



International Journal of Engineering, Business and Enterprise Applications (IJEBEA)

(Open Access, Double Blind Peer-reviewed, Refereed and Indexed Journal)

www.iasir.net

Adaptive Stegnaography Using Discrete Cosine Transformation

Shashikala.J¹, Ambika.R²

Electronics & Communication

BMS Institute of Technology & Management

Yelahanka, Bengaluru

India

Abstract: Cryptography was one of the methods of hiding the secret information by just scrambling the secret data.. The main features of steganography include security, robustness, and imperceptibility. In Steganography the method of hiding is in such a way that no one is aware that a hidden message even exists. Hence it's possible to avoid drawing suspicion of an intruder to the transmission of hidden data which enhances security. In our proposed system, the payload is embedded in to the coefficients of DCT (Discrete Cosine Transformation) adaptively. In the adaptive technique the number of bits used to hide the data varies with respect to the coefficient of the cosine transformation which will improve the PSNR(Peak signal to noise ratio) as well as the Hiding Capacity from the existing techniques.

Keywords: Cryptography, security, robustness, Discrete Cosine Transformation, Peak signal to noise ratio

I. Introduction

Network security is one of the major challenges in the present world scenario. "Cryptography", was one of the methods of hiding the secret information by just scrambling the secret data. But this method possessed major drawbacks as it led to an unauthorized person to guess a secret message transfer and strive to retrieve the data. Hence this method did not assure security and robustness. The most important condition for Steganography is its imperceptibility and that depends on amount of secret information. The data to be exchanged could even be of high integrity and confidentiality. Steganalysis is used to retrieve or to detect the payload.

The most popular hiding methods are Spatial Domain Based Steganographic Methods, Palette Based Steganographic Methods and Transform Domain Based Steganographic Methods. Spatial domain based steganography includes the LSB (Least significant bit) Replacement and Matching and BPCS (Bit-Plane Complexity Segmentation) steganography. Palette based stegnographic methods are generally used for the colour images .Images transformed in to the palette based colour representation can be widely used over the internet. Transform domain based stegnographic method hides the coefficients of the data in the represented domain.

II. Literature Survey

R.O. El Safy et al., [1] proposed an adaptive stegnographic technique in which the bits of the payload were hidden in the integer wavelet coefficients of the cover image adaptively along with optimum pixel adjustment algorithm. Hassan Mathkour et al., [2] compared the strengths and weaknesses of the existing techniques of steganography and implemented a new steganographic wizard based tool, which have been examined against several other tools like F5, Stools etc. for more robust and secure steganography. K. Suresh Babu et al., [3] proposed an authentication model of steganography to detect any attack on the stego image. This is done by verifying whether there are any modifications in the secret information like deletion, edition or forgery. Kotaro Yamamoto and Munetoshi Iwakiri ,[4] proposed a technique where the embedding of the secret information is done in the fluctuations created by the player and not in the Standard Musical Instrument Digital Interface (MIDI) File(SMF). The embedding capability of this technique is higher compared to the other conventional methods A. W Naji et al., [5] analyzed different steganographic techniques and weaknesses in the respective techniques.

III. Block Diagram

The figure 1 shows the block diagram of software implementation of the proposed method. At the transmitter a secure and robust algorithm for transmitting the secret data is designed. Special care is taken while transmitting the key from the source to the destination. Hence, while the stego image is passed through an open channel, the key should be transmitted through a secret channel. The algorithm may or may not be known to the attacker. But if the key is known, then retrieval becomes easy for the attacker.

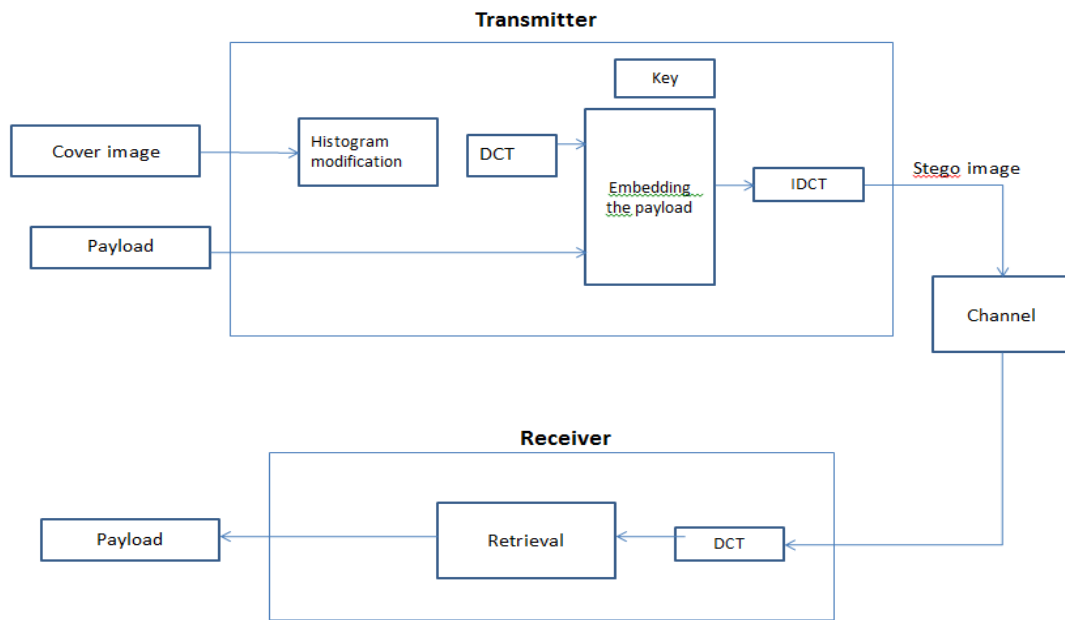


Fig. 1: Block Diagram of adaptive steganography

A. Embedding Algorithm

In this procedure the payload is hidden inside the cover image to obtain the stego image.

Input: cover image and Payload; Output: Stego image

- 1) A cover image of any size and format (bmp, jpg, tif, etc) is taken.
- 2) Applying pixel management to the cover image.
- 3) Segmentation of cover image into 8*8 blocks.
- 4) The 8*8 blocks are transformed into frequency domain using DCT.
- 5) Embedding capacity(L) for each coefficient is calculated as following:
 $L=5$, if $C0 \geq 2^5$;
 $L=4$, if $2^5 \leq C0 \leq 2^4$;
 $L=3$, if $2^4 \leq C0 \leq 2^3$;
 else $L=2$;
- 6) The payload to be embedded is taken in gray scale. Four MSB'S of each pixel of the payload are embedded into the cover image.
- 7) The stego image obtained in the DCT domain is converted back into the spatial domain using IDCT.

B. Retrieval Algorithm

In the retrieval procedure stego image is taken and the payload is retrieved from the stego image. The key used in the embedding procedure is transmitted beforehand to the receiver through a secure channel.

Input: Stego image; Output: Payload

- 1) The stego image received is read in 2D array.
- 2) Further the stego image is segmented into 8x8 blocks.
- 3) The 8*8 blocks are transformed into frequency domain using DCT.
- 4) Embedding capacity (L) for each coefficient is calculated as above.
- 5) Extract L bits from each selected coefficients. Gather all extracted bits together to form the secret data back in order. This gives the payload.

The embedding and retrieving algorithm is implemented using MATLAB software.

IV. Results

Steganography is used for covert communication. In our project the secret image which is communicated to the destination is embedded into the cover image to derive the stego image. For performance analysis we considered

cover image and payload of any size and format. Here stego image is obtained by considering Lena as cover image and Barbara as payload.



(a) Cover



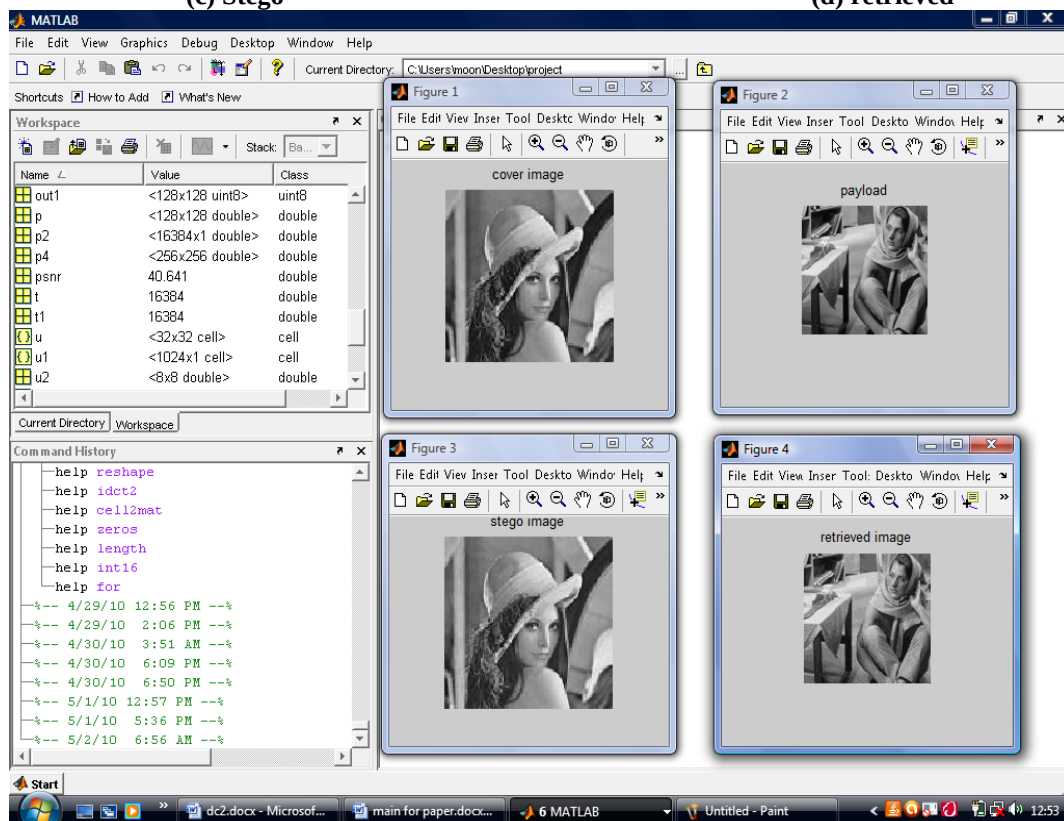
(b) payload



(c) Stego



(d) retrieved



Cover image	Method	Max H C (bits)	Max H C (%)	PSNR (db)
LENA as Cover Image and Barbara as payload	Proposed	986408	47	39.48
	Existing	986408	47	31.8

Table 1: Results of proposed method

V. Conclusions

In our proposed technique the cover image is divided into 8*8 blocks and a DCT is applied on segmented image. The payload is embedded in to the DCT coefficients adaptively. In the adaptive technique the number of bits used to hide the data varies with respect to the coefficient of the cosine transformation. By using the proposed method, we have been able to improve the PSNR as well as the Hiding Capacity from the existing techniques.

VI. References

- [1] Rowel Safy, H.H.Zayed and A.El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform," International Conference on Networking and Media Convergence, pp.111-117, March 2009.
- [2] Mathkour H, Al-Sadoon B and Tourir A , "A New Image Steganography Technique," International Conference on Wireless Communications, Networking and Mobile Computing, pp.1-4 , October 2008.
- [3] Suresh Babu K, Raja K.B, Kiran K.K, Manjula Devi T.H, Venugopal K.R and Patnaik L.M; "Authentication of Secret Information in Image Steganography," IEEE Conference on TENCON, pp. 1-6, November 2008.
- [4] Kotaro Yamamoto and Munetoshi Iwakiri, "A Standard MIDI File Steganography Based on Fluctuation of Duration," International Conference on Availability, Reliability and Security, pp. 774-779, March 2009.
- [5] A.W. Naji, Teddy .S. Gunawan, Shihab A. Hameed, B.B. Zaidan and A.A. Zaidan, "Stego-Analysis Chain, Session One," Spring Conference on Computer science and Information Technology, pp. 405-409, April 2009.