ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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

Garika Sreekanth
M.Tech (DSCE),
Department of Electronics and Communication Engineering,
Scient Institute of Technology
Ibrahimpatnam, Rangareddy Dist, Hyderabad.

Penki Ramesh M.Tech
Assistant Professor,
Department of Electronics and Communication Engineering,
Scient Institute of Technology
Ibrahimpatnam, Rangareddy Dist, Hyderabad.

Abstract:

Biometric recognition is note worthy method fore cognition 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 utilize 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.

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. Now a days, eyes have turned to use biometric concepts to meet the requirement. Biometric system, which is a pattern recognition system, exploits a user's inimitable physical traits to identify/ authenticate him/her. Two major groups of tasks that contribute in a biometric system are identification and authentication. 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. Biometrics exhibits as a potential tool when combined with traditional authentication schemes that greatly support in establishing authenticity.

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. Template based methods in biometric systems apply global-level processing to extract features after cropping certain sub-image from original sensory image. Biometric template can be created with the aid of feature extractor or key binding algorithms. Such biometric templates can be kept safe and effectively protected by exploiting watermarking techniques. Biometric watermarking embeds biometric knowledge into a digital object and hence it connects a human subject with digital media.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. 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. It can be applied to safeguard the intellectual property rights by embedding the proprietary information in the source data. However, it is expected to be robust against some attacks against biometric system. 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.

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. 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. Patterns available in the hand veins are found to be distinctive between the individuals and remain same for long term throughout the human life. These vascular patterns are complex that lead to determine ample feature sets to ensure precise personal identification 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.

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) preprocessing 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.

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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. 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.

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 wrapping 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. 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.

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 pharos lies. This can be accomplished using the following equation

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

Gabor filter can be comfortably used by segregating a 2Dnormalized pattern into numerous ID wavelets and convolving them with ID Gabor wavelets. Log-Gabor filters are more suitable than Gabor filters fore presenting natural, because Gabor filters fails to out perform in precisely representing high frequency components. Log-Gabor filter can be represented as in equation

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

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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

It takes a single masked pixel of a hand vein image with a size of 3 x 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

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

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 pixel value below the threshold is considered as vein domain. The mean and variance of the local dynamic thresholding method is calculated by the equations given below

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

and

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

Embedding of iris pattern to band vein image:

The steps included in embedding iris key to vein images is given below, The input is iris key image l(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 l)The input watermark image H(x,y)is divided into blocks of sizeB"B2,B3 ......B n of size MxN. 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 J(x,y).

3)If the number of bits in the iris template J(x,y) is less thanthe number of blocks in hand vein image, then all bits of the iris template J(x,y) can be embedded.

4)After embedding all the bit of the iris template J(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,

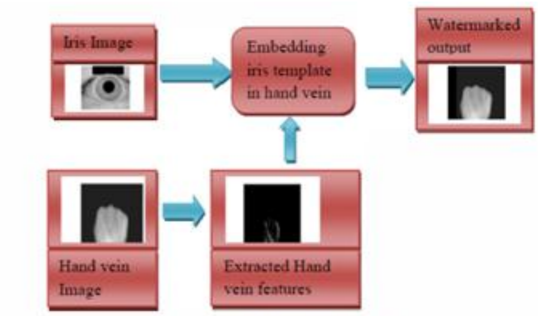

Fig. 1. Watermark Embedding

Recognition:

The recognition phase is divided in two major steps.
Step1: 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 Hw(x,y) and the size of watermarked image Hs(x,y) and the output is recovered watermark image Rw (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 x 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.

4)A matrix equal to the size of watermark image Hw(x,y)and the extracted pixels are placed in it to obtain the watermark imageH (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.

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 Diris. 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:vem for the vein image is determined.

Experimental Result:


Fig.2 (a) Original Iris Image


Fig.2(b) Iris Image with Boundaries

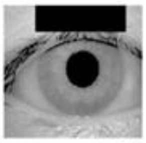
Fig.2(c) Segmented Irish Image

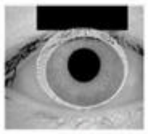
Fig.2(d)Segmented Irish Image with Boundaries


Fig.2(e) Polar array obtained after Normalization


Fig. 3 (a) Original hand vein Image


3(b) Vein Image afterPreprocessing


Fig. 3(c) Watermarked hand vein Image

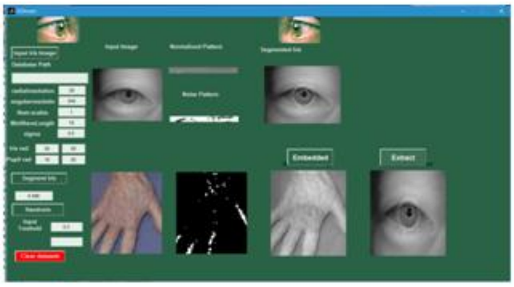
Fig: GUI of Proposed method

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, 20 I I.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[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 AuthenticationUsing Visual Cryptography," International Journal of Computer Science and Information Security, vol. 7, noJ, 20 I O.

[5] AK. 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. I 320-1 323,2013.

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

[S] 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 (lCCIC), pp.I-4, 2010.

[10] P.K. Sharma, and Rajni, "Analysis ofimage Watermarking Using Least Significant Bit Algorithm," International Journal of Information Sciences and Techniques (mST) 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 (lSSPA), pp. 25 - 28, 2010.

[12] E. Mostafa, M. Mansour, and H. Saad, "Parallel-Bit Stream for SecuringIris 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.