Enhancement of Finger Print Image using Fuzzy Filter

M.V.Kishore
Asst.Professor
Department of IT
ANITS

Ch.D.Naidu
Sr.Asst.Professor
Department of IT
ANITS

N.Aditya Sundar
Asst.Professor
Department of IT
ANITS

G.Pandit Samuel
Asst.Professor
Department of IT
ANITS

ABSTRACT

Fingerprint recognition is the most widely used biometric system for human identification. The noise is one kind of feature which disturbs the real finger print pattern and makes the identification process is not efficient. Therefore we need to eliminate the noise, and recover the original finger print from noises. In order to recover the original finger print, finger print image needs to be pre-processed. Pre-processing is a method of eliminating or reducing the noise presents in the finger prints. There are various techniques pre processing such as binarization, normalization, thinning. Another technique of pre-processing is the use of various filters. These filters are efficient and are also available to reduce noise. Enhancing Finger print is the method of improving the quality of the image by increasing contrast, brightness, sharpness etc. Finger Print Image is enhanced using various filters such as mean and median filters. In order to avoid disadvantages of existing filters fuzzy filter is proposed in which the general idea behind the filter is to average a pixel using other pixel values from its neighbourhood, but simultaneously to take care of important image structures like edges. The key idea behind the proposed filter is to distinguish between local variations due to noise and due to image structure. To achieve this, derivative a value that expresses the degree in which the derivative in a certain direction is small is determined for each direction corresponding to the neighbouring pixels of the processed pixel by a fuzzy rule.

Keywords

Fuzzy Filter, Fingerprint recognition

1. INTRODUCTION

In order to provide network security **authentication** is one of the important factors. People can be authenticated using one of the three ways: **One factor authentication** –authenticating with “something that is known” by the entity to be authenticated, i.e. password etc. **Two factor authentication** authenticating

With “something that user has” i.e. credit card, passport, etc. **Three factor authentication** authenticating with “something the user is” i.e. biometric characteristics. Three factor authentication[1] is the best way for authenticating users. Now we will go through the mechanisms for authenticating users. One of the mechanism is fingerprint recognition system [2] authenticates user with fingerprints of users. Steps that are involved in this system are-**Fingerprint sensing** in which the fingerprint of an individual is acquired by fingerprint scanner to produce a raw digital representation. **Pre-processing** in which input fingerprint is enhanced and adapted to simplify the task of feature extraction. **Feature extraction**, in which the fingerprint is further processed to generate authentic properties, also called feature vectors and **Matching**, in which feature vector of the input fingerprint is compared against one or more existing fingerprint templates. **Advantages[1]** of this system are :It is highly accurate, most economical biometric authentication technique.

But there are challenges faced by this system. The **challenges** faced are, the first challenge faced by this system is performance of a fingerprint recognition system is highly affected by fingerprint image quality. Several factors that determine the quality of fingerprint image are Skin conditions, sensor conditions, user cooperation, etc. The second challenge faced by this system is it is intrusive. In order to solve the problem faced by the fingerprint recognition system, a new recognition system that identifies user based on the images of their faces is developed called the face recognition system described in [3].

Technology for Face Recognition:

Face Detection in which the face is located in the image using a combination of skin tone and face texture. **Face Recognition**: In this step features either global or local are extracted and condensed in compact face representation. **Matching**: the features that are extracted in the previous step are stored in database and compared with face representations that are derived later.

Advantages of using this system [3] are, It is non intrusive and it is not affected by skin conditions or sensor conditions as the image is captured by using a camera at a distance.

But there are **disadvantages** in this system. Major disadvantages are,2D recognition is affected by changes in lighting ,the person’s hair ,the age ,and if the person wear glasses and requires camera equipment for user authentication ;thus it is not likely to become popular until most pc’s include cameras as standard equipment.

In order to solve the problem in face recognition system a new system was used in which users are authenticated using inner part of person’s hand called palm print recognition system[4].

Steps that are involved in Palm Print Recognition System are: **palm print acquisition** in which palm print image is captured using a CCD based scanner .**Pre Processing** is used to rectify distortions, align different palm prints and to crop the region of interest for feature extraction.ROI extraction in which the central part of the palm image is segmented after pre processing. The image is processed and then used for feature extraction. **Feature Extraction and matching**-In this step features are extracted from the image and stored in database for comparing with templates derived at later times.

Advantages of using this system[4] are, Though it requires special hardware to use, it can be easily integrated into other devices or systems and the amount of data required to uniquely identify a user in a system is the smallest by far, allowing it to be used within the smart cards only.

But there are **disadvantages** in this system . One of the disadvantage is it is very expensive and another disadvantage in this system is it is not valid for physically challenged person(person who does not have full hand), since they cannot put the hand on the scanner properly.

In order to solve the problem in palm print recognition system a new system [5] can be used in which users are authenticated by using iris pattern in the eye.

The process of capturing iris into a biometric template is made up of 3 steps. The first step is **capturing the image**, in which the image of iris is captured using a standard camera positioned within three and half inches and one meter to the image. The second step is **Defining the location of iris and optimising image** in which eye is located in the image first and then the system identifies iris that has the best quality and then precise location of iris is identified. The third step is **Storing and Comparing the Image**-Once the image is captured a 512 byte record is generated for the captured iris using a algorithm which is stored in the database for future comparison.

Advantages of this system are, The eye from dead person would decay too fast to be useful, therefore no extra precautions have to be taken to make sure that user is living human being. Another advantage of using this system is Verification time is generally less than five seconds and it is highly accurate process

But there are **disadvantages** in this system. i.e., a lot of memory is used to store the data used for identifying individuals.

In order to solve the problem a system can be used that authenticates user with the characteristics of their brain waves.

In this system [6] EEG(electroencephalogram) is used as a biometric identifier.EEG signals present some characteristics, that are not similar to the most used biometrics like iris, face and finger prints. As Brain signals are the result of the electrical activity of the cortex, they are not like face, iris, and finger prints. So, they are more privacy compliant than other biometrics since they are "secret" by their nature, it is impossible to capture them at a distance. It makes EEG biometrics also robust against the spoofing attack at the sensor, since an attacker would not be able to collect and feed the brain signals obtained from EEG, which are the result of ionic current flows within the neurons of the brain. As the brain signals the result of a psychological process, they cannot be artificially generated and feeded to a sensor, which also solves the problem of liveness detection. The use of EEG within the biometric framework has already been introduced in the recent past although it has not been extensively analyzed. In this contribution we apply the "bump" modelling analysis for the feature extraction stage to reduce the huge amount of data recorded through EEG.

The process of Bump Modelling described in [6] is as follows: The key idea behind this method is to approximate a time-frequency map with a set of predefined elementary parameterized functions called bumps; therefore, the map is represented by the set of parameters of the bumps.
The algorithm performs the following steps on the time-frequency maps (after appropriate normalization):

1) Window the map in order to define the zones to be modelled (those windows form a set of overlapping sub-areas of the map).
2) Find the window that contains the maximum amount of energy.
3) Adapt a bump β to the selected zone, and withdraw it from the original map. The parameters of the bumps are computed using the BFGS algorithm[12] in order to minimize the cost function C defined by:

$$C=1/2\sum_{t,f\epsilon W}(Z_{f,t} - \beta(f, t))^2$$

where the summing up runs on all pixels within the window W, $Z_{f,t}$ are time-frequency coefficients at time t and frequency f , and β(f, t) is the value of the bump function at time t and frequency f .

4) If the amount of information modelled by the bumps reaches a threshold, stop; else return to (3).

But using the characteristics of brain waves and analysis described in [6] is not preferred because characteristics of brain waves differ in various conditions such as eyes in resting state, eyes in closed state, etc .so in order to authenticate users optimising system[1] that is present in earlier days will be useful. The system used for authenticating users based on biometric characteristics was **Finger print Recognition System**. Disadvantage in this system is it is intrusive that is attacker who can access the database can easily get the templates and misuse them for malicious purposes .In order to avoid this Problem of intrusion we can use protection schemes on fingerprint template to protect them from attackers. One of such protection scheme is fuzzy vault described in [7] which is a cryptographic construction where in a player Alice can place a secret value k in a fuzzy vault and lock it using a set A of elements. If Bob tries to unlock the elements he can unlock the secret only if set B of Bob matches exactly with setA.
Methodology described in [8],[9],[10] used for securing fingerprint template using fuzzy vault:
1. At first helper data is extracted from the fingerprint and the secret is embedded into the polynomial.
2. Helper data or the minutiae extracted from the fingerprint template are projected onto the polynomial.
3. Random number of chaff points are generated that do not lie on the polynomial but lie near the polynomial thus forming a Fuzzy vault.
4. The polynomial can be retrieved if same set of minutiae are inserted by the user. user can access the polynomial with the same set of minutiae on the polynomial.

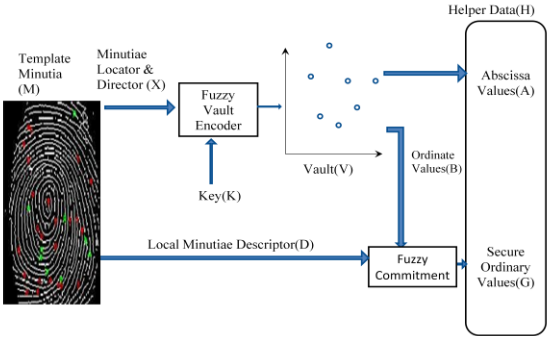


Fig. 1 Helper Data Extraction In Descriptor Based FingerPrint CryptoSystem

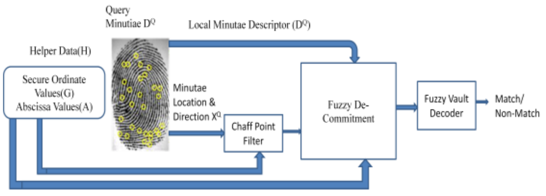

Query Minutiae D^Q
Local Minutae Descriptor (D^Q)
Helper Data(H)
Secure Ordinate Values(G) Abscissa Values(A)
Minutae Location & Direction X^Q
Chaff Point Filter
Fuzzy De-Commitment
Fuzzy Vault Decoder
Match/ Non-Match

Fig. 2 Authentication in Descriptor Based FingerPrint CryptoSystem

Using this process is advantageous but the performance is highly effected due to the quality of fingerprint image. so fingerprint image has to be enhanced. there are various filtering methods proposed in [13] used for enhancing. some of the existing filters used for enhancing the fingerprint image are mean and median filters. In order to ensure the preservance of important image structures like edges a new filter called as fuzzy filter is proposed

2. IMPLEMENTATION AND ANALYSIS

Mean filter [13] where in each pixel is replaced by averaging the neighbourhood pixels of the pixel. It can eliminate pixel values that are unrepresentative of their surroundings. But the disadvantage of this filter is sometimes useful detail is not preserved. In order to preserve useful details of the fingerprint image median filter is used in which each pixel is processed and is replaced by median value of the neighbourhood pixels. This filtering method preserves useful detail but do not take care of local variations due to noise and change in image structures. To avoid the local variations due to noise and change in image structure fuzzy filter is used.

Basics used for developing the fuzzy filter are:

2.1 Fuzzy rules

Human beings take decisions on the basis of rules. Although, we are not aware of it, all the decisions we take are all based on if-then statements. If the weather is fine, then we will wash out the car. If the forecast says the weather will be bad today, then we take a decision not to wash the car today. Rules link ideas and relate one event to another.

Fuzzy machines, which always tend to mimic the way of behaving of man, work the same way. However, the conclusion or decision and the means of choosing that decision or conclusion are replaced by fuzzy sets and the rules are replaced by fuzzy rules. Fuzzy rules operate on a series of if then statements. For example, if A then x, if y then B, where x and y are all sets of A and B. Fuzzy rules define the fuzzy patches which is the key idea in fuzzy.

2.1.1 Fuzzy Patches

In a fuzzy system this simply means that all our rules can be seen as patches and the input and output of the machine can be associated together using these patches. perceptibly, if the patches shrink, our fuzzy subsets would get narrower. It is Simple enough because even novices can build control systems that beat the best math models of control theory. Basically it is math-free system.

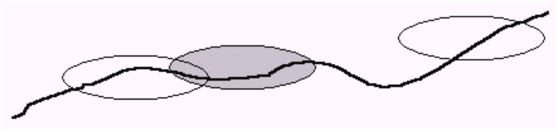


Fig. 3 Fuzzy Patches Covering The Curve

2.1.2 Fuzzy Control

To create a fuzzy controlled machine three steps are followed:

1) Fuzzification(Membership functions are adapted to a situation).
2) Rule evaluation (Application of fuzzy rules).
3) Defuzzification (Obtaining the crisp or actual results)

The process involved in fuzzy filtering method described in [11] is as follows:

The general idea behind the filter is to average a pixel using other pixel values from its neighbourhood, but simultaneously to take care of important image structures like edges. The key idea behind the proposed filter is to distinguish between local variations due to noise and due to image structure. In order to achieve this, derivative value is that expresses the degree in which the derivative in a certain direction is small is found out for each direction corresponding to the neighbouring pixels of the processed pixel by a fuzzy rule.

The further construction of the filter is then based on the observation that a noise is the cause of small fuzzy derivative, where as a large fuzzy derivative likely is caused by an edge in the image. Thereafter, two fuzzy rules are applied for each direction that take this observation into account (and thus distinguish between local variations due to noise and due to image structure), and thus find out the contribution of the neighbouring pixel values. The result of these rules (16 in total) is defuzzified and a “correction term” is obtained for the processed pixel value.

2.2 FUZZY DERIVATIVE-ESTIMATION

Estimating derivatives and filtering can be seen as a chicken-and-egg problem; for filtering we want to find the edges those are good. In our approach, the first step is we look for the edges. Trail to provide a robust estimate is made by applying fuzzy rules.

Consider the neighbourhood of a pixel as shown in the below figure.

A simple derivative at the central pixel position (x,y) in the direction D (D € dir= {NW,W,SW,S,SE,E,NE,N}) is defined as the difference between the pixel at (x,y) and its neighbour in the direction D. This value of derivative is denoted by D(x,y).

NW	*N*	*NE*
W	*(x,y)*	*E*
SW	*S*	*SE*

Fig. 4(a) Neighbourhood of central pixel(x,y)

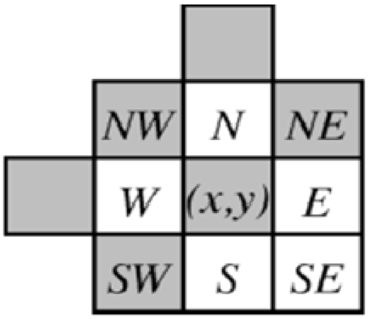


Fig. 4(b) pixel values indicated in gray are used to compute “fuzzy derivative” of central pixel(x,y) for the N-W direction

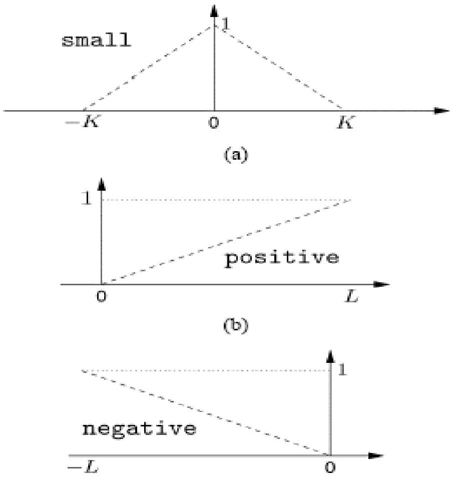


Fig. 5 Membership function

Table 1 For calculating fuzzy derivatives

Direction	**Position**	**Set w.r.t(x,y)**
NW	(x-1,y-1)	{(-1,1),(0,0),(1,-1)}
W	(x-1,y)	{(0,1),(0,0),(0,-1)}
SW	(x-1,y+1)	{(1,1),(0,0),(-1,-1)}
S	(x,y+1)	{(1,0),(0,0),(-1,0)}
SE	(x+1,y+1)	{(1,-1),(0,0),(-1,1)}
E	(x+1,y)	{(0,-1),(0,0),(0,1)}
NE	(x+1,y-1)	{(-1,-1),(0,0),(1,1)}
N	(x,y-1)	{(-1,0),(0,0),(1,0)}

$$m_{K(u)=}\begin{cases}1\text{-}|u|/K, & 0\leq|u|\leq K\\ 0, & |u|>K\end{cases}$$

Method used to find the small value

for example ,the value of the fuzzy derivative $\nabla^{F}_{NW(x,y)}$ for the pixel(x,y) in the N-W direction is calculated by applying the following rule:

if($\nabla_{NW(x,y)}$ is small and $\nabla_{NW(x-1,y+1)}$ is small) or

($\nabla_{NW(x,y)}$ is small and $\nabla_{NW(x+1,y-1)}$ is small) or

($\nabla_{NW(x-1,y+1)}$ is small and $\nabla_{NW(x+1,y-1)}$ is small)

Then $\nabla^{F}_{NW(x,y)}$ is small.

Sample rule for the fuzzy derivatives.

2.3. FUZZY SMOOTHING

To compute the correction term for every pixel value that is being processed, a pair of fuzzy rules is used for each direction. The key idea behind the rules is the following: if no edge is assumed to be present in a certain direction, the derivative value in that direction is used for computation of the correction term. The first part (edge assumption) can be realized by using the fuzzy derivative value, for the (filtering) we will have to distinguish between positive and negative values.

For example, let us consider the direction NW. using the values $\nabla^{F}_{NW(x,y)}$ and$\nabla_{NW(x,y)}$, the following two rules are fired, and truthness values are computed, λ^{+}_{NW} and λ^{-}_{NW}:

λ^{+}_{NW} : if $\nabla^{F}_{NW(x,y)}$ is small and $\nabla_{NW(x,y)}$ is positive
then c is positive

λ^{-}_{NW}: if $\nabla^{F}_{NW(x,y)}$ is small and $\nabla_{NW(x,y)}$ is negative
then c is negative

$$\Delta = L/8\sum_{D\in dir} \quad (\lambda^{+}_{D} - \lambda^{-}_{D})$$

GUI Module

Java Frames are used to implement the user interface in our project. Interface is easy and user friendly. Input from the user is taken by this module by browsing the image and placing the image in the input image section. Different filters that have been implemented are called by this module. Before applying filters to the image it has to be saved and finally the image is shown in output section .Three modules that are present in this project are: Mean Filter, Median Filter and Fuzzy Filter.

GUI Screen

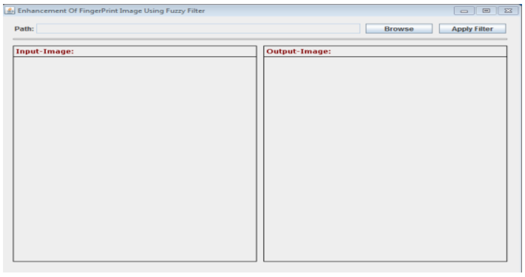


Fig. 6 GUI Screen

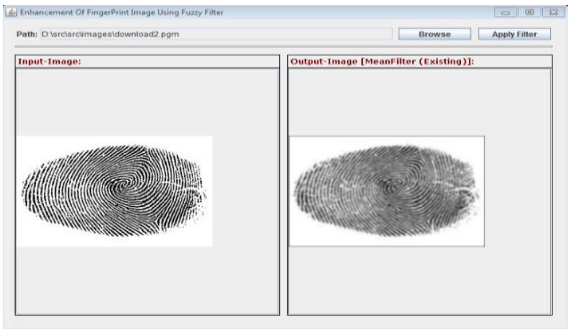
Now let us see the implementation details of the different modules.

Mean Module

This module reads the input fingerprint image and sets the fingerprint image header information for the output fingerprint image. It applies the smoothing algorithm and sets the output fingerprint image as input for the next iteration if its not the last iteration and writes the output fingerprint image after completion of all the iterations.

The mean algorithm works by adding all the surrounding or neighbour pixel values and takes the mean or average of those values. The value so obtained is placed in the central pixel.

Output Of Mean Filter


Path: D:\src\src\images\download2.pgm

Enhancement Of FingerPrint Image Using Fuzzy Filter
Browse
Apply Filter
Input-Image:
Output-Image [MeanFilter (Existing)]:

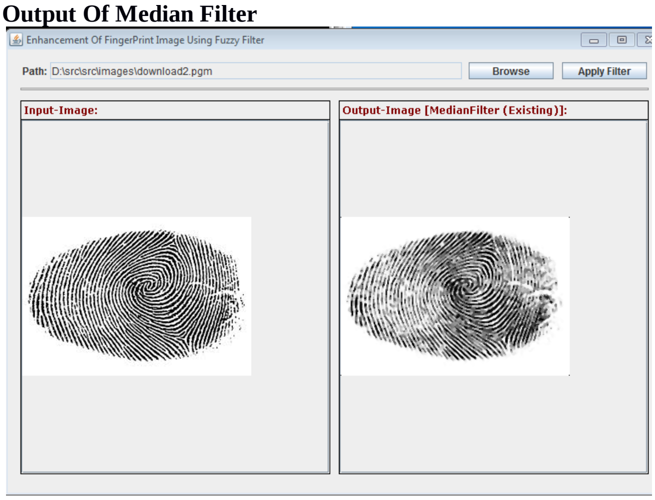
Fig. 7 Mean Filter

Median Module

This module reads the input fingerprint image and sets the fingerprint image header information for the output fingerprint image. Smoothing algorithm is applied by the module and the output fingerprint image is setted as input for the next iteration if it's not the last iteration and writes the output fingerprint image after completion of all the iterations.

The median algorithm works by arranging the surrounding or neighbour pixel values in ascending order and takes the median of those values. The value so obtained is placed in the central pixel.

Output Of Median Filter


Enhancement Of FingerPrint Image Using Fuzzy Filter

Path: D:\src\src\images\download2.pgm

Fig. 8 Median Filter Output Screen

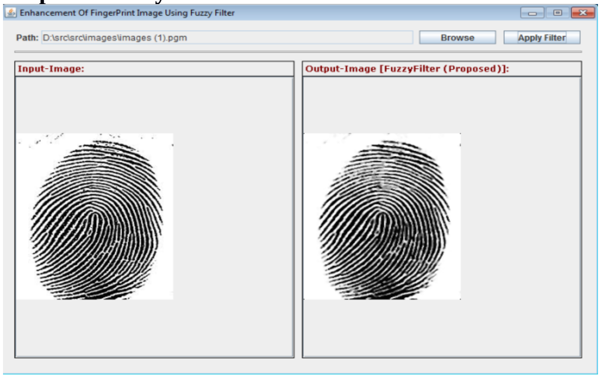
Fuzzy Filter Module

Fuzzy filtering is used to reduce narrow-tailed and medium narrow-tailed noise. There are Two important features that are required: first, a "fuzzy derivative" is estimated by the filter in order to be less sensitive to local variations due to fingerprint image structures such as edges; second one is, the membership functions are adapted accordingly to the noise level to perform "fuzzy smoothing."

Fuzzy Derivative Estimation:

To compute the correction term for each pixel value that is being processed, a pair of fuzzy rules are applied for each direction. The key idea behind the rules is the following: if no edge is assumed to be present in a certain direction, the (crisp) derivative value in that direction can and will be used to compute the correction term. The first part (edge assumption) can be realized by using the fuzzy derivative value, for the second part (filtering) we will have to distinguish between positive and negative values.

Output of Fuzzy Filter


Enhancement Of FingerPrint Image Using Fuzzy Filter

Path: D:\src\src\images\images (1).pgm

Fig. 9 Fuzzy Filter Screen

3. CONCLUSION AND FUTURE ENHANCEMENT

The proposed finger print enhancement system using fuzzy based filtering techniques gives high PSNR and low MSE when compared to Mean and Median filtering based finger print enhancement method.

The future enhancement of this project can be that it can be integrated with the downloading systems that download the finger print from the internet and apply the filters with the consent of the user and provide a better finger print to the user. This Filter can also be updated and made a little more accurate with use of other complex technologies and methodologies and implemented for use of analyzing the satellite imagerys.

4. REFERENCES

[1] Sumedha Kaushik and Ankur Singhal Department of ECE & M. M. University; Network Security Using Cryptographic Techniques; Volume 2, Issue 12, December 2012 ISSN: 2277128X International Journal of Advanced Research in Computer Science and Software Engineering.

[2] Fernando Alonso-Fernandez and (in alphabetical order) Josef Bigun, JulianFierrez, Hart wig Front haler, Klaus Koll reider, Javier Ortega-Garcia. **"**Chapter 4, Finger print Recognition".

[3] David.D.Jhang,"Biometric Solutions For Authentication In An E-World",Chapter4,FACE RECOGNITION AND ITS APPLICATION", kluwar academic publishers

[4] Sumalatha K.A, Harsha H ,Dept. of Instrumentation Technology, ,R.V. College Of Engineering, Bangalore, India;" Biometric Palm print Recognition System: A Review", Volume 4, Issue 1, January 2014 ISSN: 2277 128X ,International Journal of Advanced Research in Computer Science and Software Engineering

[5] Penny Khaw, SANS Security Essentials (GSEC) Practical Assignment,Version 1.3;" Iris Recognition Technology for Improved Authentication",www.sans.org

[6] Daria La Rocca$, Patrizio Campisi $, Jordi Sol´e-Casals $$Section of Applied Electronics,Department of Engineering, University of Roma Tre, Via Vito Volterra 62, 00146, Roma, Italydaria.larocca@uniroma3.it, patrizio.campisi@uniroma3.it $$Escola Politecnica Superior, Universitat de VicC /dela Laura, 13, 08500Vic, Catalunyajordi.sole@uvic.cat,"EEG based user recognition Using Bump Modelling".

[7] Umut Uludag, Sharath Pankanti, Anil K. Jain Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, 488242 Exploratory Computer Vision Group, IBM, T.J.Watson Research Yorktown Centre, Heights, NY, 10598;"Fuzzy Vault for Fingerprints", uludagum,jain@cse.msu.edu, sharat@us.ibm.com.

[8] Abhishek Nagar,Michigan State Univ. East Lansing, MI, USA, nagarabh@cse.msu.edu, KarthiNandakumar, Inst.for Info comm. Research, A*STAR, Fusionopolis, Singapore, knandakumar@i2r.astar.edu. Sgand Anil K.Jain, Michigan, StateUniv., East Lansing, MI, USA, jain@cse.msu.edu; "Securing Finger print Template: Fuzzy Vault with Minutiae Descriptors",www.cse.msu.edu.

[9] Umut Uludag, Michigan State University,uludagum@cse.msu.edu and Anil Jain, Michigan State University, "Securing Finger print Template:"Fuzzy Vault with Helper Data",www.cse.msu.edu.

[10] Johannes Merkle, Matthias Niesing, Michael Schwaiger secunet Security Networks AGD45128Essen,Germanyjohannes.merkle@secunet.com,matthias.niesing@secunet.com,michael.schwaiger@secunet.com HeinrichIhmor, Ulrike Korte Bund esamur Sicherheit inder Information stechnikD53175Bonn,Germanyheinrich. Ihmor@bsi.bund.de, ulrike. korte@bsi.bund.de , "Performance of the Fuzzy Vault for Multiple Fingerprints", www. arxiv.org

[11] K.Srinivasam, Department of Computer Science, Guest Lecturer, Govt Arts College, Dharmapuri, Tamilnadu, 5366075, IndiaVasanmsc23@yahoo.co.in and C.Chandrasekar, Department of Computer Science, Periyar University, Salem, Tamilnadu, 636011, India, ccsekar@gmail.com; "An Efficient Fingerprint Enhancement System using Fuzzy Based Filtering Technique", International Journal of Computational Intelligence and Informatics, Vol. 1 : No. 1, April -June 2011,ISSN : 2349 – 636348

[12] William H Press, Brian P Flannery, Saul A Teukolsky, and William TV etterling, Numerical Recipes in FORTRAN 77: Volume 1, Volume 1 of Fortran Numerical Recipes, "The Art of Scientific Computing", volume 1. Cambridge university press, 1992.

[13] Dr.S.Pannirselvam, Research Supervisor & Head ,Department of Computer Science, Erode Arts & Science College (Autonomous), Erode9, P.Raajan, Ph.D. Research Scholar, Department of Computer Science, Erode Arts & Science College (Autonomous), Erode9; "An Efficient Finger Print Enhancement Filtering Technique with High Boost Gaussian Filter (HBG)", Volume 2, Issue 11, November 2012 ISSN: 2277 128X ,International Journal of Advanced Research in Computer Science and Software Engineering