A NOVEL IMAGE STEGANOGRAPHY APPROACH USING MULTI-LAYERS DCT FEATURES BASED ON SUPPORT VECTOR MACHINE CLASSIFIER

Akram AbdelQader[1] and Fadel AlTamimi[2]

[1]Department of Multimedia Systems, AL-Zaytoonah University Of Jordan, Amman, Jordan
[2] Department of Computer Science, AL-Zaytoonah University Of Jordan, Amman, Jordan

ABSTRACT

Steganography is the science of hidden data in the cover image without any updating of the cover image. The recent research of the steganography is significantly used to hide large amount of information within an image and/or audio files. This paper proposed a new novel approach for hiding the data of secret image using Discrete Cosine Transform (DCT) features based on linear Support Vector Machine (SVM) classifier. The DCT features are used to decrease the image redundant information. Moreover, DCT is used to embed the secrete message based on the least significant bits of the RGB. Each bit in the cover image is changed only to the extent that is not seen by the eyes of human. The SVM used as a classifier to speed up the hiding process via the DCT features. The proposed method is implemented and the results show significant improvements. In addition, the performance analysis is calculated based on the parameters MSE, PSNR, NC, processing time, capacity, and robustness.

KEYWORDS

Discrete Cosine Transform (DCT), Support Vector Machine (SVM), Classifier, Steganography, Peak signal-to-noise ratio (PSNR).

1. INTRODUCTION

Recently, the growth of technology and social media communications over the internet motivate the researchers to develop new steganography techniques. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Today, steganography technology and steganalysis are attracted on much attention. Steganalysis is focusing on the detection the present of hidden message. In the literatures, many steganalytic research and schemes for digital images have been proposed [1]–[3]. Recently, the security issues are very important research due to the wide amount of information over the internet.

Steganography in the simple means hidden date in other, such as image, audio file or even a video file [2]. An image is one type of steganographic, where the secret image is hidden in a cover image based on some hiding algorithm. Form the state of the arte, many researchers use Least Significant Bits (LSB) to reduce the distortion of the stegano image [22]. The original image used

DOI : 10.5121/ijma.2017.9101

to hide image is called a cover image in steganography, and the image to hide is called a secret image [3].

The objective of steganography is hiding the data into the cover image such that the existence of data in the cover image is not seen to the human beings [4]. The figure 1.1 shows the process of hiding data.

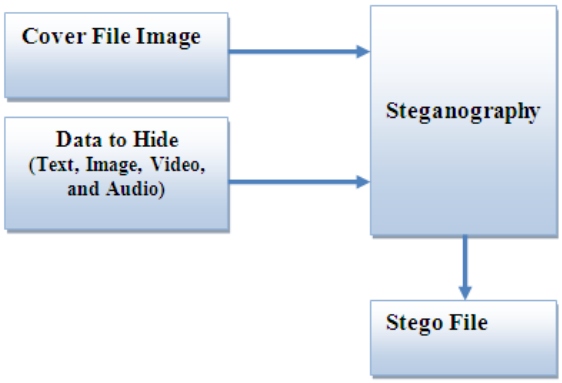


Figure1. The process of hiding data

Many techniques were proposed to implement steganography such as Spatial-Domain methods (LSB) where processing is applied directly on the pixel values of the image [22] and [23], Transform Domain Methods (DCT) and Discrete Wavelet Transform (DWT) technique pixel values are transformed and then processing is applied on the transformed coefficients, and Statistical Methods [24] (Syndrome Trellis codes).

2. DISCRETE COSINE TRANSFORM (DCT)

Discrete Cosine Transform (DCT) techniques are used in frequency domain. The DCT is a function that convert data from the spatial domain to the frequency domain. In DCT, after converting the image in frequency domain, the data is hidden in the least significant bits of the medium frequency components, secret messages are hidden in the high frequency coefficients resulted from Discrete Wavelet Transform and provide maximum robustness. In the Least Significant Bit (LSB), every pixel of an image is converting into the (1) or (0) and data is hidden into the least significant position of the binary value of the pixels of the image.

DCTs are important to numerous applications in science and engineering, from lossy compression of audio and images (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient (as described below, fewer functions are needed to approximate a typical signal), whereas for differential equations the cosines express a particular choice of boundary conditions.

The most common variant of discrete cosine transform is the simply DCT, in addition to the modified discrete cosine transforms (MDCT), which is based on a DCT of overlapping data. [6][7]. Multidimensional variants of the various DCT types follow straightforwardly from the one-dimensional definitions: they are simply a separable product (equivalently, a composition) of DCTs along each dimension. Figure 2 shows a Discrete Cosine Transform of an Image.

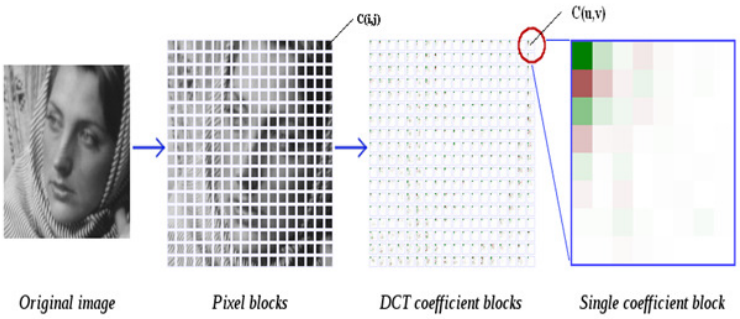


Figure 2 Discrete Cosines Transform of an Image.

$$C(u) = a(u) \sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u= 0, 1, 2….. N-1

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u,v) = a(v) \sum_{i=0}^{N-1} [\, a(u) \sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

where u, v = 0,1,2….N-1

Here, the input image is of size N X M. c (i, j) is the value of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix. DCT is used into steganography as [8]. Image is segment into 8×8 blocks or 4X4 block of pixels. Working from left to right, top to bottom, DCT is applied for each block. Each block is compressed through quantization table to scale the DCT coefficients and message is hidden in DCT coefficients. Figure 3 shows a two dimensional DCT frequencies from the RGB DCT image of 8 X8 pixels.

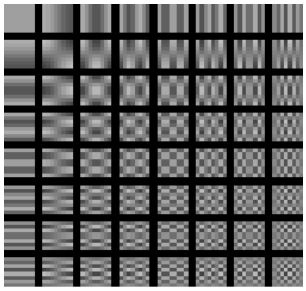


Figure 3 Two-dimensional DCT frequencies from the RGB DCT image based on 8 X8 pixels

3. SUPPORT VECTOR MACHINE

Support vector machines (SVM) also support vector networks [25] are supervised learning models with associated learning algorithms that analyses data used for classification and regression analysis. Based on training example set, each marked as belonging to one of two

categories, since SVM builds a model that assigns new examples to one category or to the other. In Linear SVM a training dataset of n points of the form as in the figure 4 below

$$(\vec{x}_1, y_1), \ldots, (\vec{x}_n, y_n)$$

where the y_i are either 1 or −1, each indicating the class to which the point $\vec{x}_i$ belongs. Each $\vec{x}_i$ is a p-dimensional real vector. We want to find the "maximum-margin hyperplane that divides the group of points $\vec{x}_i$ for which $y_i = 1$ from the group of points for which $y_i = -1$, which is defined so that the distance between the hyper-plane and the nearest point $\vec{x}_i$ from either group is maximized. Any hyperplane can be written as the set of points $\vec{x}$ satisfying $\vec{w} \cdot \vec{x} - b = 0,$

where $\vec{w}$ is the (not necessarily normalized) normal vector to the hyperplane. The parameter $\frac{b}{\|\vec{w}\|}$ determines the offset of the hyperplane from the origin along the normal vector $\vec{w}$.

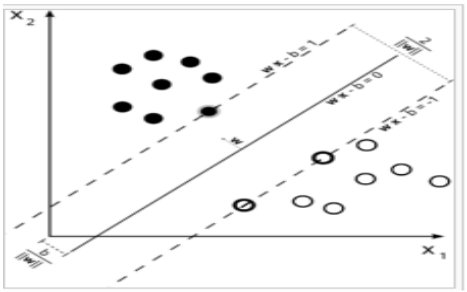


Figure 4 Linear SVM classifier

4. THE LITERATURE REVIEW

Many researches were done on Steganography because it is very important in computer multimedia fields, internet fields and in security systems. In addition, it is very important to know how much data can be concealed without image distortion. In literature, the techniques of steganography and its implementation were explained by J.R.Krenn in [1].

In [5], Chen Ming, et. al. focused on the steganography tools algorithms. Based on the analyses of the algorithms, various tools are divided into five categories: (1). Spatial domain based steganography tools; (2). Transform domain based steganography tools; (3). Document based steganography tools; (4) File structure based Steganography tools; (5) other categories, e.g. video compress encoding and spread spectrum technique based. Deshpande Neeta, et. al. [9], they proposed the Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits (LSB) of the cover image and the human eye would be unable to see the hidden data in the cover image. They explained the LSB embedding technique and presents the evaluation results for 2, 4, 6 (LSB) for a PNG images and a .bmp images.

In [10] K.B.Raja, et. al., they proposed a challenging task of transferring the hidden data to the cover without being detected. In addition, they used compression techniques on raw images to

enhance the security of the payload. Vijay Kumar Sharma, et. al. [11] the proposed a new steganography algorithm based on 8bit gray scale or 24bit color image, they used the logical operation to ensure the security against the steganalysis attack. Other researchers in [12] they proposed a new steganography technique based on different users demands on hiding capacity and image quality, they embeds the secret messages in frequency domain the proposed algorithm was divided into two modes and 5 cases. Aneesh Jain, et. al. [13] they were hide the data in a bitmap images with almost no perceptible difference between the original image and the result image. Others in [14] they discussed a survey of general steganography techniques and they proposed a novel technique to hide data in a colorful image using least significant bit. Hassan Mathkour,et. al. in [15] they analyzed and evaluated the strengths and weaknesses of the presented steganography techniques. In addition, they proposed a robust steganography technique that takes the advantages of the strengths and avoids the limitations of the studied techniques. Finally, in [17] MamtaJuneja, et. al. they proposed a Robust image steganography technique based on LSB and the RSA encryption technique.

5. THE PROPOSED APPROACH

In this paper we use the SVM classifier for training DCT Appling the linear SVM algorithm. DCT2 is used as shown in the equation 1.

Equation (1) DCT2 algorithm.

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

for u,v = 0,1,2,...,N −1 and α(u) and α(v)

$$\alpha(u) = \sqrt{\frac{1}{N}} \quad \text{for u} = 0$$

$$\sqrt{\frac{2}{N}} \quad \text{for u} \neq 0$$

5.1 DCT FEATURES EXTRACTION AND SVM TRAINING PROCESS FOR THE ORIGINAL AND COVER IMAGES ALGORITHM.

The proposed system has been designed to hide the secret message in the cover image, the following algorithm shows the process of hidden a message:

The proposed algorithm 1 and methodology is shown in figure 5 and in our algorithm we use the following steps:

Algorithm 1:

1- Read cover image and resize to 256 *256
2- Read secret image and resize to 64*64
3- Reshape image to a vector
4- Segment the cover image and secret image into 8×8 blocks
5- Apply DCT in every 8*8 block.
6- Learning process using the DCT feature based on linear SVM
7- Get the DCT of each DCT coefficient and replace with each bit of secret message.
8- Calculate the PSNR between the cover and stego image.

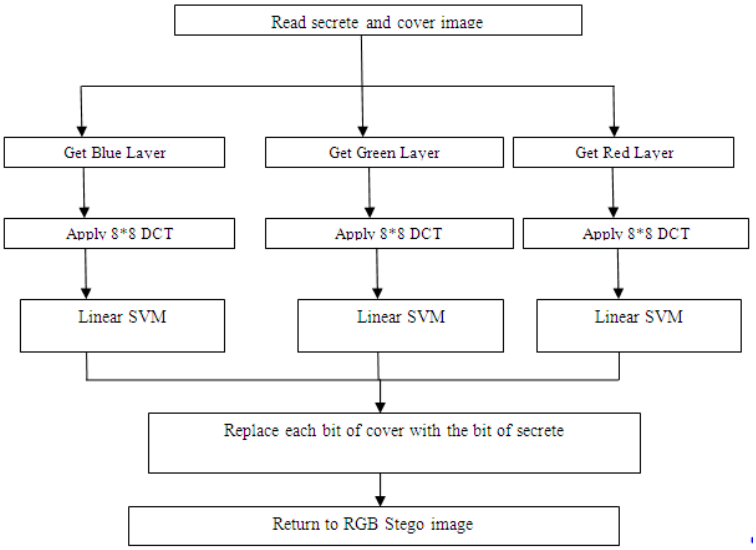


Figure 5 the proposed algorithm and methodology

The proposed algorithm and methodology are tested and the results are shown the following figures. Figure 6 shows the cover original image with size 256 *256 which used to hide the message. Figure 7 shows the original message that used to hide in the cover image of size of 64* 64. Figure 8 shows the stego image after hiding the secrete in the cover image.

Figure 6 Original cover image size 256*256

+

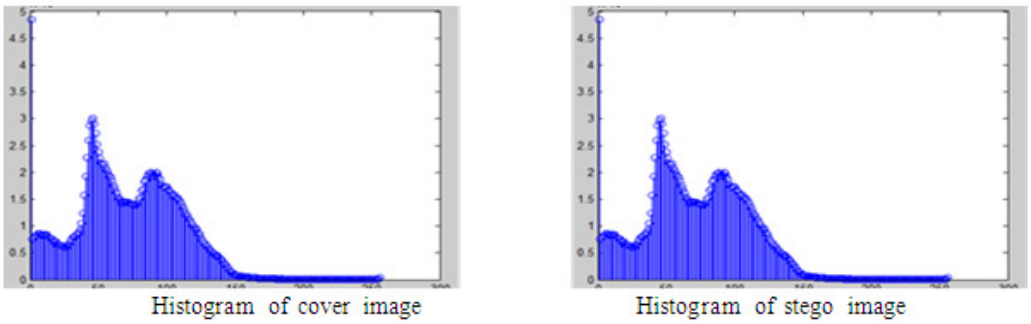
Figure 7 Original secret Image size 64*64

Figure 8 Stego image size 256*256

The proposed algorithm is implemented and tested and shows a significant results. To show the algorithm accuracy and performance many comparisons is done. The PSNR comparison is PSNR 44.3058 dB and the histogram between the original and stego images as shown in figure 9 and figure 10.

Original image Stego image

Figure 9 PSNR 44.3058 dB between original and stego



Histogram of cover image Histogram of stego image

Figure 10 Histogram of cover image and stego image

5.2 IDCT Features Extraction And SVM Training Process For The Stego Image Algorithm.

The next step of the proposed algorithm is to extracting the secret image from the stego image as shown in Algorithm 2 and in the methodology in figure 11.

Algorithm 2:

1- Get the stego image.
2- Segment Stego image to 8×8
3- Apply IDCT in every 8*8 block
4- Apply linear SVM classification
5- Reshape each 8*8 block bit into vector then message

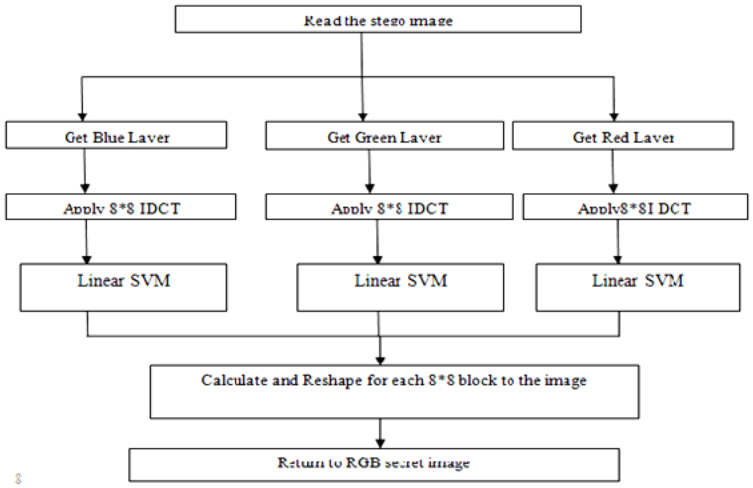


Figure 10 the proposed algorithm to regenerate the secret image from the stego image

6. System Implementation

This system was implemented using Matlab programming language over a PC Core i7 CPU with 8 GB RAM on Windows 7 Operating System. Many other applications were running such as anti-virus application which may be effect the performance rate. The proposed system is tested for many images width different sizes and different resolutions, and it shows significant results based on DCT and SVM classifier. The proposed algorithm was tested for processes; the process of hiding the secret message in the cover image and the process of retrieving the secret image from the stego image and show good results.

The proposed system is implemented and tested using many images width different sizes and different resolutions, and it shows significant results using the proposed three layer DCT methods and SVM classifier.

Many experiments were done using the proposed algorithm and the results are analyzed and reported. Table 1 shows the comparisons of PSNR between cover image and stego image. In addition table 2 shows the comparisons of PSNR between secret and message image.

Table 1 Result of PSNR between cover and stego image

Cover image	Stego image	PSNR
Cover1.jpg	stego1.jpg	40.4571
Cover2.jpg	Stego2.jpg	41.3426
Cover3.jpg	Stego3.jpg	42.1507

Table 2 Result of PSNR between secret and message image

Secret image	Message image	PSNR
secret1.jpg	message1.jpg	43.9358
Secret2.jpg	Message2.jpg	37.2983
Secret3.jpg	Message3.jpg	39.3217

The tables 1 and 2 show a significant improvement results based on the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of the two compared images.

7. CONCLUSIONS

The proposed approach shows significant results based DCT features and the using of fast linear SVM classifier that used in both processes (hiding and retrieving). Moreover, the using of the three layer of a color image based on RGB over DCT features add significant improves in the performance and the accuracy. The future work may be done by using other classifier and other features and compare the results.

REFERENCES

[1] J.R. Krenn, “Steganography and Steganalysis”, January 2004.
[2] BeenishMehboob and Rashid Aziz Faruqui, “A Steganography Implementation”, IEEE -4244-2427-6/08/ 2008.
[3] M. M. Amin, M. Salleh, S. Ibrahim, M.R.Katmin, M.Z.I. Shamsuddin, “Information Hiding using Steganography” Proceedings of 4th National Conference on Telecommunication Technology, Shah Alam, Malaysia, 2003.
[4] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, “Authentication of Secret Information in Image Steganography”.
[5] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian, “Analysis of Current Steganography Tools: Classifications & Features” , International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06),IEEE- 0-7695-2745-0/06 2006.
[6] Ahmed, N.; Natarajan, T.; Rao, K. R. (January 1974), "Discrete Cosine Transform", IEEE Transactions on Computers C–23 (1): 90–93, doi:10.1109/T-C.1974.223784.
[7] Rao, K; Yip, P (1990), Discrete Cosine Transform: Algorithms, Advantages, Applications, Boston: Academic Press, ISBN 0-12-580203-X
[8] NageswaraRaoThota, Srinivasa Kumar Devireddy, “Image Compression Using Discrete Cosine Transform”, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.

[9] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.
[10] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE-0-7803-9588-3/05 2005.
[11] Vijay KumarSharma, Vishalshrivastava, "A Steganography Algorithm for Hiding Images by improved LSB substitution by minize detection."Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645, 15th February 2012.
[12] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography",International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.
[13] AneeshJain,IndranilSen. Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images",IEEE-1-4244-1272-2/07 2007.
[14] BeenishMehboob and Rashid Aziz Faruqui, "A Steganography Implementation", IEEE -4244-2427-6/08 2008.
[15] Hassan Mathkour, Batool Al-Sadoon, AmeurTouir, "A New Image Steganography Technique",IEEE-978-1-4244-2108-4/08 2008.
[16] NageswaraRaoThota, Srinivasa Kumar Devireddy, "Image Compression Using Discrete Cosine Transform", Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008.
[17] MamtaJuneja,Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, 2009.
[18] Vijay Kumar, Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography" ,IEEE- 978-1-4244-4791-6/10 2010.
[19] Ali Al-Ataby and Fawzi Al-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" The International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.
[20] T. Narasimmalou, Allen Joseph .R, "Optimized Discrete Wavelet Transform based Steganography" , IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT),2012.
[21] NedaRaftari and Amir MasoudEftekhariMoghadam, "Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT", Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.
[22] S. M. Mohadeseh, N. Hossein, "The pair-wise LSB matching steganography with a discrete quantum behaved Gravitational Search Algorithm", Journal of Intelligent & Fuzzy Systems, vol. 30, no. 3, pp. 1547-1556, 2016.
[23] Mamta Juneja and Parvinder Singh Sandhu, "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424, (2013) .
[24] Tomas Filler, Student Member, IEEE, Jan Judas and Jessica Fridrich, Member, IEEE, (2010) "Minimizing Additive Distortion in Steganography using Syndrome Trellis Codes", IEEE Article, pp.1-17.
[25] Cortes, C.; Vapnik, V. "Support-vector networks". Machine Learning. 20 (3): 273–297. doi:10.1007/BF00994018, (1995).