International Conference on Computer Applications 2016 [ICCA 2016]

| | | | |
|---|---|---|---|
| **ISBN** | 978-81-929866-5-4 | **VOL** | 05 |
| **Website** | icca.co.in | **eMail** | icca@asdf.res.in |
| **Received** | 14 – March– 2016 | **Accepted** | 02 - April – 2016 |
| **Article ID** | ICCA022 | **eAID** | ICCA.2016.022 |


# Palmprint Recognition using Multimodal Biometrics and Generation of One Time Password

**S Pravarthika[1], S Babitha Rani[2], K Induja[3]**
[2]Assistant Professor, [1,3]Department of Information Technology Department of Information Technology
Meenakshi College of Engineering, K K Nagar, Chennai, India

**Abstract—** *Biometrics was developed with the aim of improving the overall security level in all society contexts. A biometric system describes a set of techniques to analyze certain individual's biometric features, store and then using those patterns to identify or verify the identity of a person. The palmprint contains not only principal curves and wrinkles but also rich texture and miniscule points, so the palmprint identification is able to achieve a high accuracy because of available rich information in palmprint. Various palmprint identification methods, such as coding based methods and principal curve methods have been proposed in past decades. In addition to these methods, subspace based methods can also perform well for palmprint identification. Combining the left and right palmprint images to perform multibiometrics is easy to implement and can obtain better results.*

*Multimodal biometrics can provide higher identification accuracy than single or unimodal biometrics, so it is more suitable for some real-world personal identification applications that need high-standard security. A onetime password is included for higher security and accuracy.*

*One time passwords generally expire after using once. They are generated for using it within a certain time period after which it is useless. These passwords are set as a secondary security measure for the primary palmprint recognition.*

**Keywords—***palmprints, biometrics, multimodal biometrics, One Time Password, matching score, feature extraction*

## I. INTRODUCTION

Palmprint Identification technique is a growing biometric security method in the technology market. The palmprint contains principal curves, wrinkles, rich texture, depth and miniscule points. Using these biometric features, the palmprint is identified and the personal identification is verified. In spite of these verifications, there is a possibility of an error. In order to make this technique more secure and more stable, the method also includes the generation of an OTP (One Time Password). The OTP is used for making the system more reliable more efficient and trustworthy.

Various palmprint identification methods are used in previous works. All those works use unimodal biometrics which has certain limitations such as low performance. To overcome those limitations of unimodal biometrics, multimodal biometrics are used in this system. In general the multimodal biometric system uses more than one biometric input or feature of same individual for identification. Combining more than one biometric trait of the same individual increases the accuracy and reduces the error rate considerably which makes the system more secure and increases the performance.

In addition to the multimodal biometrics, an OTP (One Time Password) is also included. This OTP further increases the performance and accuracy of the system by reducing the identification errors. Since, these one-time passwords are valid only for a period, the



**Cite this article as:** S Pravarthika, S Babitha Rani, K Induja. "Palmprint Recognition using Multimodal Biometrics and Generation of One Time Password". *International Conference on Computer Applications 2016*: 110-114. Print.

passwords cannot be forged by the individuals which increases the security of the system.

## II. Proposed Framework

In this system, a novel framework of combining the left palmprint with the right palmprint at the matching score level is provided. In this framework, four types of matching scores are obtained by the left palmprint matching, right palmprint matching, cross matching between the left query palmprint and right training palmprint and cross matching between the right query palmprint and the left training palmprint respectively. These four matching scores are then fused together to make the final decision. This method uses the similarity between the left palmprint and the right palmprint of the same subject and then generates an OTP (One Time Password) for more accurate personal identification. Extensive experiments show that the proposed framework can integrate most conventional palmprint identification methods for performing identification and can achieve higher accuracy than conventional methods.

The proposed system uses five levels of framework for working at five different stages in the entire process. These levels are: the image (sensor) level, the feature level, the matching score level, the decision level and the OTP (One Time Password) generation level.

### Image (Sensor) Level

The image sensor level uses touchless method for obtaining the image of the palmprint. Generally, scanners are used for detecting minute minuscule in the palmprint. However, the touchless method uses a high resolution camera for capturing the image and processing it. The image is then processed based on the requirements of the system.

### Feature Level

The feature level involves extracting the miniscule points and principal lines from the obtained input image. The features include the principal lines, the rich texture and other miniscule points that play a major part in identifying an individual. The features are then processed and prepared for the next level.

### Matching Score Level

The matching score is calculated in this level by using the features that has been extracted in the previous level. The matching score level uses the matching score algorithm. This algorithm is used for determining the right palmprint matching score, the left palmprint matching score and the cross matching scores. Finally, the matching scores are fused together to form the fused matching score.

### Decision Level

Based on the final fused matching score value, the decision is made on whether the palmprints match any of the existing palmprints in the database. If there is a match, then the next level is executed. If not a match, then the recognition is denied and authentication is failed.

### OTP (One Time Password) Generation Level

The One Time Password is generated based on the random permutation algorithm. The one time password is valid only for a certain period of time. Once the password is used, it expires and hence cannot be reused again.

## A. Procedure of the Proposed Framework

Initially, two query palmprint images are given: left query palmprint and right query palmprint image. The training palmprint from the database are accessed and the principal lines are extracted. Now the matching score for left palmprint, right palmprint and cross matching scores are determined. The obtained matching scores are fused together and the final matching score is acquired. Based on this score, the best match is found. Then, a One Time Password (OTP) is generated. Once the correct password is typed, the person is recognized and access is granted.

**Cite this article as:** S Pravarthika, S Babitha Rani, K Induja. "Palmprint Recognition using Multimodal Biometrics and Generation of One Time Password". *International Conference on Computer Applications 2016*: 110-114. Print.


Fig.1 Architecture of the entire palmprint recognition process

In fig.1, query indicates the input images obtained by the system and the training palmprint denotes the images stored in the database. The left query palmprint image is verified with the left training palmprint image from the database to determine the left matching score. Then the right query palmprint image is verified with the right training palmprint image from the database to determine the right matching score. Then the left query palmprint image is combined with the right training palmprint image from the database to determine the cross matching score 1. Finally, the right query palmprint image is combined with the left training palmprint image from the database to determine the cross matching score 2. The above four matching scores are fused to determine the final matching score. Based on the obtained matching score, the one-time password is generated and accuracy is maintained.

## B. Preprocessing

In this section, if the input images are color images, they are converted to their respective gray scale images from their corresponding color images. This is done because a matrix cannot store more than one value at a given position. Hence the Red Green Blue (RGB) values in each pixel is converted to a single grayscale value by processing the red, blue and green values of each pixel to a grayscale pixel and averaging them. Now, the obtained grayscale image matrix is complemented. In the complement of an image, black and white colors are reversed (i.e.) the intensity of the grayscale image is swapped. In the output image, dark areas become lighter and light areas become darker. For a method to enhance the contrast of digital image, modified histogram equalization technique is proposed.

## C. Principal Line Extraction

This subsection describes the steps to extract the principal line from the palmprint image. The principal lines of the left palmprint and the reverse right palmprint of the same individual have similar shapes and positions. But the principal lines of the left and right palmprint of different individuals have very different shapes and positions. The principal line based methods have been widely used in palmprint identification. Top-hat filtering computes the opening of the image and then subtracts the result from the original image. Here, a value from zero to 255 is selected and assigned as the threshold value. The output image BW replaces all pixels in the input image with luminance greater than the threshold level with the value 1 (white) and replaces all other pixels with the value 0 (black). However, this binary black and white image might contain several distortions and noises. In order to avoid such discrepancies, filtering is done to remove the noise. Finally, principal line images are extracted. The principal line based method is able to provide stable performance for palmprint verification.

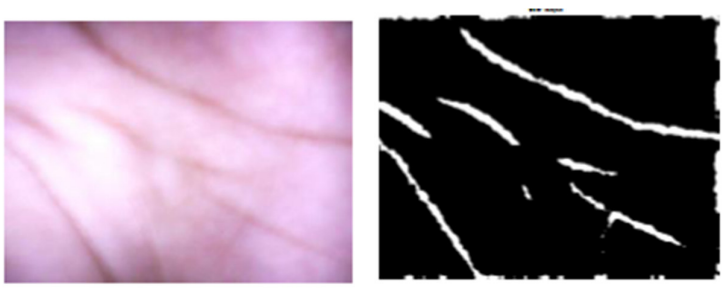

Fig.2.a Sample Left Palmprint Image Fig.2.b Extracted Principal line Image

**Cite this article as:** S Pravarthika, S Babitha Rani, K Induja. "Palmprint Recognition using Multimodal Biometrics and Generation of One Time Password". *International Conference on Computer Applications 2016*: 110-114. Print.


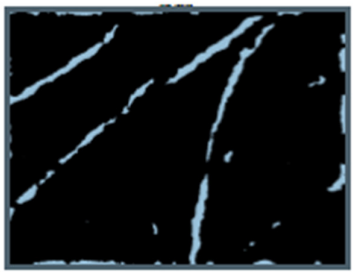

Fig. 3.a Sample Right Palmprint Image Fig. 3.b Extracted Principal line Image

The figure 2.a shows the left palmprint input image and figure 2.b represents the extracted and filtered image of the principal lines. The figure 3.a similarly shows the right palmprint input image and figure 3.b gives the extracted and filtered image of the principal lines of the corresponding image.

## D. Matching Score Level

The framework first works for the left palmprint images and uses a palmprint identification method to calculate the scores of the test sample with respect to each class. Then it applies the palmprint identification method to the right palmprint images to calculate the score of the test sample with respect to each class. After the crossing matching score of the left palmprint image for testing with respect to the reverse right palmprint images and right palmprint image with respect to left palmprint images of each class is obtained, the proposed framework performs matching score level fusion to integrate these four scores to obtain the identification result. The method has the following logic:

$S(A, B) = \text{sum}(\text{sum}(A(i, j) \& \bar{B}(i, j)))/NA$ (1)

where A and B are two palmprint principal lines images, "&" represents the logical "AND" operation, NA is the number of pixel points of A, and $\bar{B}(i, j)$ represents a neighbor area of B(i, j ).

The value of $A(i, j) \& \bar{B}(i, j)$ will be 1 if A (i, j) and at least one of $\bar{B}(i, j)$ are simultaneously principal lines points, otherwise, the value of $A(i, j) \& \bar{B}(i, j)$ is 0.

S(A, B) is between 0 and 1, and the larger the matching score is, the more similar A and B are.

The steps are presented in detail below:

Step 1: Find the matrix B~ (i,j) by adding zeros along the rows and columns of the matrix and comparing A(i,j) and B(i,j). Denote the matrix values of B~(i,j) as 1 if any one value of B(i+1,j), B(i-1,j), B(I,j+1) or B(I,j-1) are equal to A(i,j).
Step 2: Perform AND operation for A(I,j) and B~(I,j).
Step 3: Add the row values and column values of the obtained matrix separately.
Step 4: Average both the values to get the matching score value for the right palmprint.
Step 5: Similarly, perform the same method for the left palmprint images.
Step 6: For finding the matching score of the right training palmprint and the left query palmprint, generate the reverse images ˜ B(i,j) of the right palm- print image. Both B(i,j) and B~(i,j) will be used as training samples.
Step 7: The maximum matching score denotes the most closest and accurate match for the given inputs.

## E. One Time Password

A One Time Password (OTP) is included for higher security and accuracy. One Time Passwords generally expire after using once and are more secure to use than normal passwords. They are useless if not used within the given time duration. Only if the palmprint matches, the One Time Password is generated. One Time Password is generated using the random permutation method. The algorithm uses three random variables xx=1, a=1, b=2 to compute a four digit random password.

The random password is obtained using the logic,

$x = r(i) * r(i) * r(i)$, (2)
$k = x + (a*r(i)) + b$, (3)
$y(i) = \text{sqrt}(k)$ (4)
$OTP = \text{round}(xx * y)$ (5)

where OTP is the final password that has been generated.

## F. Complexity

In this method, the reverse of left and right training palmprint is processed before performing the identification which increases the complexity of the system with respect to time. The proposed system requires extra time for computation of matching score when

**Cite this article as:** S Pravarthika, S Babitha Rani, K Induja. "Palmprint Recognition using Multimodal Biometrics and Generation of One Time Password". *International Conference on Computer Applications 2016*: 110-114. Print.

compared to other conventional methods. Further, it requires an extra time for computing the One Time Password which increases the computational complexity of the system.

## III. Conclusion

This study shows that the left and the right palmprint images of the same subject are somewhat similar. The use of this kind of similarity for the performance improvement of palmprint identification has been explored. The proposed method carefully takes the nature of the left and right palmprint images into account, and designs an algorithm to evaluate the similarity between them. Moreover, by employing this similarity, the proposed weighted fusion scheme uses a method to integrate the three kinds of scores generated from the left and right palmprint imaged. Extensive experiments demonstrate that the proposed framework obtains very high accuracy and the use of the similarity score between the left and right palmprint leads to important improvement in the accuracy.

## IV. Future Enhancement

The technique implemented should be improved by creating a database all over India for security purposes. The detection technique in an image should be improved by using a camera with high resolution. The technique should be taken ahead by all the organizations for accurate personal identification and security reasons.

## References


1. A. W. K. Kong, D. Zhang, and M. S. Kamel, "A survey of palmprint recognition," Pattern Recognit., vol. 42, no. 7, pp. 1408–1418, Jul. 2009.
2. D. Zhang, W. Zuo, and F. Yue, "A comparative study of palmprint recognition algorithms," ACM Comput. Surv., vol. 44, no. 1, pp. 1–37, Jan. 2012.
3. D. Zhang, F. Song, Y. Xu, and Z. Lang, "Advanced pattern recognition technologies with applications to biometrics," Med. Inf. Sci. Ref., Jan. 2009, pp. 1–384.
4. R. Chu, S. Liao, Y. Han, Z. Sun, S. Z. Li, and T. Tan, "Fusion of face and palmprint for personal identification based on ordinal features," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2007, pp. 1–2.
5. D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online palmprint identification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 9, pp. 1041–1050, Sep. 2003.
6. A.-W. K. Kong and D. Zhang, "Competitive coding scheme for palmprint verification," in Proc. 17th Int. Conf. Pattern Recognit., vol. 1. Aug. 2004, pp. 520–523.
7. W. Zuo, Z. Lin, Z. Guo, and D. Zhang, "The multiscale competitive code via sparse representation for palmprint verification," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2010, pp. 2265–2272.
8. Y. Hao, Z. Sun, and T. Tan, "Comparative studies on multispectral palmimage fusion for biometrics," in Proc. 8th Asian Conf. Comput. Vis., Nov. 2007, pp. 12–21.
9. D. Zhang, Z. Guo, G. Lu, D. Zhang, and W. Zuo, "An online system of multispectral palmprint verification," IEEE Trans. Instrum. Meas., vol. 59, no. 2, pp. 480–490, Feb. 2010.
10. J. Dai and J. Zhou, "Multifeature-based high-resolution palmprint recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 5, pp. 945–957, May 2011.
11. S. Ribaric and I. Fratric, "A biometric identification system based on eigenpalm and eigenfinger features," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 11, pp. 1698–1709, Nov. 2005.
12. K.-H. Cheung, A. Kong, D. Zhang, M. Kamel, and J. You, "Does EigenPalm work? A system and evaluation perspective," in Proc. IEEE 18th Int. Conf. Pattern Recognit., vol. 4. 2006, pp. 445–448.
13. J. Gui, W. Jia, L. Zhu, S.-L. Wang, and D.-S. Huang, "Locality preserving discriminant projections for face and palmprint recognition," Neurocomputing, vol. 73, nos. 13–15, pp. 2696–2707, Aug. 2010.
14. P. N. Belhumeur, J. P. Hespanha, and D. Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, Jul. 1997.
15. H. Sang, W. Yuan, and Z. Zhang, "Research of palmprint recognition based on 2DPCA," in Advances in Neural Networks ISNN (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, 2009, pp. 831–838.
16. F. Du, P. Yu, H. Li, and L. Zhu, "Palmprint recognition using Gabor feature-based bidirectional 2DLDA," Commun. Comput. Inf. Sci., vol. 159, no. 5, pp. 230–235, 2011.
17. D. Hu, G. Feng, and Z. Zhou, "Two-dimensional locality preserving projections (2DLPP) with its application to palmprint recognition," Pattern Recognit., vol. 40, no. 1, pp. 339–342, Jan. 2007.
18. Y. Xu, Z. Fan, M. Qiu, D. Zhang, and J.-Y. Yang, "A sparse rep- resentation method of bimodal biometrics and palmprint recognition experiments," Neurocomputing, vol. 103, pp. 164–171, Mar. 2013.
19. D. G. Lowe, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.
20. A. Morales, M. A. Ferrer, and A. Kumar, "Towards contactless palmprint authentication," IET Comput. Vis., vol. 5, no. 6, pp. 407–416, Nov. 2011.


**Cite this article as:** S Pravarthika, S Babitha Rani, K Induja. "Palmprint Recognition using Multimodal Biometrics and Generation of One Time Password". *International Conference on Computer Applications 2016*: 110-114. Print.