

Contourlet Transform Domain based Intelligent Biometric Watermarking System

M. Arfan Jaffar

College of Computer and Information Sciences, Al Imam Mohammad Ibn Saud Islamic University (IMSIU),

Abstract

Intelligent watermarking techniques are one form of technology used to ensure the security of information. Intelligent watermarking means embed information in image, video and audio to protect this information from hacking. This paper answers the question “How can watermarks of one biometric feature can be inserted into an image while maintaining the image’s quality and ensuring the watermark’s imperceptibility and robustness?”. In this paper, answer has been provided by introducing a new method that can embed one image into another by using contourlet transform. This technique is additive watermarking technique. Two biometric images of the same individual are used include fingerprint and iris image. Information has been hidden by using the watermark of same person inside the host images by watermarking techniques. For more security, the verification process satisfied by compare the host image and the authenticate by extract and compare the watermarks for the same individuals. Quantitative measure has been used to check the performance of proposed method.

Keywords:

Segmentation, breast mammograms, classification, texture

1. Introduction

These days, our lives are very different: our daily affairs and communications occur electronically, making the Internet indispensable. Therefore, it is important to maintain the privacy of our devices and during our use of the Internet. Although many protection programs have been created to protect against viruses, privacy and identity theft issues have continued to happen. These developments have been our most challenging problems in our use of the Internet, especially when dealing with personal accounts like bank accounts. Since the development of high-speed networks, protecting digital content has become very important. Watermarking techniques are one form of technology used to ensure the security of information. Watermarking refers to information that is hidden in a visual, audio or video source that cannot be changed or removed by unauthorised

persons. This project answers the question “How can watermarks with more than one biometric feature be inserted into an image while maintaining the image’s quality and ensuring the watermark’s imperceptibility and robustness?”

The development of information security plays important roles in our lives. Since people began to share photos, videos and documents digitally, it has become important to verify users’ identity during exchanges of information to maintain security and privacy as well as to achieve maximum safety. New devices have been developed to detect identity, such as facial, fingerprint or signature recognition. Behavioural or physiological characteristics can also distinguish the identity of an individual. Biometric measures can verify one or more behavioural or physiological characteristics, such as an iris, face, fingerprint or handwritten signature. Unimodal biometrics use a single biometric, which is easy to lose and may be susceptible to hacking. If a user’s biometric data were lost or stolen, it would be difficult for another person to use because that data are unique to one person. To improve the security and privacy of biometrics, two or more biometrics are used to identify a person; these are called multimodal biometrics. Most biometric systems need strong security to protect them from hacking and other problems. As a result, watermarking techniques, cryptography and steganography are used. Over the last few years, there have been copyright issues with digital media. Many copyright owners need to protect their digital media, and watermarking offers the best solution to protect individuals’ rights. Watermarking technology can embed hidden messages or information inside different forms of media like images, audio clips or video clips without the user being able to detect or remove it.

2. Proposed Method

In this section, we discuss about how to extract features from iris. There are many of process before extract iris feature in recognition system of iris. In the localization and segmentation process, there are many steps. The first step is to isolate iris region from eye image by using hough transform which draw many of circles to covers the

boundary between iris and sclera also boundary between iris and pupil. After that, determine and select two circle as main boundaries. Then, remove various noise parts which mean remove lower and top eyelid and also the right side and left side from the boundary between iris and sclera. The goal for this step is to determine the circle object in the image. It is easy that normal relation which be between the pixels and points. According to the points (x, y) which are viewed like the coordinates forms of the pixels (x, y) . In the equations below, we determine the parameters of circle by using Hough transform.

$$x = d + r \cos \theta \quad (1)$$

$$y = f + r \sin \theta \quad (2)$$

Where; r = radius of circle, a and b = center points. When the standard equation form of circle is:

$$r^2 = (x - d)^2 + (y - f)^2 \quad (3)$$

Next step in program is to discover 3 parameters (d, f, r), but according to fixed circle then we try to find just 2 parameters which is (d, f). After that the goal is to determine positions of circles approximately. First, detect the shape of circle in 2-D grayscale image by find and try different values of center position and radius. Around the position of circle, there are non-zero gradient vectors. This is good when convert gradient field into the array which is accumulation because process transform is determine. The intensity of pixel like to probability of pixel which begin

circle's center. Circle's center place is represented by maximum intensity in the image that is accumulation. Generally, according to the dimensions we determine the accumulation array to be as the gradient field. Now we grouped the votes and make accumulative array for each non-zero of the vectors of gradient. Now, there are many of circle which finding corresponding to multiple peaks in accumulation array. The region which is extending after that discover and be the position of peak like the location of circles which is center. The circle radius if it is maximum then indicate to iris and if it minimum indicate to pupil boundary (see Figure 3.6). To detect the eyelash and resting noise, we use filter 1-D Gabor to separate it.

In this process, Hough transform for discovering the boundaries of pupil and iris. Gradients in vertical direction of the boundary between iris and sclera. Also horizontal gradients with vertical gradients boundary between iris and pupil. In [9] used the recent version of detection for the wise edge that involve the weight and gradients. To isolate eyelids, apply Hough transform that is linear. After implemented the Hough transform, we get the result of line is not proper if highest in the Hough area is lower than the threshold. For isolating the eyelashes we do thresholding method. Finally, the filter that named ideal high pass delete the rest of the eyelashes. See the figure [1] as shown below:

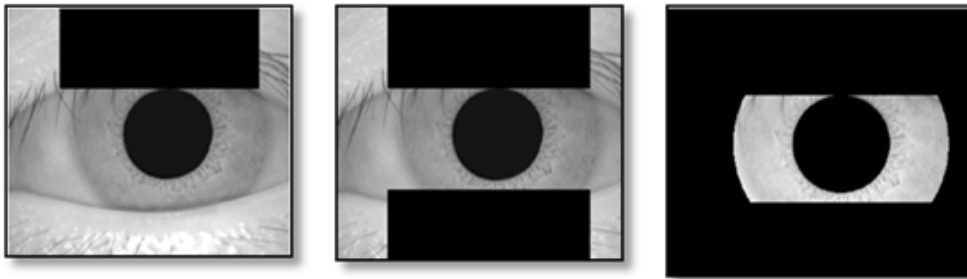


Figure 1: Delete upper eyelash Delete lower eyelash Delete of rest noise

The normalization process aim to convert segmented image into a fixed size or dimension form. In this process, we use Daugman's rubber sheet model that determine the center of pupil and radial vectors which cross within iris region. With each radial line, data point's number are taken which named as radial resolution and around iris, radial line numbers named as angular resolution. From iris region normalization process produce a 2-D array as horizontal dimension of the angular resolution and the vertical dimension of the radial resolution.

2.2 Feature encoding process

In this process, the aim is to get more accuracy of recognition of the person by giving the important information in iris pattern. So, to maintain the privacy we will encoded the iris feature. In feature encoding process, we applied two filter Gabor and log-Gabor which describe in the following points. Gabor filter provide with best representation of signal in spatial frequency. Constructs Gabor filter done by modulation of sin and cos wave with Gaussian. Sin wave placed in frequency and the sin wave which modulating with Gaussian placed in space. For any bandwidth can be take Zero DC value which using Gabor

filter that is Gaussian on logarithmic scale, known as Log Gabor filter. Encoding process implemented (see Figure-3.14), convolution of normalized iris with 1-D logs Gabor. 2-D normalized iris contains rows and columns and rows are taken as 1-D signal correspond to a circular ring on iris. For the columns of normalized iris, angular direction is considered. Intensity values on noise region in normalized iris are set to surrounding pixels average intensity to stop noise in output. Output is quantized as phase to 4 levels by using Daugman method. Feature encoding make bitwise template as form of information in bits and mark corrupt area as well. The result of this process is encoded image after doing two filters Gabor and log-Gabor . The size of all iris images is 20×480 which is fixed.

Feature Matching Process

In the last step of iris recognition system, the result of encoding process is the template. We compare the generated template with the template of iris in the database. The feature is extract from the template which size is 20×480 . The template contains the iris and pupil. The Mask of iris that black portion and pupil that white portion (see Figure 3.16) the required is just iris feature, So, to determine iris feature we applied strategy. So, we applied procedure which multiplied the mask of iris by two then join the multiplied mask to be in the template which include the iris and pupil .The value of pupil area is more than or equal two after adding. According to the remaining value that is less than two will be the desired values which is called the pure iris without contains pupil.

Fingerprint Feature Extraction

As we know, the second biometric used in this project is a fingerprint. In this section, we explain the process to extract the feature of a fingerprint. The result of this process is a minutiae extraction. We describe this process in many steps. We begin with the image obtaining and then change the size of the image into fixed size 512×512 . After that, check on the format of the image if in RGB format or not, and then transform to be in the grayscale format. Then we performed the operation of normalization the pixel. After that, we do the tensor of structure property and also coherence improvement diffusion. Then do the extraction process to get the minutiae feature as the result of the improved fingerprint image. Fingerprint enhancement technique has been applied that proposed in [12]. The aim to use an enhancement technique because there are many problems that face when get the fingerprint. These problems are the result of scanning devise are poor quality fingerprint, sometimes the image which taken from paper not given the required result and may be affected from the environmental status. Moreover, because of the methods which used for compression to store the image in

the database. The noise of the image mean consists of ridge breaks, cuts and scratches. The problems which occur because of the noise which create points of false minutiae and the points of original minutiae are destroyed. The required work by enhancement process is to remove false minutiae and recover the original minutiae. After that contrast stretching has been applied so that the gray values are contracted into the region and then stretched into the range from 0 to 255. The important step in enhancement process, the image is orientation estimation. The aim of the orientation image to determine the directional image for the orientations ridges that are black lines. To make orientation image, there are three steps [12]. First, calculate the 2D Gaussian function. Then, multiply every pixel of the image with the Gaussian function. Finally, calculate the structure tensor of every pixel. To make orientation estimation implement previous three steps. Structure tensor is the attribute that is involved in orientation estimation. Structure tensors are a matrix that includes the information of partial derivative. The tensor which represents how data in the array. In image processing, gradient or edge information obtained by the matrix for each pixel. Recognition for many objects by using the gradient rather than the edges that include the high amount of gradient. We determine structure tensor for image by using Gaussian derivative filters.

We will use a technique which improves the quality of the structure which is not affected on the minutiae features. This technique also named Gaussian filtering. To maintain the validity of minutiae, we using the attribute of the structure tensor and after that refine the image with required orientation by using coherence-enhancement diffusion that have two types. Gabor filter proposed by Dennis Gabor [13] which named also edge enhancement diffusion. The aim of using Gabor filters to find in the image and determine the edges of various objects. The advantage of Gabor filters has improved quality by improving the edges of any object. So, it is more secure and very good for enhancing the quality. From the enhanced fingerprint image, we extract minutiae feature points after enhancement process. The most minutiae points in fingerprint image which used ridge ending and ridge bifurcation. The extraction process done by the algorithm which describe it in following steps. First, using Otsu's method [17] for the enhanced image. This method determines some special threshold that decreases the variance during a class using weighted gather of two variances. Then, by using thresholding we transformed the result to a binary image. Thresholding is a operation which to divide various regions and change all the pixels to 0 values to make a binary image if the pixels values less than threshold. On the other hand, if they are greater than threshold value changing all pixels values to 1. After applying thresholding, we apply a morphological

operation to thin the binary image which having two colors. This operations is used for changing the properties of the object like structure, form, and shape. Also m using this operation to represent used the boundaries of objects. The most operators using in morphological operations are dilation and erosion. Expands the object by the dilation, which filling small holes based on the structure of element size and also links between disjoint objects. Narrow the object by erosion, which based on the structure of element size. In (Figure 3.23), explain the image determined after doing the erosion morphological process which called thin image.

Now the thin fingerprint image is determined, by helping the mask we can detect the minutiae points. The mask or filter defines by generating a matrix with size 3×3 . Then the mask moving towards the image which is thin and the pivot value always be 0. Reference to pixels which have value 1 to white small boxes and pixels which have value 0 to black small boxes. The mask is the dotted square box which contains 7 white pixels .The result of the mask is 7 which refer to the ridge ending because the location (i,j) of thin image that is accurately under the center position of the mask. The mask is the dotted square box which contains 5 white pixels .The result of the mask is 5 which refer to the ridge bifurcation because the location (i,j) of thin image that is accurately under the center position of the mask. All the pixels and locations of this centered point (i,j) are the ridge bifurcations. In the result obtain the ridge ending by red sign and obtain the ridge bifurcation by the green sign.

3. Results and Discussion

Embedding of Fingerprint features into Iris image

In this embedding, we use technique which proposed in [12]. This technique is additive watermarking which aim to embed the features of fingerprint into iris image. Watermarking include two steps; features conversion and additive Watermarking. In this step, we convert the feature of fingerprint to watermark image. For example, if we have feature size 28×3 which result is 84 bytes. After convert the result which is 84 bytes to bits we get 765 bits. The value after converted to bit can represented in 9 bit. After take the square root and take the approximation value the result of watermark image dimension is 28×28 . In this case, the goal of additive watermarking technique is the features of iris in iris image not be disturbed. First, we made a mask is the white area which include the features and the black area is the remaining image. The white area is the required area which not to disturb. The watermark will be just in the black area. To apply this technique easily we need the mask, watermark and host image. First, compared the mask image and just changes the zero values in the location of the mask image. Then, change only the last bit of host image in the same location of the zero value location in mask. There is example to show the additive watermarking technique, if we got zero value at masks position (3, 1) then at same position of host image there is number which is 21. And we represent the number 20 binary representation we get 00011111. We make exchange in the last bit 1 to 0. We watermark in this location because can't detect by human eye. The result after applying this technique is watermarked into an iris image even not disturbing the iris features.

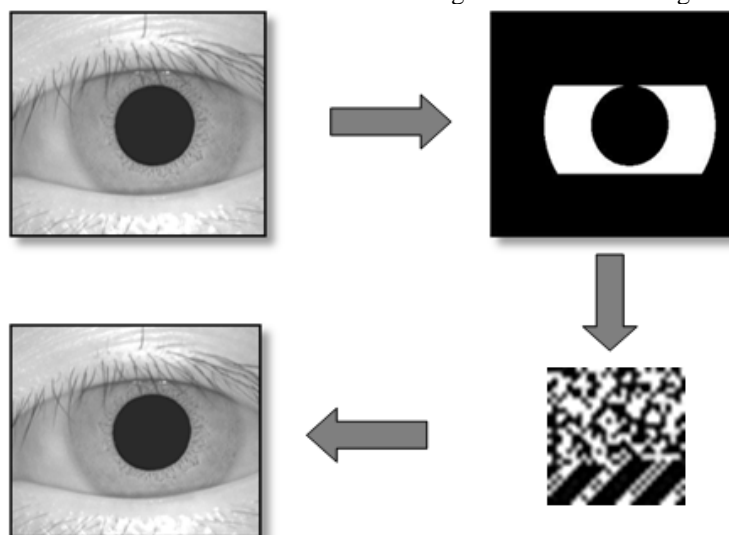
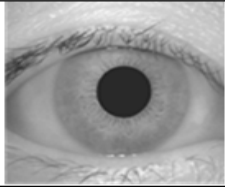
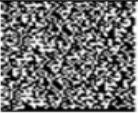
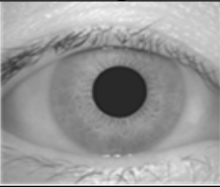
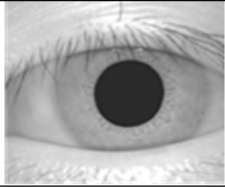
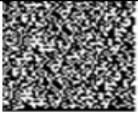
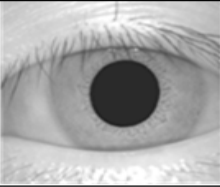
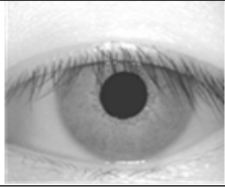
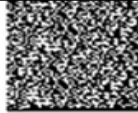
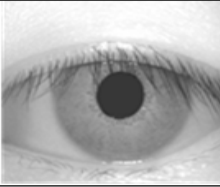


Figure 2: The result of additive watermarking on iris image

Embedding of fingerprint features into iris image
 In the third step, we applied the technique on three images and the results are the same. After extract features, did

watermarked image. The results as shown below. To know about the result, we calculate PSNR . Different values of PSNR for different

Table 1. Results of Watermarked

Example	Host image	Watermark image	Watermarked image	PSNR
1				65.3750
2				65.3879
3				65.0891

5. Conclusion

In the results, the value of PSNR determine the quality of the image after watermarking. So, we see the best quality in single watermark when embedding the fingerprint features into the iris image. According to watermarks results, the best quality when embedding the fingerprint in iris. It also shows that proposed method get optimum quality with high value of PSNR. Finally, the results is the best and robustness and also the security is high. In the first part, we explain the methods used to extract the biometric features: the iris and fingerprint. Each method results in an extraction, which is required for the conversion to a watermarked image; the watermarked image is then embedded using watermarking techniques.

References

[1] N. K. Ratha, J. H. Connell, and R. M. Bok, "Secure data hiding in wavelet compressed fingerprint images," Proceedings of ACM Multimedia Workshops, pp. 127-130,2000.
 [2] Ruud M. Bolle, Jonathan H. Connell, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, "Guide to Biometrics", Springer, 2003.
 [3] Nagar A., Nandakumar K., Jain A. K., "Multibiometric Cryptosystems Based on Feature-Level Fusion," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 255 – 268, Feb. 2012.

[4] Arun A. Ross, Karthik Nandakumar, Anil K. Jain, "Handbook of Multibiometrics," Springer, 2006.
 [5] A. K. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images", Proceedings of Third Workshop on Automatic Identification Advanced Technologies, pp. 97-102,2002.
 [6] A. K. Jain, U. Uludag, and Rein-Lien Hsu, "Hiding a Face in a Fingerprint Image," Proc. IEEE, 16th International Conference, Vol. 3, 2002.
 [7] Jain A. K., and Uludag U., "Hiding biometric Data", IEEE Trans. on PAMI, Vol.25, No.11, pp.1494-1498, 2003.
 [8] U. Uludag, B. Gunesel, and M. Ballan, "A Spatial Method for Watermarking of Fingerprint Images," Proc. 1st Intl. Workshop on Pattern Recognition in Information Systems, 2001.
 [9] Lin H., and Anil. K. J., "Integrating Faces and Fingerprints for Personal Identification", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, pp. 1295-1307, 1998.
 [10] Gui Feng, and Qiwei Lin, "Iris feature based watermarking algorithm for personal identification", Proc. of SPIE, Vol. 6790, pp. 679045, 2007.
 [11] B. Gunesel, U. Uludag, and A. M. Tekalp. Robust watermarking of fingerprint images[J], Pattern Recognition, 2002, 35(12): 2739-2747.
 [12] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. IEEE transactions on Pattern Analysis and Machine Intelligence, 29(4):561–572, April 2007.
 [13] Macq B.M., Quisquater J.J., "Cryptology for digital TV broadcasting", Proceedings of IEEE, ISSN: 0018-9219, vol. 83, pp. 944-957, June 1995.

- [14] Rhoads G.B., "Identification/authentication coding method and apparatus", World Intellectual Property Organization, vol. IPO WO 95/14289, 1995.
- [15] Ruanaidh J.J.K.O., Dowling W.J., Boland F.M., "Watermarking digital images for copyright protection", Proc. IEE Vision, Image, and Signal Processing, vol. 143, no. 4, pp. 250-256, Aug. 1996.

Authors



M. Arfan Jaffar received his B.Sc degree from Bahauddin Zakariya University Multan, Pakistan in 2000 and got distinction (Gold Medal). He later received M.Sc. degree in computer science in 2003 from Quaid-e-Azam University Islamabad, Pakistan. Then he earned his PhD. degree in computer science in July 2009 from National University of Computer and

Emerging Sciences, NU-FAST, Islamabad, Pakistan. After that, he worked as a Research Professor at Signal and Image Processing Lab, SIPL, GIST, Gwangju, Korea. Currently, he is working as Assistant Professor at Al Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia. His research interests include image processing, medical Imaging and computational intelligence.