Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhancing Palmprint-Feature Security Using PCA and Watermarking

Sneha M. Ramteke, Prof. S.S.Hatkar

Department of CSE,

SGGSIE&T, Nanded, India

Abstract: ***This paper highlight needs to solve security problem in our network society. This paper introduces a novel watermarking based approach to protect the palmprint data by hiding it into host image for personal identification purpose. Proposed the authentication scheme to protect the biometric templates and to improve the security and privacy level of biometric authentication system.To achieve this, principle lines of palmprint image is embedded in to host image. The origin of the palmprint images is proven by checking matching percentages of encoded and decoded image. Experimental results show that using this concept can efficiently protect a palmprint recognition system against replay attack and also this method improves the security of the palmprint principle lines data with hardly detectable decrease in recognition performance.***

Keywords: Palmprint Recognition, Principal Component Analysis (PCA), Watermarking, Discrete Cosine Transform (DCT), Inverse Discrete Cosine Transform (IDCT).

I. INTRODUCTION

Biometrics has been receiving attention as the substitute or complement to traditional token or key based personal identification methods. Biometrics comprises various methods for uniquely recognizing individuals by using one or more intrinsic physical or behavioural traits such as fingerprint, face, iris, hand geometry, palmprint, typing rhythm, voice, and gait. Among these traits, palmprint has a relatively short history and has received increasing interest in recent years. Palmprint is one of the most reliable features in personal identification because of its stability and uniqueness. Although the use of palmprints for identity authentication has drawn interests from some researchers, the development of an effective and efficient approach to identify and verify palmprints remains a challenging research topic. The inner surface of the palm normally contains three flexion creases, secondary creases and ridges. The flexion creases are also called principal lines and secondary creases are called wrinkles. Traditional token-based or knowledge-based personal identification techniques (such as identification cards, passwords, etc) are unable to differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person. Since biometrics characteristics are inherently associated with a particular individual, they are uneasy to be stolen, forgotten, lost or attacked. However, the problem of security and integrity of the biometrics data in networked environments poses new issues. Watermarking is a technique to increase security of the biometric data. watermarking pertain to the area of data hiding, which aims at private information protection by hiding critical information in unsuspected carrier signal. Rest of the paper is organized as follows. Section 1briefly introducesbiometrics, watermarking, steganography and encryption.In Section 2, theproposed principal lines extraction algorithm is introduced andpresents watermarking method for hiding. Experiment results are reported inSection 3 and conclusions is given in the Section 4.

II. PROPOSED METHOD FOR FEATURE EXTRACTION AND WATERMARKING

Proposed system is consisting of three important parts i.e. preprocessing, principal line extraction and matching phase. Implementation is shown in following figure.

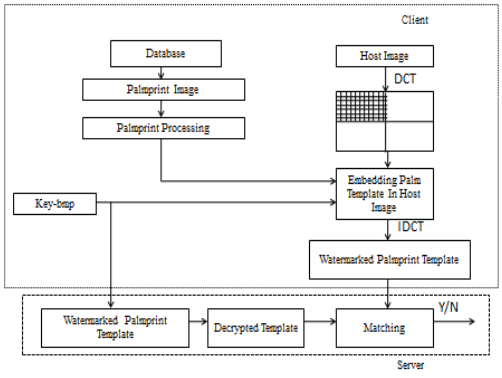


Figure 1: System Flow Diagram

2.1 Preprocessing Algorithm

Before feature extraction, it is necessary to obtain a sub-image from the captured palmprint image and to eliminate the variations caused by rotation and translation. The five main steps of palmprint image preprocessing are as follows.

Steps:

1. Convert the grayscale image to binary image. Find the one from corresponding first and last column at this row between middle and ring finger and draw a vertical line.
2. Find midpoint of these vertical line .Similarly find extreme right end point of the middle horizontal line and find midpoint of that horizontal line.
3. Find the extreme point of vertical line passing through centre of palm.
4. Similarly find the top and bottom point of this vertical line passing through centre of palm.
5. Finally, we get all six points of polygon for ROI.

Using above steps and we get polygon of ROI which is shown as follows:

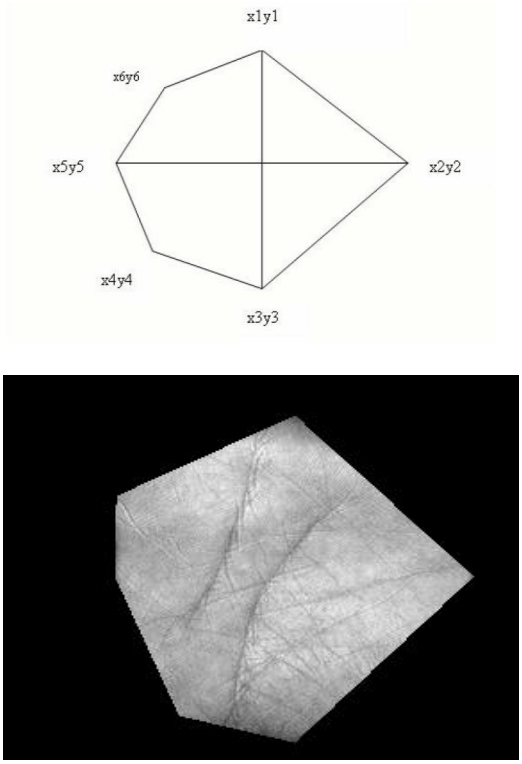


Figure 2: Polygon of ROI

Canny Edge Detection:

The Canny Edge Detector is one of the most commonly used image processing tools, detecting edges in a very robust manner. It is a multi-step process, which can be implemented on the GPU as a sequence of filters.

Steps:

1. Convert to Grayscale
2. Noise Reduction
3. Compute Gradient Magnitude and Angle

compute the gradient magnitude:

$$D = \sqrt{D^2(x,y) + D^2}(x,y) \quad (1)$$

and the angle of the gradient:

$$\Theta = \arctan\frac{Dx\,(x,y)}{Dy\,(x,y)}(2)$$

4. Non-Maximum Surpression
5. Hysteresis Thresholding

Thresholding based entirely on computation performed on the histogram of the image. It is optimal in the sense that it maximizes the between-class variance. Thresholding can be summarized as follows.

1. Compute the normalized histogram of the input image. Denote the component of histogram by P_i, I =0, 1, 2, … .L-1.
2. Compute the cumulative sums , $P_1(k)$,for k=0,1,2,…L.
3. Compute the cumulative means, M (k), for k=0,1, 2,…L-1.

4. Compute the global intensity means M_G.
5. Compute the between-class variance.
6. Obtain the ostu threshold, k*, as the value of k for which between-class variance is maximum. If the maximum is not unique, obtain k* by averaging the values of k corresponding to the various maxima detected.
7. Obtain the separability measure at k=k*.

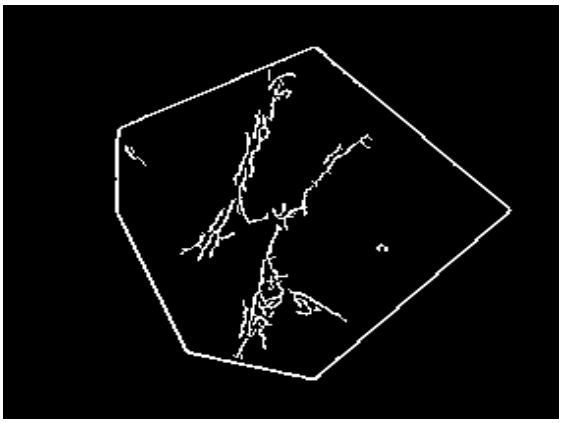


Figure 3: Edge palmprint image

2.2 PCA Algorithm for feature Extraction

We use PCA algorithm for a feature extraction. PCA has been widely used for dimensionality reduction in computer vision. It finds a set of orthogonal basis vectors which describe the major variations among the training images, and with minimum reconstruction mean square error. This is useful as it helps to decrease the dimensions used to describe the set of images and also scale each variable according to its relative importance in describing the observation PCA is theoretically the optimal linear scheme, in terms of least mean square error, for compressing a set of high dimensional vectors into a set of lower dimensional vectors and then reconstructing the original set. It is a non-parametric analysis and the answer is unique and independent of any hypothesis about data probability distribution. PCA consist of following steps.

Steps:

1. Calculate mean for each column.
2. Calculate Standard deviation.
3. Subtract mean from each value and divide by standard deviation. Subtract the mean is an integral part of the solution towards finding a principal component basis that minimizes the mean square error of approximating the data.
4. Calculate the Eigen vectors V and eigen values D.
5. Rearrange the eigenvectors and eigen values.
6. Choose the column from V whose eigen value is maximum in D and represent the original data (Z) by projecting the data.

By using a PCA algorithm we extract a principal line.

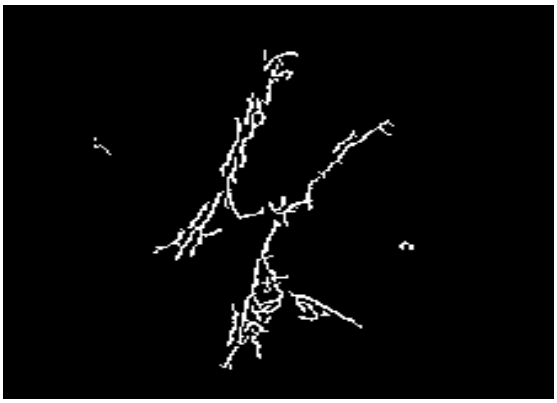


Figure 4: Extracted Principal lines

2.3 Embedding Feature Vector in Host Image

The feature vector of palmprint image obtained from PCA is embedded in host image. Embedding of feature vector in host image consist of following steps.

Steps:

1.Set gain factor (k) for embedding.

2.Set the DCT block size and define the mid-band frequencies of 8x8 dct.
3.Determine size of cover image.
4.Determine maximum message size based on cover object on cover object and blocksize.
5.Threshold coded image to 0 or 1.
6.Check that the message is not too large for cover.
7.Pad the message out to the maximum message size with one's.
8.Generate shell of watermarked image.
9.Read key for PN generator.
10.Reset MATLAB's PN generator to state key.
11.Generate PN sequence for "1" and "0", it generate 22 random number.
12.Find two highly un-correlated PN sequence correlation coefficient between pn1 and pn2.
13. Process the image in blocks and transform block using DCT.
14. If message bit contains zero then embed pn_sequence_zero into mid-band component of dct block.
15. Otherwise, embed pn_sequence_one into the mid-band component of dct block.
16. Transform block back into spatial domain.
17. Move on to next block.
18. Convert to unit 8 and write watermarked image out to 0 file.

2.4 Decoding of Embedded Feature Vector from Host Image

Extraction of palmprint image from host image is done by decoding embedded image. It consists of following steps:
Steps:
1.Set gain factor for embedding and set dctblocksize.
2.Define the mid-band frequencies of an 8x8 dct.
3.Determine maximum message size based on cover object blocksize.
4.Read in key for PN generator.
5.Reset MATLAB's PN generator to state"key".
6.Generate PN sequence.
7.Process the image in blocks.
8.Transform block using DCT.
9.Extract the middle band coefficient.
10.Calculate the correlation of the middle band sequence to PN sequence.
11.Move on to next block.
12.If correlation exceeds threshold, set bit to'0' otherwise'1'.
13.Reshape the embedded image.
14.Display recovered image.

3. Experimental Results And Analysis

The watermark should be imperceptible to human observation while the host image is embedded with secret data. How to get a method to measure the host image imperceptible is important. In this paper we employee the PSNR to indicate the transparency degree. The size of each image is 512×512. The peak-signal- to-noise ratio (PSNR) is used to measure the invisibility of the watermark and the Normalized Correlation (NC) is to detect the similarity of the original principal lines and the extracted one.if PSNR value exceeds 35dB, the invisibility of the watermarking algorithm is well ensured.The PSNR and MSEdescribe below[4].

$$PSNR = 10 \times \lg \left(\frac{255^2}{MSE}\right) \quad (3)$$

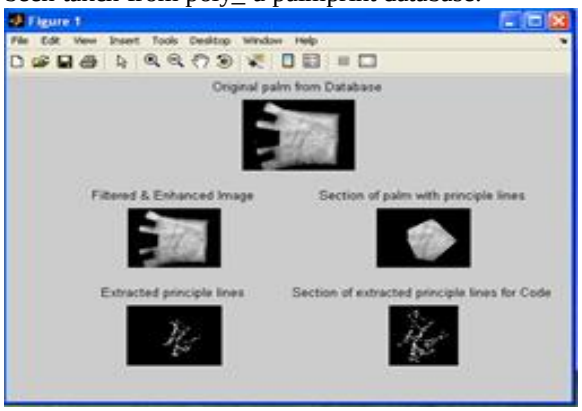
$$MSE = \frac{1}{M \times N} \sum_{i=1}^{N} \quad \sum_{j=1}^{M} \quad [I(i,j) - I^*(i,j)]^2 \quad (4)$$

Where,I(i,j) is the original image, $I^*(i,j)$ is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. A lower value for MSE means lesser error, and as seen from the inverse relation between the MSE and PSNR, this translates to a high value of PSNR. It's evident from the formula that the result is expressed in decibels. A small mean square error results in a high signal to noise ratio, if MSE tends to zero, then PSNR tends to infinity. Excellent values range from 30 to 50 dB**,** while an acceptable range in wireless transmission settles around 25dB.

$$NC(W.W^*) = \frac{\sum_{i=1}^{N} W_i . W_i^*}{\sqrt{\sum_{i=1}^{N} W_i^2} \sqrt{\sum_{i=1}^{N} W_i^{*2}}} \quad (5)$$

Where,Wis original principal lines and W* is the extracted principal lines code. Actually, NC is in the range of [0,1], which represents similarity between W and W*. The bigger this NC value, the better is. In term of palmprint feature protecting, both high PSNR and NC values are expected.

The system has been implemented using MATLAB because of powerful inbuilt mathematical and image processing functions. Palmprint images have been taken from poly_ u palmprint database.



Methods	MSE	PSNR	NC	Matching %
Proposed Method	14.173	36.67	0.697	93.1740
Existing Method	30.0026	33.3592	0.62889	72.0973

4. Conclusions

This paper proposed an authentication scheme to protect the biometric templates and to improve the security and privacy level of biometric authentication system. To solve security problems in our networked society, as the important implementation of biometric technology, palmprint verification is one of the most reliable personal identification methods which are most useful technique in forensic science. This paper proposed an improved approach to extract principal palm lines on the basis of and a new matching algorithm based on principal lines. Final extracted principal line then hide in host image to secure palmprint over the network. This mechanism is very suitable and comfortable for all users. The average PSNR after the embedding of principal lines in the host image is 38.6011dB. This implies the hackers hardly detect the secret information with their eyes. In summary, we conclude that our palmprint identification and security system can achieve good performance in terms of speed and accuracy.

Acknowledgements

I would like to extend my sincere thanks to Prof. S.S.Hatkar, Dept. Of Computer Science and Engineering, Shri Guru GobindSinghji Institute of Engineering and Technology, Nandedfor his help in the field of security, image processing, pattern recognition.

References

[1] A. K. Jain, S. Pankanti, and R. Bolle(eds.), "BIOMETRICS: Personal Identification in Networked Society," Kluwer, 1999.

[2] B. Schneier, "The uses and abuses of biometrics," Comm.ACM, vol.42, no.8, pp.136, Aug.1999.

[3] Leqing Zhu, Sanyuan Zhang, Rui Xing, Yin Zhang, "Palmprint Recognition Based on PFI and Fuzzy Logic Fifth International Conference on Fuzzy Systems and Knowledge Discovery", Proc. of IEEE ,2007,pp.182-187.

[4] Wang Na, Zhang Chiya, Li Xia, Wang Yunjin,"Enhancing Iris-feature Security with steganography", Conference on Industrial Electronics and Applicationsis, 2010, pp.451-455.

[5] De Shauang Huang, Wi Jia and David Zhang,"Palmprint verification based on principal lines, pattern Recognition", Pattern Recognition 41 (4), 2008, pp.136-1328.

[6] MoussadekLaadjel, Ahmed Bouridane, FatihKurugollu, and Said Boussakta, "Palmprint recognition using fisher-gabor feature extraction", ICASSP, March 2008, pp. 1709–1712.

[7] Ratha N. K., Connell J. H., and Bolle R. M., "Enhancing security and privacy in biometrics-based authentication systems", IBM Syst. J. 40(3), 2001, pp.614–634.

[8] Adams Kong, David Zhang, and Mohamed Kamel,"Three measures for secure palmprint identification", Pattern Recognition 41(4), 2008, pp.1329–1337.

[9] Adams Kong, David Zhang, and Mohamed Kamel, "A study of brute-force break-ins of a palmprint verification system", Proc. of the International Conference on Audioand Video-based Biometric Person Authentication, volume 3546, 2005, pp. 447–454.

[10] Khalil Zebbiche, LahouariGhouti, FouadKhelifi, and Ahmed Bouridane, "Protecting fingerprint data using watermarking",NASA/ESA conference on Adaptive Hardware and Systems, 2006, pp.451–456.

[11] Andrew TeohBeng Jin, Michael GohKahOng, David Ngo Chek Ling, "An automated palmprint recognition system", Proc. of IEEE, 2006, pp.67-89.

[12] David Zhang, Wai-Kin Kong, Jane You, Michael Wong, "Online Palmprint Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence,Vol. 25, 2003, pp.1041-1050.

[13] Fang Li, Maylor K.H. Leung, Xiaozhou You, "Palmprint Identification Using Hausdorff Distance", IEEE International Workshop on Biomedical Circuits & Systems, 2004,pp.308-315.

[14] Fang Li, Maylor K.H. Leung, Xiaozhou You, "Palmprint Matching Using Line Features", ICACT, February 2006, pp.20-22.

[15] Li Shang, De-Shuang Huang, Ji-Xiang Du, Chun-HouZheng, "Palmprint Recognition using Fast ICA algorithm and radial basis probabilistic neural network", Proc. of IEEE ,2005,pp.176-184.

[16] Md. Rajibul Islam, Md. ShohelSayeed, Andrews Samraj,"Biometric template using watermarking with Hidden password Encryption", Proc. of IEEE, 2008, pp.978-985.

[17] Tee Connie, Andrew Teoh, Michael Goh, and David Ngo,"Palmhashing: a novel approach for cancelable biometrics", Inf.Process. Lett. 93(1), 2005, pp. 1–5.

[18] D. Zhang, W. Shu, "Two novel characteristics in palmprint verification Two novel characteristics in palmprint verification: datum point invariance and line feature matching", Pattern Recognition, vol.4, 1999, pp. 691-702.

[19] Ken Cabeen, Peter Gent, "Image Compression and the Discrete Cosine Transform", Proc. of IEEE, 2007, pp.192-190.

[20] Md. Rajibul Islam, Md. ShohelSayeed, Andrews Samraj,"Biometric Template Protection Using Watermarking with Hidden Password Encryption", IEEE 2008, pp. 978-985.

[21] A.K.Jain and U.Uludag,"Hiding biometric data," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 11, Nov.2003,pp. 1494-1498.

