1st International Conference on Applied Soft Computing Techniques
22 & 23.04.2017
In association with
International Journal of Scientific Research in Science and Technology

Multi Biometric Security Pattern Using finger vein and finger print

S. Ilankumaran[1], Dr. C. Deisy[2]
Department of Information Technology, K.L.N. College of Engineering, pottapalayam, Sivagangai, Tamil Nadu, India
ilankumaran.s@klnce.edu
Department of Computer Science, Thiagarajar College of Engineering, Madurai, India
cdcse@tce.edu

ABSTRACT

Today India is moving towards cashless transactions , transformation its cities into smart cities , constructing varies potential nuclear power plant , providing aadhaar card for each citizen in the country which leads us to the need of a promising technology for the above all functionality , which should provide better security for all endorsement system because of above all functions should be performed only be the authenticated person otherwise its effect will be enormous by affecting individual person or whole country. For the promising technology , here we have proposed a new methodology which use finger vein and finger print as a key factor in which we extract both the finger vein and finger print from user to find out whether they are the authenticated users before they access the all endorsement system. For the feature extraction, Competitive Matching Code (CMC) has been used. This identification system will be well suited for endorsement system comparing to other biometric system and provide better results on EER and total processing time

Keywords: Competitive Matching Code, EER, Nearest Neighbour

I. INTRODUCTION

Biometric Authentication system is a process that validates the individual identity of person who is going to access the potential systems by evaluating their biological and behavioural traitssuch as it can besignature, palm prints, fingerprints, iris patterns and voice spectrum of that particular person. But basically there some authentication schemes are used in real world to examine whether person is authenticated user, first schemes which make use of external hardware material such as the Id cards, metal keys to authenticate them. Some schemes is based on secret software security key such that password, pattern, pin etc. finally some scheme is evaluating the biometric recognition of a particular person before they access the potential system. But First scheme can be easily hacked by duplicated the external hardware material, second scheme lead authenticated user not able to access in case if they forget their secret password lead to reset the entire security system. This problems can be come over by using Biometric authentication system in which the user need not remember any secret keys and user should physically present at the time of authenticating while using the biometric system such as finger print, palm prints, iris patterns. but it can easily extracted from the authenticated user without any acknowledge of them. it became a major problem in biometric authentication system it can resolve by the usage of finger vein which is unique identification declared in 2008 which cannot extract without any acknowledge of particular user and which overcome all the above problem. We consider the finger vein and finger print as key factor for the authentication system.

II. SYSTEM OVERVIEW

2.1. Capturing Finger vein image.

Finger vein images are captured by using near infra-red (NIR) camera through light transmission methodologies which are used here. In the method the finger dorsal is placed at NIR and finger vein is captured by passing the light through the finger. To get high contrast images, we have adapted light transmission method as shown in fig1

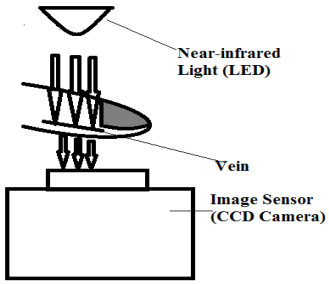


Figure 1: Light Transmission method

Figure 2: (a) Finger vein Image as raw

Figure 2: (b) Finger Print Image as raw

2.2. Capturing finger print Image

Finger print can be captured using optical scanner and capacitive scanner .Optical scanner is basically works as digital photograph, initially capture the photograph of finger and process it through ccd sensor and cmos sensor to avoid dirty black photograph and finally produce the image from which the finger print image is obtain. Capacitive scanner electrically measuring the distance of the hollows between the ridges in the particular finger and build up the finger print image based on the measuring distance.

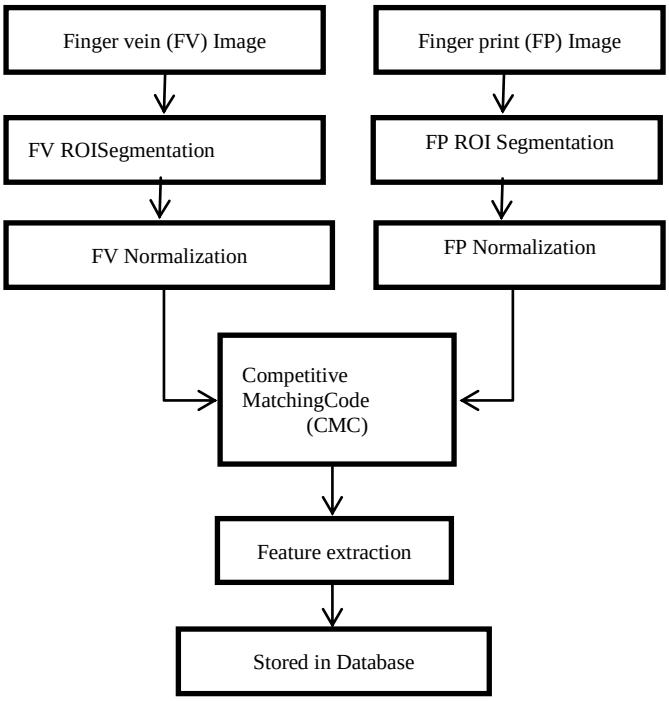


Figure 3: Proposed Verification frame work

2.3. Recognition Frame work:

The proposed recognition frame work is shown in Figure 3. After capturing both the images, the pre-processing model fulfils the ROI extraction. The extracted ROI of the finger vein image is normalized for size and intensity. Similarly the finger print image is pre-processed and the normalized. Subsequently, a feature extraction algorithm called which used on the normalized sub-image. Gabor filters are applied to these normalised finger vein and finger print images and their respective output are used to obtain the magnitude-preserved CMC code [1].CMC code is a state of biometric algorithm known as a competitive code which preserves the magnitude information of the filtered image and is used for further processing. The extracted features corresponding to the code map is stored in the Nearest Neighbour (NN) classifier and used for the verification process.

2.4 Finger print Segmentation

We have adapted the well know traditional algorithm which is used for segmentation of oldest biometric security factor which is fingerprint by mean and variance based algorithm defined by Jun ma et.al [10] In generally finger print pattern composed by two regions they are foreground and background .among these two, foreground consists of important information which is essential thing for recognising correct finger print pattern in biometric authentication system .Since background consists of noise regions here it contributes to the extraction of trivial details in the process .To restricts those type of trivial details, we perform segmentation for finger print. The main purpose of segmentation is to separate the foreground and background

Mean and variance based algorithm

1) Start with Divide the fingerprint image I into non over lapping blocks with size M*N.
2) Compute the mean value Mean for each Block

$$\text{Mean} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} I(i,j)}{M * N}$$

Where I (i, j) is the pixel gray value of the i^{th} row and the j^{th} column.

3) Use the mean value to drive the variance value for each block

$$\text{Variance} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} [(i,j) - mean]^2}{M * N}$$

4) Select a threshold value which works on different images. If the Variance is larger than threshold value then block is considered as foreground otherwise that is background.

2.4.1. Finger vein Segmentation

The fingers are located in the middle of the raw images. In the finger vein images, the horizontal direction on the finger edges has obvious jumps. Thus, we used a gradient operator as shown in Figure 4 to find the vertical lines which are the finger edges. In moving the mask from the middle of the image to the side, an edge was detected if the norm of the gradient was higher than the threshold. The left edge was obtained by image convolution by using the gradient operator shown in Figure 4(a), and the mask in Figure 4(b) is to detect the right one. The threshold was experimentally set as 212.

1	0	-1
2	0	-2
3	0	-3
4	0	-4
5	0	-5
6	0	-6
7	0	-7
6	0	-6
5	0	-5
4	0	-4
3	0	-3
2	0	-2
1	0	-1

Figure 4 (a)

-1	0	1
-2	0	2
-3	0	3
-4	0	4
-5	0	5
-6	0	6
-7	0	7
-6	0	6
-5	0	5
-4	0	4
-3	0	3
-2	0	2
-1	0	1

Figure 4 (b)

Figure 4: Edge Detection Masks

The edge lines in the X (horizontal) direction were set to 100 pixels inwards the lower and upper bounds of the captured finger area. Then, the rotational alignment algorithm proposed in [4] was applied. We normalized every row in the finger area to the same length by using linear interpolation. The final size of the finger regions was normalized to 100 x200 pixels. The segmented finger vein image is shown in Figure 5.

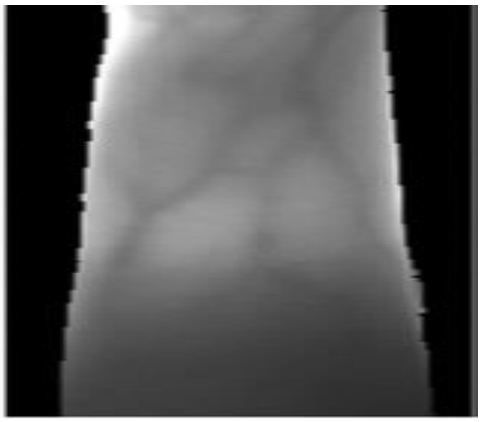


Figure 4: Finger vein image after Segmentation

Figure 5: finger print image after Segmentation

2.5. Feature extraction

The sub images of the finger vein and finger print are applied to the Gabor filter. A best extraction tool Gabor filters which have been widely used in biometric system gives three types of output such as magnitude code, Phase code and Orientation code. These outputs can be used both by individual or combining all the codes in order to apply to a system. A **C**MC Coding scheme that combines the magnitude code and orientation code of Gabor filter [1] is adapted in this paper. A two dimensional even-symmetric Gabor filter can be defined in equation (4)

$$G(x,y) = e^{(-\frac{x_\theta^2}{\sigma_x^2}+\frac{y_\theta^2}{\sigma_y^2})} \cos(2\pi f x_\theta) \quad (4)$$

$$\text{Where} \begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad (5)$$

Here, f denotes the filter centre frequency is the orientation parameter as in equation (5), and

$$\theta = \frac{j\pi}{J} \qquad , J = \{0,1,2....,J-1\} (6)$$

σ_x *and* σ_y, are the standard deviations of the elliptical Gaussian envelope, x_θ *and* y_θ are rotated versions of the coordinates (x, y) of the Gabor filter. The number of Gabor filters J is fixed to 6.

2.6. Magnitude Preserved CMC Scheme

The **CMC** code scheme [1] has been widely used in palm-print and FKP recognition. The **C**MC coding scheme that combines both the finger vein and finger print images is given in Algorithm 1. The Gabor filter is applied to finger vein and finger print images and the orientation code for finger vein and finger print images are OV Code, OPCode respectively and the Magnitude code for finger vein and finger print images are MVCode, MPCode respectively.

Algorithm 1:

Comparative Competitive Coding scheme

InputOVCode, MVCode, OPCode,MPCode

OutputCMCcode

For all CMC codeDo

If OVCode(x,y)= OPCode(x,y)then

CMC code=OVcode(x,y)

Else if MVCode (x, y) <MPCode (x, y) then

CMC code (x, y) = MVCode (x, y)

Else if MVCode (x, y) >MPCode (x, y) then

CMC code(x, y) = MPCode (x, y)

Else if MVCode(x, y) = MPCode (x, y) then

CMC code(x, y) = J

In Algorithm 1, the outputs of the Gabor filter, i.e. Magnitude code and Orientation code are considered as the input.

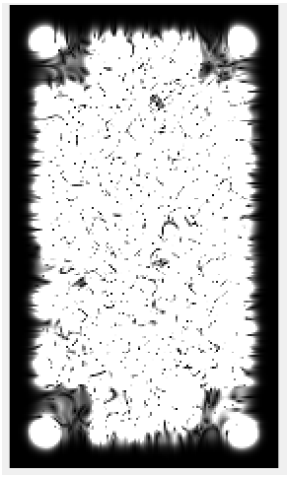


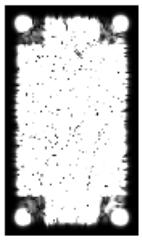
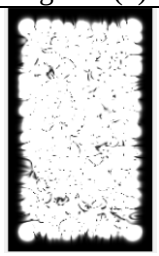
Figure 6: Final image stored in database

The Gabor filter results for some of the pixel will not have much variation, due to low quality image. So the lower value of Magcode that corresponds to the Oricode value is stored. The resulting output iscalled as CMC code. The final image stored in the database is given in Figure 6.

III. Results and Discussions

Pre-processing of images is done for ROI extraction.The segmentation of finger print is done by mean and variance. The edges of the finger vein image are detected using edge detection masks shown in Figure 5 as explained in section 2.4 with a threshold of 212.The ROI of finger vein are extracted .The ROI extracted for sample images of the person, are given in Fig.7.

	Sample 1
Finger vein after Registration and ROI extraction.	
Finger print after Registration and ROI extraction.	

	Sample 1	
	Oricode	MagCode
Finger vein image	 Figure 8(a)	 Figure 8(b)
Finger print image	 Figure 8(e)	 Figure 8(f)

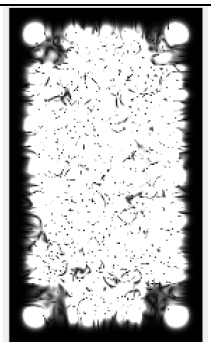
CMC code	 Figure 8(i)

Figure 8: CMC Code formulations.

IV. Conclusion and Feature work

This paper presents a new methodology to improve the performance of authentication system using finger vein and finger print. The EER is 1.5441 % where the threshold level is 0.256.0. The advantage of using this method is finger veins and finger prints are the biometric feature which seems to be too tough to get from the user without their knowledge, comparing to the other biometric features. So this method will provide better choice for authentication system, the performance and accuracy can be increased using the proposed feature work.

V. REFERENCES

[1] Wenming Yang, XiaolaHuang, "Comparative competitive coding for personal identification by using finger vein and finger dorsal texture fusion "Information Sciences 268 (2014) 20–32.

[2] Ajay Kumar, K. VenkataPrathyusha, "Personal Authentication Using Hand Vein Triangulation and Knuckle Shape", IEEE Transactions on image processing, vol. 18, no. 9, sept.2009.

[3] L. Zhang, L. Zhang, D. Zhang, H. Zhu, "Online finger-knuckle-print verification for personal authentication", Pattern Recognition 43 (7) (2010) pp.2560–2571.

[4] Zhi Liu and Shangling Song, "An Embedded Real-Time Finger-Vein Recognition System for Mobile Devices", IEEE Transactions on Consumer Electronics, Vol. 58, No. 2, May 2012

[5] J. Yang, X. Zhang, "Feature-level fusion of fingerprint and finger-vein for personal identification", Pattern Recognition Letters 33 (5) (2012) pp.623–628.

[6] W.M. Yang, Q. Rao, Q.M. Liao, "Personal identification for single sample using finger vein location and direction coding", 2011 International Conference on Hand-based Biometrics (ICHB), 2011, pp.1–6.

[7] W.K. Kong, D. Zhang, "Competitive coding scheme for palm print verification", 16th International Conference on Pattern Recognition (ICPR), 2004, pp. 520–523.

[8] V.Ramya, P.Vijaya Kumar, B.Palaniappan, "A Novel Design of Finger Vein Recognition for Personal Authentication and Vehicle Security", Journal of Theoretical and Applied Information Technology 10th July 2014. Vol. 65 No.1.

[9] Jose Anand, T. G. Arul Flora, Anu Susan Philip, "Finger-vein based biometric security system", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, 2013.

[10] Jain, A. K., Flynn, P. J. & Ross, A. eds., 2007. Handbook of biometrics. Springer.

[11] Jun Ma, Xiaojun Jing, Yuanyuan Zhang, Songlin Sun, Hai Huang "Simple effective finger print segmentation algorithm for low quality images"