Review on Multiple Biometric Fake Detection System

Asmita A. Patil
M.E. Student, Department of Electronicss & Telecommunication
Bharati Vidyapeeth's College of Engineering for Women, Pune-43
Savitribai Phule Pune University
Maharashtra, India

Prof. S. A. Dhole
Department of Electronicss & Telecommunication
Bharati Vidyapeeth's College of Engineering for Women, Pune-43
Savitribai Phule Pune University
Maharashtra , India

***Abstract*—Biometric Access control has gained popularity over the years due to limited success of physical checks in safeguarding vital assets in a world that grows more dangerous day by the day. Hence, biometric security system plays very important role in everyones life as security. Biometric system is a security system which provides conditional access after scanning for unique physical characteristics for authentication. A reader scans the face, fingers, irises, veins and palms for unique traits, then converts this data into digital format called template and then uses a complex algorithm to make a match. But, fake , synthetic or reconstructed sample is a emphasis problem in biometric authentication. These biometric systems are highly vulnerable to different types of attacks such as some types of synthetically produced artifact (e.g.,fake fingerprints ,photoprint of iris image or face mask),or sometimes tries to mimic the behavioral characteristics of the user (e.g.,gait,signature) to delusively access the biometric system. Hence, new and efficient protection measures based on hardware and software have been developed to stop these attacks. Thus,there is need to review all these efficient and reliable protection measures for all biometrics so that we can distinguish sophisticated, robust and user friendly system for users to secure their life.**

Keywords -Biometric Access Control(BAC),security system, attacks , delusively,review, robust, user- friendly

I. Introduction

Now a days, everyone wants their security in their life. If we talk about security, then first name comes in mind is that Biometrics[1][7]. So, we can say that Biometrics is a sparkling word in the world of science and technology. In last 2 decades, there are so many evaluation took place in the biometric system. But, these biometric systems are vulnerable to various types of fraudulent attacks to access the biometric systems. Hence, there is need to study of various attacks and the methods for the prevention from these attacks and hence, biometric security has became a major field of research. Various publication in this areas, various organizations focused on vulnerability assessment, various groups and laboratories specialized in the evolution of biometric security[1][2] has involved in the research of biometric security system. Hence, various systems and measures have been developed to reduce these vulnerabilities which again classified based on users behaviour and their characteristics.

These different types of threats namely direct-attacks or spoofing attacks[2] are reason for motivation to study the vulnerabilities against such types of fraudulent attacks. This attack uses the modalities in the form of the fingerprint, the face, the iris, the handprints and the signatures. In this attacks, intruder tries to mimic the behaviour of the genuine user (e.g.,gait, signature) to access the system illegally ,or uses some type of synthetically generated samples(e.g. gummy fingerprint , face mask , or printed images of face and iris).As normal eye vision cannot distinguish between real and fake samples, many biometric systems are fail to identify fake traits.Already, aforesaid works have been done in this area, but they are not that much effective. Hence, there is necessity to study, propose and develop the specific protection methods for such threats in biometric systems. Researchers and scientist are in search of specific method which make biometric system robust and highly secure by detecting the fake samples and rejecting them.

Among all the anti-spoofing techniques such as challenge-response method, researchers had been paid more attention on liveness detection techniques because of their different physiological properties which distinguishes between real and fake traits. This techniques represents a challenging engineering problems as this have to satisfied fallowing specific demanding requirements[3]:1)non-invasive, means technique should not be harmful to individual or users should not be in excessive contact with the techniques, 2)user friendly, the technique should not be keen to use it, 3)fast, the technique should produce the results fast to avoid excessive contact of users to sensors.4)low cost, cost should be minimum so that wide use can be expected, 5)performance ,the technique should not reduce the performance of the biometric system while using it. Hence, Liveness detection assessment is useful in fake biometric detection. In liveness detection techniques, many systems have been developed but those methods have a lack of generality. To overcome this limitation, image quality assessment is play very important role. Image quality assessment is based on the assumption that fake image captured in the attempt of attack will have different quality than a real samples acquired in normal operation scenario. Based on this

assumption, we can be distinguishing real and fake sample by using image quality measures[3].

II. RELATED WORK

As biometrics is based on physiological and behavioural properties, fingerprint, iries,faces are mostly used as a biometric system because every person has unique features. In last few years, handprint and finger vein are also used as biometric system because of its complicated and differentiable features presents inside the body which cant be duplicate.

If we talk about the face recognition, most of the state-of-the art facial biometric systems are basically vulnerable to attacks without anti-spoofing measures. We can fool the system easily even displaying the simple photograph of person in front of camera. To avoid this vulnerability, many researchers have been put efferts to develop a system. The research done by Pan et al. [4] exploited the observation that humans blink eyes once every 2-4 seconds and proposed an eye blink-based anti-spoofing method which uses Conditional Random Field framework to model and detect eye-blinking. Kollreider et al. [5] proposed an optical-flow based method to capture and track the subtle movements of different facial parts, which assumes that facial parts in real faces move differently than on photographs.

Some anti-spoofing methods are based on the analysis of skin properties such as skin texture and skin reflectance. For this, Li et al. [6] suggested a method for detecting print-attack face spoofing. This method is based on the analysis of 2D Fourier spectra, describing that photographs are usually smaller in size and they would contain fewer high frequency components compared to real faces. Such an approach may work well for down-sampled photos but is likely to fail for higher-quality images. The database used in this experiments is unfortunately not publicly available.

Recent work propsed by J. Maatta et.al [8] present a very effective anti spoofing method for face recognition. This approach analyzed the texture of the facial images using multi-scale local binary patterns (LBP) and encoded the micro-texture patterns into an enhanced feature histogram. The results are then fed to a support vector machine (SVM) classifier which determines whether there is a live person in front of the camera or not. Extensive experiments on a publicly available database (NUAA Photograph Imposter Database) containing several real and fake faces showed excellent results compared to previous works. In this method, fine differences between the images of real face and those of face prints are taken and then design a feature space which emphasizes those differences. If we talk about the real and dummy faces, the differences between real faces and face prints concludes that human faces and prints reflect light in different ways as a human face is made of complex non rigid 3D object and a photograph can be act as a planar rigid object. This may creates different specular reflections and shades. The surface properties of real faces and print images i.e. pigments, are also not same. In addition, face prints usually contain printing quality defects that can be detected with micro-texture patterns. Furthermore, spoof attacks when executed with face prints tend to engender some overall image blur.By image quality assessment and characterization of printing artifacts, they derive a facial representation or a feature space which is able to capture typical real and fake face images characteristics. Hence, the main idea of this approach has been emphasizing the micro-texture differences in the feature space. This method adopted the local binary patterns [8], a powerful texture operator, for describing not only the micro-textures but also their spatial information. The vectors in the feature space are then fed to an SVM classifier which determines whether the micro-texture patterns characterize a live person or a fake image. Also recently, S.A.Dhole et.al [9] reviewed on Face Recognition Using Curvelet Transform which reduces the problem in selection of features from face images. This face identification technique is robust to orientation of the face image under illumination condition same as appearance based and texture based feature extraction.

In the case of fingerprint, many hardware and software technologies have been designed and implemented to capture and process fingerprint. Thought it has advantages, detecting liveness of a presented available fingerprint sample has become a challenging research issue [1][[12], because of vulnerability to various attacks[2]. There are many fingerprint liveness countermeasures have been proposed which based on determining the presence of a user by different responses. This can be from either votive source such as passwords, smart cards, and multiple biometrics (which makes spoofing more difficult), or involuntary liveness detection by pulse oximetry, blood pressure, and heartbeat. Although many fingerprint liveness countermeasures to avoid spoof attacks are developed but the majority lack is in results and additional hardware requirements, and do not operate efficiently in different environments such as indoors, outdoors, summer and winter. In addition, there are a number of other limitations with the required hardware i.e. price, size, and the user convenience and in some cases, an artificial fingerprint possibility fool the system.

Image quality assessment method is quite good method to determine the difference between real and fake fingerprints. Hence, on the basis of this method, Detection of fine movements are calculated based on Papillary Lines[13].The solution is based on the analysis of fine movements of the pap-illary lines of the fingertips and on measurements of the distance of the fingertip surface to a laser sensor, respectively and this system is compact enough to be integrated with the optical fingerprint sensors. There are two approaches to measure fine movements of papillary lines, both based on optical principles. The first solution for this is based on a close- up view of the finger-tip captured with a CCD camera; the second one is the distance measurement with a laser sensor.Camera system based on the liveness detection techniques is to analyze the video streams. ingle frames of the video sequence are processed to find unique points (e.g. minutiae, sweat pores), which can be used as reference points to identify a region of the fingerprint that will be further analyzed.Humans heartbeat causes small volumetric changes on the fingertip. As the fingertip expands, the distance between

the papillary lines grows. These fluctuations are small, but measurable and show similarities to a cardiogram. The video stream (or the sequence of images) is analyzed and filtered so that these movements can be observed. Cheating this method by applying a silicon layer (or another attack method) on the finger should change these characteristics considerably, so that such attack can be easily detected.The second optical method for liveness detection is a laser distance measurement. The lens optical system and the CCD camera for acquisition of the complete fingerprint are the same which used in camera system based method. In contrast to the solution, the laser distance measurement module, based on the triangulation principle, is placed to the right side of the glass plate, which is L-shaped here. The user places his finger such that it is in contact with the horizontal and the vertical side of the glass plate.

Second image quality based method for liveness detection of fingerprint is Band Selective Fourier Spectrum method[14]. The 2D spectrum of a fingerprint image mirrors the distribution and strength in ridge lines spatial frequencies. The texture of ridge-valley of the fingerprint produces a ring pattern around the center in the Fourier spectral image and a harmonic ring pattern in the subsequent ring. Both real and fake fingerprints produce these rings, having different amplitudes in different spatial frequency bands. Originaly, real fingerprints show stronger Fourier spectrum in the ring patterns than the fake. This method classifies the real and the fake fingerprints by analyzing the band-selective Fourier spectral energies in the two ring patterns. There are differences between live and fake spectral images for overall spectral energy. These differences are based on the size of the foreground of fingerprint image, the distribution of histogram, and the performance of the sensors. The algorithm describes the procedure for computing the energy in three intervals. Firstly, the fingerprint image is converted into the spatial frequency domain with the help of Fast Fourier Transform. To avoid a big value contrast, logarithm operations are applied to the transformed image, and then the result image is normalized. Subsequently, the upper half-circle of the spectral image is converted into a rectangular coordinate using the homogeneous rubber sheet model presented by Daugman and then projected to the frequency axis. Finally, these energies are accumulated in the three intervals such as 25 59, 60 100, 1 100.

Also, in recent work, the liveness detection is done by using perspiration method[15]. This is based on detection of the perspiration phenomenon between the human skin and other material under different conditions. Even though it has above advantages, it is usually possible to deceive fingerprint systems by presenting a self-manufactured synthetic or dismembered finger. However, Derakhshani et al [16] introduced one method to provide fingerprint vitality authentication in order to solve this problem. In their approach, atony through fingerprint examination with capacitive scanners (based on detection of the sweating pattern from two consecutive fingerprints), is captured between 5 seconds and a final decision about atony is made by a trained neural network. In addition, there are some other methods such as enhanced perspiration detection algorithm, which improves Derakhshanis work not only including other fingerprint scanner technologies but also the use of larger, more diverse data sets along with shorter time windows. Another technique proposed is based on the statistics of signal processing on wavelet to detect the perspiration phenomenon. However, this technique has less ability for users because of low moisture and highly perspiration-saturated fingers, and may not exhibit liveness as the specific changes in moisture is necessarily observed. Hence,efficiency of such system can be improved by investigating the terms regarding to accuracy and environmental conditions.

If we talk about the biometric system which based on iris recognition, it is more accurate and plays role as important identification technique. As the iris of a human eye has unique feature for individuals, hence it is reliable source for identification purpose. The performance of the iris to use as a biometric is highly dependent on the quality of the sample. Some major factors destabilize iris recognition are focus and motion blur (due to hand-held sensors), off-angle (pose), occlusion (eye lashes, hair, and spectacles), dilation/constriction, and resolution. To compensate for this destabilization, iris capture systems developed early were bulky and cumbersome to use. However, emersion of newer and compact sensors, it becomes greater easy to measure the quality of the captured sample. Distinct to fingerprints, iris patterns dont exhibit any expected behavior of the features, thats why, quality is measured in the form of the impact of the covariate on the image.

Chen et al. proposed[17] a quality metric method for iris which based on the spectral energy in local regions. First of all, Segmentation of iris is done using Canny edge detector and Hough transform.Then, occluded regions that may occur due to eyelashes are removed using intensity thresholding. Then, 2D Mexican hat wavelet decomposition is applied on iris region, and the product of responses from multiple scales (usually three) is used as the overall response. Then the iris region is partitioned into concentric bands with fixed width (8 pixels). The energy from these concentric regions are separately computed and combined into a single quality score. Multiple overlapping filtering of the iris region approach is very essential for encoding the fine edges exhibited by the iris muscle tissue. The approach is also used for feature extraction. A similar approach is proposed by A Abhyankar et.al.In another approach, Kelka et al[18] proposed quality assessment for iris images based on the evaluation of eight quality parameters and these are defocus, motion blur, offangle, occlusion, specular reflectance, illumination, and pixel count. These individual quality scores has the nature of both image-based and biometric-specific in nature. Further, Dempster-Sheffer theory-based fusion is used to combine these individual scores to obtain a single quality value. The method for evaluating quality measures is used on the iris dataset of the West Virginia University (WVU) multimodal biometric database , by using the quality bins approach.

Now a days, non-ideal iris imagery becomes a important research topic which based on iris recognition in the visible spectrum. On this approach ,H. Proenca [19] has proposed a

operation on visible iris imagery .by using quality assessment algorithm. In this ,seven quality attributes has been estimated which is similar to Kelka et. al[18]. Here, the lowest quality images feom the database are ignored,hence, improvement in recognition rate is tested by using algorithm. Zuo et al. [20] present another approach on iris quality assessment technique that based on match score evaluation. The quality of a sample is measured using statistical fusion of two quality metrics of genuine and imposter scores by utilizing pre computed distributions: (a) statistical error between the distribution of genuine and imposter scores and (b) normalized difference between the sample match score and some hidden points selected from the genuine and imposter distributions. This approach is improved later with the help of multivariant prediction i.e. feed-forward neural networks to better map quality values with matching performance. Du et al. [21] also present a research work on iris imagery by using a feature correlation approach. This measure can differentiate between natural iris patterns belongs to the artifacts that occur during compression. From this, it is observed that the correlation between consecutive rows of an iris template increases with compression as the less significant features are lost. This metric uses this distance measure of randomness of features as a measure of biometric quality of an iris sample. In recent work , J. Galbally et.al[3]. presented liveness detection method using a image quality assessment for iris image which find out the real and fake sample by determining the quality measures. The same paper presented a liveness detection for face and fingerprint.

Another physiological characteristics from which we can identify individuals is finger vein. Biometrics system is mostly used in forensic science, but, there is vast civilian applications based on biometrics.Hence, everywhere we cant use single biometric as every possible application needs different requirement. And,now a days, finger vein is most new pattern used in the identification method as each finger has unique vein patterns . Finger vein based biometric system is newest identification techniques because it has several benefits other than various hands based biometric methods. First of all, because of internal feature, the finger vein pattern is hard to replicate. Also, the quality of the captured vein pattern is not easily influenced by skin conditions. Moreover, the size of the device can be made much smaller than other vein based identification methods and this finger vein recognition does not require contact between the finger and sensor for a hygienic viewpoint.

In the vein recognition, K.Park et. al.[22] has proposed new algorithms for finger vein recognition having three advantages and contributions. Firstly, local information of the finger veins is extracted based on Local Binary Pattern (LBP) without segmenting accurate finger vein regions. Second, the global information of the finger veins was extracted based on Wavelet transform and third, two score values by the LBP and Wavelet transform were combined by the Support Vector Machine. N. Miura et. al. have achieved robust pattern extraction for finger vein based on finger-vein patterns in which finger vein image is captured under infrared light contains the vein pattern and irregular shading produced by the various thicknesses of the finger bones and muscles. This proposed method acquires the finger-vein pattern from the distorted image by using line tracking which starts from various positions . In another approach like modified Hudson distance (MHD)-based minutiae matching method , vein pattern extraction is performed to extract minutiae points. But, vein pattern extraction procedures consumes the time. In addition, a finger image includes noise factors such as Shadows or fingerprints, due to which recognition accuracy decreases. Also, in finger-region extraction methods, distortions is added due to the stretching procedure in stretched quadrangle finger vein images.

In recent years, palm print is playing important biometric approach like iris, finger vein. A palm has a wider area and consist of more complicated vascular pattern. Hence, it contains a lot of differentiating features for identification purpose of individuals. If we talk about the palm print, several techniques have been proposed based on different approaches. I. Sarkar et al [23] proposed review on the palm vein authentication device based on blood vessel patterns to a identify persons factor. In this approach,a person inserts a smart card into the sensor device and holds her hand over the reader. The vein pattern is instantly aquired using a completely safe near-infrared light. Then reader converts the image into an encrypted biometric template and compares it to the template present on the smart card (1 to 1 matching) or templates presents in the database (1 to N matching). M. Watanabe et al presents a biometric authentication approach similar to previous work using except contactless approach between palm and sensor which used in public areas. Y. Zhou et al [24] proposed two palm vein representations, which based on Hessian phase information from the enhanced vascular patterns in the normalized images, and from the orientation encoding of palm vein line-like patterns based on localized Radon transform. After observing the experimental results, the proposed representation using localized Radon transform achieves better or similar performance than other alternatives offering significant computational advantage for online applications. This approach achieves the best equal error rate of 0.28

Another approach is proposed by Y.B. Zhang et.al.[25] about personal authentication using palm vein. This developed system consists of : 1) Capturing of infrared palm images; 2) Region of Interest detection ; 3) Extraction of palm vein by multiscale filtering; and 4) Matching. After performing the experimental results, the recognition rate of this system is fine but not good to become a real system. The capture device used in this scheme is very sensitive to the outside lights. The outside lights can affect the inside infrared light source so that some image quality became very poor. Image quality can be improve by using better capture device hence the system performance can be better. S.A.Dhole et. al.[26] proposed Palm Print Recognition Using Contour let Transform based on texture approaches, line approaches and appearance approaches. Here the palm print image is acquired from the digital camera as scanner and pagged system has lower user

acceptability.Then palm print cropping is done to detect the actual palm print image from hand images. ROI extraction are done by using steps fallowed RGB to gray, Thresholding, edge detection, finding maxima and minima points, extraction of ROI. After detecting ROI, next step is to obtain features that are provided to a palm print recognition system and these features can be principle line, appearance, texture. After extraction the features, input image is compared with the features in the database to get results.

CONCLUSION

This paper presents the analysis of the proposed techniques or methods that used in biometric systems like face, fingerprint, iris, finger vein and palm prints. From this techniques it is noticed that researcher mostly give preference to the liveness detection method as it has more reliable, faster, user-friendly than the non-liveness detection techniques. Previous proposed techniques is mostly focused on the authentication and detection motive. But,they are unable to restrict the vulnerabilities that are in the form of dummy fingerprints,face mask, printed photo of iris image, also in the form og behavioral characteristics like gait and signature. Also, in liveness detection techniques, Image Quality Assessment(IQA)plays an important role that can distinguishes between real and fake traits by calculating image quality measures.

ACKNOWLEDGMENT

I would like to thank my all the staff members of BVCOEW,Pune for being moral support through the period of my project study in BVCOEW, Pune whose help and shared knowledge was the main support to my review work in project.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, Biometric recognition:Security and privacy concerns, IEEE Security Privacy, vol. 1, no. 2,pp. 3342, Mar./Apr. 2003.

[2] K. A. Nixon, V. Aimale, and R. K. Rowe, Spoof detection schemes, Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008,pp. 403423.

[3] J. Galbally, S. Marcel, and J. Fierrez, Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition, IEEE Transactions on Image Processing, VOL. 23, NO. 2, FEBRUARY 2014

[4] G. Pan, Z.Wu, and L. Sun. Liveness detection for face recognition. In K. Delac, M. Grgic, and M. S. Bartlett, editors, Recent Advances in Face Recognition, page Chapter 9. INTECH,2008.

[5] X. Tan, Y. Li, J. Liu, and L. Jiang. Face liveness detection from a single image with sparse low rank bilinear discriminative model. In Proceedings of the 11th European conference on Computer vision: Part VI, ECCV10, pages 504517, Berlin, Heidelberg, 2010. Springer-Verlag.

[6] J. Li, Y. Wang, T. Tan, and A. K. Jain. "Live face detection based on the analysis of fourier spectra". In Biometric Technology for Human Identification, pages 296303, 2004.

[7] Mrs.Dhole S.A. Dr. Prof. Patil V.H, Review of Multimodal Biometric Identification Using Hand Feature and Face, Bulletin of Electrical Engineering and Informatics, IAES Indonesia section in collaboration with UAD,Vol.1, No.3, pp. 179-184, September 2012

[8] J. Maatta, A. Hadid,and M. Pietikainen, "Face Spoofing Detection From Single Images Using Micro-Texture Analysis", IEEE Transaction of Image processing, 2011

[9] Mrs.Dhole S.A. Dr. Prof. Patil V.H, Face Recognition Using Curvelet Transform, International Journal of Applied Engineering Research, Volume 10, No. 14 (2015), pp.33949-33954, August 2015(Impact factor-0.166),Scopus indexing

[10] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li. Face liveness detection by learning multispectral reflectance distributions. In International Conference on Face and Gesture, pages 436441,2011

[11] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans. Pattern Anal. Mach. Intell.,24:971987, July 2002.

[12] Mrs.Dhole S.A. Dr. Prof. Patil V.H., Minutiae Based Fingerprint Identification, Journal of Signal and image Processing, Volume 3, Issue 3, March 2012, PP.122 125(Impact factor-6.94)

[13] Martin Drahansky, Dana Lodrova, Liveness Detection for Biometric Systems Based on Papillary Lines International Journal of Security and Its Applications Vol. 2, No. 4, October, 2008

[14] C.Jin, H. Kim,S. Elliott, "Liveness detection of fingerprint based on band-selective Fourier spectrum", in 10th International Conference on Information Security and Cryptology,2007.

[15] M. Sepasian, C. Mares, and W. Balchandran ,"Liveness and Spoofing in Fingerprint Identification: Issues and Challenges", in Recent advances in Computer Engineering and Apllications

[16] R. Derakhshani, S. Schuckers, L. Hornak, L.O'Gorman, Determination of vitality from a noninvasive biomedical measurement for use in fingerprint scanners, Pattern Recognition. v36 i2.383-396.

[17] Y Chen, S Dass, A Jain, Localized iris image quality using 2-D wavelets,Advances in Biometrics, Lecture Notes in Computer Science, vol. 3832.(Springer, Berlin Heidelberg), pp. 373381

[18] ND Kalka, J Zuo, N Schmid, B Cukic, Estimating and fusing quality factors for iris biometric images. IEEE Trans. Syst. Man Cybern. 40(3), 509524 (2010)

[19] H Proena, Quality assessment of degraded iris images acquired in the visible wavelength. IEEE Trans. Inf. Forensics Secur. 6(1), 8295 (2011)

[20] J Zuo, F Nicolo, NA Schmid, H Wechsler, Adaptive biometric authentication using nonlinear mappings on quality measures and verification scores, in Proceedings of IEEE International Conference on Image Processing (Hong Kong, 2629 September 2010), pp. 40774080

[21] Y Du, C Belcher, Z Zhou, R Ives, Feature correlation evaluation approach for iris feature quality measure. Signal Process. 90(4), 11761187 (2010)

[22] F. E. Mohammed, Eman M. ALdaidamony and A. M. Raid, Multi Model Biometric Identification System: Finger Vein and Iris, in International Journal of Soft Computing and Engineering (IJSCE),Volume-4 Issue-4, September 2014,50

[23] Ishani Sarkar, Farkhod Alisherov, Tai-hoon Kim, and Debnath Bhattacharyya, Palm Vein Authentication System: A Review, International Journal of Control and Automation, Vol. 3, No. 1, March, 2010.

[24] Yingbo Zhou, Ajay Kumar, Contactless Palm Vein Identification using Multiple Representations, Department of Computing, The Hong Kong Polytechnic University

[25] Yi-Bo Zhang, Qin Li, Jane You, and Prabir Bhattacharya Palm Vein Extraction and Matching for Personal Authentication, Biometrics Research Centre, Department of Computing, Concordia University,

[26] Mrs.Dhole S.A. Dr. Prof. Patil V.H, Palm Print Recognition Using Contour let Transform,International Journal of Video Image Processing and Network Security,Vol: 15 Issue: 04, pp.6-11(Impact factor-0.938)