Performance Analysis on Real Time Fingerprint Verification

Sankar Kumar S[1], Vasuki S[2]
[1, 2] Department of ECE
[1, 2] Velammal College of Engineering and Technology, Madurai – 625 009

Abstract- *For verification and identification of a person, fingerprint is one of the most common biometric attributes. Moreover, any automated biometric based recognition systems, which are designed to detect an individual for both identification and verification, utilization has increased because of the advent of recent advancements in computer technology. At the same time, since these systems are composed of a series of complex technologies to provide a preferred result, designing such type of systems is a complex one also. Minutiae, Ridge and Correlation are the existing three methods of fingerprint matching, but among which though the best performance is provided by both minutia and ridge based algorithms as far as partial or low quality fingerprint images is concerned only few minutiae are extracted successfully while matching whereas the third method of fingerprint matching, i.e., correlation based one which uses the fingerprint's richer gray scale information directly with which no need to extract minutiae unlike the other two methods. Hence this correlation based method can overcome such issues and is capable of dealing with bad quality fingerprint images. In this paper, the authors discuss the experimental results and performance analysis of the developed real time correlation based fingerprint matching system which is implemented on the Raspberry Pi platform along with a fingerprint scanner.*

Keywords- Biometrics, fingerprint, minutia, ridge, correlation, image, fingerprint matching..

I. INTRODUCTION

With the advent and advancements in computer technology both hardware and software have enabled researchers towards the development of inexpensive automated systems using biometrics for identification and verification. Such systems are being used in a wide range of applications such as banking, social welfare, law enforcement and most frequently in security. For identification and verification of an individual, several biometrics like face, iris, retina, fingerprint, hand geometry, signature, hand writing, vein, voice etc. have been used. Since every biometric has its own advantages as well as disadvantages, based on the performance criteria and operating environment for specific application an appropriate one is chosen. In this paper, fingerprint biometric is identified for verification and this paper discusses about fingerprint verification system. Fingerprint is composed of two basic structures which are ridges and valleys on human fingertips as shown in Figure 1. The dark lines like regions are ridges and the bright regions are valleys and they run often in parallel. Constitution of these ridge lines in the fingerprint, though they run in parallel sometimes the occurrence of discontinuities such as bifurcation, termination and intersection will also be in their run which are known as minutiae.

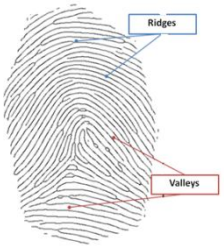

Fig.1. Ridges and Valleys structures in a fingerprint

They may be sometimes independent beginning or ending of ridges or may divide, but immediately reunite approximately as an enclosed small circular or elliptical space. These are the main details of source for the information to be extracted when fingerprints are used for recognition systems.

In a fingerprint, possibilities are there to identify two levels of detail which are directional field and minutiae. At each position in the fingerprint the local orientation of the ridge-valley structure is referred as the directional field and as far as classification of fingerprints is concerned directional field is used since it describes the fingerprint's basic shape or the coarse structure. Moreover, the ridge-valley structures details such as ridge bifurcations, endings and so on are provided by minutiae and for one-to-one matching comparison minutiae are used.

Basically there are two approaches of fingerprint based recognition systems existing namely identification and verification. In both the approaches the user only offers his / her fingerprint. The identification approach searches its internal database for matching with the claimed one and if any matching is found means the claimed person is identified;

whereas the verification approach checks whether the claimed person is who actually claims to be. In any biometric based recognition system, a user first identifies either through an Identity card or a username followed by puts his / her finger on a sensor instead of entering password or any other code for personal identification. Then the system starts retrieving a fingerprint of the user from its database, called primary fingerprint and checks whether it matches the live scanned finger, called secondary fingerprint. If both primary and secondary fingerprints match then the user gets access to the system assuming the user is genuine otherwise the user is classified as imposter. With the help of a matrix the performance of a fingerprint matching system can be shown, in which I is imposter class, G is the genuine class, I0 and G0 are the corresponding assigned classes.

In the matrix shown below, TRR stands for True Rejection Rate; FRR stands for False Rejection Rate; FAR stands for False Acceptance Rate and TAR stands for True Acceptance Rate and are controllable.

	I	*G*
I_0	TRR	FRR
G_0	FAR	TAR

The performance and operating modes of most of the fingerprint matching systems can be determined through a plot called Receiver Operating Curve (ROC), which is shown in Figure-2, a plot of FRR against FAR. The point at which both FRR and FAR are equal to zero, performance of the system is the better and the point at which FRR = FAR, then the operating mode is referred to Equal Error Rate (EER).

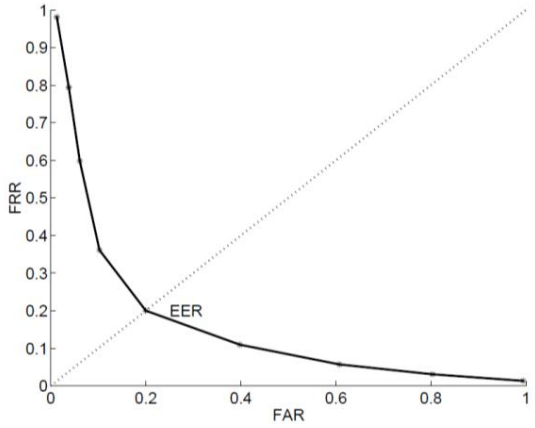

Fig.2.Receiver Operating Curve – FRR against FAR

Whenever fingerprints are captured, each time they differ slightly and so by calculating the cross correlation of two points simply, the matching cannot be carried out when comparing one fingerprint to another print of the same finger because of the presence of two types of distortions noise and shape. Noise distortion is caused by the sensor which can be reduced by applying appropriate filters whereas shape distortion is caused on the flat sensor by pressing the convex elastic fingerprint surface that results towards stretch, rotation and shear. Moreover, non-uniform pressure of finger also leads to shape distortions and these distortions cannot be easily compensated. Development of a reliable automatic fingerprint matching algorithm is a very challenging task, even though the fingerprints comprise the discriminatory information. Images of two different fingers seem like fingerprints and are having the same global configuration as shown in Figure-3.

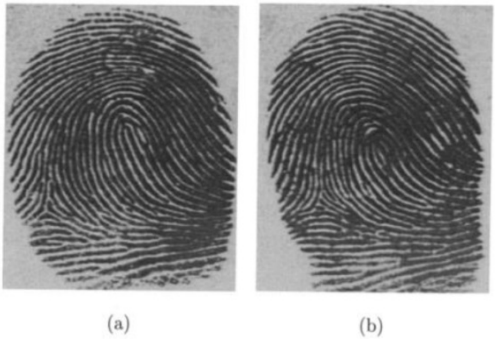

Fig.3.Like fingerprint images from two different fingers
Related Works

In this paper, related to this work Section II describes the existing traditional fingerprint matching methods minutiae-based and ridge-feature based verification systems and Section III describes the proposed correlation-based verification system that uses gray level information directly. The experimental setup of the proposed system is discussed in Section IV and Section V provides the results obtained followed by the conclusions.

II. RELATED WORKS

Classifications of fingerprint matching are: (i) minutiae based matching; (ii) ridge-feature based matching and (iii) correlation-based matching.

Minutiae based matching requires only a small part of fingerprint image for verification when template size is important and development of minutiae based algorithms depends upon the local discontinuities in the ridge flow pattern. Usage of these algorithms would be ideal where space restrictions impact and biometrics deployment, but this approach requires high quality of fingerprint image and extensive pre-processing operation in order to minimize the number of false minutiae detected erroneously from noisy fingerprint images.

Ridge-feature based matching often makes an assumption which is not valid in practical that the two fingerprints to be matched should be of approximately same in size. Using two different scanners, even two fingerprints are captured they may be of different sizes. In addition, if orientation is different for two images that may fail to match especially in minutiae based matching technique only because of relative change in their minutiae locations. Similarly, if the fingerprints to be matched are rotated images, then it is difficult to match them, because coordinate locations of all the minutiae points are changed due to rotation. It is also difficult to match the minutiae of two images in partial fingerprint matching because of the missing part of the fingerprint. Obviously small fingerprints have very few minutiae points and in such case minutiae based matching algorithms do not perform well. Moreover, reliable extraction of minutiae from poor quality images is another difficult task and registering such minutiae representation is very challenging one too. Hence, the designers worked on the fingerprint recognition looked for the features beyond minutiae and launched the alternative technique the most commonly used which is Ridge (or) Texture feature based matching technique.

II. CORRELATION BASED MATCHING

Correlation based matching is also referred as Image based matching and this algorithm uses both the micro and macro features of a fingerprint. Since this approach directly uses the gray scale fingerprint image without or very less pre-processing instead of using only the minutiae locations, computationally this approach is more efficient. In this work, a template fingerprint called primary fingerprint and a test fingerprint called secondary fingerprint are used. In the correlation based approach, from the primary fingerprint appropriate template is selected first, then it uses the template during matching to locate in the secondary fingerprint and compares the positions of both the fingerprints.

When the template is entire fingerprint, then during correlation possibilities are there for misalignments while aligning specific corresponding position due to displacements, rotations and distortions and hence it is not a robust one if the template is entire fingerprint because different positions and angles are to be considered and suppose to be measured. Moreover, some of the challenges, such as dealing with highly rotated images, additional computational power requirement especially for real time applications and locating incorrect template position, affect the matching performance.

As an alternate technique to overcome such challenges that exist in the template matching method which are mentioned above, matching a portion of image with larger image simply by sliding over the input is experimented. This technique matches a portion of image (i.e. an image patch) and larger image (i.e. input image) and finds the area of similarity (the match) to the image patch. Two primary components are required to experiment this, which are Source Image, which is expected to find a match and Template Image, the image patch to be compared to the source image. In this technique the image patch slides over the input image from left to right (or) up to down, one pixel at a time, compares at each location and to represent how “good” or “bad” the match at that location, computes a metric and returns a gray scale image, which denotes how much every pixel’s neighborhood matches with template.

In the template matching algorithm, the first crucial step is the appropriate selection of templates because localization at the right position will be easy in the secondary print as far as good templates are concerned whereas for bad templates which will not be. Generally, unique localization of the template should be in the fingerprint, that is at other locations the template should fit as badly as possible and at the same location as well as possible.

The size of the templates is to be considered as the first template property because template size should be an optimal one. If W x H is the size of input image and w x h is the size of template image then the size of the output image will be of (W-w+1) x (H-h+1). Then the small segments of the selected template in the primary fingerprint is used to locate the positions at which the best match in the secondary fingerprint and finally both are compared to declare the decision whether both the prints match or non-match.

In this work, among several types of template matching methods Correlation coefficient, Cross correlation and Sum of squared difference methods are implemented on Raspberry Pi and based on matching results their performance is computed. For the above said three experimented methods assuming Template image as T and Input image as I, after matching the numerical index are , and for correlation coefficient, cross correlation and sum of squared difference respectively in the range [0,1] at position (x,y) and the expressions for them are given below:

$$\eta_{corr\_coeff}(x,y)=\frac{\sum_{x',y'}[T'(x',y')I'(x+x',y+y')]^2}{\sqrt{\sum_{x',y'}T'(x',y')^2\sum_{x',y'}I'(x+x',y+y')^2}}$$

$$\eta_{cros\_corr}(x,y)=\frac{\sum_{x',y'}[T(x',y')I(x+x',y+y')]^2}{\sqrt{\sum_{x',y'}T(x',y')^2\sum_{x',y'}I(x+x',y+y')^2}}$$

$$\eta_{sqd\_diff}(x,y)=\frac{\sum_{x',y'}[T(x',y')-I(x+x',y+y')]^2}{\sqrt{\sum_{x',y'}T(x',y')^2\sum_{x',y'}I(x+x',y+y')^2}}$$

Where the average value of template T is $T'(x',y')$ and the average value of I in the region coincide with T is $I'(x+x',y+y')$. The expressions for the average values are given below:

$$T'(x',y')=T(x',y')-\frac{1}{w\times h}\sum_{x',y'}T(x',y')$$

and

$$I'(x+x',y+y')=I(x+x',y+y')-\frac{1}{w\times h}\sum_{x',y'}I(x+x',y+y')$$

where $x'=0,1,.....,w-1$ and $y'=0,1,.....,h-1$.

In addition, because of the introduction of two improvements over the original one these three methods are also experimented with their normalized method which is an enhanced version of the correlation method. First one is the consistent darkening and brightening of either image has no effect on the result, which is accomplished by subtracting the mean image brightness from each pixel value and so the results are invariant to the global brightness changes. Another one is the final correlation value Z is scaled to [-1,1] range such that if two images are identical, the Normalized Correlation Coefficient (NCC) will be 1.0, otherwise -1.0. The expressions for Z and normalization for the experimented three methods are given below:

$$Z_{(x,y)}=\sqrt{\sum_{x',y'}T(x',y')^2.\sum_{x',y'}T(x+x',y+y')^2}$$

$$\eta_{corr\_coeff\_normed}(x,y)=\frac{\eta_{corr\_coeff}(x,y)}{Z_{(x,y)}}$$

$$\eta_{cros\_corr\_normed}(x,y)=\frac{\eta_{cros\_corr}(x,y)}{Z_{(x,y)}}$$

$$\eta_{sqd\_diff\_normed}(x,y)=\frac{\eta_{sqd\_diff}(x,y)}{Z_{(x,y)}}$$

IV. EXPERIMENTAL SETUP

For the development of low cost Real Time Operating System (RTOS) based embedded modules a card sized single board computer called Raspberry Pi is made available and the same is utilized in this work for experimentation in real time. The block diagram of Raspberry Pi is shown in Figure-4 along with its features.

Raspberry Pi is an ARM processor based computer which supports various operating systems such as Raspbian (i.e. Linux), ubuntu, android, fedora and so on. Moreover, it is provided with python platform and C compatibility. The System on Chip is Broadcom BCM 2835 with built-in ARM 1176JZF-S @700 MHz processor, IV GPU videocore and 256MB RAM which is expandable up to 512MB. Though it is a single board computer, it is not provided with built in solid-state drive (or) hard disk for booting instead it uses a long term storage device SD card for booting and also bootable from network.

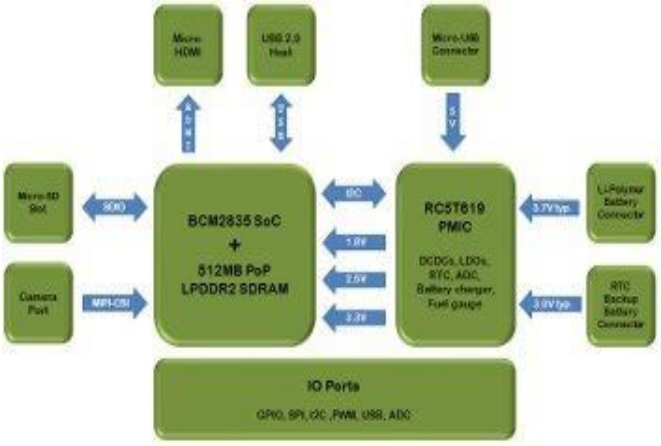

Fig.4. Block diagram of Raspberry Pi

Unlike minutiae and ridge based matching methods as far as correlation based (or) image based matching technique is concerned there is no need to extract minutiae because of the capability of dealing with bad quality fingerprint images and direct usage of richer gray scale information. However, preprocessing will be done if required in order to enhance the quality of the fingerprint image as soon as the input image is acquired thereby an appreciable matching is achieved with the template image(s) in the database. The functional flow diagram of this experiment is shown in Figure 5.

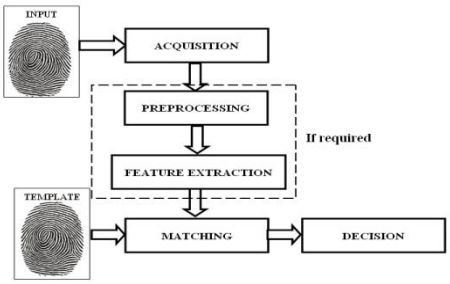

Fig.5. Correlation based matching – Functional flow diagram

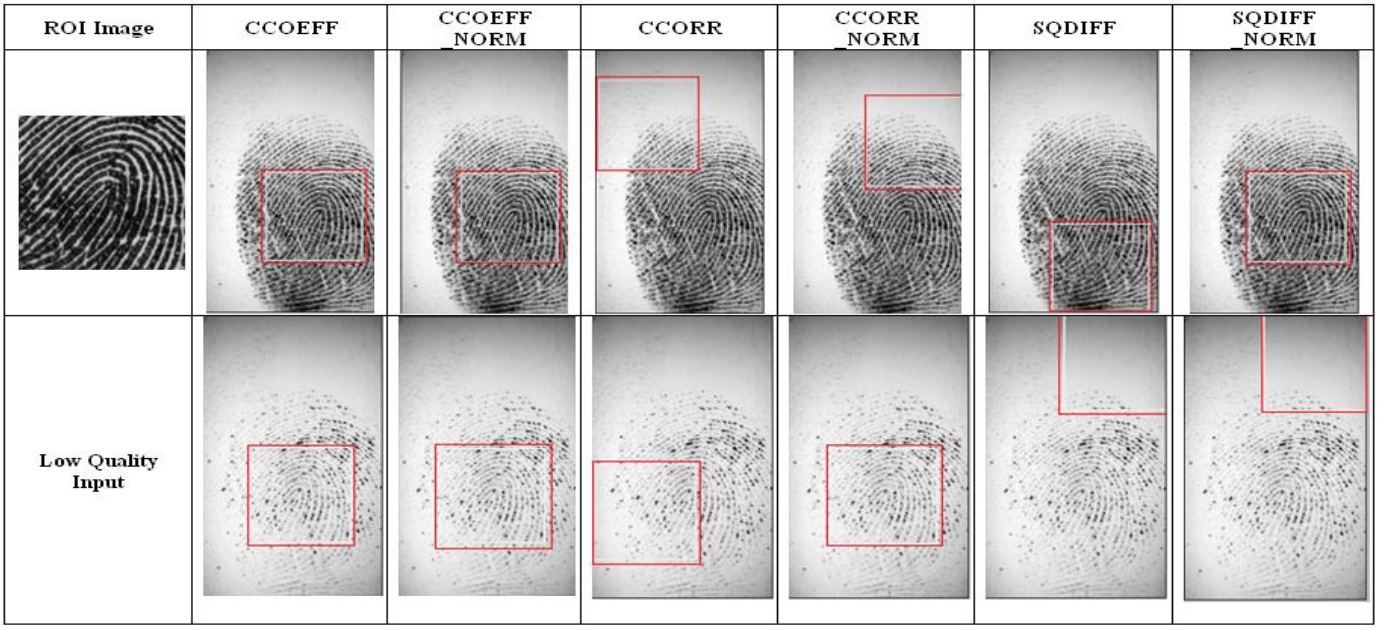

Fig.6.Experimental results for low quality fingerprint images on Raspberry Pi

Standard public databases, like FVC 2004 DB3 where manually perturbed fingerprints and FVC 2006 DB2 where fingerprints of a heterogeneous population which includes manual workers as well as elderly people, are used for initial stage experimentation followed by Secugen fingerprint scanner is introduced for real time experiment later.

V. RESULTS AND DISCUSSIONS

Experiments are done on Raspberry Pi using Normal, low quality, displaced, rotated, noisy and unsized with cut fingerprints with the three template matching methods so far discussed along with their normalization too. In this work, the identity verification experiments of each type of correlation calculation evaluate the performance for computational time and success rate. The observed results for low quality input fingerprint image during experimentation is shown in Figure-6 and Table-1, the time taken for computation is tabulated for various types of input images, is given.

From the experimental results among the three methods, it is inferred that the highest match set is given by Correlation coefficient method because of its exact differentiation of the correctly matched data set from the other wrongly matched data set. Hence, the large match correlation coefficient technique can be recommended and utilized for real time recognition applications to minimize the rate of false acceptance or false rejection while recognizing a person.

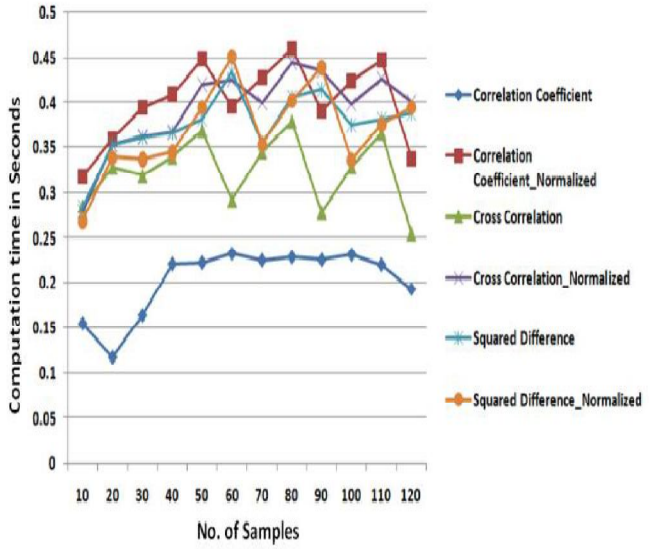

Figure-7: Plot between No. of samples and Computation time

For the recommended correlation coefficient approach, the threshold (or) cut-off value for normal and displaced fingerprint images is up to 0.98 and for rotated, low quality and with cut images is varying between . Based on the computation of various matching approaches, time taken for computation plot is shown in Figure 7.

Table No I: Various types of correlation approaches computation time

Type of Fingerprint Image	Computation Time in Seconds					
	Correlation Coefficient	Cross Correlation	Squared Difference	Correlation Coefficient Normalized	Cross Correlation Normalized	Squared Difference Normalized
Low Quality	0.164266	0.318972	0.359962	0.394086	0.362743	0.337266
	0.221685	0.339415	0.365872	0.408756	0.367126	0.344935
Noisy	0.226327	0.277997	0.413778	0.389974	0.435487	0.438765
	0.232237	0.3281	0.374607	0.424082	0.398276	0.336365
Un sized with cut	0.22082	0.365137	0.380494	0.446285	0.426395	0.375851
	0.19352	0.25484	0.387496	0.33687	0.400564	0.394264
Displaced	0.223153	0.368316	0.38123	0.44812	0.4203	0.394201
	0.233348	0.291643	0.433782	0.39563	0.42551	0.4509
Rotated	0.225838	0.345385	0.35428	0.427253	0.399831	0.35356
	0.229363	0.378466	0.405765	0.459574	0.444872	0.401923
Normal	0.155036	0.285022	0.284061	0.318092	0.279731	0.268482
	0.118187	0.327944	0.352427	0.359077	0.353013	0.339316

V. CONCLUSION

This paper discussed various matching techniques of approximately same in size fingerprints, different sized fingerprints captured from two different scanners, fingerprints with different orientations and so on under correlation based (or) image based (or) template based experimentation in real time approaches such as Correlation coefficient, Cross correlation and Sum of squared difference along with their normalization.

It is inferred from the experiments results obtained in Template matching, among several correlation calculation methods, correlation coefficient based template matching is the best method, since it exhibits the coefficient values of correctly matched image clearly than the mismatched images which is a very essential one for reducing the possibilities of false identification as imposter.

REFERENCES

[1] Nalini K.Ratha, Kalle Karu, Shaoyun Chen and Anil K. Jain, “A Real-Time Matching System for Large Fingerprint Databases”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.18, No.8, August 1996

[2] Qijun Zhao, David Zhang, Lei Zhang and Na Luo, “High resolution partial fingerprint alignment using pore-valley descriptors”, Elsevier, Pattern Recognition 43(2010) 1050-1061

[3] Reiko Iwai and Hiroyuki Yoshimura “Matching Accuracy Analysis of Fingerprint Templates Generated by Data Processing Method using the Fractional Fourier Transform”, International Journal of Communications, Network and System Sciences, 2011, 4, 24-32

[4] Liu Wei-Chao and Guo Hong-tao “Occluded Fingerprint Recognition Algorithm based on Multi Association Features Match”, Journal of Multimedia, Vol.9, No.7, July 2014

[5] Prateek Verma, Maheedhar Dubey, Praveen Verma “Correlation based method for Identification of Fingerprint – A Biometric Approach”, International journal of Engineering and Advanced Technology (IJEAT), ISSN:2249-8958, Volume-1, Issue-4, April 2012.

[6] Arunkumar L and Arun Raja A “Biometrics Authentication using Raspberry Pi”, International journal for Trends in Engineering and Technology, Volume 5 Issue 2, May 2015.

[7] Yesu Raja A and Arumuga Perumal S “Survey on Fingerprint Verification Methods based on Different type of Feature Extraction”, International Research Journal of Engineering and Technology (IRJET), Volume 2, Issue 04, July 2015.

[8] Dr Sunil Kumar Singla "A Review of Image based Fingerprint Authentication Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.

[9] Jianjiang Feng, Zhengyu Ouyang, Anni Cai "Fingerprint matching using ridges", Elsevier, Pattern Recognition 39 (2006), 2131-2140.

[10] Praveen Kumar Nayak and Devesh Narayan "Mutimodal Biometric Face and Fingerprint Recognition using Adaptive Principal Component Analysis and Multilayer Perception", International journal of Research in Computer and Communication Technology, Vol 2, Issue 6, June 2013.

[11]Shruthi A B, Srinivasa M G and Sheshagiri Jois "Fusion based Fingerprint Recognition based on CLBP descriptor and DWT", IOSR Journal of VLSI and Signal Processing, Volume 5, Issue 3, Ver.I, May - June 2015, pp 45-49.

[12]Gurgen Khachatrian and Hovik Khasikyan "Correlation based Password generation from Fingerprints", International journal of Information Models and Analyses, Vol.1, 2012.

[13]Jin Fei Lim, Renee Ka Yin Chin "Enhancing Fingerprint Recognition using Minutiae-based and Image-based Matching Techniques", International conference on Artificial Intelligence, Modeling & Simulation, 2013.