Al-Qadisiya Journal For Engineering Sciences, Vol. 5, No. 3, 224-234, Year 2012

SECRET MESSAGE ENCODED BY EBCDIC IN MULTIPLE DCT FOR TWO COVERS

Ahmed Hassan Hadi
Technical College of Najaf

ABSTRACT
This paper suggest a proposed algorithm to hide message encoded using "**EBCDIC**" in multiform DCT's coefficients for two images. The DCT has the property that, for a typical image, most of the visually significant information about the image is concentrated in just a few coefficients of the DCT. Notice that most of the energy is in the upper left corner. Hiding message can be obtained without use original image with high quality. The experiments for embedding and extracting was successfully simulated by MATLAB.

KEYWORDS: Steganalysis, Steganography, EBCDIC, DCT, Data Hiding

الرسالة السرية المشفرة برمز التبادل العشري الثنائي الموسع مخفية في معاملات تحويلة الجيب تمام المميزة متعددة الشكل لغطاءين

أحمد حسن هادي
الكلية التقنية / النجف

الموجز
تم في هذا البحث اقتراح خوارزمية لإخفاء رسالة هامة مشفرة بشفرة **"EBCDIC"** مخفية داخل معاملات تحويلة الجيب تمام المميزة (DCT) للصورتين. تم الاستفادة من تحويلة الجيب تمام المميزة(DCT) للصورة المثالية بان اغلب المعلومات الهامة المرئية حول الصورة مركزة في بضعة من معاملات ال (DCT) وان اغلب الطاقة في الزاوية اليسرى العليا . علماً ان الرسالة المخفية يمكن ان تنتزع بدون استعمال الصور الأصلية وبدقة عالية النوعية. التجارب تمت بنجاح لإخفاء واستخلاص الرسالة وتمت المحاكة باستخدام برنامج (MATLAB).

INTRODUCTION
Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. (**Cheddad, et al, 2010**).
In the literature, many techniques about data hiding have been proposed (**Bender, et al, 1996**), (**Chen, et al,1998**), (**Marvel, et al, 1999**) and (**Chung, et al, 2001**). One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity.
(**Wang, et al, 2000**) proposed to embed secret messages in the moderately significant bit of the cover-image. A genetic algorithm is developed to find an optimal substitution matrix for the embedding of the secret messages. They also proposed to use a local pixel adjustment process (LPAP) to improve the image quality of the stego-image.

(**Matsui, et al, 1994**) embedded information in dithered images by manipulating the dithering patterns and in fax images by manipulating the run-lengths. (**Maxemchuk, et al, 1997**) changed line spacing and character spacing to embed information in textual images for bulk electronic publications. These approaches cannot be easily extended to other binary images and the amount of data that can be hidden is limited. (**Bhattacharjya, et al, 1999**) marking a binary document is proposed by treating a binary image as a grayscale one and manipulating the luminance of dark pixels slightly so that the change is imperceptible to human eyes yet detectable by scanners.
(**Zhang X., 2011**) proposes a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be successfully extracted and the original image can be perfectly recovered.
(**Pavan, et al, 2005**) proposed a hybrid image registration algorithm to identify the spatial or intensity variations between two color images. The proposed approach extracts salient descriptors from the two images using a multivariate entropy-based detector. The transformation parameters are obtained after establishing the correspondence between the salient descriptors of the two images.
(**Pang, et al, 2004**) introduced StegFD, a steganographic file driver that securely hides user-selected files in a file system so that, without the corresponding access keys, an attacker would not be able to deduce their existence. They proposed two schemes for implementing steganographic B-trees within a Steg FD volume.
In this paper, 8-bit grayscale images are selected as the cover media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images.

THE EXTENDED BINARY-CODED DECIMAL INTERCHANGE CODE

The Extended Binary-Coded Decimal Interchange Code (EBCDIC) contains 8 bits with no parity. The EBCDIC code is given in **Table 1**. It is used extensively in IBM computer systems. Let the secret message is **" Jackdaws love my big sphinx of quartz"**. and encode it by **EBCDIC** that is illustrated in **Table 2.**

THE ALGORITHM

The algorithm can be divided into two sections: Insertion algorithm and detection algorithm

Insertion Algorithm

Figure 1 represent the insertion algorithm as

1. Encode the message using EBCDIC for each letter.
2. Read two images:
   internal image with size (64×64) pixels, and external image with size(512×512) pixels.
3. Take (32 × 32) discrete cosine transform to hide message with unrecognizable effect of the internal cover image with size (64×64) pixels.
4. Take (2 × 2) discrete cosine transform to make high quality of the external cover image size (512×512) pixels.
5. Distribute each bit of EBCDIC message into coefficients of DCT for internal image (multiply "1 or 0 " according to bit by each last (4×4) coefficients).
6. Distribute DCT for internal image into DCT for external image by replace each last (8×8) coefficients.
7. Take (2 × 2) inverse discrete cosine transform for coefficient in step 6 to get stego-image.

Detection Algorithm

Figure 2 represent the detection algorithm as

1. Take (2 × 2) discrete cosine transform of stego-image.

2. State (8 × 8) coefficients of DCT of step1.
3. Take (32 ×32) inverse discrete cosine transform for coefficients stated in step 2 to get internal image.
4. Take (32 ×32) discrete cosine transform for internal image.
5. State (4×4) coefficients of DCT of step4.
6. any value assume '1' and any value approach to zero assume zero for coefficients stated in step 5 "i.e. value*exp(-10) ≈ zero ".
7. Decoded 1, 0 to letter using EBCDIC and get the secret message.

EXPERIMENTAL RESULTS:

This section presents experimental results obtained for two cover-image sets. The first set of cover-images consists of four standard grayscale images, (a), (b), (c), and (d) in **Figure 3**, each of 512 × 512 pixels (with height 50 % and width 50 %). The second set of cover-images consists of four standard grayscale images, (a), (b), (c), and (d) in **Figure 4**, each of 64 × 64 pixels (with height 100 % and width 100 %).

(Experiment 1, experiment 2, experiment 3, and experiment 4) described embedded the message encoded by using EBCDIC for each letter into (32 × 32) DCT coefficients of the internal set cover-images of size 64 × 64 pixels that distribute in (2 × 2) DCT coefficients of the external set cover-images of size 512 × 512 pixels as shown in **Figure 5**, than Take (2 × 2) inverse discrete cosine transform to get stego-image as shown in **Figure 6.** Detect the internal set cover-images of size 64 × 64 pixels as shown in **Figure 7.**

Table 4 shows the result for experiment 1, any value assume'1' and any value approach to zero assume zero for coefficients above to get secret message **" Jackdaws love my big sphinx of quartz".**

The Mean Square Error (MSE) and Peak Signal to Noise ratio PSNR shown in **equation 1,2** to determine the error between stego-images and original images

$$MSE = \frac{1}{M_c \; N_c} \sum \sum \left| I^{'} - I \right|^2 \qquad (1)$$

I : is the original image
$I^{'}$: is the stego-image
M_c: is the row size of image
N_c: is the column size of image

$$PSNR = 10 \;\; \log \frac{255^2}{MSE} \;\; dB \qquad (2)$$

Table 3 shows the values of RMSE's and PSNR's of stego-images that embed an image.

CONCLUSIONS

In this paper, data hiding technique is proposed able to embed massage encoded EBCDIC into a DCT's coefficients of (64×64) pixel grayscale image that embedded in DCT's coefficients of (512×512) pixel grayscale image while guaranteeing the high PSNR of the marked image versus the original image and low MSE. The hidden data can be extracted without using the original image, the secret message can be extracted efficiently, and unrecognizable effect on internal image due to embedding procedure

REFERENCES

Bender W., Morimoto N., Lu A., (1996), "Techniques for data hiding," IBM Syst. J. 35 (3/4) pp. 313–336.
Bhattacharjya A. K. and Ancin H., (1999), "Data embedding in text for a copier system," in Proc. IEEE ICIP'99, Vol. 2,Kobe, Japan, pp. 245–249.

Cheddad A., Condell J., Curran K., and Kevitt P., (2010), "Digital Image Steganography: Survey and Analysis of Current Methods", Elsevier Signal Processing, Vol. 90, issue 3, pp. 727-752.

Chen T.S., Chang C.C., Hwang M.S., (1998), "A virtual image cryptosystem based upon vector quantization," IEEE Trans. Image Process.Vol. 7, No. 10, pp. 1485–1488.

Chung K.L., Shen C.H., Chang L.C., (2001), "A novel SVD- and VQ-based image hiding scheme," Pattern Recognition Lett. 22(9), pp. 1051–1058.

Marvel L.M., Boncelet C.G., Retter C.T., (1999), "Spread spectrum image steganography," IEEE Trans. Image Process. Vol.8, No. 8, pp. 1075–1083.

Matsui K. and Tanaka K., (1994), "Video-steganography: how to secretly embed a signature in a picture," Proc. IMA Intellectual Property Project, Vol. 1, No. 1.

Maxemchuk N. F. and Low S., (1997), "Marking text documents," in Proc. IEEE ICIP'97.

Pang H. H., Tan K. L., and Zhou X., (2004), "Steganographic schemes for file system and B-tree," IEEE Transaction on Knowledge and Data Engineering, Vol. 16, No. 6, pp. 701-713.

Pavan S., Sridhar G., and Sridhar V., (2005), "Multivariate entropy detector based hybrid image registration," IEEE ICASSP, Vol. 2, pp. 873-876.

Wang R., Lin C., Lin J., (2000), "Hiding data in images by optimal moderately significant-bit replacement," IEE Electron. Lett. 36 (25) , pp.2069–2070.

Zhang X., (2011), "Reversible data hiding in encrypted image," IEEE Signal Processing Letters, Vol. 18, No. 4., pp. 255-258.

Table 1 The Extended Binary-Coded Decimal Interchange Code (EBCDIC)

Bit Position			4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
			3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
			2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
8	7	6	1 5	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	0	0																
0	0	0	1																
0	0	1	0																
0	0	1	1						Other Symbol										
0	1	0	0																
0	1	0	1																
0	1	1	0																
0	1	1	1																
1	0	0	0		a	b	c	d	e	f	g	h	i						
1	0	0	1		j	k	l	m	n	o	p	q	r						
1	0	1	0			s	t	u	v	w	x	y	z						
1	0	1	1																
1	1	0	0		A	B	C	D	E	F	G	H	I						
1	1	0	1		J	K	L	M	N	O	P	Q	R						
1	1	1	0			S	T	U	V	W	X	Y	Z						
1	1	1	1	0	1	2	3	4	5	6	7	8	9						

Table 2 Coding message by EBCDIC

Jackdaws love my big sphinx of quartz.																
	J	**a**	**c**	**k**	**d**	**a**	**w**	**s**	**l**	**o**	**v**	**e**	**m**	**y**	**b**	**i**
B1	1	1	1	0	0	1	0	0	1	0	1	1	0	0	0	1
B2	0	0	1	1	0	0	1	1	1	1	0	0	0	0	1	0
B3	0	0	0	0	1	0	1	0	0	1	1	1	1	0	0	0
B4	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
B5	1	0	0	1	0	0	0	0	1	1	0	0	1	0	0	0
B6	0	0	0	0	0	0	1	1	0	0	1	0	0	1	0	0
B7	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
B8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	g	**s**	**p**	**h**	**i**	**n**	**x**	**o**	**f**	**q**	**u**	**a**	**r**	**t**	**z**	
B1	1	0	1	0	1	1	1	0	0	0	0	1	1	1	1	
B2	1	1	1	0	0	0	1	1	1	0	0	0	0	1	0	
B3	1	0	1	0	0	1	1	1	1	0	1	0	0	0	0	
B4	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	
B5	0	0	1	0	0	1	0	1	0	1	0	0	1	0	0	
B6	0	1	0	0	0	0	1	0	0	0	1	0	0	1	1	
B7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
B8	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

Table 3 Values of RMSE's and PSNR's of stego-images that embed an image.

	$\sum\sum\left\|I^{'}-I\right\|^{2}$	**MSE**	**PSNR**
Exp.1	700.2949	2.6714×10^{-3}	73.8634
Exp.2	984.2254	3.7545×10^{-3}	72.3852
Exp.3	2.0443e+003	7.7983×10^{-3}	69.2108
Exp.4	684.7394	2.6120×10^{-3}	73.9610

Table 4 The result for experiment 1: Any value assume'1' and any value approach to zero assume zero for coefficients below to get secret message

J	a	c	k	d	a	w	s
0.7756	-0.2654	0.0800	0.0000	0.0000	-0.0910	-0.0000	0.0000
0.0000	-0.0000	0.3291	0.0754	0.0000	-0.0000	0.1681	0.0409
0.0000	0.0000	0.0000	-0.0000	-0.1337	0.0000	-0.0697	-0.0000
0.0000	0.0000	-0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
0.0823	0.0000	0.0000	0.1151	0.0000	-0.0000	-0.0000	0.0000
-0.0000	-0.0000	0.0000	-0.0000	0.0000	-0.0000	-0.0182	-0.0365
-0.0007	0.0000	0.0000	-0.0000	-0.0000	0.0000	0.0000	0.0000
0.0212	0.0651	0.0275	-0.0107	0.0113	0.0274	0.0075	0.0225

g	s	p	h	i	n	x	o
-0.4919	-0.0000	0.0434	-0.0000	0.1063	0.1009	-0.0488	0.0000
0.0190	0.0235	0.2756	-0.0000	0.0000	0.0000	0.0144	0.0143
0.2213	0.0000	0.0758	-0.0000	0.0000	0.0067	0.0674	-0.0477
0.0000	0.0000	-0.0000	0.1723	0.0110	-0.0000	0.0000	0.0000
0.0000	0.0000	0.0865	0.0000	0.0000	-0.0143	-0.0000	0.0045
-0.0000	-0.0621	0.0000	0.0000	-0.0000	-0.0000	0.0125	-0.0000
-0.0000	0.0000	0.0000	0.0000	-0.0000	0.0000	0.0000	-0.0000
-0.0353	0.0042	0.0054	-0.0125	-0.0112	-0.0063	-0.0087	0.0086

l	o	v	e	m	y	b	i
-0.1327	-0.0000	-0.1595	-0.0319	-0.0000	0.0000	0.0000	-0.0311
0.0312	-0.0727	0.0000	-0.0000	0.0000	-0.0000	-0.0498	0.0000
0.0000	0.1173	-0.0628	0.1778	-0.0055	0.0000	-0.0000	0.0000
-0.0000	-0.0000	0.0000	0.0000	0.0000	0.0003	0.0000	-0.0205
0.0169	-0.0868	0.0000	0.0000	0.0032	0.0000	0.0000	0.0000
0.0000	-0.0000	0.0302	0.0000	0.0000	0.0021	-0.0000	0.0000
0.0000	-0.0000	-0.0000	0.0000	-0.0000	0.0000	0.0000	-0.0000
0.0276	0.1380	-0.0653	-0.0743	-0.0174	-0.0367	-0.0077	0.0215

f	q	u	a	r	t	z
0.0000	0.0000	-0.0000	-0.0721	-0.0466	0.0424	-0.0172
-0.3752	0.0000	-0.0000	-0.0000	-0.0000	-0.0201	0.0000
-0.0172	0.0000	0.0123	-0.0000	0.0000	0.0000	0.0000
0.0000	0.0057	-0.0000	-0.0000	-0.0620	-0.0000	-0.0022
-0.0000	-0.0752	-0.0000	-0.0000	-0.0084	-0.0000	0.0000
-0.0000	-0.0000	0.0167	0.0000	-0.0000	0.0162	0.0110
0.0000	-0.0000	-0.0000	-0.0000	-0.0000	0.0000	0.0000
0.0109	0.0181	0.0227	-0.0072	0.0126	0.0088	-0.0177

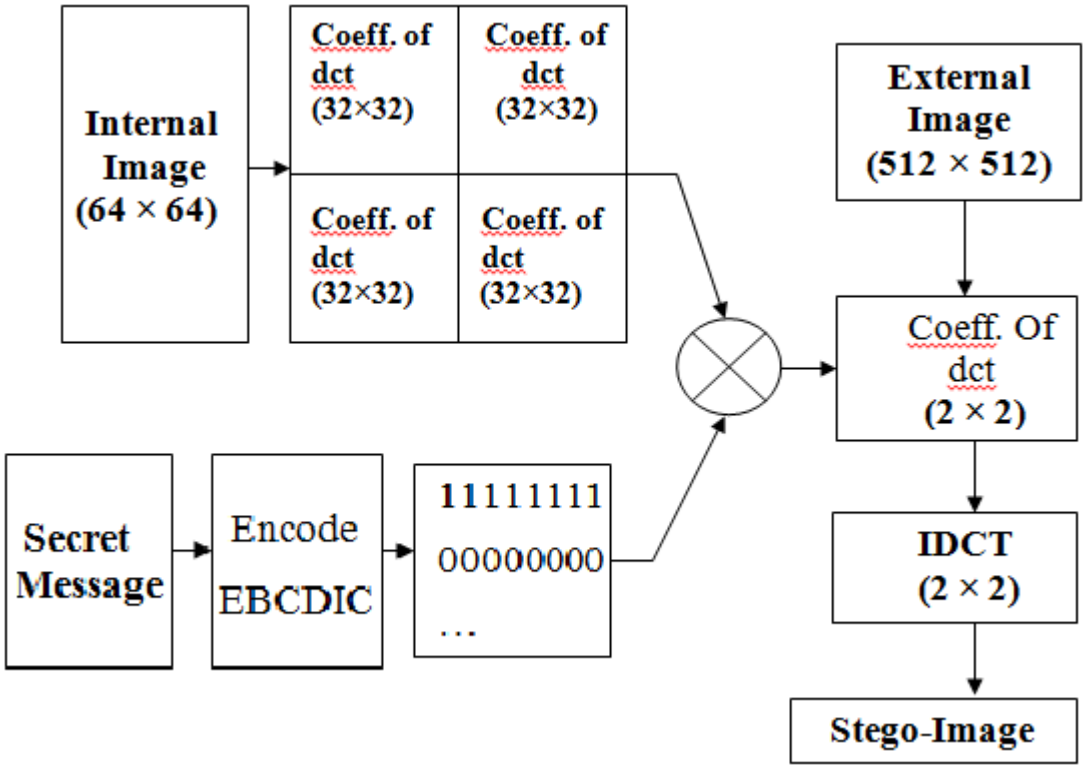


Figure 1 block diagram represent the insertion algorithm

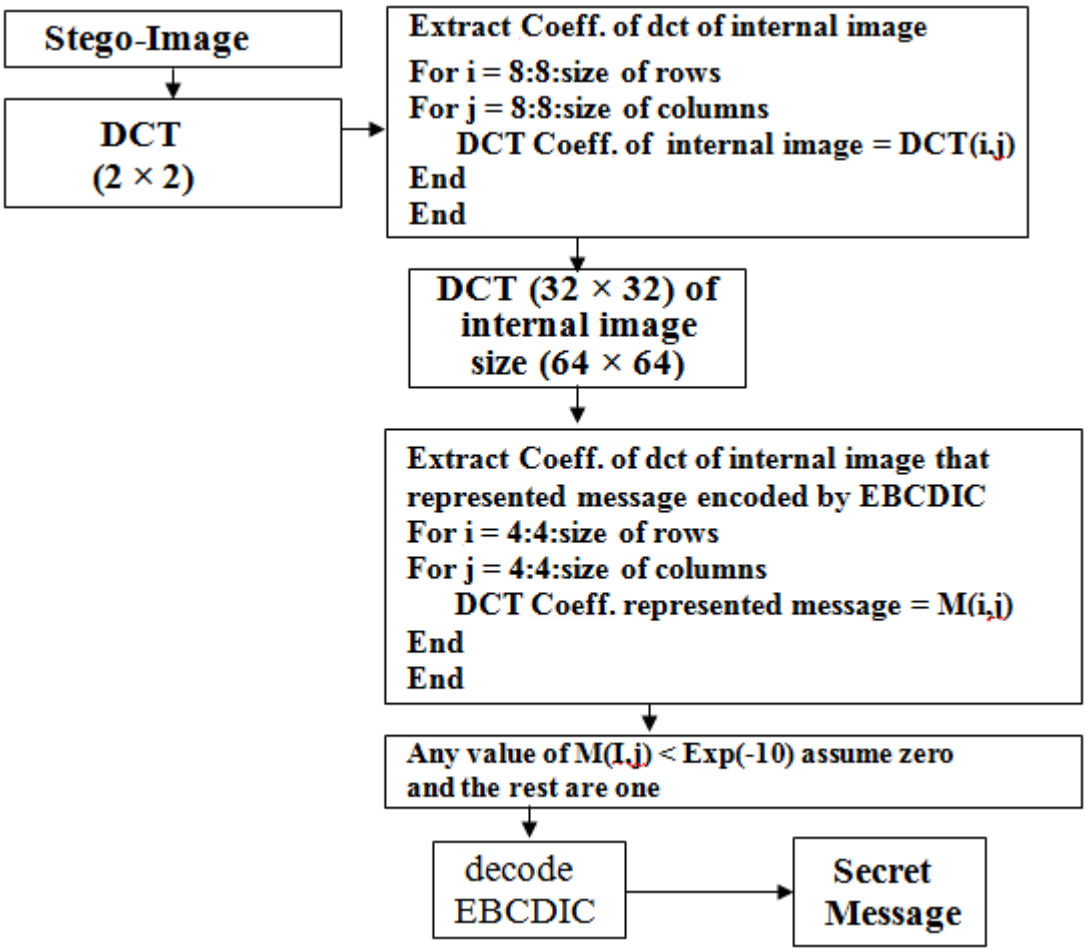
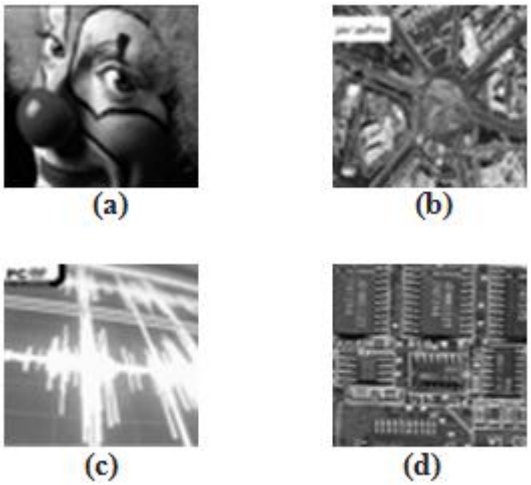


Figure 2 block diagram represent the detection algorithm

(a) (b) (c) (d)

Figure 3 The external set cover-images of size 512 × 512 pixels (with height 50 % and width 50 %).



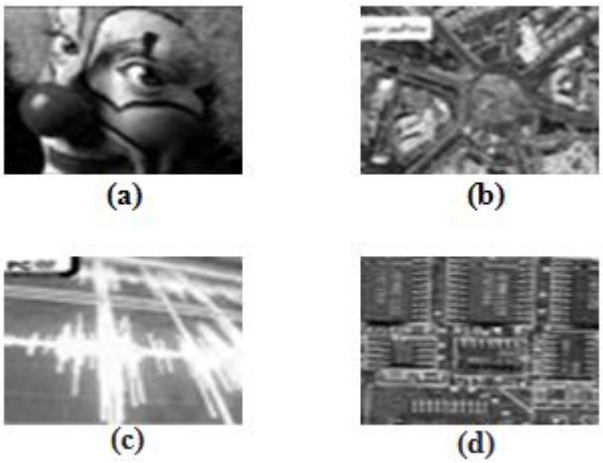
(a) (b) (c) (d)

Figure 4 The internal set cover-images of size 64 × 64 pixels (with height 100 % and width 100 %).

Figure 5 (2 × 2) DCT coefficients of the external set cover-images of size 512 × 512 pixels including (32 × 32) DCT of the internal set cover-images of size 64 × 64 pixels that embedded the message encoded by using EBCDIC for each letter.

(a) (b) (c) (d)

Figure 6 Stego-images obtained of size (with height 50 % and width 50 %).



(a) (b) (c) (d)

Figure 7 Detect the internal set cover-images of size 64 × 64 pixels (with height 100 % and width 100 %).