Embedding of Iris Data to Hand Vein Images Using Watermarking Technology to Improve Template Protection in Biometric Recognition

N. Lalithamani
Department of Computer Science and Engineering
Amrita School of Engineering Amrita Vishwa Vidyapeetham
Amritanagar (PO) Ettimadai, Coimbatore – 641 112
n_lalitha@cb.amrita.edu

Dr.M.Sabrigiriraj
Department of Electronics and Communication Engineering
SVS College of Engineering, JP Nagar, Arasamplayam
Coimbatore – 642109
sabari_giriraj@yahoo.com

Abstract—**Biometric recognition is noteworthy method for recognition of person in recent years. Here, a common concern is biometric security which is the privacy issues derived from storage and misuses of the template data. In order to handle this issue, researches have proposed different algorithms to be confronted by security of biometric systems. Two major ways are, (1) Encryption, and (2) watermarking by securing biometric images and templates. In this paper, we utilise a watermarking technology to improve the template security in biometric authentication. According to, two modalities such as, iris and hand vein is taken to preserve the characteristics of liveliness and permanency. Our proposed technique for embedding of iris data to hand vein images using watermarking technology to improve template protection in biometric recognition is done based on the following steps, i) pre-processing of iris and hand vein images, ii) iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images. In the recognition phase, iris pattern is extracted from the embedded image and then, matching is done with query images. The final decision of authentication is done based on the product rule-based score level fusion. The implementation is done using MATLAB and the performance of the technique is analysed with FAR, FRR and accuracy.**

***Keywords*—template; watermarking; embedding; extraction; authentication**

I. INTRODUCTION

Increased usage of electronic commerce and the adversarial effects of terrorism have increased application of authenticating persons. Nowadays, eyes have turned to use biometric concepts to meet the requirement [1]. Biometric system, which is a pattern recognition system, exploits a user's inimitable physical traits to identify/ authenticate him/her [2]. Two major groups of tasks that contribute in a biometric system are identification and authentication [3]. Biometric techniques considers numerous traits such as facial thermo-gram, hand vein, gait, keystroke, odor, ear, fingerprint, face, hand geometry, retina, palm print, iris, voice and signature [4]. Biometrics exhibits as a potential tool when combined with traditional authentication schemes that greatly support in establishing authenticity [5].

Few serious issues that adhere with the biometric system and data are their weakness against security issues and adversarial attacks. Hence, fool-proof methodologies have to be adopted to store biometric templates, instead of using plain texts [6]. Template based methods in biometric systems apply global-level processing to extract features after cropping certain sub-image from original sensory image [7]. Biometric template can be created with the aid of feature extractor or key binding algorithms [8]. Such biometric templates can be kept safe and effectively protected by exploiting watermarking techniques [7]. Biometric watermarking embeds biometric knowledge into a digital object and hence it connects a human subject with digital media [9]. When key based embedding algorithm and pseudo noise pattern are used, digital watermarks can be predominantly inserted into the source data as transformed digital signal, through which the security can be substantially improved [10]. Watermarking can be said as an art of inserting crucial information which cannot be recognized by humans. It can ensure multimodal biometric authentication if the template is concealed with other biometric representation [11]. It can be applied to safeguard the intellectual property rights by embedding the proprietary information in the source data [12]. However, it is expected to be robust against some attacks against biometric system [13]. Least significant bit (LSB) method is identified as a best popular watermarking method in which the least significant bits of pixels are replaced for information hiding [10].

Nevertheless, the increase in security needs have necessitates the research on developing permanent form of, irreproducible biometrics. One among such biometrics is iris of humans. Iris recognition works on the basis of visual features such as rings, freckles, furrows and corona. Due to the high degree of randomness in such features, iris recognition is found to be very challenging [14]. Further developments on infrared technology that are observed in the recent days, more accuracy can be accomplished by including more human features, especially like probing veins and hand backs, which are richer in veins than fingers. This leads research concepts in hand vein recognition as one of hot spot areas in biometric authentication [15].

978-1-4799-6085-9/15/$31.00©2015 IEEE

Patterns available in the hand veins are found to be distinctive between the individuals and remain same for long term throughout the human life [16]. These vascular patterns are complex that lead to determine ample feature sets to ensure precise personal identification [17, 11]. From the literature survey, [3], [4], [18], [19], [20], [21] , [10] and [22], the researchers had discussed about various template security method and their importance in security of biometric template protection. Also, we found that there is need of robust biometric recognition technique for template protection. So here we design a biometric recognition system by embedding iris data to hand vein images using watermarking technology.

The main contribution of the paper is as follows

i) We propose a secure watermarking scheme to improve security of the templates used in biometric authentication.
ii) The embedded iris template is extracted in the recognition phase and matching is done using proposed algorithm.

The reminder of the paper is structured as follows: Section II presents the proposed methodology of embedding iris data with hand vein images. Section III discusses the experimental results and Section IV concludes the paper.

II. Proposed embedding iris data to hand vein images using watermarking technology

The aim of our biometric recognition system is to improve the template protection by embedding the iris data to hand vein images based on watermarking technology. The proposed technique of embedding of iris data to hand vein images using watermarking technology consist of following steps, i) pre-processing of iris and hand vein images, ii) iris template extraction, iii) Vein extraction, iv) Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images.

(i) Irish Image Pre-processing and key generation

The initial stage of our proposed method is pre-processing in which the iris images are acquired and process to extract the iris key. By subsequent localization, the information related with iris part is selected from the entire image.

a) Iris Localization

Nevertheless, localization can be said successful, when it is accomplished with minimum absences in the number of pixels inside the circle boundary. The reduction of number of pixels inside the circle boundary leads to fast and easy computation. Then, the peaks of the gradient image can be localized using non-maximum suppression. The process of non-maximum suppression on a pixel with its gradient imgrad(x,y) and orientation theta(x,y) can be framed by using an edge intersects through two of its eight neighborhood connected pixels. A point at (x,y) can be said as maximum in such a way that its pixel value should not be smaller than the pixel values of the two intersection points. Subsequently, hysteresis thresholding is performed so that the weak edges that are below certain threshold value and that are not connected with an edge, which is above high threshold, through a chain of pixels, which are above the low threshold, can be eliminated. Boundaries of the iris and the pupil are determined to perform edge detection process. These boundaries and radii can be determined by integro-differential operator proposed by Daugman. It is given in equation (1) as

$$\max(r,a_0,b_0)\left|G_\sigma(r)*\frac{\partial}{\partial r}\oint_{r,a_0,b_0}\frac{I(a,b)}{2\pi r}ds\right| \tag{1}$$

The aforesaid operator searches the gradient image along with boundary of circles with high radii and hence it behaves as a circular edge detector. The circles centers and radii can be calculated using the maximum sum, which can be determined based on the likelihood of all circles.

Few concerns are associated with Hough transformation. They are, determining threshold values by trial and error basis and intensification in computation. These issues can be resolved by using eight-way symmetric points in the circle for each search point and radius. Thresholding concept can be used to segregate eyelashes and these pixels are marked as noisy pixels, because they are not included in the iris key.

b) Image Normalization

The next stage after iris segmentation is normalization to generate iris key and their comparisons. Normalization process is comprised of two steps that are uwrapping the iris and conversion of it into polar equivalent. This can be done using Daugman's rubber sheet model. Center of the pixel is set as the reference point and the points are converted from Cartesian scale to polar scale using a remapping formula.

The modified version of the model is given in equation (2) as follows.

$$R' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2} - \alpha - R_1{}^2 \tag{2}$$

Where, R_1 represents iris radius.

$$\alpha = a_x{}^2 + b_y{}^2$$

$$\beta = \cos\left(\pi - \arctan\left(\frac{b_y}{a_x}\right) - \theta\right)$$

Radial resolution and angular resolution of the image are set to 100 and 2400, respectively. An equivalent position for each iris pixel is determined in the polar scale. "interp2" function is exploited to interpolate the normalized image to size of the original image. A normalized value can be obtained by dividing NaN, which is obtained through the parts in the normalized image, using the sum of the parts.

c) Encoding

Generation of iris key is defined as the final process for which the most unique feature in the iris pattern is extracted.

As the assigned phase angles are independent to the image contrast, only the phase information from the patter is used. Due the dependency of amplitude information with inappropriate factors, it is not used. According Daugman, phase information can be extracted using 2D Gabor wavelets. It estimates the quadrant in which the resulting phasor lies. This can be accomplished using the following equation (3).

$$H\{R_e,I_m\}=\text{sgn}\{R_e,I_m\}\int_\rho\int_\phi I(\rho,\phi)e^{-i\omega(\theta_0-\phi)}.e^{-(r_0-\rho)^2/\alpha^2}e^{-(\theta_0-\phi)^2/\beta^2}\rho d\rho d\phi \quad (3)$$

Where, $H\{R_e,I_m\}$ has both the real and imaginary part with 1 or 0 as their constituents based on its quadrant.

Gabor filter can be comfortably used by segregating a 2D normalized pattern into numerous 1D wavelets and convolving them with 1D Gabor wavelets.

Log-gabor filters are more suitable than Gabor filters for representing natural, because Gabor filters fails to outperform in precisely representing high frequency components. Log-Gabor filter can be represented as in equation (4) below

$$G(f)=\exp\left(\frac{=(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right) \quad (4)$$

Gabor – convolve function results in complex value convolution output with size similar that of the size of input image.

Formation of iris key can be done using the output of Gabor-convolve by assigning dual elements to every pixel of the image. Each element has either 1 or 0 based on positive or negative sign of the real and imaginary part, respectively. If the magnate of an element is very small, then it is considered as noise bits and they are integrated with noisy portion that is obtained from normalization.

(ii) Hand Vein image pre-processing and feature extraction

In this the dorsal hand vein images are acquired by an array of infrared light-emitting diode (LED) and a thermal camera. Further to reduce the noise, the obtained hand vein image is pre-processed initially.

Then apply mask to the pre-processed hand vein image. The size of the image obtained after masking is same as the input. Then find the values greater than zero values in the obtained masked image. After this the blood vessels from the hand vein image are obtained by using kirsch's template extraction method. It takes a single masked pixel of a hand vein image with a size of 3×3 and determines it strength of the edges by rotating it in 45 degree increments through all 8 directions. It is defined by the equation (5) given below,

$$K_{a,b}=Max_{d=1..8}\sum_{n=-1}^{1}\sum_{m=-1}^{1}W_{nm}^{(d)}\cdot p_{a+n,b+m} \quad (5)$$

Were d is the 8 direction as given below,

$$d=\{W^{(1)},W^{(2)},W^{(3)},.....W^{(8)}\}$$

Finally the maximum magnitude for the selected mask pixel of an image at all direction is determined. Then the next process is called local thresholding which is applied here to separate the foreground from the background of the hand vein image. It is different from conventional thresholding process which changes the threshold dynamically over the images. Here thresholding is done by setting all pixels of the hand vein image whose intensity values are above a threshold is foreground value and all the remaining pixels is consider as background value.

The main idea of the method is calculating the mean $m(x,y)$ and variance $v(x,y)$ of the points in $r\times r$ neighbourhood of every pixel. Then the segmentation is done based on the equation (6) given below,

$$T(x,y)=m(x,y)+c\times v(x,y) \quad (6)$$

Where, $T(x,y)$ is the threshold, c is the coefficient of correction.

The pixel value below the threshold is considered as vein domain. The mean and variance of the local dynamic thresholding method is calculated by the equation (7) and (8) given below,

$$\text{Mean } m(x,y)=\frac{1}{r^2}\sum_{i=x-r/2}^{x+r/2}\sum_{j=y-r/2}^{y+r/2}f(i,j), \quad (7)$$

and

$$\text{Variance } v(x,y)=\sqrt{\frac{1}{r^2}\sum_{i=x-r/2}^{x+r/2}\sum_{j=y-r/2}^{y+r/2}f^2(i,j)} \quad (8)$$

Here the variance of our method calculated as by the modified equation (9) given below,

$$v(x,y)=\sqrt{\frac{1}{r^2}\sum_{i=x-r/2}^{x+r/2}\sum_{j=y-r/2}^{y+r/2}(f(i,j)-m(x,y))^2} \quad (9)$$

Here the value obtained by kirsch' method is sorted and calculated its length. It is further multiplied as by the given equation (10) below,

$$L=0.97\times \textit{Length of the blood vessel obtained} \quad (10)$$

Then choose the obtained pixel value as a threshold. Finally the pixel value below the threshold is selected as the features of the hand vein.

(iii) Embedding of iris pattern to hand vein image

The steps included in embedding iris key to vein images is given below,

The input is iris key image $I(x,y)$ and the watermark image is the hand vein image $H(x,y)$. The output is the watermarked image $H_w(x,y)$.

The various steps in watermark embedding is

1)The input watermark image $H(x,y)$ is divided into blocks of size $B_1,B_2,B_3......B_n$ of size $M\times N$. Then the divided block is sorted. From the sorted block of the input image $H(x, y)$ the first wavelet coefficient with positive phase and the value below the threshold $T(x, y)$ is chosen.

2)Then the second LSB of the selected block of the watermark image $H(x, y)$ is replaced by one bit from the iris template $I(x, y)$. This process is shown below in equation (11),

$$C_w^{'}(x,y) = \begin{cases} LSB(C_w(x,y) = I(x,y) if\ phase\left(C_w(x,y)\right) \geq 0 \,\&\, C_w(x,y) < T(x,y) \\ C_w(x,y) if\ phase\left(C_w(x,y)\right) < 0 \end{cases} \tag{11}$$

Where, $C_W(x, y)$ is the coefficient in block B_n. Here $T(x, y)$ is the threshold whether the watermark bit is inserted or not.

4)If the number of bits in the iris template $I(x, y)$ is less than the number of blocks in hand vein image, then all bits of the iris template $I(x, y)$ can be embedded.

5)After embedding all the bit of the iris template $I(x, y)$ in hand vein image an IDWT (Inverse Discrete Wavelet Transform) is applied to the watermarked hand vein coefficient to generate the final secure watermarked hand vein image. the watermark embedding process is shown in the figure below,

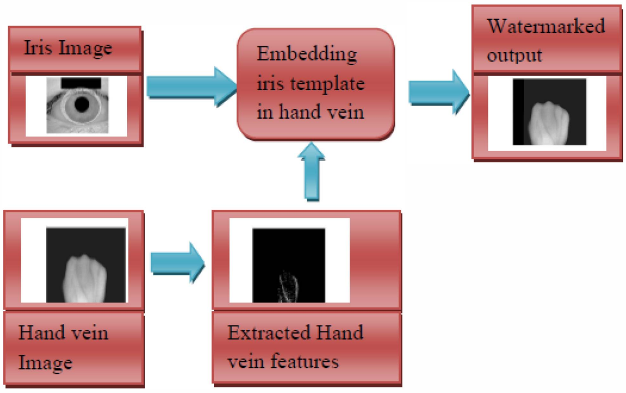

Iris Image
Embedding iris template in hand vein
Watermarked output
Hand vein Image
Extracted Hand vein features

Fig. 1. Watermark Embedding

(iv). Recognition Phase using Score level fusion

The recognition phase is divided in two major steps.

Step.1. Watermark extraction

In this recognition phase the watermarked image is given as input and the iris key and hand vein features are extracted. The watermark extraction phase consists of various steps.

The input is watermarked image $H_W(x, y)$ and the size of watermarked image $H_s(x, y)$ and the output is recovered watermark image $R_w(x, y)$.

1)The watermarked image is divided in to the detail sub band of watermarked image in to blocks. The each block of the watermarked image is of size $2M - 1 \times 2N - 1$.

2)Identify the value below the threshold $T(x, y)$ in each block which has the first coefficient with positive phase.

3)The pixel value 1 from the watermarked image is extracted if the embedded pixel value is greater than the mean pixel value otherwise pixel value '0' is extracted. This process is repeated until all the pixels from the watermarked image are y given in equation (12) below

$$H_S^{'}(x,y) = \begin{cases} 1, & B_{(i)} > B_n, 0 < i < n \\ 0, & otherwise \end{cases} \tag{12}$$

4)A matrix equal to the size of watermark image $H_W(x, y)$ and the extracted pixels are placed in it to obtain the watermark image $H_S^{'}(x, y)$.

In recognition phase the both iris and vein image of an individual is taken. Then both the obtained iris image and the hand vein image are pre-processed separately as by the above procedures. After this pre-processing stage the iris key from the iris image and the vein features from the vein image are obtained. Further in order to find whether the input user is genuine or imposter we have to compare the obtained feature with the feature stored in the database. But in the database the iris key is embedded in the hand vein image to improve the template protection. So here we have to extract the iris key and vein image separately.

Step 2: Matching

Now the distance between iris key generated from the input query image and iris key extracted from the embedded image stored in database is determined. The matching distance for the input iris key and the extracted iris key from embedded image is denoted as D_{Iris}. Likewise the pre-processed vein image of the same person is matched with the vein image feature extracted from the embedded image stored in database. Finally a matching distance $D_{\cancel{Vein}}$ for the vein image is determined. Further the two normalized similarity distance D_{Iris} and D_{Vein} are fused linearly using sum rule as given in equation (13) below,

$$MS = \alpha * D_{Iris} + \beta * D_{Vein} \tag{13}$$

Where α and β are two weight values that can be determined using some function. In this paper a combination of linear and exponential function is used. The value of weight is assigned linearly if the value of matching score is less than the threshold; otherwise exponential weightage is given to the score. The value of MS is used as the matching score. So if matching score is greater than threshold value then individual is allowed to enter the system otherwise rejected.

III. RESULTS AND DISCUSSION

In this section we analyzed and discussed about the proposed technique. The experimental setup and evaluation metrics are discussed in section III.A. The dataset description is given in section III.B. The experimental result is given in section III.C. The performance evaluation is given in section III.D.

A. Experimental Setup and Evaluation metrics

We had implemented the proposed method using MATLAB in a system having 6 GB RAM and 2.6 GHz Intel i-7 processor. Also, the evaluation metrics used here is the accuracy. The accuracy in multimodal biometric is computed based on FAR (False Acceptance Rate) and FRR (False Rejection Rate). Here, FAR is rate for which the system identifies the non-authorized person. It occurs due to the wrong matching of template with the input. False Rejection Rate is the rate of authorized person incorrectly rejected by the system. Here FAR is represented as,

$$FAR(t) = \frac{GMS}{NGRA}$$

Were, GMS means genuine matching score and NGRA means Number of Genuine Recognition Attempts

Also the FRR is calculated by

$$FRR(t) = \frac{IMS}{NIRA}$$

IMS ⟶ Imposter Matching Score
NIRA ⟶ Number of Impostor Recognition Attempts

B. Dataset Description

In conjunction with the University of Bath, Smart Sensor Limited has collected a significant database of high quality iris images for use in research and evaluation. The pixel resolution of the collected iris image is 1280 x 960. Currently the full database consists of 800 people, i.e., 1600 eyes with 20 images of each left and right eye. A deliberate decision has been taken to start off with images of pristine quality, as there is a significant need in the scientific and research community to understand how iris recognition performance is affected by various image degradations including focus blur, motion blur, image compression, occlusions and gaze angle. Many of these degradations can be simulated for the purposes of research under mathematically calculated conditions which are usually unavailable when capturing images from commercial iris cameras.

In addition to the high quality images, large numbers of 'non-ideal' images from the same subjects can also be made available on request [23].The hand vein database is a sample consists of images of 100 hands where each hand has 5 images, hence totalling to 500 images. Each has 5 images per person per each hand and hence it is associated to 50 distinct person for left and right hands of which the first 50 are for the right hands, the last 50 are for the left hand of the same person hand. So 1 in first set is RH HV and 51 is left hand to same person 1 in RH. This dataset is for both females and males in the range of 16-65 years age. Subjects are of healthy conditions and are from all folks of life including students, professors, engineers' workers, house wives, etc. [24].

C. Experimental Result

The result obtained at various stage of our method is shown below.

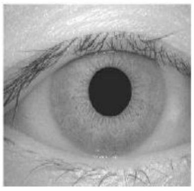


Fig.2 (a) Original Iris Image

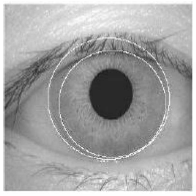


Fig.2(b) Iris Image with Boundaries

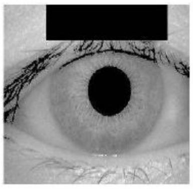


Fig.2(c) Segmented Irish Image

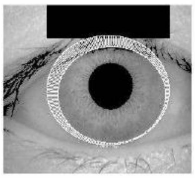


Fig.2(d)Segmented Irish Image with Boundaries

Fig.2(e) Polar array obtained after Normalization

Initially the original iris image obtained is shown in the fig.2(a). Further the obtained original iris image is process to obtain the boundaries of the image using canny edge detector which is shown in the fig. 2(b). After obtaining the boundaries the iris image is segmented this is shown in the above fig.2(c). Then the boundaries from the segmented image are obtained that contain information which is shown in the fig.2(d). The fig.2(e) represents the polar array obtained after iris image normalization process. Finally the iris key feature is extracted from the boundaries. The next stage of our proposed method is vein image extraction. Here the original hand vein image is shown in the fig.3 (a).

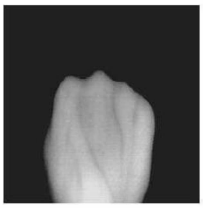
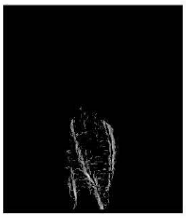


Fig. 3 (a) Original hand vein Image



3(b) Vein Image afterPreprocessing

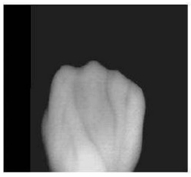


Fig. 3(c) Watermarked hand vein Image

After this the obtained original hand vein image is pre-processed at various stages to obtain the vein feature which is shown in the fig. 3(b). After this the iris key extracted in the first stage is embedded in to the pre-processed vein image. Finally the watermarked vein image obtained is shown in the fig.3(c).

D. Performance Evaluation

The performance analysis is made based on the evaluation metrics such as accuracy, FAR and FRR. Here, the iris key generated from the iris image is embedded in the plain image. The evaluation metrics may vary based on varying the bit position. The accuracy, FAR and FRR obtained for the 1st bit substitution is shown below,

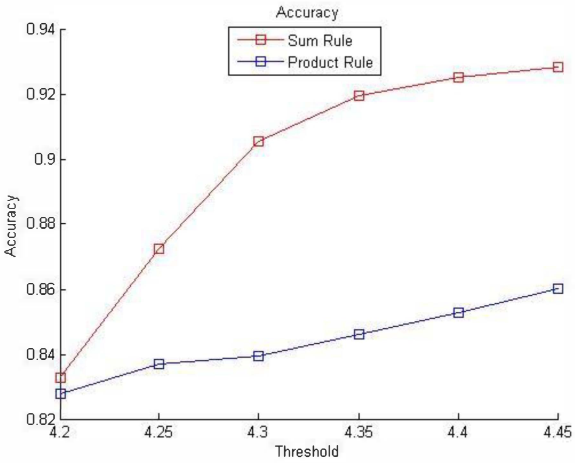


Fig 4. Accuracy for 1st Bit substitution

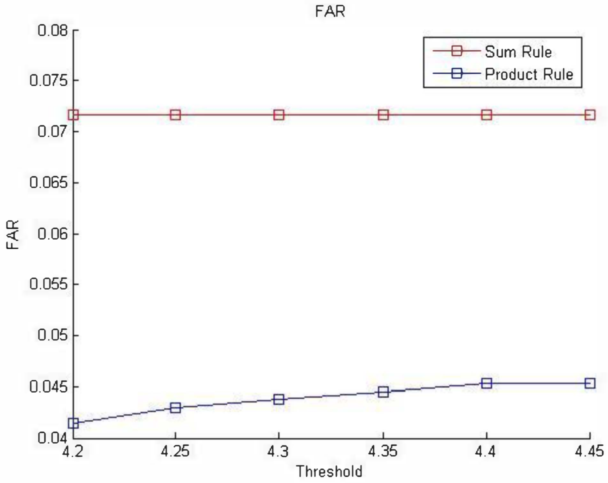


Fig. 5 FAR obtained 1st bit substitution

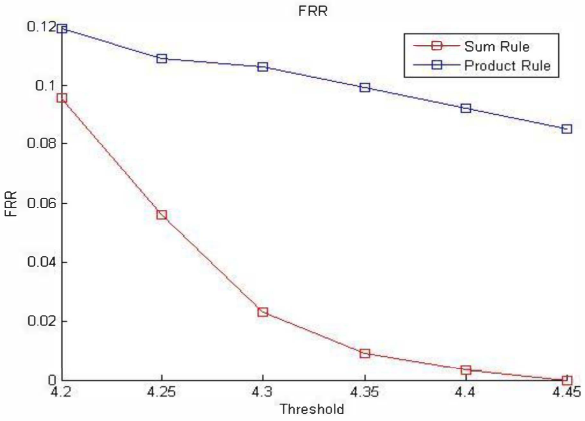


Fig. 6 FRR obtained 1st bit substitution

For the 1st bit substitution the accuracy for both sum and product rule is obtained by varying threshold value. Here, the accuracy obtained for the product rule is not much increasing than the sum rule for varying threshold. Likewise, the false acceptance rate for both sum and product rule is obtained by varying threshold. From the FAR we noted that the FAR for sum rule is not varying with varying threshold but for product rule there is a lighter variation with varying threshold. Similarly from the False Rejection Rate obtained we found that, the FRR for the product rule is decreasing slightly with varying threshold and also for sum rule the FRR is very low when threshold is very high.

The accuracy, FAR and FRR obtained for sum rule for different threshold value is given in the below table.I

TABLE.I ACCURACY, FAR AND FRR OBTAINED FOR SUM RULE

Threshold	Accuracy	FAR	FRR
4.2	0.913242	0.050228	0.03653
4.25	0.929224	0.054795	0.015982
4.3	0.931507	0.06621	0.002283
4.35	0.929224	0.070776	0
4.4	0.924658	0.075342	0
4.45	0.920091	0.079909	0

Similarly the accuracy, FAR and FRR obtained for product rule for different threshold is given in the below table

TABLE.II ACCURACY, FAR AND FRR OBTAINED FOR PRODUCT RULE

Threshold	Accuracy	FAR	FRR
4.2	0.863014	0.102857	0.011429
4.25	0.858447	0.106667	0.011429
4.3	0.863014	0.108571	0.005714
4.35	0.860731	0.110476	0.005714
4.4	0.863014	0.112381	0.001905
4.45	0.863014	0.112381	0.001905

IV. CONCLUSION

In this paper, we have presented an efficient biometric recognition system for template protection. We have used a watermarking technology to improve the template protection based on the two modalities the iris and the hand vein. The iris template was extracted from the pre-processed iris image. Then the features of the hand vein were extracted. After this the extracted iris template was embedded in to the hand vein and stored in the database. Subsequently in recognition phase the iris template and hand vein features were extracted from the watermarked image. Finally the extracted features were matched with input query image. The final decision of authentication was done based on the product rule-based score level fusion. The results obtained from the experimentation shows that our proposed watermarking techniques provide better results with higher accuracy.

The accuracy of our proposed method can be further improved by improving the embedding strength and embedding location by various search algorithms.

REFERENCE

[1] P. Poongodi, and P. Betty, “A Study on Biometric Template Protection Techniques,” International Journal of Engineering Trends and Technology (IJETT), vol. 7, no. 4, 2014.

[2] R. Yadav, Kamaldeep, R. Saini, and R. Nandal, “Biometric Template security using Invisible Watermarking With Minimum Degradation in Quality of Template,” International Journal on Computer Science and Engineering, vol. 3, no. 12, 2011.

[3] J.L. Jimenez, R.S. Reillo and B.F. Saavedra, “Iris Biometrics for Embedded Systems,” IEEE Transactions on Very Large Scale Integration (VLSI) systems, vol. 19, no. 2, 2011.

[4] P.S. Revenkar, A. Anjum and W.Z. Gandhare, “Secure Iris Authentication Using Visual Cryptography,” International Journal of Computer Science and Information Security, vol. 7, no.3, 2010.

[5] A.K. Jain, A. Ross, and U. Uludag, “Biometric Template Security : Challenges and Solutions,” In Proceedings of European Signal Processing Conference, 2005.

[6] N. Hajare, A. Borage, N. Kamble, and S. Shinde, “Biometric Template Security Using Visual Cryptography,” Journal of Engineering Research and Applications (IJERA), vol. 3, no. 2, pp.1320-1323, 2013.

[7] C.L. Li, Y.H. Wang, and B. Ma, “Protecting Biometric Templates using LBP-based Authentication Watermarking,” Chinese Conference on Pattern Recognition, pp.1-5, 2009.

[8] M. Arjunwadkar, and R.V. Kulkarni, “Robust Security Model for Biometric Template Protection using Chaos Phenomenon,” International Journal of Computer Applications, vol. 3, no. 6, 2010.

[9] D. Mathivadhani, and C. Meena, “Digital Watermarking and Information Hiding Using Wavelets, SLSB and Visual Cryptography Method,” IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1-4, 2010.

[10] P.K. Sharma, and Rajni, “Analysis of Image Watermarking Using Least Significant Bit Algorithm,” International Journal of Information Sciences and Techniques (IJIST) vol. 2, no. 4, 2012.

[11] M. Fouad, A.E. Saddik, and E. Petriu, “Combining DWT and LSB Watermarking To Secure Revocable Iris Templates,” 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA), pp. 25 – 28, 2010.

[12] E. Mostafa, M. Mansour, and H. Saad, “Parallel-Bit Stream for Securing Iris Recognition,” IJCSI International Journal of Computer Science Issues, vol. 9, no. 2, 2012.

[13] S. Edward, S. Sumathi, and R. Ranihemamalini, “Person authentication Using Multimodal Biometrics with Watermarking,” International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), pp. 100 – 104, 2011.

[14] K. Seetharaman, and R. Ragupathy, “Iris Recognition based Image Authentication,” International Journal of Computer Applications, vol. 44, no. 7, 2012.

[15] M.Y. Sheng, Y. Zhao, F.Q. Liu, Q.D. Hu, D.W. Zhang, and S.L. Zhuang, “Acquisition and Pre-processing of Hand Vein Image,” pp. 5727 – 5729, 2011.

[16] M.M. Pal, and R.W. Jasutkar, ” Implementation of Hand Vein Structure Authentication Based System,” International Conference on Communication Systems and Network Technologies, pp. 114 – 118, 2012.

[17] Sanchit, M. Ramalho, P.L. Correia, and L.D. Soares, “Biometric Identification through Palm and Dorsal Hand Vein Patterns,” International Conference on Computer as a Tool, pp.1-4, 2011.

[18] R.M. Thanki, and K.R. Borisagar, “Novel Approach For Multimodal Biometric System Using Compressive Sensing Theory Based Watermarking,” International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), vol. 3, no. 4, pp. 81-90, 2013.

[19] A. Bamatraf, R. Ibrahim, and M.N. Salleh, “A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit,” Journal of Computing, vol. 3, no. 4, 2011.

[20] S. Majumder, K.J. Devi, and S.K. Sarkar, “Singular value decomposition and wavelet-based iris biometric watermarking,” IET Biometric, vol. 2, no. 1, pp. 21–27, 2013.

[21] G. Kaur, and K. Kaur, “Image Watermarking Using LSB (Least Significant Bit),” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, 2013.

[22] S. Malhotra, and C. Kant, “A Novel approach for securing biometric template,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, 2013.

[23] http://www.smartsensors.co.uk/irisweb/

[24] A.M. Badawi, “Hand Vein database,” At systems and biomedical engineering, Cairo University.