ISSN NO. 2320-5407

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/1719
DOI URL: http://dx.doi.org/10.21474/IJAR01/1719

RESEARCH ARTICLE

AUTHENTICATION THROUGH BIOMETRIC MULTIMODAL PALMPRINTS USING MATCHING SCORES AND OTP.

Dr. D. Pugazhenthi[1] and R.P.Hemalatha[2].

1. Assistant Professor, PG & Research Dept. Of Computer Science, Quaid-E-Millath Govt. College for Women(A), India.
2. M.Phil Research Scholar, PG & Research Dept. Of Computer Science, Quaid-E-Millath Govt.College for Women (A), India.

……………………………………………………………………………………………………....

Manuscript Info

……………………….

Manuscript History

Received: 12 July 2016
Final Accepted: 19 August 2016
Published: September 2016

Key words:-
Multimodal, Matching scores, OTP, RLOC, Authentication.

Abstract

……………………………………………………………….

The multimodal biometric system refers to the term which integrates multiple biometric traits of the same person like the left and right palmprint images of the user which is used in this process of the palmprint authentication system. In this paper, the left and right palmprint images are used where the right palmprint image is reversed. The matching scores are the score values which are calculated from the templates that are extracted from the query palmprint image and matched with the corresponding models in the training palmprint image in the database. Thus the matching scores are calculated from the left training and left query palmprint image, left query and right reverse training palmprint image and from the right reverse training and right query palmprint image using the Robust Line Orientation Code (RLOC) which is summed to form the combined matching score. The One Time Password (OTP) which is the randomly generated password is sent as the text message to the user's network medium by a service provider. In this paper, the combined matching score, which is calculated, helps to authenticate the user along with the OTP which is generated using the proposed method. Thus, this article aims to provide a more secure and efficient multimodal palmprint authentication system.

……………………………………………………………………………………………………....

Introduction:-

In modern days, the security process using the biometric system is a fast improving, efficient and reliable system. Biometric relates to the utilization of the physiological or behavioral characteristics of a person to authenticate their identity. The physiological and behavioral characteristics of the human include the face, retina, iris, ears, teeth, hands, palmprints, fingers, feet, veins, signature, typing styles, voice, DNA, and odors, etc., Biometric system, which obtains and uses only a single source of information or data to recognize an individual is known as Unimodal biometric system. Though these systems are safe and perfect, according to Benaliouche et al. [4] they also suffer from several problems like noise, non-universality, lack of individuality, and sensitivity to attack. To overcome these challenges, the multimodal biometric system can be used which combines the two or more different biometric traits of the same person. According to Mane V, et al. [14] states that in the orthogonal multimodal biometrics, different biometrics (i.e. face, iris, fingerprint) are involved with little or no interaction between the individual

Corresponding Author:- Dr. D. Pugazhenthi.
Address:- Assistant Professor, PG & Research Dept. Of Computer Science, Quaid-E-Millath Govt. College for Women(A), India

biometrics whereas independent multimodal biometrics processes the individual biometrics independently. In the course of the multimodal biometric system after the data is being captured from the person, there are different levels like the image level, feature level, match/score level, and decision level.

In this multimodal biometric system, the left and right palmprint images of a person are being used, which uses two different biometrics of the same person to identify the individual. The palmprint of every human has three primary principal lines, namely, the heartline, the headline and the lifeline which is the longest and widest lines in the palmprint image that has the stable position and shape which can be used in the process of recognition. In this process of palmprint biometric system, the palmprint image is captured through the biometric sensors which are stored in a specified database that are used to extract the features from the palmprint images using the feature extraction level. Then the extracted features are used to calculate the matching scores for the palmprint image at the matching score level. These calculated matching scores are then utilized in the authentication process of the biometric user to recognize the user at the decision level.

Though the biometric systems are much safer, they can be made more secure and unique to a single user by using the OTP. The OTP is the randomly generated password by the system which can be used only once by the user to authenticate through the biometric system. The OTP may be a text message which can be sent to the specified biometric user using the network of the service provider when the user tries to access the system. In this paper, the multimodal process of palmprint authentication using the left and right palmprint images are handled in different levels where the left and right palmprint images of the user are captured, in which the right palmprint image is reversed to calculate the matching scores. The matching scores are calculated for left training and left query palmprint image, then for the left query and right reverse training palmprint image and then for the right query and right reverse training palmprint image. These three matching scores are combined to form a single matching score for the specified user which is used in the decision level for the recognition process. Once the user gets access into the decision level, then the OTP is sent to the user’s specified medium to authenticate the user into the system.

Existing Model:-
The biometric palmprint authentication system consists of the process which takes place in the different levels of fusion namely the image level, feature level, match/score level and decision level. The palmprint images are obtained using different sensors for capturing the contact/touch-based or contactless palmprint images for the recognition process as in Morales et al. [15]. In this paper contact based images are used in the process of the recognition which gives accurate, less error free and noiseless images. The palmprint images are processed using various methods like line-based methods, subspace methods, representation based methods and SIFT-based methods which are applied in different stages of palmprint authentication as on Xu et al. [20].

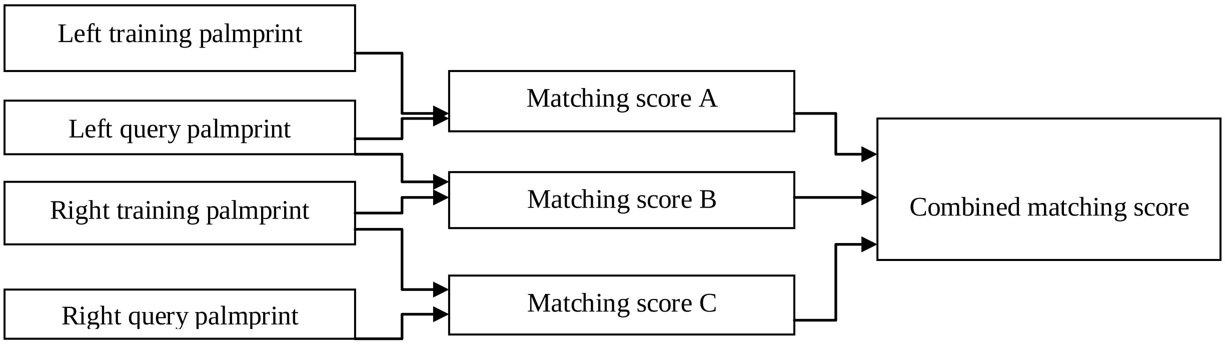


Figure 1:- The existing model for the palmprint authentication.

The existing model for the palmprint authentication system is denoted in figure 1.The line- based methods are usually used to extract the principal line features from the palmprint images. In this paper, the image level is processed using histogram equalization to preprocess the palmprint image. The preprocessed palmprint image is then used to extract the features using principal line-based methods based on Xu et al. [20].The features are extracted at the feature level, using which the matching scores are calculated in the score level. According to Jia et al., [10], the pixel-to-area strategy is adopted using the Robust Line Orientation Code (RLOC) which is used to define the principal lines matching scores of the palmprint images. Using RLOC the matching scores for the principal lines are calculated like:

$$S(A,B)=\left(\sum_{i=1}^{m}\sum_{j=1}^{n} A(i,j)\&{\sim}B(i,j)\right)/N_A$$

Where A and B denote the left and right palmprint images, '&' represents the logical AND operator, N_A represents the number of pixels of A(i,j) and ~B(i,j) which represents the neighbor area of the B(i,j). The matching scores thus calculated could be used at the decision level. Once the user tries to authenticate into the biometric system, then the subspace methods are used. The subspace methods like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), etc., as mentioned by Tee Connie et al. [19] which are used in the automated palmprint identification system for the purpose of classification. The query samples are converted into the class of low-dimensional feature space which is used as the separate class to identify the class with the minimum Euclidean distance. Thus the query samples are authenticated into the class of access with which the particular user is authorized.

To make the process of the palmprint authentication system more secure and uniquely authenticated to the particular user, the process of OTP can be integrated along with this process as in Abdellaoui et al. [2]. In this proposed model, along with palmprint authentication, OTP can be used to authenticate the user in the system.

Proposed Model:-

The palmprint authentication in the proposed model uses the images of the left and reverse of right palmprint images. The proposed model works as shown in the figure 2.

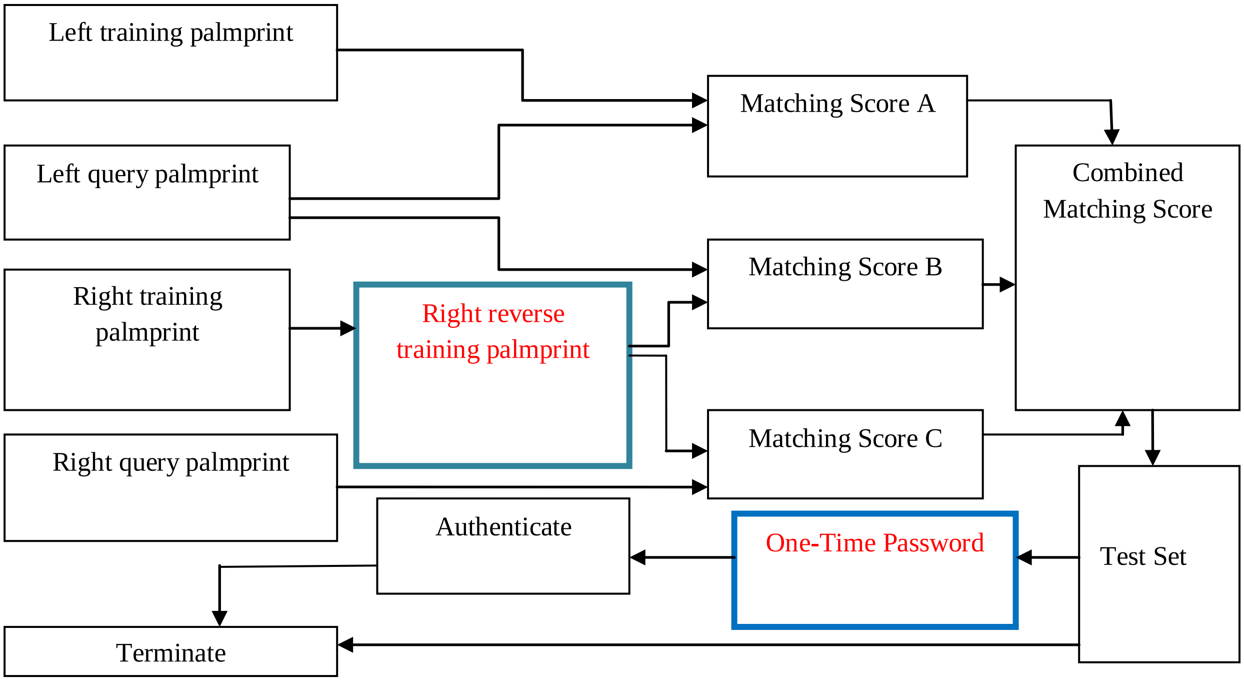


Figure 2:- The proposed model for the palmprint authentication

The palmprint authentication consists of five levels, which ultimately define the recognition process.

Image Level:-

The left palmprint and right palmprint images are captured using contact-based sensors which are stored along with the specified user information into the database. These palmprint images are the training images which will be utilized by the palmprint biometric system.

Feature Level:-

The left and right palmprint images of the user in the database are used as the training image while the user input is used as the query image. The images obtained are primarily converted into the grayscale image which converts the image into binary images as 0's and 1's, where the pixel values of the picture are reversed, that is the ones are converted into zeros and zeros are converted into ones. This process makes the dark area of the image into the lighter area and the lighter area of the image into darker, which gradually highlights the principal lines in the palmprint images as shown in figure 3. This helps in the process of score level.

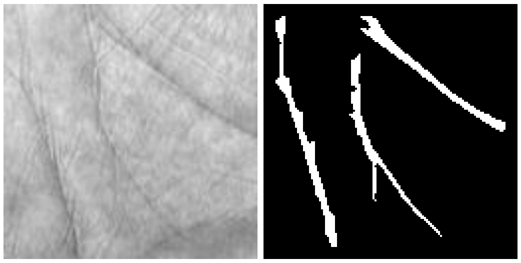


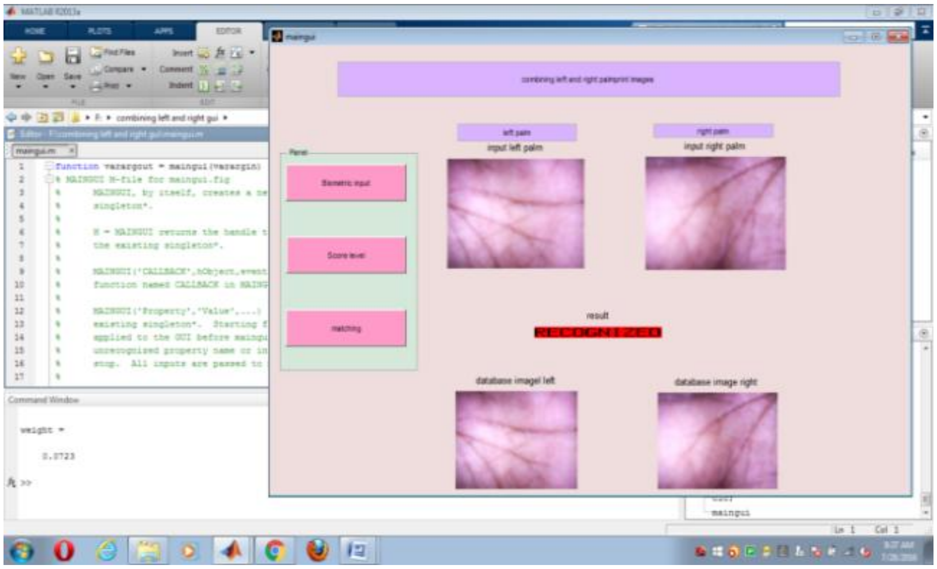
Figure 3:- The palmprint image and its binary image

Score Level:-

The principal lines obtained are used to calculate the matching scores for each user. The principal lines in the right training palmprint image are reversed. Then the matching scores are computed for the left training palmprint, and the left query palmprint and the left query palmprint and the right reverse training palmprint and finally for the right reverse training palmprint and right query palmprint image and they are combined to form a single combined matching scores. This process is performed using the RLOC as specified by Jia et al.[10] using which the query palmprint can be classified into the class that produces the maximum matching score.

Decision Level:-

Once the matching score for the query palmprint image as the maximum matching score than its specified as “RECOGNIZED” as shown in Figure 4a but if the query image does not gets classified into the class of the maximum matching score, then the query palmprint is defined as “NOT MATCHED” as shown in Figure 4b and the processes gets terminated at decision level itself.



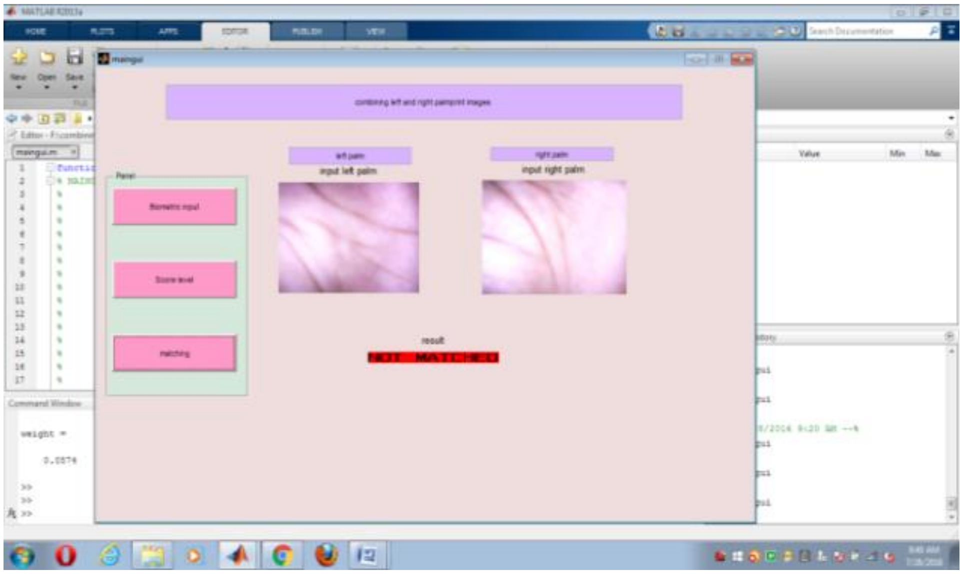
```
function varargout = maingui(varargin)
% MAINGUI M-file for maingui.fig
%      MAINGUI, by itself, creates a ne
%      singleton*.
%
%      H = MAINGUI returns the handle t
%      the existing singleton*.
%
%      MAINGUI('CALLBACK',hObject,event
%      function named CALLBACK in MAING
%
%      MAINGUI('Property','Value',...)
%      existing singleton*.  Starting f
%      applied to the GUI before maingu
%      unrecognized property name or in
%      stop.  All inputs are passed to
%
```

```
weight =

    0.2723

>>
```

Figure 4a:- The GUI which denotes an authorized user.



```
weight =

    0.0574

>>
>>
>>
```

Figure 4b:- The GUI which denotes an unauthorized user

OTP Level:-

When the query palmprint images get recognized, then they get processed into the level of OTP. In this level, the password gets generated randomly using one-way hashing function and is sent from the service provider to the biometric user once the palmprint gets recognized, and the system requests for the password from the user immediately as shown in figure 5. Once the user enters the password, and if the password entered is correct then the system authenticates the user into the system. But if the password entered is incorrect, then the user is denied access into the system.

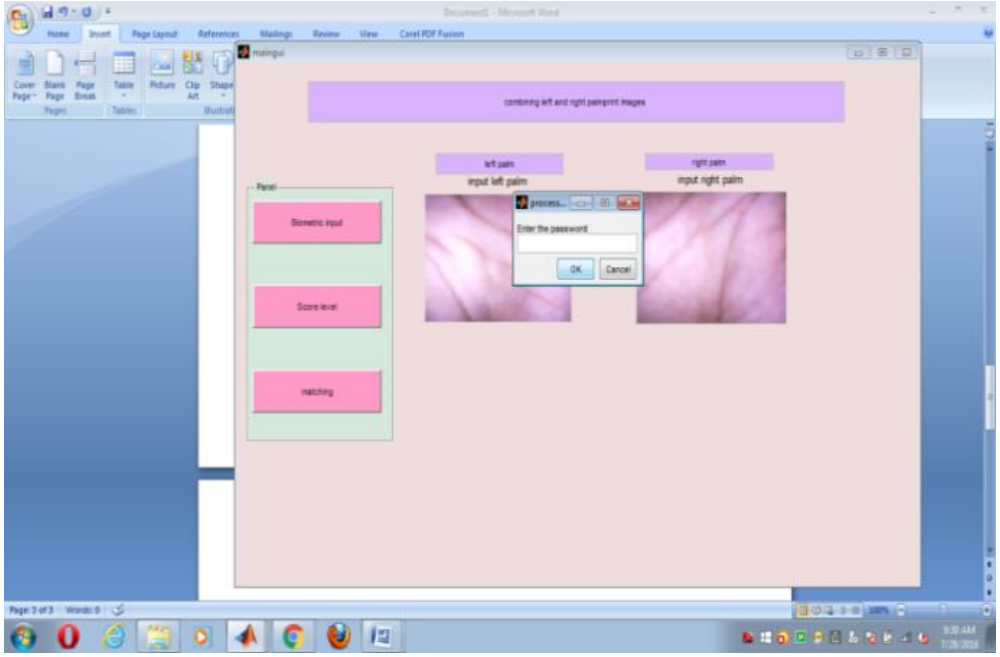


Figure 5:- This GUI denoted the request for the OTP when the palmprint of the user was authorized

Experimental Results:-

This model works well with the software tool MATLAB 8.1.0.604 in the system with the processor Intel(R)Core i3-4005U (1.70GHz) which has the RAM capacity of 4.00 GB and with the operating system Windows 7 Ultimate. The combined matching scores calculated using the RLOC for the left and right reverse palmprint images are stored in the database which has the definite value which is greater than the value 0.07 that is the combined matching score value which is calculated from the left training and left query palmprint images, the left query and right reverse training palmprint images and from the right reverse training and right query palmprint images. The table 1 below denotes samples with 17 input images from the database consisting of combined matching score values which are classified either as matched or not matched.

Table 1:- Sample palmprint image data with their matching scores and recognition status

Input Image	Combined Matching scores	Recognition
Input 1	0.0889	Matched
Input 2	0.0950	Matched
Input 3	0.0574	Not Matched
Input 4	0.0723	Matched
Input 5	0.0513	Not Matched
Input 6	0.0508	Not Matched
Input 7	0.0637	Not Matched
Input 8	0.1453	Matched
Input 9	0.1251	Matched
Input 10	0.0171	Not Matched
Input 11	0.0479	Not Matched
Input 12	0.0743	Matched
Input 13	0.0237	Not Matched
Input 14	0.0898	Matched
Input 15	0.0550	Not Matched
Input 16	0.1038	Matched
Input 17	0.0236	Not Matched

Pros of the authentication system:-

This palmprint authentication system helps the user in the following ways namely,

- The palmprint authentication system is **efficient** since it calculates the combined matching scores.
- The system is **more secure** to the user since the OTP is generated.
- It is more **reliable and accurate** for each of the users in the database.

Limitations:-

This palmprint authentication system has though been an efficient method for providing security it has certain limitations namely:

- The time required for generating three matching score values is **longer than the time** needed to produce two matching score values.
- If the user **losses the registered** mobile number or E-Mail ID then it is **hard** to authenticate.
- Any changes in the principal lines on the palmprint then the user is considered as unauthorized by the system.

Conclusion:-

This Multimodal biometric system uses the combined matching scores of the left and right reverse palmprint to give a better accuracy, and the OTP is integrated with this palmprint authentication system to process the biometric system more securely. In the future this process can be extended to the other biometric systems like finger, face, voice, signature, etc., to be more secure and unique to the user.

References:-

1. Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2015). An Efficient Framework for Enhancing User Authentication in Cloud StorageUsing Digital Watermark. International Review on Computers and Software (IRECOS), 10(2), 130-136.
2. Abdellaoui, A., Khamlichi, Y. I., & Chaoui, H. (2015). Out-of-band Authentication Using Image-Based One Time Password in theCloud Environment. International Journal of Security and Its Applications (IJSIA), 9(12), 35 - 46
3. Aboshosha, Ashraf, Kamal A. El Dahshan, Eman A. Karam, and Ebeid A. Ebeid. "Score Level Fusion for Fingerprint, Iris, and Face Biometrics."*International Journal of Computer Applications* 111, no. 4 (2015).
4. Benaliouche, Honda, and Mohamed Touahria. "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint." *The Scientific World Journal* 2014 (2014).
5. Cappelli, Raffaele, Matteo Ferrara, and Dario Maio. "A fast and accurate palmprint recognition system based on minutiae." *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)* 42, no. 3 (2012): 956-962.
6. Celik, N., N. Manivannan, W. Balachandran, and S. Kosunalp. "Multimodal Biometrics for Robust Fusion Systems using Logic Gates." *Journal of Biometrics & Biostatistics* 2015 (2015).
7. D. Zhang, F. Song, Y. Xu, and Z. Lang, “Advanced pattern recognitiontechnologies with applications to biometrics,” *Med. Inf. Sci. Ref.*, Jan.2009, pp. 1–384.
8. D. Zhang, W. Zuo, and F. Yue, “A comparative study of palmprintrecognition algorithms,” *ACM Comput. Surv.*, vol. 44, no. 1, pp. 1–37,Jan. 2012.
9. Jain, Anil K., Arun Ross, and Salil Prabhakar. "An introduction to biometric recognition." *IEEE Transactions on circuits and systems for video technology* 14, no. 1 (2004): 4-20.
10. Jia, Wei, De-Shuang Huang, and David Zhang. "Palmprint verification based on robust line orientation code." *Pattern Recognition* 41, no. 5 (2008): 1504-1513.
11. Kumar, Rajeev, Ruhul Amin, Arijit Karati, and G. P. Biswas. "Secure remote login scheme with the password and smart card update facilities." In*Proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA) 2015*, pp. 495-505. Springer India, 2016.
12. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24**(11),770–772 (1981)
13. Lee, Young Sil, HyoTaek Lim, and HoonJae Lee. "A study on efficient OTP generation using stream cipher with the random digit." In *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*, vol. 2, pp. 1670-1675. IEEE, 2010.
14. Mane, V., and Dattatray V. Jadhav. "Review of multimodal biometrics: applications, challenges and research areas." *International Journal of Biometrics and Bioinformatics (IJBB)* 3, no. 5 (2009): 90-95.
15. Morales, Aythami, Miguel A. Ferrer, and Ajay Kumar. "Towards contactless palmprint authentication." *IET computer vision* 5, no. 6 (2011): 407-416.
16. Nimmy, K., & Sethumadhavan, M. (2014, February). Novel mutual authentication protocol for cloud computing using secret sharingand steganography. In Applications of Digital Information and WebTechnologies (ICADIWT), 2014 Fifth International Conferenceon the (pp. 101-106). IEEE.
17. Raghavendra, R., and Christoph Busch. "Texture-based features for robust palmprint recognition: a comparative study." *EURASIP Journal on Information Security* 2015, no. 1 (2015): 1-9.
18. Sherawat, Heena, and Sumit Dalal. "PALMPRINT RECOGNITION SYSTEM USING 2-D GABOR AND SVM AS CLASSIFIER." *IJITR* 4, no. 3 (2016): 3007-3010.
19. Tee Connie, Andrew Teoh Beng Jin, Michael Goh Kah Ong, David Ngo Chek Ling, *“An automated palmprint recognition system”*, Image andVision Computing, Vol.23, pp.501–515, 2005.
20. Xu, Yong, Luke Fei, and David Zhang. "Combining left and right palmprint images for more accurate personal authentication." *IEEE Transactions on Image Processing* 24, no. 2 (2015): 549-559.
21. Yassin, A. A., Jin, H., Ibrahim, A., Qiang, W., & Zou, D. (2013). Cloud authentication based on the anonymous one-time password.In Ubiquitous Information Technologies and Applications (pp. 423-431). Springer Netherlands.