

# Cancelable Iris Biometrics Based on Data Hiding Schemes

<sup>1</sup>Bismita Choudhury, <sup>1</sup>Patrick Then, <sup>1</sup>Valliappan Raman, <sup>2</sup>Biju Issac, <sup>1</sup>Manas Kumar Haldar

<sup>1</sup>Faculty of Engineering, Computing and Science, Swinburne University of Technology, Malaysia

<sup>2</sup>School of Computing, Teesside University, UK

**Abstract**— The Cancelable Biometrics is a template protection scheme that can replace a stolen or lost biometric template. Instead of the original biometric template, Cancelable biometrics stores a modified version of the biometric template. In this paper, we have proposed a Cancelable biometrics scheme for Iris based on the Steganographic technique. This paper presents a non-invertible transformation function by combining Huffman Encoding and Discrete Cosine Transformation (DCT). The combination of Huffman Encoding and DCT is basically used in steganography to conceal a secret image in a cover image. This combination is considered as one of the powerful non-invertible transformation where it is not possible to extract the exact secret image from the Stego-image. Therefore, retrieving the exact original image from the Stego-image is nearly impossible. The proposed non-invertible transformation function embeds the Huffman encoded bit-stream of a secret image in the DCT coefficients of the iris texture to generate the transformed template. This novel method provides very high security as it is not possible to regenerate the original iris template from the transformed (stego) iris template. In this paper, we have also improved the segmentation and normalization process.

**Keywords** - Cancelable biometrics, Non-invertible Transformation, Steganography, DCT, Huffman Encoding.

## I. INTRODUCTION

Biometric systems are generally used for automatic identification or verification of a person, on the basis of physical or behavioral characteristic of that person. Compared to password or token based authentication system, biometric system using fingerprint, iris, face, voice, etc. provides better security as people cannot lose or forget their biometric trait. But, people leave their fingerprints on whatever they touch; hence one can easily steal the fingerprint and can even make an artificial finger using the stolen fingerprint. The person's face can be captured by the camera even from a distance without their concern. In such situation, the security of the biometric based authentication system is at a stake.

To overcome the problem of the compromised biometrics, the researchers have developed the cancelable biometrics. The cancelable biometrics provides a way for authentication even when the biometric pattern is compromised or stolen. Cancelable Biometrics is a template protection mechanism, where the original biometric pattern is distorted intentionally to enroll in the authentication system. The biometric template protection scheme is mainly categorized into two types: i) Biometric Cryptosystem and ii) Cancelable Biometrics. These schemes are designed to meet the criteria of Irreversibility, Unlinkability and Performance [1].

This paper presents a cancelable biometric scheme using the concept of steganography. The proposed methods also incorporated an improved method of segmentation and normalization. The Masek's [2] algorithm is improved to provide better performance by feeding the pre-calculated inner boundary of the iris to Circular Hough Transformation. Daughman's rubber sheet model [3] for normalization is improved by introducing a scaling factor to focus on the iris region near the pupil. The combination of Huffman Encoding and Discrete Cosine Transformation (DCT) is taken as a non-invertible transformation. The transformed template is generated by embedding the Huffman Encoded bit stream of a randomly selected image in the DCT coefficients of the unwrapped iris image. The proposed method provides a very secured and non-invertible cancelable biometric scheme. The feature extraction is done by considering three types of features, viz. Haar wavelet, Principal Component analysis (PCA) and Gray Level Co-occurrence Matrix (GLCM).

## II. IRIS RECOGNITION

Iris recognition is a biometric authentication process that follows the pattern-recognition methods. Any Iris recognition system includes: *Image acquisition*, *Preprocessing* to remove noise, *Segmentation* to isolate the iris region, *Normalization* to transform the iris region into Cartesian form, *Feature extraction* to identify distinct characteristics and finally *Matching*. [4]

The proposed cancelable iris recognition process has an additional step of transformed template generation after the normalization. Fig. 1 shows the flow diagram of the necessary stages for iris recognition. In the proposed cancelable iris recognition process, the segmentation is done by combining the Canny edge detection and Hough transformation. For normalization, Daughman's method is exploited. Transformed templates are generated using the non-invertible transformation that is a combination of DCT and Huffman Encoding. Three types of feature sets are extracted from the Haar wavelet, Principal Component Analysis (PCA) and Gray Level Co-occurrence Matrix (GLCM). The matching scores are calculated by Hamming distance and Euclidean distance.

## III. IRIS SEGMENTATION

Iris segmentation is the process of localizing the iris by detecting the inner and the outer boundary. Iris segmentation plays the significant role as all the next steps for the iris recognition relies on it. Many research works have been carried out to find a more accurate method for segmentation.

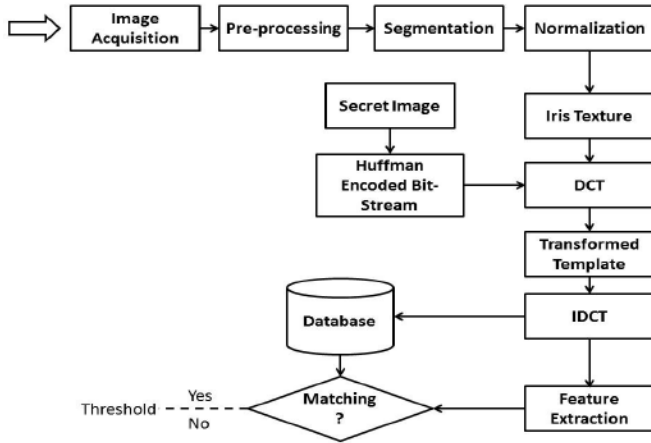


Figure 1. Flow Diagram of the Proposed Cancelable Iris Recognition

For the iris segmentation, we have followed the popular method of Edge Detection and Circular Hough Transformation. In this approach, at first, the input image is transformed into binary edge map using Canny edge detection. Then Hough transformation is applied to localize the contour of the iris. L. Masek [2], Wildes [6], exploited this method for segmentation. The disadvantage of this method is that it is reliant on the threshold values of the edge map constructed by edge detector. Moreover, it is difficult to decide on a threshold value to calculate the parameters for the circular contour of the iris and the pupil.

We have fused two processes to segment the iris region. For detecting the center and the pupil boundary or iris inner boundary, we have modified I. U. Nkole1 et al. [5] algorithm. To detect the outer boundary of the iris, we have modified Masek's [2] methods.

#### A. The Center and The Pupil Detection

The pupil and the iris are considered as concentric circles. To find the center of the pupil, the eye image is filtered to remove noise. Then filtered image is converted into a binary image. Sometimes, the pupil is occluded by the eyelashes. To avoid the eyelashes, a dilation followed by erosion is done after performing erosion followed by dilation. Extract two largest areas in the inverted image. When only one largest area is extracted the probability of getting the pupil region having the highest area is high. But, sometimes, due to the eyelids or the eyelashes, the regions other than pupil having the largest area are extracted. In that situation, segmentation process fails. To avoid that situation, two largest areas are extracted and then the eccentricities of those areas are calculated. The eccentricity is the ratio of the distance between the foci of the ellipse and its major axis length whose value lies between 0 and 1. When eccentricity tends to 0, it is actually a circle. So, set a threshold and find the extracted area which satisfies the threshold. Then, find the centroid, area and radius of that region. Apply circular Hough transform by feeding the calculated centroid and radius to detect the circular boundary of the pupil. The algorithm for detecting center and the pupil boundary is as follows:

#### Algorithm:

**Input:** Grayscale eye image.

**Output:** Grayscale eye image with pupil boundary and the center detected.

**Step 1:** Filter the grayscale image using an Average filter to smoothen the image

**Step 2:** Convert the filtered image into a binary image.

**Step 3:** Perform erosion followed by dilation.

**Step 4:** Perform dilation followed by erosion.

**Step 5:** Invert the image.

**Step 6:** Extract the two largest connected areas.

**Step 7:** Find the eccentricity of the extracted areas.

**Step 8:** Select an eccentricity threshold.

**Step 9:** Select one of the two extracted areas that satisfy the threshold.

**Step 10:** Find the centroid of the selected area.

**Step 11:** Find the area of the selected area.

**Step 12:** Find the radius of the circular area.

**Step 13:** Apply circular Hough transformation on the grayscale image by feeding the radius.

**Step 14:** Draw the circle by defining the pupil.

#### B. Iris Segmentation

The difference in the pixel intensities of the iris and the sclera region is very low. Therefore, it is a critical task to distinguish between iris boundary and its background. Here, after finding the center and the pupil boundary, the Hough transformation is applied on the grayscale image. Then, Canny edge detection is applied for generating the edge map. After that, perform the circular Hough transformation using the pre calculated center to detect the outer boundary of the iris. Circular Hough transformation finds circle using the equation:

$$(X - X_c)^2 - (Y - Y_c)^2 = R^2 \quad (1)$$

Where (X, Y) is the co-ordinate of any point at the boundary of the circle, (X<sub>c</sub>, Y<sub>c</sub>) is the co-ordinate of the center and R is the radius. The algorithm for iris segmentation is as follows:

#### Algorithm:

**Input:** Grayscale filtered eye image.

**Output:** Segmented iris region.

**Step 1:** Enhance the contrast of the filtered grayscale image by histogram equalization.

**Step 2:** Apply 2-dimensional Fourier transformation.

**Step 3:** Find Hough transformation of the transformed image.

**Step 4:** Apply Canny edge detection to find the edge map.

**Step 5:** Use circular Hough transform to detect the circle of the outer iris boundary with the given center.

**Step 6:** Set the pixel values greater than outer boundary and less than inner boundary to 0 using Eq. 1.

**Step 7:** Create a matrix with the size half of the original image.

**Step 8:** Scan the image from step 6 from left to right and top to bottom to find the pixels whose values are not 0.

**Step 9:** Store the non-zero pixels from left to right and top to bottom in the new matrix.

#### IV. IRIS NORMALIZATION

Once the segmentation is done, normalization is done to prepare the iris image for matching on the later stage. For



normalization, we used Daughman's Rubber Sheet Model [3] with some parameters changed. All the points are re-mapped within the iris region to a polar form with the coordinate  $(r, \theta)$  where  $r$  is in the interval  $[0,1]$  and  $\theta$  is the angle in the range  $[0,2\pi]$ . It transforms the Cartesian image  $I(x,y)$  to the normalized polar image  $I(r,\theta)$  along  $\theta$  direction using the following equations:

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \quad (2)$$

Where,

$$x(r, \theta) = (1 - r)x_i(\theta) + x_o(\theta) \quad (3)$$

$$y(r, \theta) = (1 - r)y_i(\theta) + y_o(\theta) \quad (4)$$

Where  $(x_i, y_i)$  is the coordinate of the inner iris boundary and  $(x_o, y_o)$  is the coordinate of the outer iris boundary.

Sometimes, segmentation process cannot get rid of the eyelashes or eyelids. Thereby, in the subsequent normalization process, unwrapped iris image is disturbed as well. Here, we have introduced a scaling factor. Using the scaling factor we can re-scale the normalized iris image such that it emphasizes only on the iris region near the pupil and not covered by the eyelids. Again, in some of the previous methods, when segmentation is not done properly the normalization process also gets affected. Then recognition rate decreases. But in this case, even when segmentation is not done properly, normalization process is compensating that error. That means, if segmentation is not detecting the iris properly, we can still get a better normalized iris image.

#### Algorithm:

**Input:** Grayscale segmented iris image.

**Output:** Unwrapped iris image.

**Step 1:** Find the center of the segmented iris image.

**Step 2:** Set minimum and maximum value of  $r$  in between 0 to 1 such that  $r_{\min} < r_{\max}$

**Step 3:** Set  $\theta$  value in the range  $[0,2\pi]$ .

**Step 4:** Set a scaling factor.

**Step 5:** Taking center as the reference point, use Eq. 3 and Eq. 4 to find all the points within the iris inner and outer boundary.

**Step 6:** Use Eq. 2 to map the points within the iris region along  $r$  axis and along  $\theta$  axis.

**Step 7:** Create a matrix of  $M \times N$  dimension.

**Step 8:** Use the scaling factor to rescale the generated normalized iris images into  $M \times N$  matrix so that it emphasizes on the iris region near the pupil.

**Step 9:** Write the normalized iris image of size  $M \times N$ .

## V. CANCELABLE BIOMETRICS

Cancelable Biometric is a template protection mechanism, where the original biometric pattern is distorted intentionally to enroll in the authentication system. When cancelable biometric scheme is applied, instead of the original biometric template a deformed version of the template is stored. Many research works have been carried out on the cancelable biometrics schemes. Some of them are as follows-

### A. Biometric Salting

In biometric salting, a user specific data (password or any random number) are combined with the biometric data to get the distorted version of the biometric template. Since the biometric salting process is completely dependent on the external auxiliary data, the method is revocable by simply changing the password. P. Lacharme in [8], used a Personal Identification Number or PIN to generate the cancelable template for iris recognition. Apart from the user specific helper data, some methods use random noise pattern, synthetic pattern etc. to create the transformed template. Zuo et al. in [9], provided a method GRAY-SALT and BIN-SALT where a random noise pattern is added to generate the cancelable iris template.

### B. Non-invertible Transformation:

In case of non-invertible transformation scheme, the biometric data are transformed by applying a one-way non-invertible function. The parameters of the transformation are modified to provide updatable templates. The advantage of the non-invertible transform is that the imposter cannot reconstruct the original biometric template even if the transforms are compromised [10]. But the use of non-invertible transformation degrades the overall performance due to information loss and difficulty in alignment of the templates. Ratha et al. in [11], proposed three transformation functions for fingerprints: Cartesian, Polar and Surface folding. Mesh warping is another non-invertible transformation methods explained by Hammer-Uhl et al. in [12].

### C. Random Projection:

In this approach, after feature extraction, the extracted features of the biometric pattern are projected into a random subspace. J. K. Pillai et al. in [13] provided sectorized random projection for cancelable iris biometrics.

### D. Random Permutation:

Random permutation of the features is another popular approach for generating cancelable biometric templates. Here, the extracted features are randomly permuted and seeded by some helper data. Zuo et al. in [9], the Gabor features extracted from the iris texture are shifted and the rows are combined to generate the transformed template. This approach is known as GRAY-COMBO. In another method BIN-COMBO, the iris code is randomly selected and combined. In [12], instead of permutation, block remapping is done.

### E. Bloom Filter:

A bloom filter is a probabilistic data structure that represents a set to support membership queries. Rathageb et al. in [14], applied an adaptive Bloom filter to the binary iris feature vector in order to obtain rotation invariant transformed iris code

## VI. CANCELABLE TEMPLATE GENERATION USING HUFFMAN-ENCODING AND DCT

In this paper, an approach of cancelable biometrics has been proposed based on the concept of steganography. The main goal here is to generate a non-invertible transformation

function that can satisfy the criteria of irreversibility, unlinkability, security and performance simultaneously.

To achieve non invertibility, a combination of DCT (Discrete Cosine Transformation) and Huffman encoding scheme has been used. In [16], DCT and Huffman encoding has been used for image steganography and it was claimed 100% extraction of the secret image from the stego image. Later, in [17], it is explained that when both DCT and Huffman encoding is used successful retrieval of the exact secret image is not possible. Before applying DCT, the cover image is converted into DOUBLE format. The Huffman encoded bit stream of the secret image is embedded in the LSBs of DCT coefficients. To generate the stego image, DOUBLE format is converted into UINT8 format. During this transformation of the format, the fractional values are rounded off. But the Huffman encoded bit stream is embedded in the fractional part itself. Therefore, it causes damage in the Huffman encoded bit stream and the Huffman table as well. For this reason, it is not possible to extract the secret image from the stego image once DCT and Huffman encoding is used together. In this way, we get a one way function or a non-invertible transformation function. Therefore, using the similar concept, the unwrapped iris image will be distorted by embedding Huffman encoded bit stream of a randomly selected image (from the selected standard image sets) in the DCT coefficients of the iris image and the transformed template will be constructed.

The unlinkability criteria will be achieved by randomly selecting one image from the standard selected images. Therefore, each transformed template generated will be unique as different images will be used for each of them. Generated templates can be used in different applications and it will avoid the cross matching.

The transformed iris template is generated by the following steps:

- i) Consider a set of standard images. Here, we considered the eye image of the user itself.
- ii) Perform Discrete Cosine Transformation (DCT) on the unwrapped iris image.
- iii) Find Huffman Encoding of a randomly selected image from the standard image set.
- iv) Embed the Huffman encoded bit-stream in the DCT coefficients of the unwrapped iris image.
- v) Perform Inverse DCT (IDCT) and generate the transformed template.

The combination of DCT (Discrete Cosine Transformation) and Huffman encoding is a powerful non-invertible transformation function. In case of steganography, it is not possible to reconstruct the exact original image from the stego-image when the combination of DCT and Huffman encoding is used. Similarly, after embedding the image into the unwrapped iris image to distort the iris template, it will be not possible to reconstruct the exact original biometric template from the transformed template again. Because most of the pixel details of the iris template will be destroyed during the embedding process. Due to steganography, the hacker will have no idea about the embedded image as they can't see any sign of the other entity.

Since, different images will be used to generate the transformed templates it can achieve the unlinkability criteria. Moreover, the users will be unaware of the technique used for generating transformed template and the images used. Therefore, it will less likely to compromise the transformed parameters/images.

#### A. A Combination of DCT and Huffman Encoding

The Discrete Cosine Transformation (DCT) transforms a signal from the spatial domain to the frequency domain. The DCT subdivides an image into  $8 \times 8$  blocks and transforms the pixels into 64 DCT coefficients in each block. The DCT stores the most of the energy in the lower frequencies arranged in the upper left corner of the DCT matrix. Let us consider, an image is represented as  $f(i, j)$  intensity values of pixels along  $i$  row and  $j$  column. After applying 2- dimensional DCT the image is transformed into the frequency domain  $F(u, v)$ . The general equation of 2D DCT is given as,

$$F(u, v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i, j) \cos \left[ \frac{\pi u(2i+1)}{2M} \right] \cos \left[ \frac{\pi v(2j+1)}{2N} \right] \quad (5)$$

Where,

$$1 \leq u \leq M-1, 1 \leq v \leq N-1$$

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}}, & u = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq u \leq M-1 \end{cases} \quad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}}, & v = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq v \leq N-1 \end{cases}$$

The Huffman encoding is another lossless image compression technique. Huffman encoding represents the data or image pixels into a minimum possible bit stream. A table is generated by finding out the probability of occurrence of each pixel intensity values. The most frequently occurring pixel intensity value is encoded using a lower number of bits. First, the Huffman table is generated by arranging the probability of occurrence of the pixel intensity values in decreasing order. Then the lowest probability values are combined together in each step until it is reduced to only two probability values. The remaining two probabilities are assigned either 0 or 1. Then each intensity value is encoded with the binary bit stream according to the associated probability value. Therefore, the output of the Huffman encoding is a binary bit stream and a Huffman table or code book. Using the generated code book, the symbols can be decoded.

#### B. Proposed Algorithm for cancelable biometrics

##### Algorithm:

**Input:** Unwrapped iris image of size  $M \times N$  and selected secret image of size  $m \times n$

**Output:** Transformed template.

**Step 1:** Read the unwrapped iris image of size  $M \times N$ .

**Step 2:** Convert the cover image, i.e. unwrapped iris image into DOUBLE format.

**Step 3:** Divide the cover image into  $8 \times 8$  block and apply 2D DCT on each block of the unwrapped iris image.



**Step 4:** Find the minimum value of the DCT coefficients and subtract the minimum value from all the DCT coefficients to convert the negative values into positive values.

**Step 5:** Convert the modified DCT coefficients into UINT32 format to remove the fractional part.

**Step 6:** Resize the selected secret image (original eye image) to  $m \times n$  such that  $m \leq M$  and  $n \leq N$ .

**Step 7:** Generate Huffman Table from the intensity values of the selected secret image.

**Step 8:** Create Huffman encoded bit stream of the secret image using the Huffman table.

**Step 9:** Compute the size of the encoded bit stream in bits.

**Step 10:** Convert the encoded bit stream of the secret image into 1-D block of size 8 bits.

**Step 11:** Embed each bit computed in Step 7 in the first 8x8 block of the unwrapped iris image by changing the LSBs of the modified DCT coefficients computed in Step 5.

**Step 12:** Embed the Huffman table and the Huffman encoded bit stream of 8 bit block generated in Step 8 by altering the LSBs of the modified DCT coefficients in each block (excluding the first 8x8 block) of the unwrapped iris image.

**Step 13:** Add the minimum value to the modified DCT coefficients generated in Step 12.

**Step 14:** Apply Inverse DCT (IDCT).

**Step 15:** Convert image into UINT8 format to generate the transformed template.

## VII. FEATURE EXTRACTION

For feature extraction we have considered three different types of features. The first type of feature is the energy, entropy and standard deviation of the detailed coefficients of the Haar wavelet. The second type of feature is the combination of the Haar Wavelet and the Principal component analysis (PCA). The third type of feature is the statistical features extracted by GLCM (Gray Level Co-occurrence Matrix).

The generated transformed template of size 50x500 is decomposed into 4 levels using 2-dimensional Haar Wavelet. After that, features are extracted as follows:

### A. Feature Type 1

After wavelet decomposition, we get the horizontal, vertical and diagonal details. Then, Energy is calculated for all the detailed coefficients. Again, Entropy and Standard Deviation are calculated for the detailed coefficients in the 4<sup>th</sup> level of decomposition. After that, the values for Energy, Entropy and Standard Deviation are combined to generate a feature set.

### B. Feature Type 2

Next, we considered only the diagonal details and Principal Component Analysis (PCA) is applied upon the diagonal details. The feature vector is generated by considering all the PCA values of the diagonal coefficients of 4<sup>th</sup> level and mean PCA values from each of the remaining 3-levels. The feature vector of size 1x96 is converted into binary bits by converting negative values into 0 and positive values into 1. The final feature vector is of size 96 bits.

### C. Feature Type 3

We have also considered statistical features to match the templates. We used Gray Level Co-occurrence Matrix or GLCM on the PCA coefficients to calculate Contrast, Correlation, Energy and Homogeneity. The GLCM examines the texture by analyzing the spatial relationship of the pixels. It characterizes the texture of an image by calculating how often the pairs of pixel with specific values and in a specified spatial relationship occur in an image.

So, these three types of features are considered to calculate the matching score between the templates. Feature type 1, 2 and Feature type 3 are combined and matched using Hamming distance.

## VIII. SIMULATION AND RESULTS

For the testing purpose, all the simulation has been done in MATLAB 2014b on Windows 10 platform. We are using CASIA version 4 Iris database. We tested on CASIA Interval set. All images are grayscale images of size 320 x 280 in .jpg format.

Fig. 2 shows the whole segmentation process. Fig. 2(a) is the right eye image of CASIA interval subset. Fig. 2(b) shows the conversion of the grayscale image into a binary image. Fig. 3(c) shows the extraction of the largest area that satisfies the eccentricity threshold. Fig. 2(d) shows successful detection of the pupil boundary. Fig. 2(e) shows the Hough transformation to generate the edge map. Fig. 2(f) shows the successful detection of the iris' outer boundary. Fig. 2(g) shows the localization of the iris. Fig. 2(h) shows the segmentation of the iris region. Using the proposed segmentation method we attained an accuracy rate of 99.71%. Table I shows the accuracy rate of different existing method and the proposed method. Fig. 3 shows the normalization of the iris after segmentation. Using the normalization method, 100% images are normalized successfully.

Fig. 4 shows Cancelable template generation process. Fig. 4(a) shows the secret image of the user to embed in the unwrapped iris image. Fig. 4(b) shows the generated transformed template. The proposed cancelable biometrics scheme achieved EER 1.2% and recognition rate 98.8%. Fig. 5 shows the ROC between False Acceptance Rate and Genuine Acceptance Rate. The Table II shows the comparison of different cancelable biometrics and the proposed method.

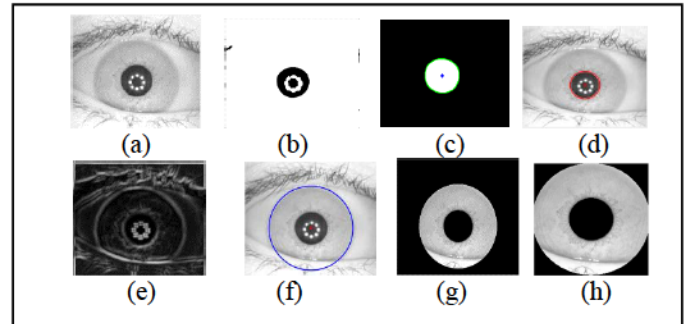


Figure 2. Eye image of CASIA Interval set, (b) Binarised image, (c) Extraction of the largest areas from the inverted image, (d) Pupil boundary detection. (e) Edge map creation using Hough transformation, (f) Iris outer boundary detection, (g) Iris localization, (h) Segmentated iris region.

TABLE 1. ACCURACY OF VARIOUS SEGMENTATION METHODS

Segmentation	Accuracy (%)
Masek [2]	81
Daughman [3]	98.6
Nkole et al.[5]	98.9
Wildes [6]	99.9
Cui et al. [7]	99.3
<b>Proposed Method</b>	<b>99.71</b>



Figure 3. Normalized Iris Image

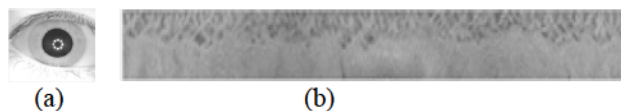


Figure 4. (a) Secret Eye image of the user, (b) Transformed template

TABLE II EQUAL ERROR RATE(EER) OF DIFFERENT CANCELABLE BIOMETRICS

Cancelable Biometric Schemes	Equal Error Rate (%)
Uhl et al.[12]	1.33
Pillai et al. [13]	2.33
Dwivedi [15]	5.75
<b>Proposed Method</b>	<b>1.2</b>

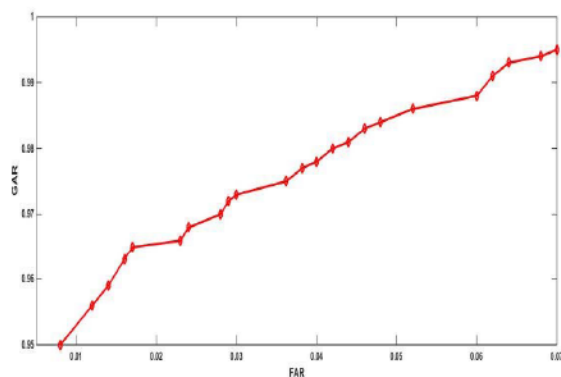


Figure 5. ROC between Genuine Acceptance Rate and False Acceptance Rate

## IX. CONCLUSION

In this paper, we have proposed an improved segmentation process, normalization process and a novel non-invertible transformation function to generate cancelable iris template. We used steganography to generate the transformed biometric data and so, it is more difficult for the intruder to perceive the modification done in the biometric data. Even if the intruder is aware of the steganographic technique and secret image used to construct the transformed template, it is not possible to reconstruct the original biometric data, because 100% extraction of the secret image is not possible in the combination

of DCT and Huffman encoding. Therefore, this method for cancelable biometrics is highly secure. With a segmentation accuracy of 99.71%, Equal Error Rate of 1.2% and Recognition Rate of 98.8%, the proposed method is a good option. The main drawback of the scheme is that if the database is large, then it requires a large number of secret images which needs more processing power. In the future, we will use learning classifier to improve the overall system performance.

## REFERENCES

- [1] C. Rathgeb, A. Hammerle-Uhl, "A Survey on Biometric Cryptosystem and Cancelable Biometrics", *EURASIP Journal on Information Security*, 2011
- [2] L. Masek, "Recognition of Human Iris Patterns for Biometric Identification". The University of Western Australia, Perth, 2003.
- [3] J. G. Daughman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 15, Issue 11, pp. 1148-1161, November, 1993.
- [4] K. W. Bowyer, K. Hollingsworth, P. J. Flynn, "Image Understanding for Iris Biometrics: A Survey", *ELSEVIER journal on Computer Vision and Image Understanding*, Vol. 110, Issue 2, pp. 281-307, 2008.
- [5] I. U. Nkole, G. B. Sulong, "An Enhanced Iris Segmentation Algorithm Using Circle Hough Transform", *Proc. of the IEEE International Conference on Digital Signal and Image processing*, pp.1-7, 2011.
- [6] R. P. Wildes, "Iris Recognition: An Emerging Biometric Technology", *Proceedings of the IEEE*, Vol. 85, Issue 9, pp. 1348 - 1363, 1997.
- [7] J. Cui, Y. Wang, T. Tan, L. Ma, and Z. Sun, "A Fast and Robust Iris Localization Method based on Texture Segmentation," in *Proceedings of SPIE*, 2004, vol. 5404, pp. 401-40.
- [8] P. Lacharme, A. Plateaux, "PIN-based Cancelable Biometrics", *International Journal of Automated Identification Technology*, Vol. 3, Issue 2, pp. 75-79, 2011.
- [9] J. Zuo, N. K. Ratha, J. H. Connell, "Cancelable Iris Biometrics", *Proc. of 19th Int. Conf. on Pattern Recognition*, Tampa, FL, December 8-11, pp. 1-4, 2008.
- [10] C. Rathgeb, A. Hammerle-Uhl, "A Survey on Biometric Cryptosystem and Cancelable Biometrics", *EURASIP Journal on Information Security*, 2011.
- [11] N. K. Ratha, S. Chikkerur, J. H. Connell, R. M. Bolle, "Generating Cancelable Fingerprint Templates", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, Issue 4, pp. 561-572, 2007.
- [12] J. Hammerle-Uhl, E. Pschernig, A. Uhl, "Cancelable Iris Biometrics Using Block Re-Mapping And Image Warping", *Springer Lecture Notes on Computer Science Information Security*, Vol. 5735, pp. 135-142, 2009.
- [13] J. K. Pillai, V. M. Patel, R. Chellappa, N. K. Ratha, "Sectorized Random Projections for Cancelable Iris Biometrics", *Proc. of ICASSP*, pp. 1838 - 1841, 2010.
- [14] C. Rathgeb, F. Breiting, and C. Busch, "Alignment-free Cancelable Iris Biometric Templates based on Adaptive Bloom Filters", *Proc. of International Conference on Biometrics*, pp. 1-8, June, 2013.
- [15] R. Dwivedi, S. Dey, "Cancelable Iris Template Generation using Lookup Table Mapping", *Proc. of 2nd International Conference on Signal Processing and Integrated Networks (SPIN)*, Noida, Feb 19-20, pp. 785-790. 2015.
- [16] A. Nag, S. Biswas, D. Sarkar, P. P. Sarkar, "A Novel Technique for Image Steganography based on Block-DCT and Huffman Encoding", *International Journal of Computer Science and Information Technology*, Vol. 2, Number 3, June 2010.
- [17] R. Das, T. Tuithung, "A Review On "A Novel Technique For Image Steganography Based On Block-DCT And Huffman Encoding", *Proc. SPIE 8768, International Conference on Graphic and Image Processing (ICGIP)*, March 2013.