High Secured and Authenticated Secret Message Sending using TIRI-DCT-DWT based Iris Recognition and Steganography

N.Suresh Singh
Asst.Professor&Head
Department of Computer Applications,
Malankara Catholic College,Tamilnadu, India

G.Suganthi, PhD.
Associate Professor
Department of computer science, Women's Christian College,Nagercoil, Tamilnadu, India

ABSTRACT

In the world of modern communication, securing information is a very important task. Hence Cryptographic systems are integral parts of communication systems in majority applications. Security requirements demand that these systems need to be operated with large secret keys. Since it is very difficult to remember large private keys, these keys are replaced by biometric features and this is called biometric security.The biometric identification system is one of the royal technologies used in the recognition system. Iris recognition system is the most reliable system for an individual identification. Of all biometrics-based techniques, the iris pupils and the outer areas provide very high accuracies in verifying an individual's identity. The iris is unique across peoples. Only the iris bit code template specific to an individual need to be stored for future identity verification. In this paper customer information is embedded in the iris. The Low Distortive Transformation (LDT) method is used to retrieve the information from the stego image in the server system. The iris authentication process is performed after the preprocessing on iris image with the reference of the iris database. Authentication process is implemented using Temporal Informative Restorable Image(TIRI) method. And this paper proposes a method to authenticate a person based on iris. The system will allow the process if the authentication process is success, otherwise it will send non authentication information to the client. The data embedding by LDT ensures the minimization of the mean square error. This paper combines the embedding, reversible data retrieval and iris feature based authentication. It is experimentally verified that the proposed system outperforms existing biometric security systems.

Keywords:-Biometric, Multimodel iris feature map, low-distortion transform, lookup table, Temporal Informative Representative Images**.**

1.INTRODUCTION

Nowadays, many applications have been implemented with this High secured and authenticated secret message sending using TIRI-DCT-DWT based Iris Recogonization and steganography method is used the time attendance system, business centers, bank, hospitals, airports, government agencies, educational facilities, and etc. The conventional method applied on the security is not reliable as the passwords may be forgotten or hacked and ID cards may be lost or forged. The biometrics has gained a lot of attention over recent years as a way to identify individuals. Iris recognition is one of the most promising approaches in biometric authentications [1]. Existing algorithms based on extracting and matching features from iris have reported very high recognition rates on clean data sets [2].However, since the method rely on the features extracted from the iris, their performances degrade significantly when the image quality is poor [1], [3]. This seriously limits the application of the iris recognition system in practical scenarios where the acquired image could be of low quality due to motion, partial cooperation, or the distance of the user from the scanner. When the acquisition conditions are not constrained, many of the acquired iris images suffer from defocus blur, motion blur, and occlusion due to the eyelids, specula reflections, and segmentation errors. Hence, it is essential to first select the "recognizable" iris images before employing the recognition algorithm. Recently, Wright et al. [4] introduced a sparse representation-based face recognition algorithm, which outperforms many state-of-the-art algorithms when a sufficient number of training images are available. The performance of most existing iris recognition algorithms strongly depends on the effectiveness of the segmentation algorithm. Iris image segmentation normally involves identifying the ellipses corresponding to pupil and iris, and detecting the region inside these ellipse area that is not occluded by eyelids,eyelashes,specula reflections. Unfortunately, in unconstrained scenarios, correctly segmenting the iris images is extremely challenging [5]. The proposed selection algorithm removes input images with poorly segmented iris and pupil ellipses. Furthermore, since the introduced recognition scheme is robust to small levels of occlusions, accurate segmentation of eyelids, eyelashes, and specula reflections are no longer critical for achieving good recognition performance. Another important aspect in iris biometrics is the security and privacy of the users. When the texture features of one's iris are stored in a template dictionary, a hacker could possibly break into the dictionary and steal these patterns. Unlike credit cards, which can be revoked and reissued, biometric patterns of an individual cannot be modified. So, directly using iris features for recognition is extremely vulnerable to attacks. Since Iris biometrics is increasingly becoming a large-scale application in which data is kept and used for long periods of time.

This paper is organized as section II introducing the proposed system and methodology, and its Result and Analysis discussed in section III. Finally the conclusions are discussed in section IV.

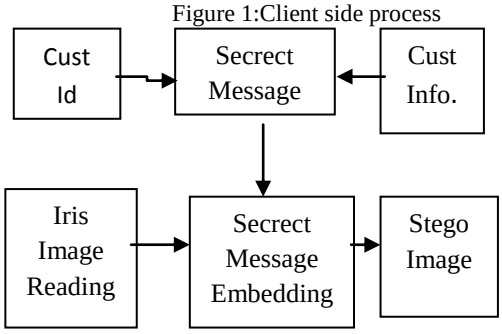
2. PROPOSED METHOD AND METHODOLOGY

Human Iris is selected for data embedding on the Human face. Also the poor quality iris and the pupil are improved to find out the required pixel for the data embedding. The user (client) activity and server (authentication) activity are the two major phases of this proposed system. The system allows the user for the input data. The input message being embedded into the iris image of the concerned user. In the server side process, first the reversible process for image restoration and data are extracted from the iris image and the authentication process is performed. Then the system allows to continue a subsequent process if the authentication process got success.

A. Data Embedding and Extraction using Methodology using LDT

The following steps describe the detailed process of message embedding, message retrieval authentication and message retrieval process. The following Figure(1) shows the message embedding. Process,

Figure 1:Client side process



The data embedding process uses the Low-Distortion Transform (LDT) for prediction-error expansion reversible watermarking [3]. The transform is derived by taking a simple linear predictor and by embedding the expanded prediction error not only into the current pixel but also into its prediction context. The embedding ensures the minimization of the square error introduced by the watermarking. The proposed transform introduces less distortion than the classical prediction-error expansion for complex predictors such as the median edge detector or the gradient-adjusted predictor. Difference expansion reversible watermarking, introduced by Tina [3], creates space by expanding a difference. The data and the auxiliary information are further added to the expanded difference and embedded into the image. The expanded difference is the one between adjacent pixels [1]–[4], original and predicted pixels [5]–[13]; pixels of a block and the mean value of the block [15]; pixels of a block and the median value of the block [16]; and so on. By expanding two times the difference, one data bit can be embedded. The embedding is possible if it does not generate overflow or underflow. At detection, as long as the expanded difference is recovered, the embedded bit is extracted and the original pixels are recovered. The high correlation between image pixels ensures rather low values for the differences referred above. It is known that the difference between adjacent pixels or, more generally, the difference between pixels and their predicted values (i.e., the prediction error) is modeled by the Laplacian distribution. Generally, at low difference values, no overflow/underflow appears, and consequently, high embedding capacity can be entailed. Furthermore, low-difference values ensure low distortion of the embedding. The lower the value of the difference, the lower the distortion.

Figure. 2. Pixels and their context for prediction

Nw	n	ne	y
W	x	e	z

The basic principle of our approach is to reduce the distortion introduced by the watermarking by embedding not only into the current pixel but also into its prediction context [9]. The minimization of the square error is considered. Let n,w and nw be the north, west, and north-west neighbors of pixel x, respectively (see Figure. 1). Pixel x can be estimated as

$$\hat{x} = n+w-nw \qquad (1)$$

Let b be the data bit to be embedded, and let p be the prediction error, i.e. $p=x-\hat{x}$ .Let us take $p_b=p+b$. The classical prediction error expansion reversible watermarking additively embeds p_b into the current pixel.

Let d be a fraction of p_b , and let us transform x and its entire context as follow,

$$\left.\begin{aligned} &X=x+P^b-3d, \quad N=n-d, \\ &W=w-d, \\ &NW=nw+d \end{aligned}\right\} \qquad (2)$$

Let us calculate the value of d in order to minimize the square error. The square error is,

$$E^2=(X-x)^2+(N-n)^2+(W-w)^2+(NW-nw)^2 \qquad (3)$$

By substituting the values from equation(2),

$$E^2=(p_b-3d)^2+3d^2=12d^2-6p_bd+p_b^2 \qquad (4)$$

solving eq(4) minimum error value can be obtained as,

$$E^2_{min}=p_b^2/4. \qquad (5)$$

From (2), the minimum error can be calculated as adding or subtracting a quarter of pb from the current pixel and its context, since pixel takes integer value d also be integer. The p_b value can be split into four parts as d_x,d_w,d_{nw},d_n ,where

$$\left.\begin{aligned} &d_x=\left[\frac{pb}{4}\right], \quad d_w=\left[\frac{pb+1}{4}\right] \\ &d_{nw}=\left[\frac{pb+2}{4}\right], \quad d_n=\left[\frac{pb+3}{4}\right] \end{aligned}\right\} \qquad (6)$$

and show that $d_x + d_n + d_w + d_{nw} = p_b$ with
d_x, d_w, d_{nw} and d_n are computed and (2) becomes
$X=x+d_x$, $N=n-d_n$,
$W=w-dw$, $NW=nw+d_{nw}$ (7)

The rounding proposed above ensures that the difference between $Max(d_x, d_w, d_{nw}, d_n)$ and $min(d_x, d_w, d_{nw}, d_n)$ is at maximum one gray level. By taking a simple

rounding as, for instance, d=$\left\lfloor (pb/4) + (\frac{1}{2}) \right\rfloor$, one may have a difference between d and $pb - 3d$ of up to three gray levels. In this way data embedded.

The proposed transform is reversible. Let us suppose that the transformed pixels, i.e., N, W and NW are not subject to overflow or underflow, i.e., for 8-bit images, $0 \leq X,N,W,NW \leq 255$. At detection, by using (1), one gets the following for the transformed context:

$\hat{X}$=N+W-NW=$\hat{x} - dw - dn - dnw$ (8)

The prediction error for the transformed context is,

P= (X-$\hat{X}$) = $x - \hat{x} + dx + dw + dn +$

$dnw = 2p + b$. Embedded data b follows as

the least significant bit (LSB) of X _ $\hat{X}$,

b=(X - $\hat{X}$)- 2[(X- $\hat{X}$)/2] (9)

and p is recovers as, p=$\left\lfloor (X - \hat{X} - b)/2 \right\rfloor$ (10)

Then , d_x, d_w, d_{nw} and d_n are computed with (6).And the values X,N,W and NW are inverted.

x=X- d_x , n=N+ d_n ,

w=W+ dw , nw=NW- d_{nw} (11)

Thus the original pixel values x,n,w and nw are recovered.

B. Detection System Using TIRI-DCT-DWT

The original image can be detected using TIRI-DCT method along with the search algorithm specifically developed for it introduces an authenticating system that is robust, discriminate, and fast. Figure.3 shows the overall structure of the iris authenticating system. This method calculates a weighted average of the images to generate a representative image. The resulting image is basically a blurred image that contains information. The TIRI-DCT is generated using [10].Let L be the luminance value of the pixel of the image. The pixels of TIRI are then obtained.Different weight factors (constant, linear, and exponential) has been examined.

As explained in [9], features are derived by applying a 2D-DCT on overlapping blocks of size $2w \times 2w$ from each TIRI. The first horizontal and the first vertical DCT coefficients (features) are then extracted from each block. The value of the features from all the blocks are concatenated to form the feature vector. Each feature is then compared to a threshold (which is the median value of the feature vector) and a binary image is generated. The Discrete Wavelet Transform (DWT), which is based on sub-band coding is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduce the computation time and resources required.

1. Segment each TIRI into overlapping blocks size $2w \times 2w$.Extract two DCT coefficients from each block. These are the first horizontal and vertical coefficients adjacent to the DC coefficient. For images, there exist an algorithm similar to the one-dimensional case for two-dimensional wavelets and scaling functions obtained from one-dimensional ones.
2. This kind of two-dimensional DWT leads to a decomposition of approximation coefficients at level *j* in four components: the approximation at level *j* + 1, and the details in three orientations (horizontal, vertical, and diagonal).

C. Authentication process

The following Figure (3) shows the activities of different phases of authentication process and the server. In response to challenge iris authentication, the original iris image is retrieved after extracting original message using TIRI-DCT-DWT method. Iris segmentation is an essential module in iris recognition because it defines the effective image region used for subsequent processing such as feature extraction. Several challenges are noted in practical iris segmentation. For example, the iris is often partially occluded by eyelids, eyelashes, and shadows (EES), especially for oriental users. It can also be occluded by specula reflections when the user wears glasses

Figure.4. Iris images with eyelid occlusion

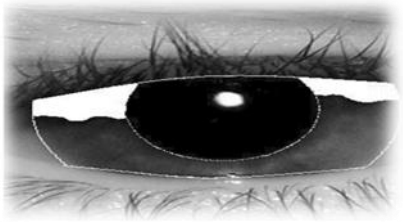
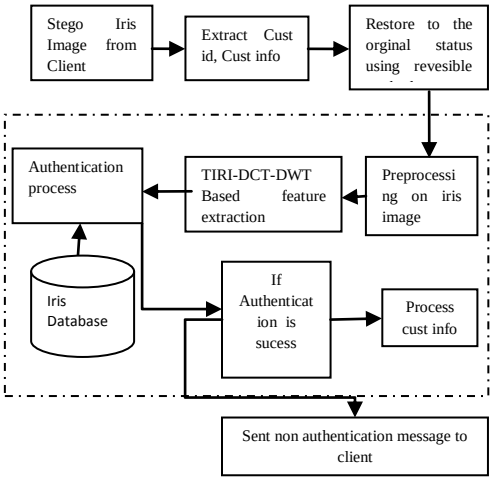


Figure 3.Schematic of a server side iris authentication system.



D. Iris Detection after Reflection Removal

An efficient reflection removal of iris detector is first built to extract a rough position of the iris center. Edge points of iris boundaries are then detected. The center and radius of the circular iris boundaries are iteratively refined. Usually, specula reflections appear as the brightest points in the iris image $I_{(x,y)}$. In this work, A bilinear interpolation method has been used to fill the reflections. This is using an adaptive threshold Tref to calculate a binary "reflection" map $R_{(x,y)}$of I(x,y).In order to interpolate the reflection point $P^0(X_0,Y_0)$,four envelop points $\{P^{left}_{(xl, y0)}, P^{right}_{(xr, y0)}, P^{top}_{(x0, yt)}, P^{down}_{(x0, yd)}\}$ are defined and find the values as follows,

$$xl=\max_x\{x : \sum_{i=0}^{L-1} R_{(x+i,y0)} =0, R_{(x+L,y0)} =1, x<x_0\}$$

$$xr=\max_x\{x : \sum_{i=0}^{L-1} R_{(x-i,y0)} =0, R_{(x-L,y0)} =1, x>x_0\}$$

$$yt=\max_y\{y : \sum_{i=0}^{L-1} R_{(x0,y+i)} =0, R_{(x0,y+L)} =1, y<y_0\}$$

$$yd=\max_y\{y : \sum_{i=0}^{L-1} R_{(x0,y-i)} =0, R_{(x0,y-L)} =1, y>y_0\} \quad (12)$$

Where L controls the necessary separation between the reflection points and their envelop points. L is set to 2 in this work. Obviously, all of the neighbour points lying in the same line share the same P^l and P^r, while all of the neighbour points lying in the same column share the same P^t and P^d. Once all of the envelop points are obtained, the reflection point is filled by $I(P^0)$.

$$I(P^0)=\frac{I(P^l)(x_r-x_0)+I(P^r)(x_0-x_l)}{2(x_r-x_l)}+\frac{I(P^t)(y_d-y_0)+I(P^d)(y_0-y_t)}{2(y_d-y_t)} \quad (13)$$

The objective of iris detection is not only to identify the presence of an iris in input, but also to determine its position and scale. Iris detection, or object detection in general, is a challenging problem in computer vision due to the vast variations of appearances of the object (e.g., illumination, occlusions, deformation, etc.).Recently, a technique proposed by Viola and Jones [10] has been proven to be effective for detecting well-structured objects such as faces. In order to get proper illumination, most iris cameras use infrared illuminators, which introduce specula reflections in the iris images. In this method ,we are selecting the intensity to the binary threshold $T_{ref.}$ Figure.5.original iris images with specular reflection.

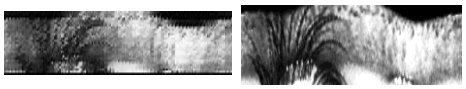
Figure.5.original iris images with specular reflection.

Another problem involved in iris segmentation is to locate the upper and lower eyelids. The shape of eyelids is so irregular that it is impossible to fit them with simple shape assumptions. In addition, the upper eyelid tends to be partially covered with eyelashes, making the localization more difficult.

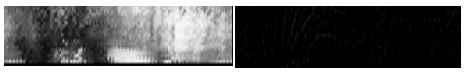
The pupil round area is calculated after removing reflections on iris. The iris pupillary area is identified and it allows to calculate center point, left,right,top and right boundary points. Using Histogram based normalization, polar coordinate values are transformed and the image being localized. The converted image is displayed as in the rectangular shape and it will allow removing the unwanted areas from the localized image. The original pupil area identified and compared with the preprocessed iris images in the database.

3. RESULT AND ANALYSIS

The cover Image (CI) holds the secret message. The secret message (SM) may be plain text, cipher text or any kind of data. It can be implemented by the stego function (SF) and its inverse (SF^{-1}).In the first phase of work the message embedded into the iris image.



(a)DCT image (b)Histogram Equalized Image



(a)TIRI Image (b)DWT Image

Figure 6:Converted Iris Image

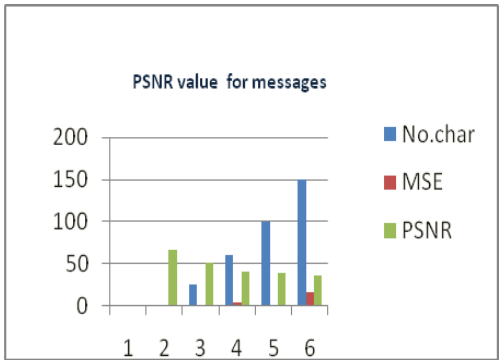
The MSE and PSNR values on two gray level test image of size 128×128 were calculated and tabulated in the Table-1.The data embedded time value and data extraction time value is tabulated in the table Table-1 for the above two images.

Table-I Shows PSNR and Time constrains of Iris Image

Message size (no.char)	MSE	PSNR	Time Embedded	Time Extraction
1	0.0126	67.114	0.0468	0.4368
25	0.4567	51.537	0.0780	0. 5331
60	4.9006	41.223	0.0468	0.4524
100	0.0624	38.681	0.0624	0.4212
150	16.521	35.950	0.0624	0.04680

After the data extraction the Mean square error leads zero and the PSNR value becomes infinitive.

Figure 7 :PSNR value Difference for Message Size



The above Figure(7) shows the performance of PSNR values for data embedding change depends on the size of message .The result shows that our system gives better result for the message with minimum characters.

4. CONCLUSION

In this paper, A data embedding technique using low distortion transformation for reversible watermarking has been presented. And proposed a method TIRI-DCT-DWT which added more value for the authentication of particular person. The experimental result on these two above said technique achieves state-of-art iris message embedding and

iris authentication is accuracy, while being computationally much more efficient.

5. REFERENCES

[1] Jai shanker K. Pillai, Rama Chellappa, Fellow, IEEE, and Nalini K. Ratha, Fellow, IEEE.IEEE transactions on pattern analysis and machine intelligence, VOL. 33, NO. 9, SEPTEMBER 2011.Secure and Robust Iris Recognition Using Random Projections and Sparse Representations.

[2] K.W. Bowyer, K. Hollingsworth, and P.J. Flynn, "Image Understanding for Iris Biometrics: A Survey," Computer Vision and Image Understanding, vol. 110, no. 2, pp. 281-307, 2008.

[3] J. Tian, "Reversible data embedding using a difference expansion,"*IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896,Aug. 2003.

[4] J. Daugman, "Probing the Uniqueness and Randomness of Iris Codes: Results from 200 Billion Iris Pair Comparisons," Proc.IEEE, vol. 94, no. 11, pp. 1927-1935, Nov. 2006.

[5] E.M. Newton and P.J. Phillips, "Meta-Analysis of Third-Party Evaluations of Iris Recognition," IEEE Trans. Systems, Man, and Cybernetics, vol. 39, no. 1, pp. 4-11, Jan. 2009.

[6] J. Wright, A.Y. Yang, A. Ganesh, S.S. Sastry, and Y. Ma, "Robust Face Recognition via Sparse Representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 31, no. 2, pp. 210-227, Feb.2009.

[7] H. Proenca and L.A. Alexandre, "Iris Segmentation Methodology for Non-Cooperative Recognition," IEE Proc. Vision, Image and Signal Processing, vol. 153, pp. 199-205, 2006.

[8] Low Distortion Transform for Reversible Watermarking, Dinu Coltuc, *Member, IEEE*IEEE transactions on image processing, vol. 21, no. 1, January 2012.

[9] X. Li, "Modeling Intra-Class Variation for Non-Ideal Iris Recognition,"Proc. Int'l Conf. Biometrics, pp. 419-427, 2006.

[10] Mani malek Esmaeili,Mehrdad Fatourechi, and Rabab ward. IEEE transactions on information forensics and security, vol. 6, no. 1, march 2011'A Robust and Fast video copy detection system using content-based Fingerprinting.