Image Hiding Using Discrete Cosine Transform

Iman M.G. Alwan **Farah Jasim Mohammed**
University of Baghdad - College of Education for Women - Computer Science Dept.

Abstract

Steganography is a mean of hiding information within a more obvious form of communication. It exploits the use of host data to hide a piece of information in such a way that it is imperceptible to human observer. The major goals of effective Steganography are High Embedding Capacity, Imperceptibility and Robustness. This paper introduces a scheme for hiding secret images that could be as much as 25% of the host image data. The proposed algorithm uses orthogonal discrete cosine transform for host image. A scaling factor (a) in frequency domain controls the quality of the stego images. Experimented results of secret image recovery after applying JPEG coding to the stego-images are included**.**

إخفاء الصور بالاعتماد على تحويلة الجيب تمام المتقطعة

إيمان محمد جعفر علوان **فرح جاسم محمد**
جامعة بغداد - كلية التربية للبنات - قسم الحاسبات

الملخص

Steganography هو وسيلة لإخفاء المعلومات داخل نموذج أكثر وضوحا من الاتصالات. فهو يستثمر استخدام المضيف (host) لإخفاء قطعة من المعلومات باسلوب غير محسوس إلى المراقب . الأهداف الرئيسة لطرق الاخفاء الفعالة هي قدرة تضمينها العالية ومتانتها ضد طرق الهجوم المختلفة . يقدم هذا البحث مخطط لإخفاء الصور السرية والتي بحجم 25٪ من حجم الصورة المضيفة. تستخدم الخوارزمية المقترحة تحويلة الجيب تمام للصورة المضيفة. وهناك عامل التحجيم (a) في مجال التردد يسيطر على نوعية الصور stego. وقد تم تضمين النتائج الخاصة باسترجاع الصور السرية بعد تعريض الصور ال stego الى ضغط من نوع JPEG .

Keywords: Image hiding, Discrete Cosine Transform, Steganography, JPEG Compression

Introduction

Steganography systems transfer information over the public communication channels in such a way that an attacker is unable to identify the transmission of secret information on the background of a public communication [1]. In general, efficiency of the secret information detection in any Steganography system is related to the size of the hidden secret data. The Steganographic Systems use media that may be a digital still image, audio file, or video file. Once the data has been embedded, it may be transferred across insecure lines or posted in public places. Therefore, the dummy container should seem innocent under most tests [2]. Hiding the subjects with Steganographic techniques using meaningful images involves the spatial [3, 4], and frequency [5, 6, 7] domains of those cover images.

In the spatial domain approach, the secret message is embedded directly into the pixels of a cover image. Least significant bit (LSB)-based hiding strategies are most commonly used in this approach. For example, in Lee and Chen's scheme [8], the LSB of each pixel in a cover image is modified to hide the secret message. In Chang et al.'s scheme [4], a dynamic programming strategy is used to find the optimal LSB substitution in order to hide images. In addition to LSB-based hiding strategies, several schemes that use different strategies to hide secret messages in the spatial domains of cover images also have been proposed. For example, Chung et al. offered the singular value decomposition (SVD)-based hiding scheme

[9], Tsai et al. used the bit plane of each block truncation coding (BTC) block to embed secret messages [10]. In the frequency domain [5,6,7], cover images must first be transformed using a frequency-oriented mechanism such as discrete cosine transform (DCT), discrete wavelet transform (DWT) or similar mechanisms, after which the secret messages can be combined with the coefficients in the frequency-form images to achieve embedding. For example, in Chang et al.'s scheme [6], the medium-frequency coefficients of DCT transformed cover images are used to embed a secret message. The proposed scheme embeds the secret information in the discrete cosine transform domain of the host image. Spatial distribution of the discrete cosine transform coefficients helps to recover the secret message even when the images are compressed using JPEG lossy compression . The proposed scheme focuses on hiding the secret messages mostly in the high discrete cosine transform bands, stable reconstruction can be obtained in the reconstruction process. Acceptable reconstruction of secret image can be achieved if the stego-image is compressed to low level of compression.

Discrete Cosine Transformation (DCT):-

Image transforms are very important in digital processing they allow to accomplish less with more .For example the Fourier Transform may be used to effectively compute convolutions of images or the Discrete Cosine Transform may be used to significantly decrease space occupied by images without noticeable quality loss [11]. The DCT transforms a signal or image from the spatial domain to the frequency domain. It separates the image into parts (or spectral sub-bands) of differing importance (with respect to the image visual quality). It can separate the Image into High, Middle and Low Frequency components [12].

The Two-Dimensional (2D-DCT)

The 2-D DCT is a direct extension of the 1-D case, and is given by the equation (1)

$$C(u,v) = a(u)a(v) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad ------(1)$$

For u, v=0, 1, 2,………., N-1 and a(u) and a(v) are defined in equation (2) .

$$a(u) = \begin{cases} \sqrt{\frac{1}{N}} & for \quad u = 0 \\ \sqrt{\frac{2}{N}} & for \quad u \neq 0 \end{cases} \quad --------(2)$$

The inverse transform is defined in equation (3).

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} a(u)a(v)c(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad --------(3)$$

For x, y=0,1,2,…………………,N-1. The 2-D basis functions can be generated by multiplying the horizontally oriented 1-D basis functions with vertically oriented set of the same functions [13].

The Proposed Algorithm:-

A Steganography scheme must be extremely secure, and does not reduce the visual quality of the cover Image when the secret image is concealed. the overall concealing process of our proposed scheme is shown in Fig.(1).The proposed algorithm depends on normalized the secret image by multiplying it by a scaling factor (a) then embed the secret image into the high frequency band of the host image after applying Discrete Cosine Transform. An inverse

DCT is applied to get the stego-image. The Algorithm proposed hiding three secret images of gray scale into one color image. By experimental test the best value of (a) is (0.8).

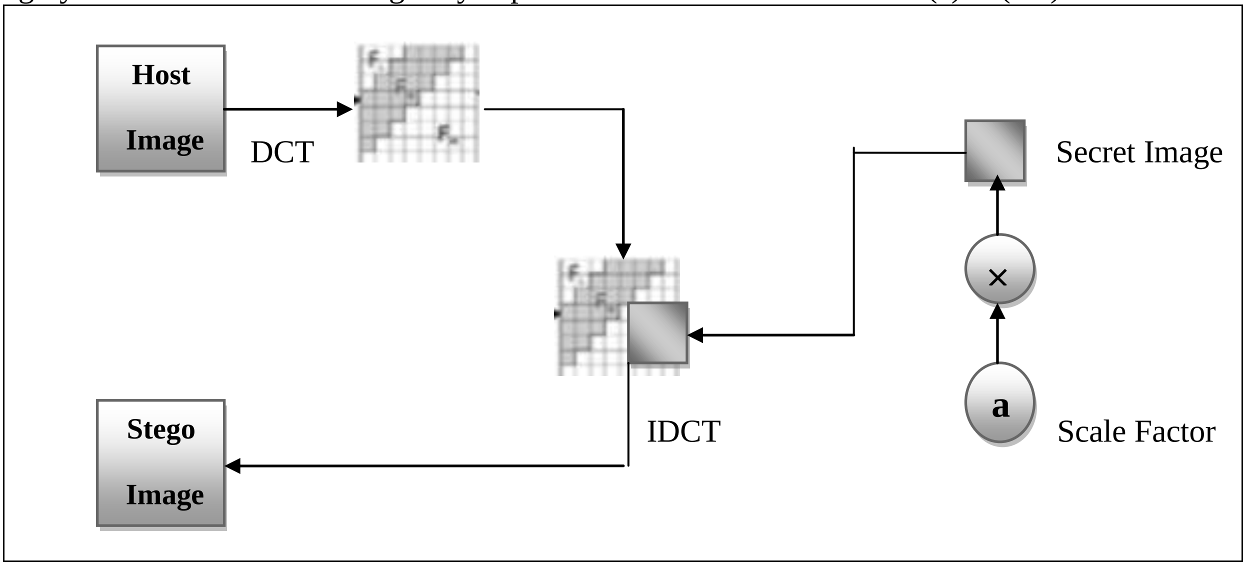


Fig (1). A schematic of the data embedding approach

Embedding Algorithm:-

Input: Three grey scale secret images of size ($\frac{N}{2} \times \frac{N}{2}$), cover (one color image) of size (N× N).

Output: Stego – image.

For each band (R , G , B) of cover image :

Step 1: Apply Discrete Cosine Transform.

Step 2: Normalize the secret image by multiplying it with factor (a).

Step 3: Replace the coefficients of the cover band in the fourth quarter where high band Frequency reside with coefficients of the normalized secret image according to the equation:

C (m, n)= a* s(k , j) ; where m , n = $\frac{N}{2} + 1 \ to\ N$; k, j = $1 \ to\ \frac{N}{2}$, C is cover image , S is the secret image .

Step 4: Reconstruct the stego image by applying Inverse Discrete Transform.

Step 5: End.

Extracting Algorithm:

Input: Stego – image.

Output: Three secret images.

For each band of Stego color image (R , G , B) :

Step 1: Apply Discrete Cosine Transform .

Step 2: Extract the embedded secret image by applying

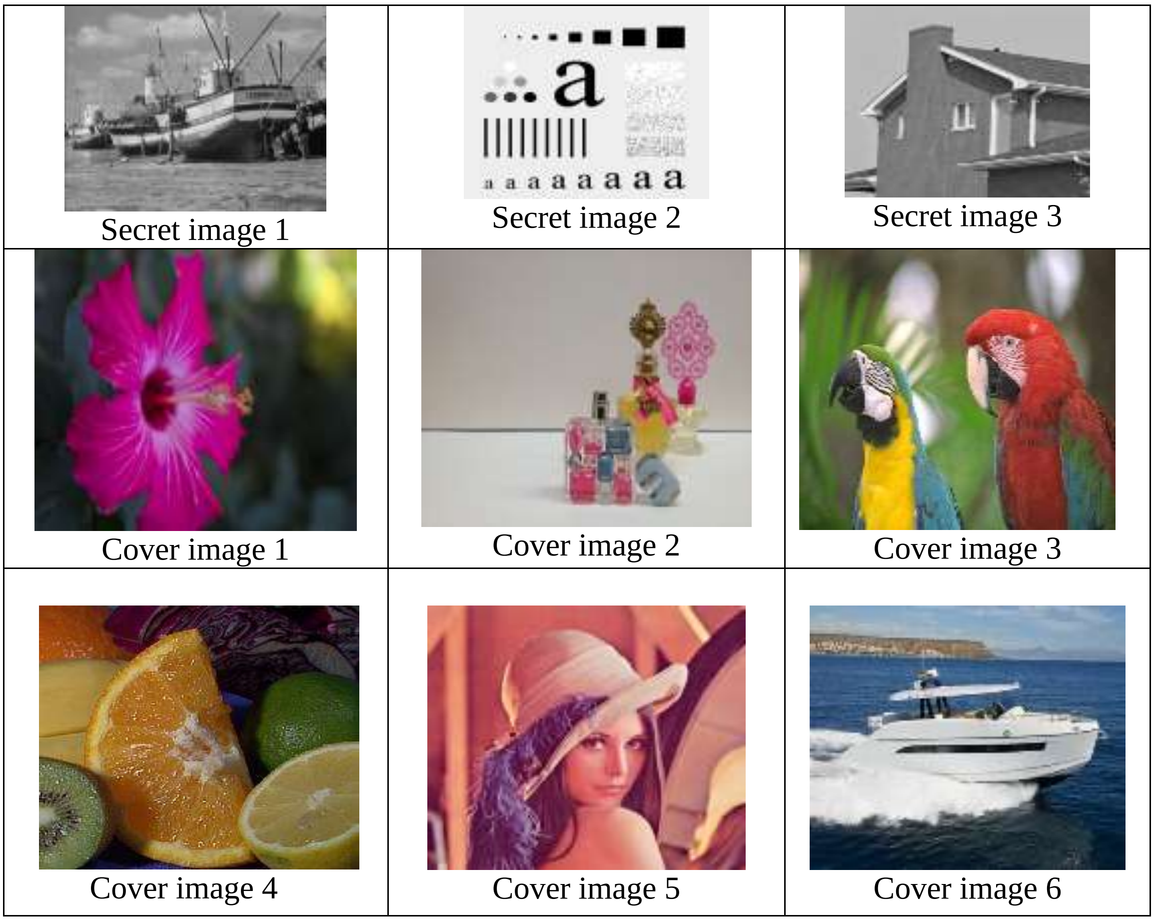
S(k , j) = Stego (m , n) / a ;

where m= $\frac{N}{2} + 1$, n= $\frac{N}{2} + 1$ to N ; k, j = 1 to $\frac{N}{2}$, Stego is the Stego-image S is the secret image .

Step 3: End.

The Experimented Results:

The proposed algorithm is implemented and tested on several standard images. The cover Images are of (256 × 256) color – scale, and the secret images are of (128 ×128) size (gray-scale). Fig.(2) shows at the first row the secret test images, the second ,and third row is for test cover images .



Secret image 1 | Secret image 2 | Secret image 3
Cover image 1 | Cover image 2 | Cover image 3
Cover image 4 | Cover image 5 | Cover image 6

Fig. (2) The Secret, Cover Images.

The same three secret images are embedded in the cover images at every time .**Peak Signal to Noise Ratio (PSNR)** measure and **Correlation** measure **[15]** are used to evaluate the quality of stego- image with respected to the original cover –image. When the stego - image is perceptually similar to the original cover – image , the correlation equals one . These Metrecs are defined as follows:

$$PSNR = 10\log 10\left(\frac{255^2}{MSE}\right) \qquad ------------(4)$$

$$MSE = \left(\frac{1}{N}\right)^2 \sum\sum \left(x_{ij} - x'_{ij}\right)^2 \qquad ------------(5)$$

where xij denote the original pixel values , x'_{ij} denote the modified pixel values , and N is the dimension of the image.

$$Corr = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)-\bar{x}) - (y^{-}(i,j)-\bar{x})}{\sqrt{[\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j)-\bar{x})^2][\sum_{i=1}^{M}\sum_{j=1}^{N}(y(i,j)-\bar{y})^2]}} \qquad ---------(6)$$

where M.N: height and width of the two images.

$x(i,j)$: The original image.

y (i,j): the modified image.

$\bar{x}$ and $\bar{y}$: Mean of original and modified images , respectively. Fig. (3) shows the results of the proposed algorithm. As shown the stego images are of good quality.Fig. (4) shows the reconstructed secret images which are the same from each stego image, they are of very good quality and without any lose of information.

 Cover image 1 PSNR=39.53 dB CORR= 0.9999	 Cover image 2 PSNR= 34.78 dB CORR= 0.9994	 Cover image 3 PSNR= 34.29 dB CORR=0.9996
 Cover image 4 PSNR= 36.39 dB CORR= 0.9998	 Cover image 5 PSNR= 32.15 dB CORR= 0.9996	 Cover image 6 PSNR= 31.56 dB CORR= 0.9998

Fig. (3) The PSNR and the CORR for the stego – images

 Reconstructed secret image 1	 Reconstructed secret image 2	 Reconstructed secret image 3

Fig. (4) The reconstructed secret images from Stego images

The Stego images were compressed by using JPEG compression system to study the effect of compression on the proposed system. Fig. (5) shows the Stego-image (Parrot) at various levels of JPEG compression and the reconstructed secret images for 10%, 20%, 30% compression ratio .The compression ratio used is [15] .

CR= (size of the compressed file /size of uncompressed file)* 100 % -------------(7).

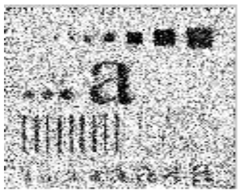
 Stego image Compression 10% (PSNR= 34.30 dB)	 Stego image compression 20% (PSNR= 34.21 dB)	 Stego image compression 30% (PSNR= 33.83 dB)
		
		
		
Reconstructed images of compression 10%	Reconstructed images of compression 20%	Reconstructed images of compression 30%

Fig.(5) The results of Stego(Parrot) and reconstructed secret images for JPEG compression

From the results of JPEG lossy compression on the stego images, we can notice that the system offers good response for low ratio of compression while it offers very poor response for mid and high compression ratios. The reason is that, the hiding algorithm depends on hide secret information in high band frequencies which it's firstly affected by compression process.

Conclusion:

In the proposed algorithm, a scheme of embedding secret image of size (1/4) of the cover image is proposed, it depends on applying discrete cosine transform to the cover image, embedding the secret image in the high frequency band after multiplying it by a scaling factor (a) in order to prevent visual artifacts, leaving the low frequency subbands unchanged. The algorithm is secure because the restriction of the embedding algorithm (i.e., the use of transform, and the value of scaling factor).

References:

[1] Arnold, M., Schmucker, M., and Wolthusen, S., "Techniques and Applications of Digital Watermarking and Content Protection". Artech House, London, 2003.

[2] Noda, H. , Niimi , M, and , Kawaguchi , E., " High performance JPEG Steganography using quantization index modulation in DCT domain " , Preprint submitted to Elsevier Science , 3 August , 2005.
[3] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber," Lossless Generalized-LSB Data Embedding", IEEE Trans. Image Processing, vol. 14, no. 2, pp. 253-266, Feb. 2005.
[4] C. C. Chang, J. Y. Hsiao, and C. S. Chan, "Finding Optimal Least-Significant-Bit Substitution in Image Hiding by Dynamic Programming Strategy", Pattern Recognition, vol. 36, no. 7, pp.1595-1683, July 2003
[5] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in DCT-Based compressed images", Information Sciences, vol. 177, pp. 2768-2786, July 2007.
[6] C. C. Chang, T. S. Chen, and L. Z. Chung, "A Steganographic Method Based upon JPEG and Quantization Table Modification", Information Sciences, vol.141, pp. 123-138, 2002.
[7] J. Fridrich, M. Goljanb, R. Du, "Invertible Authentication Watermark for JPEG Images", IEEE Int. Conf. Information Technology: Coding and Computing, pp., 223–227, 2001.
[8] Y.K. Lee and L. H. Chen, "High Capacity Image Steganographic Model", Proc., of IEEE International Conference on Vision, Image and Signal Processing, vol. 147, no. 3, pp. 288– 294, 2000.
[9] K. L. Chung, C. H. Shen and L. C. Chang, "A Novel SVD- and VQ-based Image Hiding Scheme", Pattern Recognition Letters, vol. 22, no. 9, pp.1051–1058, 2001.
[10]. P. Tsai, Y. C.Hu and C. C. Chang, "An Image Hiding Technique Using Block Truncation Coding", Proc. of Pacific Rim Workshop on Digital Steganography, pp. 54-64, July 2002.
[11]. Sumbera, T., " Wavelet Transform using Haar Wavelet", MSOE Final Project,2001.
[12].Rafferty, C.," Steganography & Steganalysis of Images", Msc Communication System Theory, 2005.
[13]. Ali Khayam ,S., "The Discrete Cosine Transform(DCT):Theory and Application", Michigan State University, Seminar, 2003.
[14]. Almohammad , A.,and Ghinea, G.,"Image Steganography and Chrominance Components ", 10th IEEE International Conference on Computer and International Technology ,pp.996- 1001, 2010.
[15]. Poobal, S., and Ravindran, G.,"Arrving at an Optimum Value of Tolerance Factor for Compressing Medical Images", World Academy J.Sci. Eng. Tech vol.24, pp.169-173, 2006.