, FRR computed is 18.75%.

Genuine acceptance rate (GAR) is the percentage of genuine matches and is defined as

$$GAR = 1 - FRR$$

The GAR is found to be 81.25%. For a good security system, the GAR should be high.

Half Total Error Rate (HTER) is a possible way to measure the performance of the biometric system by combining both types of system errors i.e. false accept and false reject. Therefore HTER is a biometric measure which combines the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) and is defined by following formula:

$$HTER = \frac{1}{2}(FAR + FRR)$$

HTER obtained in this case is 21.875%.

Accuracy is defined as the percentage efficiency of a system in terms of its ability of authentication.The accuracy is calculate as,

$$Acuracy = 100 - \frac{FAR + FRR}{2}$$

Accuracy of the system calculated is 78.125%.

V. CONCLUSION

Biometrics is being used all over the globe and is undergoing constant development. Human palm print and hand geometry has proved to be a reliable biometric.In this work an algorithm is proposed to generate security key for authentication of an individual using human palm print. Biometrics used alone may prove to be a weak authentication tool as the human palm print can be sensed by some false means without making individual aware of it. Thus, the integration of cryptography with the biometric technology makes the security key a powerful tool with least chances of getting forged or attacked. The system aims at generating a security key which can be applied for security systems in highly secure areas like nuclear plants, banks, military base, airports, parliaments, secretariats etc. Most of the security system studies have used fingerprint recognition, facial recognition, iris recognition & voice recognition as their biometric modality means whereas fewer studies have been reported using human palm prints as an input to generate security keys. The proposed system is used to compute 512- bit security key and the performance on the results of FAR, FRR, HTER, GAR and Accuracy is suitable for security key. The performance of the proposed algorithm is highly suitable for real time applications.

As a future work, feature extraction techniques either in palm print feature or hand geometry can be enhanced.

VI. ACKNOWLEDGEMENT

The authors gratefully acknowledge the management of Vidya College of Engineering for providing us all facility and support needed for this work.

VII. REFERENCES

[1] Liang Wang and XinGeng, Behavioral Biometrics for Human Identification, Medical Information Science Reference, 2010.

[2] N.V. Boulgouris, Konstantinos N. Plataniotis and E. M. Tzanakou, Biometrics: Theory, Methods and Applications, Wiley-IEEE Press, 2009.

[3] Arun A. Ross, KarthikNandakumar and Anil K. Jain, Handbook of Multibiometrics,International Series on Biometrics, Springer, 2006.

[4] James Wayman and Anil Jain, Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.

[5] Samir Nanavati, Michael Thieme and Raj Nanavati ,Biometrics: Identity verification in a networked world, John Wiley & Sons, 2002.

[6] Anil Jain, Ruud Bolle and SharathPankanti, Biometrics: personal identification in networked society, Boston: Kluwer Academic, 1999.

[7] KasturikaB.Ray andRachita Mishra, Palmprint as a Biometric Identifier, International Journal of Electronics and Communication Technology, 2011

[8] D. Zhang, Wai-Kin Kong, J. You and M. Wong, Online Palmprint Identification, IEEE Transaction on Pattern Analysis and Machine Intelligence, 2003.

[9] N. Duta, A.K. Jain, K.V. Mardia, Matching of Palmprints, Pattern Recognition Letters, 2002

[10] W.X. Li, D. Zhang, S.Q. Xu, Palmprint Recognition Based on Fourier Transform, Journal of Software, 2002.

[11] X.Q. Wu, K.Q. Wang, and D. Zhang, An Approach to Line FeatureRepresentation and Matching for Palmprint Recognition, http://www.jos.org.cn/10010-9828/15/869.htm, 2004.

[12] A.K. Jain, N. Duta, Deformable Matching Of Hand Shapes For User Verification, International Conference on Image Processing, 1999.

[13] College of Engineering, Pune-411005(An Autonomous Institute of Government of Maharashtra), http://www.coep.org.in/index.php?pid=367.

[14] http://en.wikipedia.org/wiki/Edge_detection

[15] M. Vatsa, R. Singh, A. Noore, "Reducing the False Rejection Rate of Iris Recognition using Textural and Topological Features", International Journal of Signal Processing, 2006.

[16] R. Wang, B. Bhanu, "Performance prediction for multimodal biometrics", in Proceedings of the IEEE International Conference on Pattern Recognition, 2006.

[17] L. Hong, Y. Wan and A. I. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998.