Biometric Data Hiding: A 3 Factor Authentication Approach to Verify Identity with a Single Image Using Steganography, Encryption and Matching

Neha Agrawal and Marios Savvides
Carnegie Mellon University
Pittsburgh, PA-15213
nehagrawal.nsit@gmail.com, http://www.cs.cmu.edu/~msavvid

Abstract

Digital Steganography exploits the use of host data to hide a piece of information in such a way that it is imperceptible to a human observer. Its main objectives are imperceptibility, robustness and high payload. DCT Domain message embedding in Spread Spectrum Steganography describes a novel method of using redundancy in DCT coefficients. We improved upon the method of DCT embedding by using the sign of the DCT coefficients to get better accuracy of retrieved data and more robustness under channel attacks like channel noise and JPEG compression artifacts while maintaining the visual imperceptibility of cover image, and even extending the method further to obtain higher payloads. We also apply this method for secure biometric data hiding, transmission and recovery. We hide iris code templates and fingerprints in the host image which can be any arbitrary image, such as face biometric modality and transmit the so formed imperceptible Stego-Image securely and robustly for authentication, and yet obtain perfect reconstruction and classification of iris codes and retrieval of fingerprints at the receiving end without any knowledge of the cover image i.e. a blind method of steganography, which in this case is used to hide biometric template in another biometric modality.

Index Terms– *Steganography, DCT, Biometrics, Stego-Image, iris code templates*

1. Introduction

A number of researchers have studied the interaction between biometrics and steganography, two potentially complementary security technologies. Biometrics is the science and technology of measuring and analyzing physiological characteristics e.g., a person's iris, fingerprints or voice etc. It has the potential to identify individuals with a high degree of assurance [5]. The problem of ensuring security and integrity of the "storage and transmission" of biometric templates is critical so they need to be transmitted with the utmost security. Steganography is the science of communication in a hidden manner [3]. Steganography deals with hiding information in the cover so that not only the information but the very existence of information is hidden. Incorporating cryptography with steganography adds another level of security and can be used to exchange biometric data. We can combine biometrics with steganography of encrypted biometric data to boost security [5] while at the same time provide encryption of the template and the ability to revoke or provide cancellable biometric templates as well.

Due to the prospering of electronic commerce and fear of terrorism, traditional ways of personal identification like ID cards and passwords are no longer sufficient. Biometrics, is a more secure option because it uses parts of the body for authentication, which are practically impossible to get lost, stolen or forgotten [6]. Among the different biometrics, iris recognition, face recognition and fingerprint authentications are most popular [9]. In order to promote the utilization of biometric techniques, an increased security of biometric data seems to be necessary. Encryption, watermarking and steganography are some of the possible schemes to achieve this [8][10].

Steganography, meaning "covered writing" in Greek, involves hiding critical information in unsuspected carrier data. It differs from cryptography, where the communication is evident but the content is concealed. In steganography, the occurrence of communication in itself is not evident. Overall, steganographic systems need to achieve high imperceptibility, be robust against cover modifications, have a large capacity and high message security levels [2][3][12].

Steganographic systems typically use digital multimedia signals in images, audio or video as basis or cover signals for communication. Digital signals typically have high redundancies with respect to human perceptibility which can be exploited to embed data imperceptibly with high data hiding rate and tractable data extraction methods [2]. We also require that data extraction methods in steganographic

978-1-4244-3993-5/09/$25.00 ©2009 IEEE

systems be blind to cover signals.

Some popular methods in steganography include [2][11][13] where different redundancies of a cover image are exploited for hiding the message. Some methods hide data in the image pixel domain e.g., hiding in the LSB of cover image [4] or embedding the data within noise and then hiding in the LSB or adding to the cover image and doing filtering at the receiving end [12]. Some hide data in the frequency domain as in Discrete Cosine Transform (DCT) domain [13]. In one recent paper [2], symmetry in DCT coefficients is exploited for data hiding. In our method, we highlight other redundancies present in DCT coefficients, specifically in the sign of DCT coefficients which can be exploited to hide data in images, keeping the visual quality of the image nearly intact. We also improve the accuracy of the retrieved data as compared to other methods based on DCT coefficients [2] and also increase the payload. Our method is more robust to previous approaches. We also provide a formal analysis of error incurred and relate it with the error involved in DCT coefficients manipulation in standard JPEG compression techniques.

In this paper, we introduce our steganographic model using DCT Embedding of biometric data in section 2, and explain the DCT Embedding technique used in paper [2] in section 3. We proceed to propose our DCT Embedding method in section 4. In section 5, we explore the method further to increase its payload and reduce the bit-error rate while maintaining the visual imperceptibility of the stego image. We discuss our experiments and results under different channel attacks in section 6. There, we also discuss the ability of the proposed method to give perfect reconstruction of iris codes. We present discussions and future work in this method in section 7 and provide the conclusion in section 8.

2. Steganographic Model using DCT Embedding

A simple steganographic method has a stego-system encoder which embeds the message in a digital image using a key. The resulting stego-image is then transmitted over a channel to the receiver where it is processed by the stego-system decoder using the same key as the encoder. Thus the recipient needs to possess only a key to reveal the hidden message, otherwise the very existence of the hidden information is virtually undetectable to any unintended viewer [11][12]. The block diagram in Fig. 1 shows the stego-system encoder of the proposed system. The biometric data (e.g. iris codes or fingerprints) is first encrypted using any cryptographic technique; it may be a public key or private key provided the key is shared between the sender and the receiver, so as to ensure security of the critical biometric information. The encrypted data is then converted into a binary signal after incorporating the error correcting codes (e.g. hamming codes). Now 3x3 blocks of the cover image (here face images are used as cover) are taken and their DCT coefficients are calculated. Our binary signal is then embedded bit by bit per block of the DCT coefficients exploiting the redundancy of these coefficients [13] [15] with respect to image reconstruction. Inverse DCT of the modified block is taken which finally generates our stego-image. This describes the method of encoding. The stego-image is transmitted through a channel and then passed through a stego-system decoder as shown in Fig. 2 where at first DCT unembedding is done to extract the hidden data which is then decoded and decrypted to retrieve biometric data that can be used for identification purposes at the receiving end.

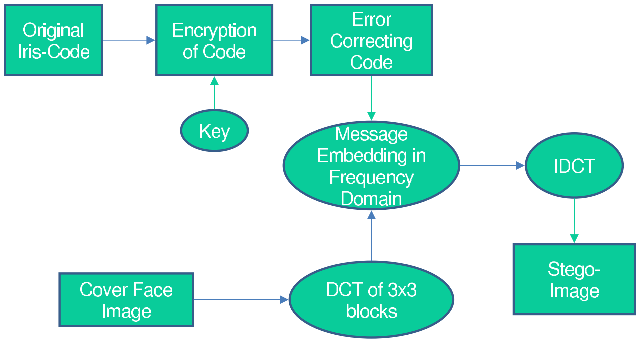


Figure 1. **DCT Embedding Steganographic Encoder**

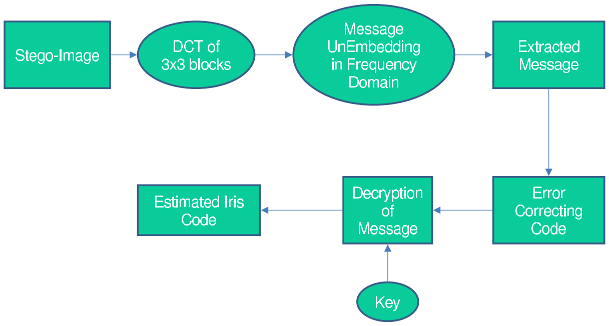


Figure 2. **DCT Embedding Steganographic Decoder**

3. DCT Domain Message Embedding exploiting Symmetry

A large number of methods in image steganography work in DCT domain where they exploit some redundancies and hide data. One recent method was described by Agrawal and Gupta in their paper [2], where they exploited the symmetry of DCT coefficients to embed the quantized modulated data. This method gave more accurate results compared to the simple spread spectrum steganographic method. They also made use of the observation that small changes in DCT coefficients do not significantly alter the visual quality of the image. They took 3x3 DCT blocks of cover image to hide modulated data bit by bit. If we assume a typical DCT coefficients block in Fig. 3, then for hiding a message bit 1 the DCT coefficients d_{31} and d_{13} are exchanged if

$$d_{31} < d_{13} \tag{1}$$

Similarly, bit 0 is hidden by interchanging d_{31} and d_{13} if $d_{31} > d_{13}$. The message deembedding process mirrors the embedding process where DCT coefficients of the received stego-image are evaluated and bit 1 is inferred if $d_{31} > d_{13}$ else bit 0. This method gave a payload of 6.3% bits per pixel and a bit-error rate of 8.5%.

d_{11}	d_{12}	d_{13}
d_{21}	d_{22}	d_{23}
d_{31}	d_{32}	d_{33}

Figure 3. **3x3 block DCT coefficients**

Here the bit-error rate is high for biometric information transmission, which should be done as accurately as possible. In our method we improve upon the error rate and reduce it to a much lower value and even make the payload reach to double that capacity.

4. Proposed Phase Change Method of DCT Embedding

In this section we present our method of embedding the message (here we use iris codes and fingerprints of a person as the message) in DCT domain of the cover image(can be any image but here we take face image). We noted in section 2 that at first, the message is encrypted using any public or private key encryption technique, converted into binary signal. In addition the error-correcting code is incorporated (here we use $(4, 7)$ hamming code) and the resulting message is then hidden bit by bit in the DCT blocks of the cover image.

We know that DCT coefficients of a block denote the rate of change of intensities over that block with the first coefficient d_{11} generally having the highest value and denoting a value proportional to the mean of intensity values in that block. In a typical image the adjacent pixels usually have similar intensity values, so the rest of the DCT coefficients are usually small and as such we can exploit this property of the DCT coefficients to hide our data. In our method we use the sign of the DCT coefficients that offers potential redundancy, for hiding our data without altering the visual quality of the image. Since these coefficients are very small denoting small rate of change from the mean, just by changing the sign and preserving the magnitude, leaves the reconstructed image block from those changed DCT coefficients block imperceptible to human eyes.

In our scheme we operate on the redundancies present in the sign of the DCT coefficients and try to modify the sign, keeping the magnitude same, in order to hide our critical biometric data. We take a 3x3 DCT block of the face image. Then we sort the elements in block in ascending order of absolute values of the DCT coefficients. Let *lav* (lowest absolute value) be the coefficient having the lowest magnitude or first position in sorted list. In order to hide message bit 0, we make *lav* negative, i.e. if *lav* is positive, we use equation (2) else leave it unchanged.

$$lav = -|lav| \tag{2}$$

In order to hide a message bit 1, we make *lav* positive, i.e. if *lav* is negative, we do

$$lav = +|lav| \tag{3}$$

The message de-embedding process mirrors the embedding process where again a 3x3 DCT block of received stego-image is calculated and sorted. Sign of the *lav* is checked. If $lav > 0$ message bit 1 is inferred else bit 0.

4.1. Formal Analysis of Phase Based DCT Embedding method

Here we give a formal analysis of the error incurred in our method and relate it with the error involved in DCT coefficient manipulation in standard JPEG compression techniques.

In the method of JPEG compression 8x8 blocks of an image are taken and their corresponding DCT block is obtained. Let I be one such 8x8 block of the cover image. If we take DCT of that block we obtain a coefficient matrix C as shown below:

$$I \xrightarrow{DCT} C \tag{4}$$

Let C_{ij} be a DCT coefficient and B_{ij} be the corresponding basis image of that coefficient, i.e. one of the 64 basis images for the 8x8 block, then image I can be reconstructed using the below equation:

$$I = \sum_{i=1}^{8} \sum_{j=1}^{8} C_{ij} B_{ij} \tag{5}$$

We first analyze the error incurred in manipulating the DCT coefficients in JPEG compression type method. Using that method we can develop a data hiding method, where for hiding message bit 0 we make $lav = 0$ and leave it unchanged for hiding a message bit 1. Assume (i,j) = (m,n) be the index of the lowest absolute value, then we can get the reconstructed image $\hat{I}_z$ and the error involved E_{z_0} when hiding a 0, and E_{z_1} when hiding a 1, as shown in the equations below:

$$\begin{aligned} \hat{I}_z &= \sum_{i=1,i\neq m}^{8} \sum_{j=1,j\neq n}^{8} C_{ij}B_{ij} \\ E_{z_0} &= I - \hat{I}_z = C_{mn}.B_{mn} \\ E_{z_1} &= 0 \end{aligned} \tag{6}$$

Since the probability of occurrence of both 0's and 1's are 0.5. Thus, we see that overall error E_z involved in this method is

$$E_z = \frac{1}{2}E_{z_0} + \frac{1}{2}E_{z_1} = \frac{1}{2}C_{mn}.B_{mn} \tag{7}$$

In our method we make *lav* negative for hiding 0 and for hiding a 1 we make it positive. Therefore, we get the error involved E_{sc_0} for hiding a message bit 0 as shown in the equations below.

$$\begin{aligned} \hat{I}_{sc_0} &= \left(\sum_{i=1,i\neq m}^{8} \sum_{j=1,j\neq n}^{8} C_{ij}B_{ij} \right) - |C_{m,n}|B_{m,n} \\ E_{sc_0} &= I - \hat{I}_{sc_0} = (C_{m,n} - |C_{mn}|)B_{m,n} \end{aligned} \tag{8}$$

For hiding a message bit 1, the error involved E_{sc_1} is

$$\begin{aligned} \hat{I}_{sc_1} &= \left(\sum_{i=1,i\neq m}^{8} \sum_{j=1,j\neq n}^{8} C_{ij}B_{ij} \right) + |C_{m,n}|B_{m,n} \\ E_{sc_1} &= I - \hat{I}_{sc_1} = (C_{m,n} + |C_{mn}|)B_{m,n} \end{aligned} \tag{9}$$

We know that probability of occurrence of 0's and 1's are equal and equal to 0.5. Thus, we obtain an overall error E_{sc} for our method as

$$E_{sc} = \frac{1}{2}E_{sc_0} + \frac{1}{2}E_{sc_1} = C_{mn}.B_{mn} \tag{10}$$

But, this value $C_{m,n}B_{m,n}$ is very small, so whether it is $\frac{1}{2}C_{mn}B_{mn}$ or $C_{mn}B_{mn}$ there is little difference. On the other hand, it increases the range of safety in which the noise or any other factors may change the data without resulting into any error in extracted data.

5. Exploring the Sign-Change Method of DCT Embedding in Detail

In this section we enhance the accuracy of the retrieved message by using a different DCT coefficient than *lav* from the sorted list. We also use multiple DCT coefficients for hiding a message bit which can significantly improve accuracy of data at the receiving end. We also attempt to double the payload without making a significant effect on the error rate, so that more and more data can be transmitted securely without causing any visual changes.

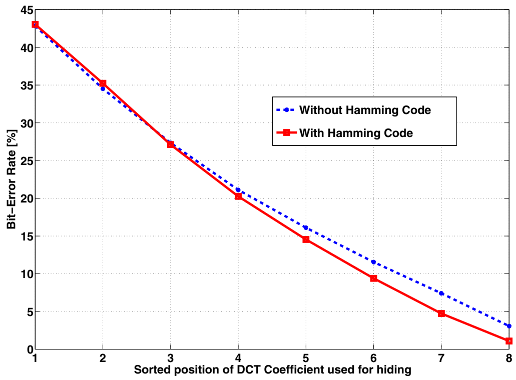


Figure 4. **Bit-error rate on changing the order of DCT Coefficients used**

5.1. Single-Bit hiding using different orders of Single DCT coefficient

Now, we know that our sign-change method performs well both from point of view of visual perception as well as the accuracy of extracted data, but since the biometric data is very important and we want it to be as accurate as possible, so we try to increase the accuracy of this sign-change embedding method by hiding data in different orders of coefficient in the sorted list, i.e. now instead of *lav*, we use second lowest absolute values and so on. We get a plot which is shown in Fig. 4. Observing the plot we can see that using higher order DCT coefficients i.e. coefficients having higher absolute values (leaving the first one i.e d_{11}) as compared to lower order DCT coefficients, we get better accuracy of retrieved data and bit-error rate reduces from 42% (for lav) to 3% (for second *hav* leaving the highest i.e. d_{11}). In addition, use of Hamming codes further improves the accuracy. Thus, we can infer that higher absolute values are more suitable for hiding data from point of view of error-rate and even the visual imperceptibility is not much effected.

5.2. Single Bit hiding using Multiple DCT Coefficients

Now, instead of using only one coefficient for hiding our data, if we increase the number of coefficients used for sign change i.e. for hiding one bit of information we change the sign of multiple coefficients, in order to make the embedding repeatable and robust to some image noise and compression artifacts. We can observe a plot as shown in Fig. 5. We see that as the number of coefficients involved in sign change increases, the accuracy of retrieved message increases with error rate going up to 0.8% when all 8 coefficients, except the highest absolute value, of the 3x3 block are used.

Further, we can also change the sign of multiple DCT

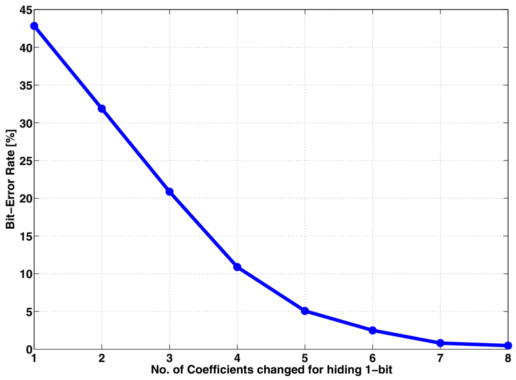
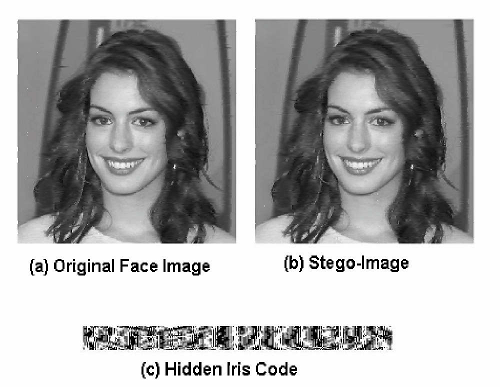


Figure 5. **Bit-error rate on increasing the number of DCT coefficients used**

coefficients for hiding 1 bit and taking the *mean* of the coefficients of the received stego-image and making an inference based on the sign of the *mean*. If the $mean > 0$ we infer a message bit 1 else 0. In this method we not only observe very low error but also the stego-image is visually imperceptible as can be seen in Fig. 6(b). The payload for this method is 6.3% bits per pixel and bit-error rate goes to as low as 0.3%.



(a) Original Face Image

(b) Stego-Image

(c) Hidden Iris Code

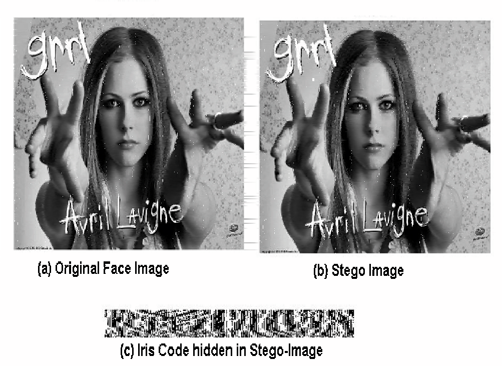
Figure 6. **Sample Stego Image when all 8 DCT coefficients are used**

5.3. Multiple Bit hiding using Multiple DCT Coefficients

In previous sections we were hiding 1 bit in each 3x3 DCT block, we can also try to embed multiple message bits in a block. For this, we again sort the DCT coefficients in ascending order of their absolute values. Let these sorted coefficients be represented by $s_1, s_2, ...s_9$. We experimented different combinations of these sorted coefficients.

1. If we hide the first message bit in s_1, s_3, s_5 and s_7 and the second bit in s_2, s_4, s_6 and s_8 then payload = 12.6% and bit-error rate = 3.2%.
2. If we hide first message bit in s_3 and s_8, second bit in s_4 and s_7 and third bit in s_5 and s_6 then we have 3 bits per DCT block with payload = 18.9% bit-error rate = 9.5%.
3. Hiding 1 bit in each of $s_2, s_3, s_4, s_5, s_6, s_7$ and s_8 then we have 7 bits per DCT block thus giving a payload of 44.1% and bit-error rate of 29.54%.

Thus we can increase the payload but that compromises accuracy of data. Compromising accuracy of critical biometric data is not acceptable and we use embedding process described in Section $5.3.2$ that gives an error rate of 3.2% without causing any visual change which can be seen below in Fig. 7.



(a) Original Face Image

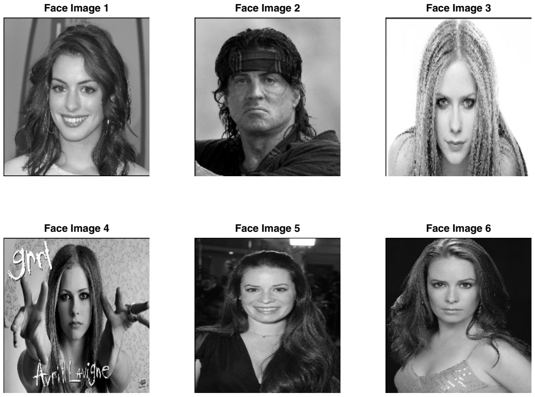
(b) Stego Image

(c) Iris Code hidden in Stego-Image

Figure 7. **Sample Stego Image with 2 message bits per DCT block**

6. Experiments and Results

We tested the method explained in section 5.2 in different face images for hiding different iris codes with masks and different fingerprints as well. If we consider 6 sample face images as shown in Fig. 8 and test embedding process



Face Image 1

Face Image 2

Face Image 3

Face Image 4

Face Image 5

Face Image 6

Figure 8. **Sample Face Images**

of section 5.2 using different iris codes we find a result as shown in Fig. 9 which shows that bit error rate is practically independent of the iris codes but has a dependency on the face image that is being used as the cover image. We did a similar testing for embedding of fingerprints in place of iris codes and masks (some sample fingerprint images are shown in Fig. 10) and found similar results with error as low as 0.8% for some cover face images.

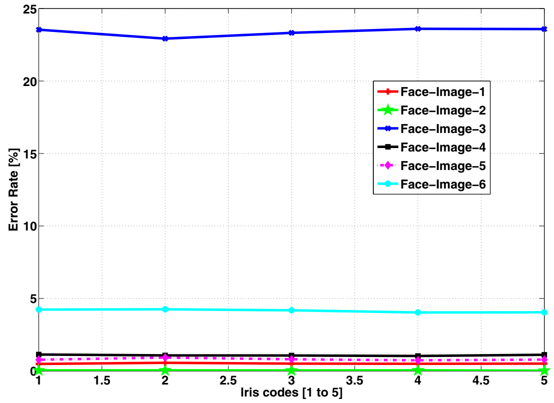


Figure 9. **Hiding** 1**-bit using the sign of all** 8 **DCT coefficients**

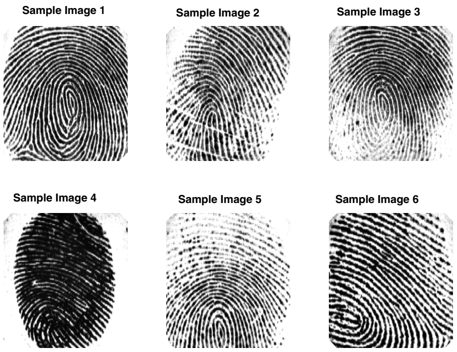


Figure 10. **Sample Fingerprint Images**

Thus, we can infer that changing of the message image doesn't have much effect on error rate while changing of cover image does. Face images like face image 3 and face image 6 as shown in Fig. 8 having an uniform background show higher error rates since uniform background implies little or no DCT information, thus, encoding is futile here, which is expected. Rest of the face images having a real background show negligible error rates. So this method will work on real non-uniform images. In practice, the images would use cropped face images so this will not be an issue worrying about blank backgrounds.

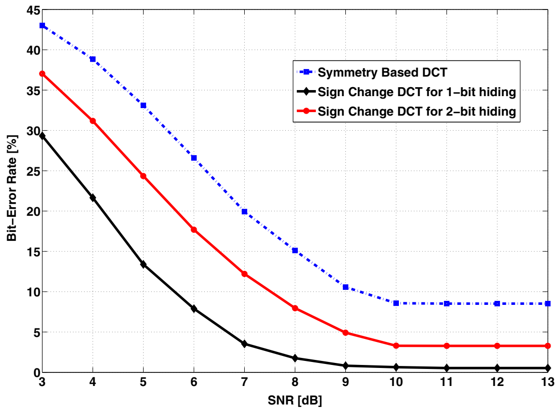


Figure 11. **Performance comparison under channel noise-attack on Sign Change DCT and Symmetry Based DCT**

6.1. Testing under Channel Noise Attack

We tested our sign change based method under channel noise attack and as seen in Fig. 11, it outperforms the symmetry-based method discussed in Section 3, where at SNR of 25 dB we get an error-rate of $\approx 9\%$. Besides, the sign change method for 2-bit hiding as discussed in Section 5.3.2 also shows much better performance compared to symmetry-based method. Thus, we can say that this method is much more robust as compared to earlier methods of DCT embedding.

6.2. Testing under JPEG Compression

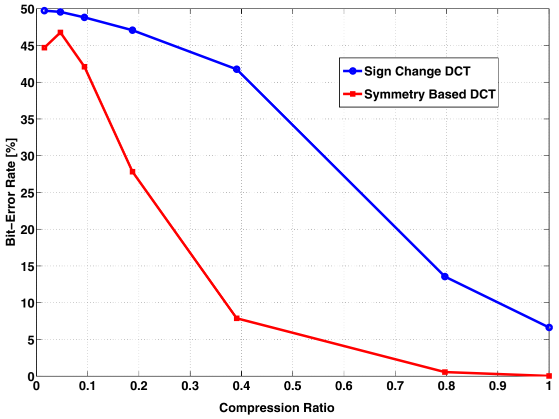


Figure 12. **Performance Comparison under JPEG-compression attack on Sign Change DCT and Symmetry Based DCT**

We also tested our method under JPEG compression channel attack and present the corresponding results in Fig. 12. Here too, we observe that our method clearly outperforms the symmetry based method.

6.3. Hamming Distance Calculation for Extracted Iris Codes and Classification Errors

We also applied our data hiding method for hiding iris codes in face images and did experiments for evaluating authenticity of extracted iris codes. We used Hamming Distance criterion to evaluate correspondence between actual and extracted iris codes. In this criterion, we integrate the density function raised to the power of the number of independent tests. A fractional hamming distance is used to quantify the difference between iris patterns. The hamming distance of two vectors is the number of components in which the vectors differ in a particular vector space [7]. We tested our method for hiding 7 different iris codes for 15 different people in the 6 different face images shown in Fig. 8. We conducted our research on a subset of the NIST Iris Challenge Evaluation (ICE) dataset [1]. We calculated the actual hamming distance for inter-class and intra-class comparisons, where, intra-class means different iris codes of same person are compared and hamming distance between them is calculated and inter-class means comparison between iris codes of different persons. The result was obtained as shown in Fig. 13. We also calculated the hamming distance for extracted iris codes from different stego-images (obtained using our method of embedding) with different iris codes of same person for intra-class and of different persons for inter-class comparisons and results were obtained in Fig. 14. We calculated False Accept Rate (FAR) and False Reject Rate (FRR) and a Detection Error Rate curve was plotted for both the original iris codes as well as for the extracted iris codes as can be seen in Fig. 15. We see that FRR is slightly higher in this method when FAR is very less, however it decreases and becomes comparable to actual iris codes FRR as FAR increases. The Equal Error Rate of extracted iris codes is very close to that of Original iris codes. Original iris codes have an EER of 1.25% with Fisher Ratio (FR) of 15.6236. Extracted ones have 1.58% of EER and FR of 11.7297 where

$$FisherRatio(FR) = \frac{(\mu_{imposter} - \mu_{authentic})^2}{\sigma^2{}_{imposter} + \sigma^2{}_{authentic}} \quad (11)$$

Here μ represents the mean of the hamming distances and σ represents the variance.

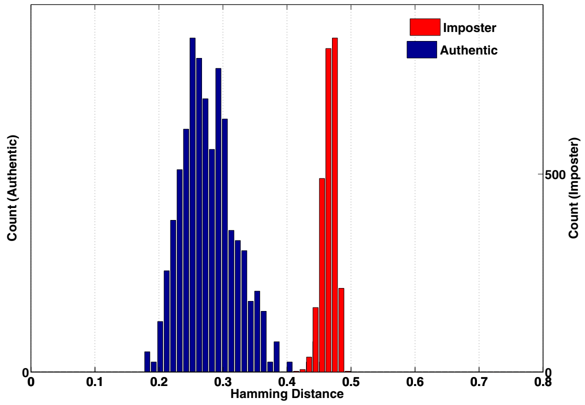


Figure 13. **Inter-class (Imposter) and Intra-class (Authentic) comparison of Original Iris Codes**

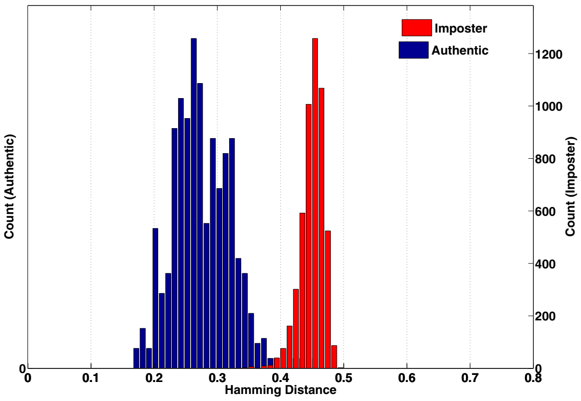


Figure 14. **Inter-class (Imposter) and Intra-class (Authentic) comparison for Extracted Iris Codes**

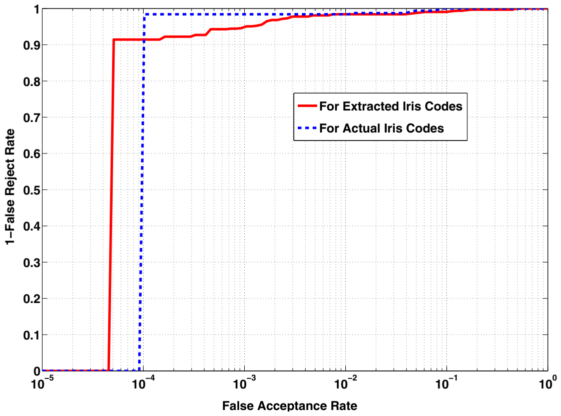


Figure 15. **Detection Error Rate curve for Original and extracted Iris Codes**

7. Discussion and Future Work

Our approach can be used to verify authenticity of the original image from the stego-image. We can use the extracted biometric template to verify that original face image remained unaltered. Thus iris and face make the two safety factors. The 3^{rd} factor is the key or seed/password one needs to remember to decrypt the iris template. Thus even if someone knows the stego-encryption-method, one could not put their face and 'encrypt' the iris template in the same way. One could steal the face but the iris template is protected and can be cancelled/revoked.

Next we discuss some of the issues that we came across in our method. We observed that our method is bound by the type of cover image and thus shows inferior results for face images that have uniform backgrounds but works very well on non-uniform cover images. In order to tackle this problem, we can decide when to hide a message bit in a DCT block, e.g., we can hide bits in those DCT blocks only where all are non-zero coefficients or at most 2 coefficients are 0 i.e. we can reject those blocks having more than 2 zero DCT coefficients and move on to the next block. We can even insert a high frequency background in those cover images or find high frequency regions and hide our data in those regions. Since selecting a cover image is purely on the discretion of the user and it is data that is to be hidden, is of more importance, we can modify the cover image to fit our requirements and even if we don't do so, error is still negotiable.

We can further improve the accuracy of the retrieved data by using better error-correcting codes as compared to hamming codes used here, but that might result in payload reduction. In noiseless channels we expect exact recovery of our data, we don't get that in practice, due to the rounding-off error problem [14], which occurs if we make even a small change to the magnitude of these DCT coefficients thus resulting in rounding off of the values when we take inverse DCT transform of the modified block, leading to erroneous results. We can also try to handle this error to further improve accuracy.

8. Conclusion

In this paper, we introduced a new and more robust method of hiding biometric data in DCT coefficients of cover image which can be exploited for hiding any type of information, an image or biometric data like fingerprints and iris codes, imperceptibly and robustly. The method can be extended to increase the payload by hiding more than one bit in a 3x3 DCT block. We tested our algorithm in terms of visual performance, additive channel noise and JPEG compression and observed a significant overall improvement in the steganographic performance under our method over the symmetry based method. We observed that the hamming distance and EER of the extracted iris codes were comparable to those of original and as such the method can give us nearly perfect reconstruction and classification of iris codes. Thus, we can we conclude that this method is very efficient and robust in secure transmission of critical information. It can be used to verify the authenticity of original image as well as transmitted image. Thus, this method can be widely used in exchange of biometric data.

References

[1] Iris challenge evaluation. National Institute of Standards and Technology, http://iris.nist.gov/ICE/, 2006. 7

[2] N. Agrawal and A. Gutpa. Dct domain message embedding in spread spectrum steganography system. Accepted at Data Compression Conference 2009 and to be published by IEEE Computer Society Press, 2009. 1, 2

[3] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for images, audio and video. volume 111, pages 243–246, 1996. 1

[4] S. Dumitrescu, X. Wu, and Z. Wang. Detection of lsb steganography via sample pair analysis. *IEEE Trans. Signal Processing*, 51. 2

[5] R. A. F. Hao and J. Daugman. Combining crypto with biometrics effectively. *IEEE Trans. on Computers*, 55(9):1081–1088, 2006. 1

[6] Y. W. Fana, V. P. Paucaa, R. J. Plemmonsa, S. Prasadb, T. C. Torgersena, and J. V. D. Grachtc. Hamming distance optimized phase masks for iris recognition system. *Topical Meeting on Computational Optical Sensing and Imaging (COSI)*, 2005. 1

[7] J. Horst. Overview of iris recognition. *Journal of Student Reserch*, pages 19–24, 2008. 7

[8] A. K. Jain and U. Uludag. Hiding fingerprint minutiae in images. In *Proceedings of Third Workshop on Automatic Identification Advanced Technologies (AutoID)*, pages 97–102, 2002. 1

[9] A. K. Jain and U. Uludag. Hiding biometric data. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 25(11):1494–1498, 2003. 1

[10] N. F. Johnson, Z. Duric, and S. Jajodia. *Information Hiding*. Kluwer Academic Publishers, 2001. 1

[11] N. F. Johnson and S. Katzenbeisser. *A survey of steganographic techniques, Information Hiding*. Artech House, Norwood, 2000. 2

[12] L. M. Marvel, C. G. Boncelet, and C. T. Retter. Spread spectrum image steganography. *IEEE Trans. on Image Processing*, 8(8):1075–1083, 1999. 1, 2

[13] X. Qi and K. Wong. An adaptive dct-based mod-4 steganographic method. *IEEE International Conference on Image Processing*, 2:297–300, 2005. 2

[14] F. Y. Shih. *Digital Watermarking and Steganography*. CRC Press, 2007. 8

[15] Y. Wang and P. Moulin. Steganalsis of block dct image steganography. *IEEE Workshop on Statistical Signal Processing*, pages 339–342, 2003. 2