International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 5, May 2017

ISSN: 2394-4404

Contactless Palm Vein Recognition

Anamika Ramdas

Chandrika P R

Dhanya Nair

UG Scholar, Dept. of ECE, College of Engineering, Munnar

Biju V G

Associate Professor, Dept. of ECE, College of Engineering, Munnar

Anith Mohan

Assistant Professor, Dept. of ECE, College of Engineering, Munnar

Abstract: ***With immense amount of data being handled in our day to day lives, there is an increasing demand for more robust security systems. There are many methods for establishing security systems through passwords, patterns, fingerprints etc. Biometric methods, especially when coupled with contact less imaging of human palm vein networks offers a strong recognition method. Here we adopt two methods wherein first the original Local Binary Pattern (LBP) of the image is modified as a MF-LBP (Mutual Foreground LBP). Mutual foreground is used to improve the reduced performance of the LBP. For this, we gradient normalize the image and then the maximal principal curvature algorithm is performed giving the texture extracted image. It helps to improve accuracy and performance. LBP performs similarity matching on the extracted palm veins. MF-LBP suppresses noise by excluding the background. The second method uses matched pixel ratio to find the best matching region (BMR). Finally, the LBP matching score was fused with the score obtained on finding the BMR. Each time the user has an option to train a new image into the database and to authenticate as the authorized user.***

Index Terms: ***Biometrics, palm vein recognition, local binary pattern, mutual foreground, principal curvatures, matched pixel ratio.***

I. INTRODUCTION

The terms authentication and authorization may seem interchangeable and are used synonymously. Both these terms have a common application when it comes to security systems. It's most basic definition is "a method by which something is secured through inter working components and devices". Security systems are very necessary these days as the world is not getting any safer place to live. Each individual may have something he wishes to keep safe from the rest of the world. In the present days, the financial activities, the growth of technology and the need for preserving confidentiality is increasing hand in hand on a global scale.

All security systems have an authorized user and works on the basis of a proper authentication procedure. Logically, authentication precedes authorization. But prior to this there is the identification step. Therefore, the working can be generalized in the following three steps:

IDENTIFICATION

Identification is nothing more than claiming you are somebody. In the information security world, this is analogous to entering a username. It's not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as, and that's the next one

in process. Once the person trying to gain access to the system has identified themselves to be the authorized user, it is the duty of the system to authenticate the claim.

AUTHENTICATION

Authentication is the action of verifying the identity of a user or process. It is a process in which the credentials provided are compared to those in a database of authorized user. If the credentials match, the process is completed and the user is granted authorization for access. Authentication is how one proves that they are who they say they are. You've claimed to be that person by entering the name into the username field (in the identification part), but now you have to prove that you are really that person. Most systems use a password for this, which is based on "something you know", i.e. a secret between you and the system. Once the system identifies you to be a genuine user, you've successfully authenticated, you have now done two things: you've claimed to be someone, and you've proven that you are that person. The only thing that's left is for the system to determine what you're allowed to do.

AUTHORIZATION

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use. Assuming that someone has logged into a computer operating system or application, it may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Authorization is what takes place after a person has been both identified and authenticated; it is the step determines what a person can then do on the system.

II. LITERATURE REVIEW

Here we present a brief essence of the previously implemented ideas related to recognition systems.

According to Wenxiong Kang *et al.* [1] suggested, an improved mutual foreground LBP method is presented for achieving a better matching performance for contactless palm vein recognition. Vijaytha Chowdhary *et al.* [2] employs the vein pattern in the human palm for verification. This paper presents new approaches to improve the performance of palm-vein-based identification systems using the Gabor filter. Zamen Fadhel Jabr *et al.* [3] proposes a system for hand palm recognition and analysis based on features presented by hand palm lines. First, the region of interest (ROI) is extracted from hand palm image in order to find two groups of features, the first group contain 6 texture features represented from gray ROI whereas the second group contain 10 features extracted from white-black ROI. JinXin Xu *et al.* [4] proposes, a novel online biometric identification system based on palm vein is proposed. The characteristics extraction algorithm of palm vein image is two dimensional Fisher linear discriminant (2DFLD). This paper puts forward that projecting the palm vein image matrix based on 2DFLD directly, then the system calculates the Euclidean distance projection matrix, classification system based on the most recent distance. Roshni C Rahul *et al.* [5], presents a review of different palm vein recognition techniques that are widely used today. The analysis mainly focuses on different local descriptors which can efficiently extract vein texture.

By Anil K Jain *et al.* [6], [7], a wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. And [7], provides an overview of biometrics and discuss some of the salient research issues that need to be addressed for making biometric technology an effective tool for providing information security. According to Vishnavi N Choudhari *et al.* [8], Local binary patterns (LBP) are a type of visual descriptor used for classification in computer vision. Yingbo Zhou *et al.* [9], investigates some promising approaches for the automated personal identification using contactless palm vein imaging. In the paper, two new palm vein representations, using Hessian phase information from the enhanced vascular patterns in the normalized images and secondly from the orientation encoding of palm vein line-like patterns using localized Radon transform.

The research of Shivam Khare *et al.* [10] aims at introduction of a hand gesture recognition based system to recognize real time gestures in natural environment and compare patterns with image database for matching of image pairs to trigger unlocking of mobile devices. In the paper of Lei Yang *et al.* [11], an Open Sesame method is proposed, which employs the users' waving patterns for locking/unlocking. The key feature of the system lies in using four fine-grained and statistic features of hand waving to verify users. Taking in action all these problems, Ms. Shilpa L Dhapade *et al.* [12] presents a model, which will provide a best security to your folders. The passwords are usually short and memorable, and easily imposture. According to Faizan Ahmed *et al.* [13], face recognition from image or video is a popular topic in biometrics. Goal of this paper is to evaluate various face detection and provide complete solution for image based face detection and recognition with higher accuracy. In paper of PreethInder Singh *et al.* [14] an enhanced password based security system has been proposed based on user typing behavior, which will attempt to identify authenticity of any user failing to login in first few attempts. Now a day's most of the users are facing problem for providing the security to the folder, so that it will not be accessed by the unauthorized user. By Anitha K Jones *et al.* [15] a method of user password authentication is described which is secure (by encryption) even if an intruder can read the system's data, and can tamper with or eavesdrop on the communication between the user and the system.

The study of Renu Nagpal *et al.* [16] aims to give the basic review on the biometric techniques and discussion to facial expression recognition in still images and in videos also and to discuss both the techniques for intelligent computers or robots that are mind implemented. Paper of Nareem Bawany *et al.* [17] presents different biometric authentication

techniques with reference to the past research work and focuses on common authentication techniques and the issues faced by the users. C Nandakumar *et al*. [18] states that image authentication techniques have recently gained great attention and face recognition can be employed for vehicle security. The aim of Adil Haouzia Rita Noumeir et al. [19] is to present a survey and a comparison of emerging techniques for image authentication.

III. METHODOLOGY

The most common techniques such as face recognition, finger print recognition, voice recognition and Iris recognition are readily available even for those using smart phones. But these biometrics information can be easily forged which leads to weak security. Since vein information is internal to the human body, it is very hard to duplicate. A vascular pattern of an individual's palm is used as personal identification data for palm vein authentication. Palm vein pattern is unique biometric identity feature of the human beings which more efficiently secure our data from unlawful intervention compared to other existing biometric techniques. The main application includes banking, government offices, hospitals and passport issuing. The palm vein recognition can be done using two methods namely touch based design and contactless authentication.

Generally, the contact less palm recognition systems consist of four major steps which produce efficient result. First stage is palm vein detection i.e. the region of interest (ROI) is detected from the image so that computation need to be performed only where the required data resides and it increases the computation speed. Along with it, normalization is done which convert data image into a normalized value according to the requirement of the application. Next step is feature extraction which extracts the distinct features and the irrelevant features are eliminated in feature selection process. Final step is palm vein recognition which can be done using supervised or unsupervised techniques. Here the user who wishes to gain access has to use a camera to obtain an image and the texture extracted from this image has to compared with the images saved in the database. In this project two matching procedures have been adopted. In the first method Mutual Foreground LBP score is obtained. It has an advantage of enhancing the foreground and reducing the noise due suppressed background. Secondly a matched pixel ratio is obtained. This give best matching region between the image in the database and the image, giving a matching score. These matching scores are fused. And depending on the matched score the palm vein images can said to be matched or not matched. The entire project has been hence divided into four distinct section based on which a block diagram can be obtained as given below. This diagram gives an insight into the methods adopted for implementing the concept. Within each of these sections, a number of subsections and steps are involved which are mentioned in the sections below.

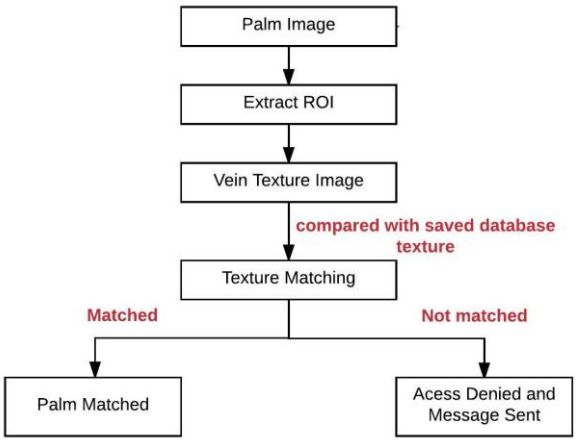


Figure 1: Schematic overview of the proposed approach

A. ROI EXTRACTION

The image obtained from the networking camera is a full sized image of the palm. But our intention is to match two palm vein texture images. Within the human palm, the palm veins are more concentrated in the middle of the palm. Hence this region is of more importance and is called Region of Interest (ROI) of the image. A ROI can be defined as a portion of the image on which one wishes to perform further processing and steps involved in achieving the desired result. This is the most important region of the image obtained and the rest of the regions find use only in extracting the coordinates of the ROI. Before extracting the ROI, certain preprocessing steps are necessary for enhancing the image, suppress the variations due to illumination differences while obtaining the image and to present the image in a form suitable for ROI extraction The initial palm image obtained using the camera is an RGB image. On this image, the first step is to perform Gaussian filtering. In image processing, a Gaussian blur (also known as Gaussian smoothing) is the result of blurring an image by a Gaussian Function After obtaining a smoothened Gaussian RGB image, it has to be converted to a gray scale image and further to a binary image. On this preprocessed image further ROI extraction takes place. By the end of the sequence of steps the coordinates of the middle region of the palm is obtained and these coordinates can be superimposed on the grayscale image to give the ROI.

Boundary Detection is the method by which the boundary pixels of the palm image are obtained. Here the boundary of the palm image and the boundary of the entire image is obtained. Edge detection is an image processing technique for finding the boundaries of objects within images. It works by detecting discontinuities in brightness. The boundary pixels are useful for extracting the RDF - Radial Distance Function i.e. the distance between the midpoint of the base line and each palm boundary pixel is taken. The outer image boundary is not considered. This helps to determine the peak and valley points. Peak points correspond to the points on the tip of each finger and the valley points corresponds to points between each fingers. The midpoint of the valley points on the either sides of both the little finger and forefinger is taken and using

ISSN: 2394-4404

this line a square is formed on the binary image. The coordinates are superimposed on the gray scale image to obtain the ROI extracted image.

B. TEXTURE EXTRACTION

After obtaining the ROI image, we need to extract the vein texture image which will be saved as database for further processing. The obtained ROI is smoothened for accuracy using filter. Neighborhood averaging can suppress isolated out-of-range noise, but the side effects is that it also blurs the sudden changes. The texture of the vein from ROI image can be obtained from a mean principal curvature (MPC) image. Mean curvature of a surface is an extrinsic measure of curvature that comes from differential geometry and that locally describes the curvature of a surface. The maximal curvature k1 and minimal curvature k2 are known as the principal curvature of the surface.

The principal curvatures k1 have a large value on the palm vein texture. So in order to get the extracted texture image of the vein, k1 curvatures are used and an MPC (Maximum Principal Curvature) image is obtained. Direct vein texture extractions do not obtain an ideal strategy for contactless palm vein method. Thus Gradient Normalization is performed on the MPC image and the obtained image is then used to find the extracted veins. Gradient Normalization is performed on an image by taking its gray value point and the module value. Gaussian curvature, average of the principal curvatures k1 and k2 and the mean curvature, product of k1 and k2 are used to find the MPC image. To get the Gaussian and mean curvature, gradient of extracted ROI image is found. The gradient field is the first derivatives of the mean image. This is done by getting the mean image from the extracted ROI image and then taking the first and second derivatives of the output image. By applying the equations using second derivatives, Mean curvature (H) and Gaussian curvature (K) are obtained.

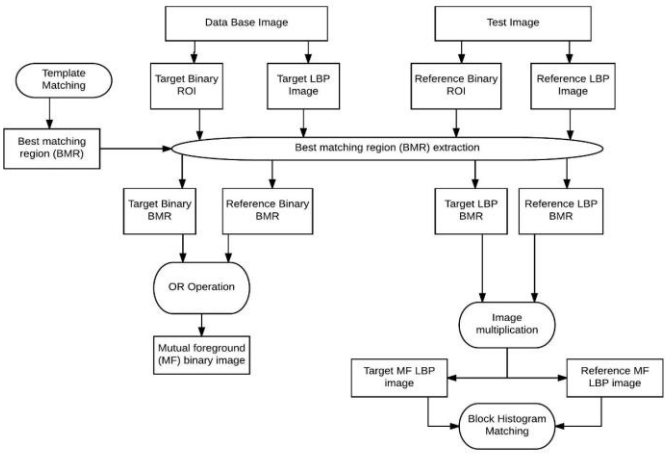


Figure 2: Block diagram of Matching

$$k_1 = H + \sqrt{H^2 - K} \quad (1)$$

$$H = \frac{(1+h_v^2)h_{uu} - 2h_u h_v h_{uv} + (1+h_u^2)h_{vv}}{2(1+h_u^2+h_v^2)^{3/2}} \quad (2)$$

$$K = \frac{h_{uu}h_{vv} - h_{uv}^2}{(1+h_u^2+h_v^2)^2} \quad (3)$$

From the equation (1) MPC image is obtained using principal curvature k1. Gradient normalization is performed on the obtained MPC image. It is the ratio of the gray value of a point to the modulus value of that particular point and the same is done for every point. The image obtained using the principal curvature and gradient normalization is further processed using K means clustering algorithm. k-means is one of the simplest unsupervised learning algorithms that solve the well-known clustering problem. The main idea is to define k centers, one for each cluster. Clusters must be placed as possible far away from each other. The next step is to take each point belonging to a given data set and associate it to the nearest center. When no point is pending, the first step is completed and an early group age is done. At this point we need to re-calculate k new centroids as barycenter of the clusters resulting from the previous step. After we have these k new centroids, a new binding has to be done between the same data set points and the nearest new center. A loop has been generated. The grouping of white and black pixels gives a better distinguishable binary texture image of palm veins in ROI.

C. MATCHING

The third stage of our work is the matching process. This is represented in fig 2. Block diagram of Matching. For the matching procedure, we require the test image and the database image. Test image is the image which is used during authentication and the database image is the one which is already saved in the folder. Database may contain more images which may help in providing more accuracy. Matching is divided into three sections. First section deals with the template matching. Usual adopted method for biometric applications is the correlation method.

Correlation for the two images is obtained and the value is compared with the threshold value. Template matching is a technique in digital image processing for finding small parts of an image which match a template image. Template Matching techniques are flexible and relatively straightforward to use, which makes them one of the most popular methods of object localization. Their applicability is limited mostly by the available computational power, as identification of big and complex templates can be time-consuming.

TEST IMAGE	DATA BASE IMAGES BEING COMPARED WITH														
	IMAGE 1			IMAGE 2			IMAGE 3			IMAGE 4			IMAGE 5		
	m	q	r	m	q	r	m	q	r	m	q	r	m	q	r
IMAGE 1	1	1	1	0.3895	1	0.6948	0.4117	1	0.7059	0.3429	1	0.7145	0.4061	1	0.6053
IMAGE 2	0.3895	1	0.6948	1	1	1	0.4103	1	0.7051	0.4264	1	0.7132	0.2347	1	0.6174
IMAGE 3	0.2347	1	0.8948	0.4103	1	0.7051	1	1	1	0.4264	1	0.7132	0.4264	1	0.6174
IMAGE 4	0.2347	1	0.7059	0.4117	1	0.7051	0.2437	1	0.6218	1	1	1	0.2487	1	0.6218
IMAGE 5	0.2107	1	0.6053	0.2347	1	0.6174	0.2437	1	0.6218	0.2335	1	0.6167	1	1	1
IMAGE 6	0.2340	1	0.6170	0.3762	1	0.6881	0.3762	1	0.6881	0.4548	1	0.7274	0.2340	1	0.6170

m- score 1 ; q – score 2 ; r – fused score

IMAGE 6 IS NOT IN THE DATABASE

Table 1: Comparison of Results

The extracted vein texture image is rotated towards both the directions (left and right) in order to get an efficient and accurate system. By rotating the image, the matching scores or the percentages are obtained for each direction and then compared in order to get the result. For templates without strong features, or for when the bulk of the template image

constitutes the matching image, a template-based approach may be effective. This method evaluates the MPR (Maximum Pixel Ratio) as the matching score and the corresponding region is marked as the Best Matching Region (BMR). Thus the MPR which is expressed as the matching score 1 is obtained. MPR is the ratio of the number of matching pixels to the total number of pixels in the matching patterns. BMR for the test image and the database image is obtained. The two BMR 's of the images are then combined using a logical OR operation in order to get an MF binary image (Mutual Foreground).

Next section in matching is the Mutual Foreground Local Binary Pattern matching (MF-LBP). For the MF-LBP matching, first an LBP image has to be obtained. Local binary patterns (LBP) is a type of visual descriptor used for classification in computer vision. An LBP feature vector is used for creating an LBP image. The MF binary image formed from the OR operation is then used to multiply the two to be compared LBP-BMRs and the two to be compared MF-LBP images are obtained. MF-LBP images are divided into n*n sub regions and calculate a grayscale histogram for each sub region to form the histogram vector. This is termed as histogram matching where histogram vector is obtained from the concatenation of all the n∗n histogram vectors. The second matching score is obtained from the correlation coefficient of the histogram vectors. The matching scores are observed for validation. The average of the two matching scores is taken and depending on the value, the output is displayed.

IV. RESULT AND DISCUSSION

The results are mentioned for each section of the process.

A. IMAGE ACQUISITION

To evaluate the method, images of different people where saved into the database. The captured images are color images but the ROI image is 8-bit gray level image. The images where captured at different sessions and with random intervals between the sessions. These images are to form a part of the database. The database has a size of 15 images. The dimensions of each image is 480*640. The time delay takes for the execution of the program to obtain the output is 2.49 minutes. This time delay was observed while using intel core i3 3217U CPU @ 1.80 GHz. The images of the genuine users are saved in the database. On execution, each image in the database is compared with every database image and the score 1, score 2 and the fused score is obtained. Score 1 corresponds to that obtained while finding the Best Matching Region and score 2 corresponds to that obtained while finding the Local Binary Pattern. The same can be obtained for an image outside the database i. e. belonging to an imposter. The images are said to be matched only if all the three scores cross their respective thresholds. These thresholds are found on a trial and error basis. It was observed that while an unauthorized user whose palm image is not saved in the database tries to access the system, a matching score as high as 0.7 was obtained. So in order to reduce the probability of error, a threshold value of 0.85 to 0.9 was chosen. During the matching process, this test image is compared with all the images in the database. This sequential comparison is the key factor in deciding the delay. As the number of images in the database increases, it enhances the performance but simultaneously increases the delay. The resultant scores obtained Images 1 to 5 in the database and Image 6, not within the database are sequentially compared with all images in the database are shown in the table 1 and the stepwise outputs of various stages are given in the following sections.

B. ROI EXTRACTION

The results for the various steps involved in the preprocessing and ROI extraction is given below.

On applying the Gaussian filtering, we get a smoothened out RGB image. This image is converted to binary image from which the boundary of the palm is obtained. The radial distance function is used to obtain the peak and valley points from which the coordinates of the ROI image is formed. This on superimposing on the gray scale image gives the ROI extracted gray scale image. The resultant images are shown in Fig 3.

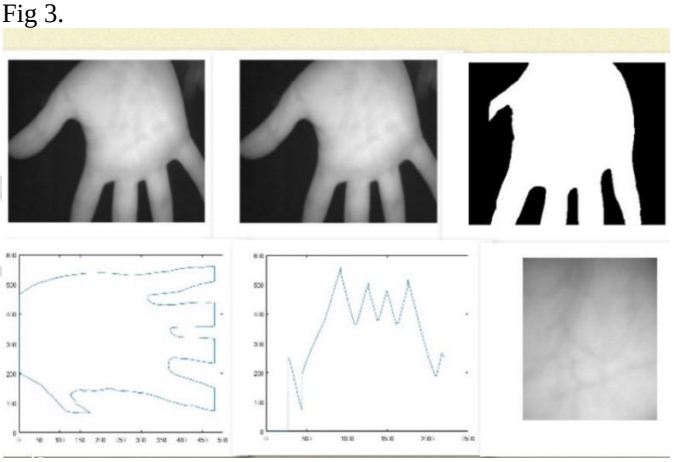
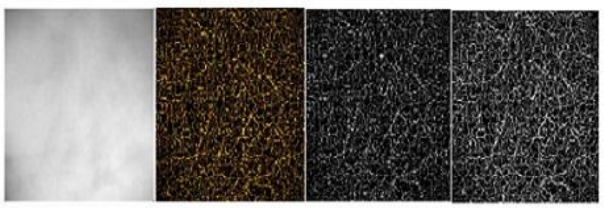


Figure 3: ROI Extraction Results from TOP left: RGB image, Gaussian image, Binary image, Palm Boundary, Peak and Valley points, Extracted ROI image

C. TEXTURE EXTRACTION

The ROI image is smoothened and the derivatives are obtained as per the equations in order to find the mean curvature and Gaussian curvature. Using both the curvatures the MPC image is obtained and it is further gradient normalized. Employing k means clustering binary image of the vein texture of palm is obtained. The resultant images are as shown in Fig 4.



(a) (b) (c) (d)

Figure 4: Illustrations of ROI extraction: (a) mean image, (b) MPC image, (c) binary image, and (d) final vein texture image

D. MATCHING

After the extraction of texture, the user can either train the image into database or continue to authenticate as a valid user. For the valid users training is done and further authentication is done each time when he needs access. If user selects for training, then the texture extracted image of the palm image is saved to the database. Otherwise if the user is opting for authentication then test image is compared with all the database images and declares either matched or not.

V. CONCLUSION

Various studies have utilized LBP for vein image recognition due to its higher texture representation ability. However, mostly all ideas where designed to operate on the entire palm image. Therefore, in this project we adopted to use an ROI which corresponds to region where palm veins are most densely concentrated, the method is able to highlight the texture in palm vein images and achieve better recognition performance. Another major factor used by us to improve performance is the non-contact imaging. This adds on advantage, because of immunity from differences due to dirt on the palm. It can also be seen that the use of MF-LBP has improved the performance over ordinary LBP method by suppressing the background and the noise within. To improve the matching accuracy of the to-be-matched regions from palm vein images we use two matching strategies instead of one and fuses the scores of the two matching strategies. Also the use night vision networking camera provides images under all lighting conditions and better quality images. To demonstrate the effectiveness of our proposed method, Palm print Image Database, including several images from many individuals, was adopted for testing and a low EER was achieved. In addition to the above mentioned improved recognition performance, the proposed method also has other advantages. For example, the palm vein extraction method can also be used in palm print extraction. Therefore, the method can be extended to palm print recognition and achieve better performance after employing a fusion strategy. The proposed method focuses on contactless palm vein images, which is suitable for real world scenarios.

REFERENCES

[1] Wenxiong Kang, Qiuxia Wu, "Contactless Palm Vein Recognition Using a Mutual Foreground-Based Local Binary Pattern," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 9, no. 11, NOVEMBER 2014.

[2] Vijayta Chowdhary, Kamini Verma, Himanshu Monga, "Human Identification Using Palm-Vein Images Using Gabor Filter," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, no. 7, July 2014.

[3] Zamen Fadhel Jabr, "Hand Palm Recognition using Combination of Freeman Chain Code and Texture Features with Fuzzy Logic Classifier," International Journal of Computer Science and Mobile Computing, vol. 4, no. 3, pp. 585-598, March- 2015.

[4] JinXin XU, "An Online Biometric Identification System Based on Two Dimensional Fisher Linear Discriminant," in 8th International Congress on Image and Signal Processing (CISP 2015), 2015.

[5] Roshni C Rahul, Merin Cherian [Manu Mohan C M, "Literature Survey On Contactless Palm Vein Recognition," International Journal of Computer Science Trends and Technology (IJCST), vol. 3, no. 5, Sep-Oct 2015.

[6] Anil K. Jain, Fellow, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition," IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, vol. 14, no. 1, JANUARY 2004.

[7] Anil K. Jain, Fellow, Arun Ross, Sharath Pankanti, "Biometrics: A Tool for Information Security," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 1, no. 2, JUNE 2006.

[8] Vaishnavi N. Chaudhari1, Vijay B. Baru2, "A Survey on Improved Authentication Technology-Contactless Palm Vein Recognition," International Journal of Innovative Research in Science, Engineering and Technology.

[9] Yingbo Zhou, Ajay Kumar, "Contactless Palm Vein Identification using Multiple Representations".

[10] SHIVAM KHARE, "Finger Gesture and Pattern Recognition Based Device Security System".

[11] Lei Yang, Member,Yi Guo,Xuan Ding,Silun Wang Jinsong Han, Yunhao Liu, "OpenSesame: Unlocking Smart Phone through Handwaving Biometrics," IEEE TRANSACTIONS ON MOBILE COMPUTING.

[12] Ms. Shilpa. L. Dhapade, "Implementation Of A Graphical Based Password For Folder Cryptography," International Journal of Engineering Research Technology (IJERT).

[13] Faizan Ahmad, Aaima Najam,Zeeshan Ahmed,, "Image-based Face Detection and Recognition," IJCSI International Journal of Computer Science Issues, vol. 9, no. 1, November 2012.

[14] PreetInderSingh,"EnhancedPasswordBasedSecuritySystemBasedonUserBehavior using Neural Networks," Information Engineering and Electronic Business, vol. 2, pp. 29-35, 2012.

[15] Anitha K Jones, "Password Authentication With Insecure Communication".

[16] Renu Nagpal, Pooja Nagpal, Sumit Malhotra, "BIOMETRIC TECHNIQUES AND FACIAL EXPRESSION RECOGNITION-A REVIEW," Journal of Global Research in Computer Science, vol. 3, no. 11, November 2012.

[17] Narmeen Bawany, Rabia Ahmed and Qanita Zakir, "Common Biometric Authentication Techniques: Comparative Analysis, Usability and Possible Issues Evaluation," Research Journal of Computer and Information Technology Sciences.

ISSN: 2394-4404

[18] C. Nandakumar, G. Muralidaran and N. Tharani, "Real Time Vehicle Security System through Face Recognition," International Review of Applied Engineering Research. ISSN 2248-9967, vol. 4, no. 4, pp. 371-378, November 2014.

[19] Adil Haouzia Rita Noumeir, "Methods for image authentication: a survey," Springer Science, Business Media, 2007.