FINGER-VEIN EXTRACTION AND AUTHENTICATION FOR SECURITY PURPOSE

Aayush Sinha
B. Tech, Computer Science and Engineering Department, SRM University, Kattankulathur. Chennai. India
aayush.sinha7@gmail.com

Ajay Bhadu
B. Tech, Computer Science and Engineering Department, SRM University, Kattankulathur. Chennai. India
ajaybhadu2929@gmail.com

A. Selva Kumar
Assistant Professor, Computer Science and Engineering Department, SRM University, Kattankulathur. Chennai. India
selvakumar.a@ktr.srmuniv.ac.in

S. Nirmal Sam
Assistant Professor, Computer Science and Engineering Department, SRM University, Kattankulathur. Chennai. India
nirmalsam.s@ktr.srmuniv.ac.in

Abstract
Biometrics have been used for authentication and security for a long time. The most common biometric methods are fingerprint, iris scanner, face recognition, voice recognition, etc. But the fact is that these methods are not failsafe or fully secure. Hence, newer methods have been introduced in recent times that are more efficient and reliant. One of the best methods of biometric authentication is finger-vein technology. It is one of the most secure, reliable and efficient biometric mechanisms. In this paper, we study the complete implementation of finger-vein authentication system and use it as a biometric method to provide vehicle security.

The project has a software and hardware component. The software component deals with the complete image processing process using MATLAB and checking for authenticity of the input image. We propose a finger-vein technique that uses HAAR transform in the Discrete Wavelet Transform to perform the feature extraction and SVM classifier for training the data set. The performance is measured using the mean squared error (MSE) and peak signal to noise ratio (PSNR). Hardware component uses the Arduino microcontroller which will be used to decide whether the ignition will be switched on or not depending on the result of the authentication.

Key Words
Finger-vein, Biometrics, Wavelet Transforms, Vehicle Security, DWT, SVM, Security

Introduction

Historically, many methods for security of private information or a device have been invented. Most common means of protection used are passwords or PINS (personal identification numbers), but the security provided by these methods are minimal as they can

easily be bypassed using trivial methods. There is always the risk of the password being forgotten or a simple password being used. Many hacking methods are there to bypass such methods. Hence to improve the security greatly, biometric methods for security have been introduced. Biometric methods are methods that use features of human beings for authentication. Since the features such as fingerprints [1], voice, iris [2], etc are unique in each person, the security provided is very high when compared to conventional methods like passwords. These may include fingerprints, palm prints, iris scanners, voice recognition, face recognition etc.

As we show subsequently, the current biometric methods are subject to risk and failure. Face recognition system depends on many external factors such as lighting, hair style of the person, etc. Aging also alters the appearance of a person significantly. This makes face recognition very less secure. Fingerprint can easily be forged or tampered and any changes to the external skin of the finger can pose a problem for authentication. A recorded voice can be used to bypass a voice recognition system. Events such as a cold can change the voice of a person. A high resolution photograph of a person can similarly be used for bypassing a face recognition system. Iris scan methods are expensive and take a lot time for authentication.

The need of a biometric method that is reliable and fast is solved by the finger vein [3] recognition system. This is a method of biometric authentication which uses the patterns of the vein beneath the skin of the finger. Since this pattern is unique for each finger, verification of identity can be done. As the blood vessels are beneath the surface of the skin, forgery is not possible. Also, the physical presence of the human is guaranteed as the authentication cannot be done otherwise. The authentication process matches the previously recorded pattern available in the database for authorisation. This technology was developed by Hitachi and is patented by them. The applications of fingerprint technology are in vehicle security, ATM security, employee time and attendance tracking, computer authentication, etc. Finger-vein system solves the need of a highly secure biometric process which is very efficient, fast and reliable.

Some advantages of using finger-vein technology are :

- Accuracy: Finger-vein authentication is extremely accurate as wrongful acceptance or true-user rejection rates are one of the lowest amongst biometric authentication.
- Speed: The whole process from execution to authentication takes less than half a second to complete. Hence it is very fast.
- Secure: Finger-vein technique is immensely secure as forgery is impossible. This is due to the fact that the veins are inside the skin, and forgery cannot be done. Also, physical alteration in the skin such as dryness, etc have no impact on this.
- Size: The devices is small, and hence can be used in a wide variety of applications.
- Not visible: Since the veins are inside the skin, they are invisible to the naked eye.
- Back-up: A user can have multiple vein patterns of different fingers stored as each finger will have a separate vein pattern, giving extra security.

Working of Finger-vein Technology

The finger vein authentication system is a method in which the pattern of the veins beneath the surface of the skin is captured. This pattern is unique for each finger of the person. A small device is used in which the person places his finger. This device consists of near infrared LED light emitter and a charge coupled device (CCD) camera [1-5]. The

haemoglobin present in the blood absorbs this near infrared light which makes the vein appear in a unique pattern. The CCD camera captures this pattern. This pattern is stored in the database and compared during authentication process. According to the results the validation is done. The whole process is very accurate and fast and takes less than 0.5 seconds to match and validate. The device used for the capture of the finger vein image is shown figure 1.

Figure 1: A Finger-vein scanner device

Existing Systems And Drawbacks

A biometric system is basically a system that uses the physical characteristics or traits of a person to identify that person accurately. Since these traits or characteristics such as eyes, voice, fingerprints, face, etc are unique from person to person, the authentication of that person is reliable. The biometric system will collect the physical data from a person and run an algorithm for a particular desired result. Authentication takes place when a new sample is matched with the previously recorded sample stored in the database. The current biometrics systems are all subject to risk and have a higher rate of failure. A comparison of biometric methods is shown in Table 1.

Fingerprint recognition: Fingerprint reading can have errors if the finger is dry or there is dirt on the skin of the finger. Even with age, the contours of the fingerprint change. Fingerprints may be unreadable and distorted if the finger is improper or there are smudges during the fingerprinting process. If there is a cut or injury to the skin, the finger print authentication will not work. Forged authentication can be done performed easily too, if the fingerprint of a person can be captured.

Iris recognition: . Iris scanner is very expensive and it takes a long time for the authentication process. Lot of memory is also used up. Iris scanner will not be able to work correctly, if people wear lenses. External features such as eyelashes might also create problems for accurate recognition.

Facial recognition: Face recognition uses a system, which is dependent on changes in lighting, the person's hair, whether the person wears glasses or not and his age, as people's faces change over time. Facial recognition will only be accurate, if the image of user's face is evenly lit, which is not always possible and can hence become very hard for recognition.

Voice recognition: Voice recognition has low accuracy. A person's voice can be easily recorded and used for authorization. An illness such as a cold or growing older can change a person's voice or making identification difficult or impossible.

Biometric system	Accuracy	Security	Attack stoppage	Cost
Finger vein	Very High	Very High	Very High	Medium
Finger print	High	High	High	Low
Voice recognition	Medium	Medium	Medium	Medium
Iris recognition	High	High	High	High
Facial recognition	Medium Low	Medium	Medium	High

Table 1:Comparison of Biometric Methods

Process Overview

This paper proposes to use finger-vein technology for authentication and security purpose. The finger vein reader S-E3F1-609UE by Hitachi is used for capturing finger-vein images of various test users. The images are stored in the database and MATLAB language is used for image processing to extract the features of the images, so that authentication can be performed. MATLAB is chosen to perform image processing since its ease of doing image processing in it. MATLAB has a dedicated image processing toolkit that makes this task simple. It's very large number of built-in algorithms for image processing also help a lot.

All the steps of image processing are performed. Before the algorithms for feature extraction can be implemented, image pre-processing steps like noise removal (Gaussian Bilateral Filter), image enhancement (Histogram Equalization), segmentation K-Means Clustering) are done. Different algorithms are used for various tasks. Once the image is ready, the feature extraction takes place. The algorithm used for feature extraction is the Discrete Wavelet Transform- HAAR wavelet. Various parameters are extracted using the above algorithm, which will then be used for authentication process. Finally, SVM (Support Vector Machine) algorithm is used for training the data set into whether it is an authenticated image or not. The flowchart is shown in the figure 2.

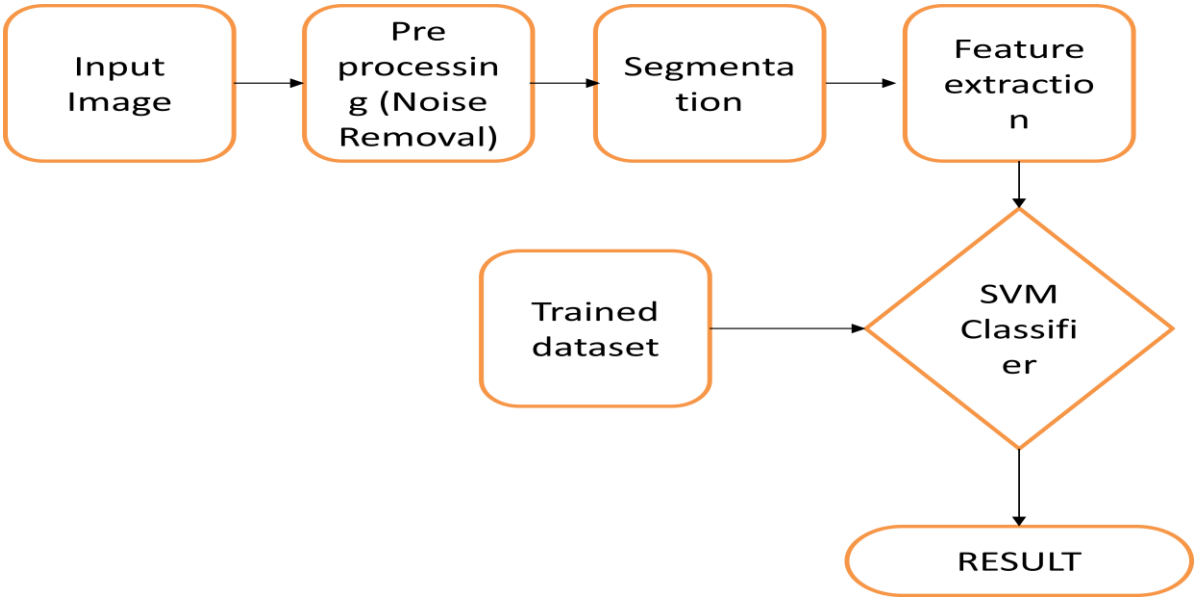

Figure 2: Block Diagram of the whole process

Process Description

This section covers the detailed processes and algorithms that were used in each of the process.

A. Noise Removal

Digital images are subject to many types of noise. Noise is the result of errors in the image acquisition process that result in pixel values that do not reflect the true intensities of the real scene[10]. For image processing to take place, noise removal is important. Feature extraction will only be accurate if the image is free from noise. For this project, Gaussian Bilateral Filter is used for noise removal. The result is shown in figure 3.

Gaussian Bilateral Filter: Bilateral Filter is basically a technique to smooth images while preserving the edges. The bilateral filter converts any input image to a smoothed version. It removes most texture, noise, and fine details, but preserves large sharp edges without blurring. The bilateral filter converts any input image to a smoothed version. It removes most texture and fine details, but preserves large sharp edges without blurring. It depends only on two parameters that indicate the size and contrast of the features to preserve [4].

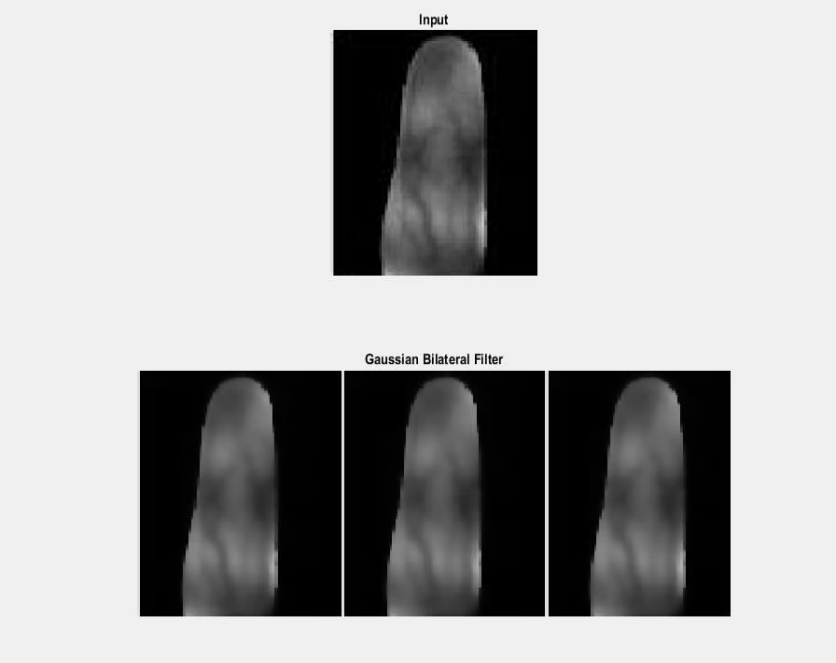

Figure 3: The application of Gaussian Bilateral Filter

B. Image Enhancement

Image enhancement [11] is basically improving the quality of the digital image when the source of the degradation is not known. To improve the contrast, the method used is Histogram Equalization

Histogram Equalization : In image processing, histogram equalization [12] is a technique to enhance contrast by modifying image intensities. The histogram of the image is drawn, before and after the equalization technique is applied. The enhanced image will have flattened or smoother histograms. The application is shown in figure 4 and figure 5.

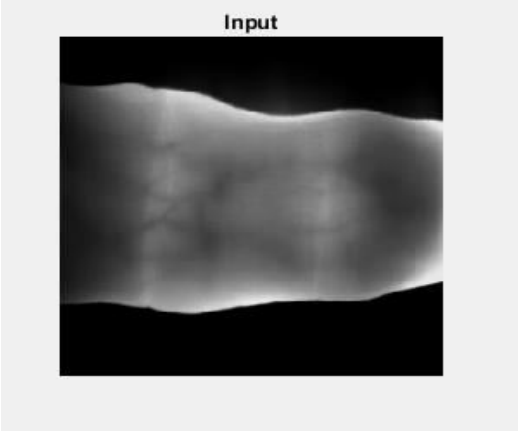

Figure 4: The input image of finger-vein

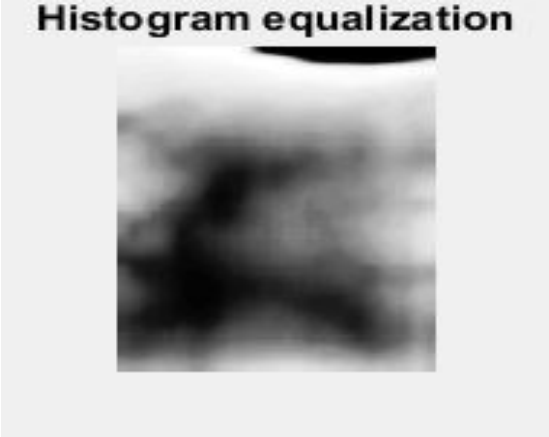

Figure 5: The image after Histogram Equalization

C. Image Segmentation

In the input image, not all parts of the image is useful to perform feature extraction. Hence, using the technique of image segmentation [13], the input image will be divided into parts multiple parts. The basic goal of image segmentation is to modify or change the representation of the image in such a way that makes further processing easier. These separate part are known as super pixels. The pixels in each segment contain the same label. The part which contains the region of interest will then be used for the subsequent step-feature extraction. The application is shown in figure 6 and figure 7. For image segmentation we use K-Means Clustering algorithm [6-13] , which is explained below.

K-Means Clustering : K -means clustering algorithm is an unsupervised algorithm and it is used to segment the interest area from the background. K-Means Clustering is a least square partitioning method, which divides a collection of objects into certain K groups. The mean of each cluster and the distance of each point from each cluster is computed. K-means clustering treats each object as having a location in space. It finds partitions such that objects within each cluster are as close to each other as possible, and as far from objects in other clusters as possible [14]. K-means clustering requires that you specify the number of clusters to be partitioned and a distance metric to quantify how close two objects are to each other[15].

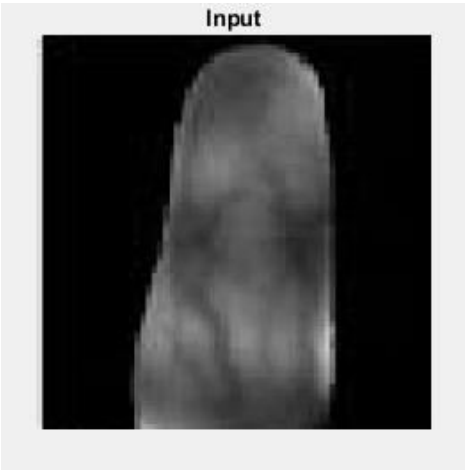

Figure 6: The input image of finger-vein

Figure 7: The image after segmentation

As can be seen in figure 7, the input image has been segmented into different clusters using K-Means algorithm.

D. Feature Extraction

A feature is a distinctive attribute or aspect of something that has some values or parameter which distinguishes itself from its counterparts. Feature extraction starts with an initial set of parameters and builds features that are unique. In image processing, various algorithms are used to detect the desired portion and extract the features of that region. One of the most common algorithms used for feature extraction is by using wavelet transform. Wavelets are a mathematical tool for hierarchically decomposing functions in multiple hierarchical sub bands with time scale resolutions[16]. Since wavelet transform is not Fourier based, the areas where there is a discontinuity in data are handled better. Under the Discrete Wavelet Transforms (DWT), we use the HAAR Wavelet Transform (HWT) as it has the easiest implementation of the DWT [7-8].

Haar Wavelet Transform

HWT is used as it is one of the easiest of the wavelet transform. This transform cross multiplies a function with shifts, just like the Fourier transform. In the HAAR transform [17], the input and the output lengths are the same, but the length should be in the power of 2. When applied for image processing, the image is transformed into a matrix, in which elements of a matrix represents each pixel of the image. Now, any transformations made in the matrix will alter the pixel information of the image. Hence, the Haar transform is derived from the Haar matrix. Discrete Haar functions are function determined by sampling the Haar functions at 2^n points.

E. Parameters Measured

After running the DWT-HAAR wavelet transform algorithm for the feature extraction, various parameters of the image are calculated. These parameters define the image uniquely. They are mentioned below:

Mean: Mean value gives the contribution of individual pixel intensity for the entire image. It is basically a texture feature that represents the average pixel value of the given image. Mean is used in noise filtering as well.

Variance: Variance is normally used to find how each pixel varies from the neighbouring pixel (or centre pixel) and is used in classify into different regions. It can also be used to determine edge position

Standard Deviation: Standard Deviation shows how much variation or dispersion exists from the average (mean, or expected value). A low value of standard deviation shows that the points are in proximity to the mean while high standard deviation shows the points are widely spread. The standard deviation is calculated and the value is assigned to the central pixel.

Entropy: Entropy gives information about the texture of the image. Entropy can be measured from the histogram of an image. In an 8-bit pixel there are 256 states. If all such states are equally occupied, spread of states is maximum. In this case, the entropy value will be maximum and vice-versa.

Skewness: Skewness is gives an idea about the surface of the image. Darker surfaces have higher skew values than lighter values. Skewness can be used to measure the edge of an image that has a white background.

Kurtosis: In general, Kurtosis is used to determine if a distribution is flat or has a peak. It is a measure of the shape of the distribution. Kurtosis values are related to noise and resolution of the image.

F. Training Dataset - Support Vector Machine

Support Vector Machine [9] is an algorithm that is used with learning algorithms that are used for classification. SVMs are one of the best known methods for pattern and image classification. SVMs are used to separate a set of training in two different classes. Hence, when there are two classes and the image is to be classified as one of them, the SVM classifier is used. Based on the features extracted of the input images, the data set is trained to be in one of the categories of 'authenticated' or 'not authenticated'. SVM builds a separating hyper-plane based on a kernel function. If the feature vector lies on one side of the plane, it is categorised as belonging in the first class and if it lies on the other side, it is classified as belonging in the second class.

Application In Vehicle Security

One of the application of using finger vein technology is to make an authentication system to provide vehicle security. The result from the finger-vein authentication can be used to decide whether the ignition of the vehicle should switch on or not. The database of the finger vein images of the people who are authorised to drive that vehicle can be recorded and kept. The finger-vein scanner will be attached to the microcontroller that will decide if the ignition can be switched on or not. On successful authentication of the person, a signal will be sent to the microcontroller, that will allow the ignition to switch on. If the authentication is not successful, a message can be sent to the real owner intimating about the unsuccessful attempt at authentication. This method can be used to prevent vehicle thefts and provide security to vehicles. The flowchart is shown in figure 8.

As can be seen, the driver will have to input the finger vein image by getting it scanned by the finger vein scanner. The authentication will then be done. The results are sent to the Arduino controller, which according to the result, will allow the ignition to switch on. If the

result of the match is negative, the controller will then be used to send a message to the owner, informing about the failed attempt.

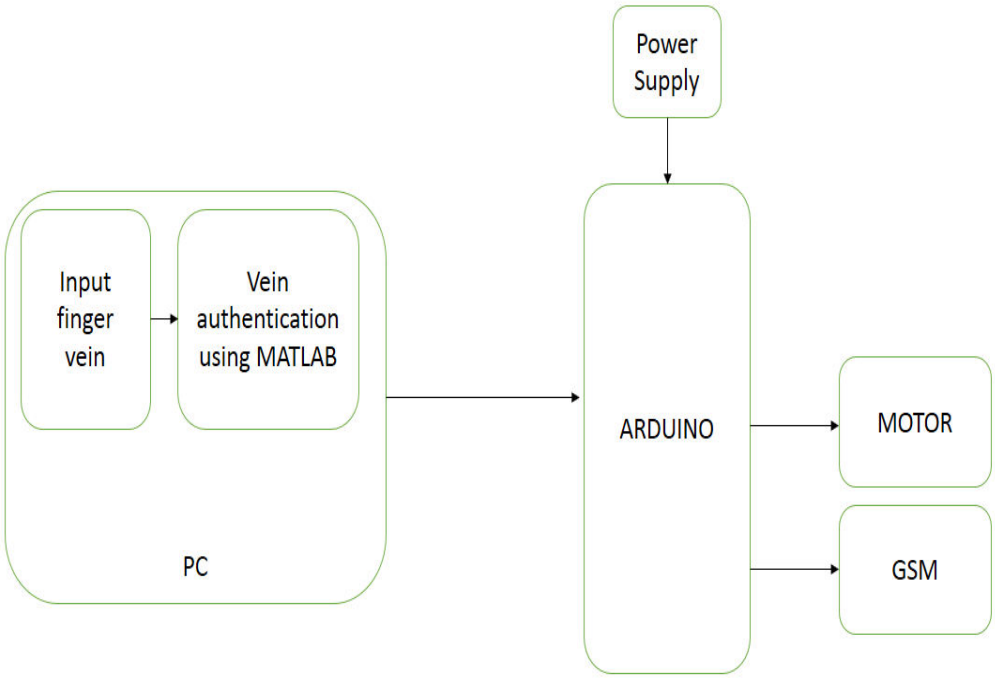

Figure 8: Flowchart for vehicle security

Results

The performance of the model is measured using two parameters- Mean square error (MSE) and peak signal to noise ratio (PSNR) [18-19]. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to compare the squared error between the original image and the new trained image. There is an inverse relationship between PSNR and MSE. Higher the value of PSNR, better is the quality of the image. For demonstration purpose as shown in table 2, we have tabulated the MSE and PSNR values for 6 of the finger vein images.

Image \ Parameter	Mean Squared Error	Peak Signal to Noise
1	9.9691e-04	78.1443
2	4.1199e-04	81.9820
3	0.0013	77.0014
4	1.2716e-04	87.0874
5	0.0011	77.5450
6	0.0015	76.2956

Table 2 Mean squared error and Peak signal to noise ratio for 6 finger-vein images

Conclusion and Future Work

As discussed, we used finger-vein technology for authentication and described an application of it for vehicle security. The finger vein authentication is one of the best biometric methods that is available for use as it gives one of the highest accuracy amongst all the biometric methods. It can be executed easily and the whole authentication and verification process takes

less than 0.5 seconds. In this project, we have been able to have the mean square error down to 0.0009059833 and the average peak signal to noise ratio as 79.67595. For future improvements, we look for faster execution time and try to bring the cost down for the whole setup so that finger vein technology can be used for various security applications.

References

[1] Desong Wang, Jianping Li, and Gokhan Memik, "User Identification based on Finger-vein Patterns for Consumer Electronics Devices", IEEE Transactions on Consumer Electronics, Vol. 56, No. 2, pp. 799-804, May 2010.

[2] Hashimoto J.,"Finger Vein Authentication Technology and its Future", 2006 Symposium on VLSI Circuits, Digest of Technical Papers, pp. 5-8, 2006.

[3] Lee H, S. H. Lee, T. Kim, and H. Bahn, "Secure User Identification for Consumer Electronics Devices", IEEE Transactions on Consumer Electronics, Vol. 54, No. 4, pp. 1798-1802, Nov. 2008.

[4] V.R.Vijaykumar et al. "Fast and Efficient Algorithm to Remove Gaussian Noise in Digital Images" IAENG International Journal of Computer Science, 37:1, JCS_37_1_09 1 Feb, 2010.

[5] Wu J. D., and S. H. Ye "Driver Identification using Finger-Vein Patterns with Random Transform and Neural Network", Expert System Applications, Vol. 36, pp. 5793-5799, 2009.

[6] S. P. Lloyd, " Least squares quantization in PCM ", IEEE Trans. Inf.Theory, vol. IT-28, no. 2, pp. 129 – 136, Mar.1982.

[7] Ramakrishnan S. et al., "SVD Based Digital Image Watermarking Using DWT", Proceedings of the National Conference on Intelligent Computing and Control Engineering Applications, pp. 83-86, Anna University of Technology, Coimbatore.

[8] G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y. Q. Shi, and Z. Ni. "Lossless data hiding using histogram shifting method based on integer wavelets". 2006, Proc. Int. Workshop on Digital Watermarking, Vol. 4283, pp.323–332.

[9] Wen-Chang C, Ding-Mao J. "Triaxial Accelerometer-Based Fall Detection Method Using a Self-Constructing Cascade-AdaBoost". Biomedical and Health Informatics, IEEE Journal. 2013; pages 411-419.

[10] Anita Pati Mishra "Noise Smoothing- Improving Image Filtering Methodology" International Journal of Research Volume 03 Issue 09 May 2016.

[11] Ms.Seema Rajput Prof.S.R.Suralkar "Comparative Study of Image Enhancement Techniques" IJCSMC, Vol. 2, Issue. 1, January 2013, pg.11 – 21.

[12] Rajesh Garg, Bhawna Mittal "Histogram Equalization Techniques For Image Enhancement" IJECT Vol. 2, Issue 1, March 2011.

[13] Nameirakpam Dhanachandra et al. "Image Segmentation Using K -means Clustering Algorithm and Subtractive Clustering Algorithm" Procedia Computer Science Volume 54, 2015, Pages 764-771.

[14] Tara Saikumar et al. "Colour Based Image Segmentation Using Fuzzy C-Means Clustering" 2011 International Conference on Computer and Software Modelling IPCSIT vol.14 (2011).

[15] Ravindra S et al. "Segmentation of Google Map Images Based on Color Features" Proceedings of International Conference on Communication, Computation, Management & Nanotechnology (ICN-2011), September 23-25, 2011.

[16] Murali Mohan. S et al. "VLSI Architecture for Fast Computation of 2D-Discrete Wavelet Transform and Low Power Feed Forward Neural Network Architecture for Image Compression" American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-02, Issue-10, pp-136-145 www.ajer.org.

[17] Kamrul Hasan Talukder, Koichi Harada "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image" IAENG International Journal of Applied Mathematics, Volume 36, Issue 1, 2007.

[18] Cui, L., & Allen, A.R. ." An Image Quality Metric Based on a Colour Appearance Model". 2008 Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems, France, pp.696-707.

[19] Wang, Z., Bovik, A.C., Sheikh, H.R., & Simoncelli, E.P (2004) Image quality Assessment: from error visibility to structural similarity. IEEE Tran. Image Processing 13(4), pp. 600-612.