Contents lists available at ScienceDirect

Ain Shams Engineering Journal

journal homepage: www.sciencedirect.com

Electrical Engineering

Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3

Abdelhamid Awad Attaby [a,*], Mona F.M. Mursi Ahmed [b], Abdelwahab K. Alsammak [b]

[a] Electrical Department, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt
[b] Computer Department, Faculty of Engineering, Shoubra, Benha University, Cairo, Egypt

ARTICLE INFO

Article history:
Received 10 May 2016
Revised 8 August 2016
Accepted 16 February 2017
Available online 28 February 2017

Keywords:
Steganography
Steganalysis
Data hiding
LSB
DCT-M3

ABSTRACT

Information security relies mainly upon encryption, and in some cases, steganography for an extra layer of security. Steganography is the science and art of secret communication between two sides that attempts to conceal the existence of the message. Many steganographic techniques have been proposed, all of them make statistically noticeable changes in the properties of the cover carrier particularly when the message payload is high. In this paper, we propose a new methodology of transform domain JPEG image steganography technique that provides high embedding performance while introducing minimal changes in the cover carrier image. The algorithm, named DCT-M3, uses modulus 3 of the difference between two DCT coefficients to embed two bits of the compressed form of the secret message. The proposed algorithm reduces significantly the number of changes in the cover image; the embedding capacity has been improved by 16.7% approximately while maintaining minimum detectability against blind steganalysis schemes.

1. Introduction

Today the growth in the information technology, especially networks such as mobile communication, Internet and digital multimedia applications has opened new opportunities for steganography and information hiding techniques. Steganography is a method of hiding secret messages into an innocent-looking cover media known as stegogramme such that an unintended observer will not be aware of the existence of the hidden messages. With steganographic techniques, it is possible to hide information within images, audio, video files or text which is perceptually and statistically undetectable. Digital image are the most popular cover media due to their high degree of redundancy [1,2]. In video steganography, the same method may be used to embed a message in each of the video frames [3,4]. Audio steganography embeds the message into a cover audio file as noise at a frequency out of human hearing range [5]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [6]. When comparing steganography with cryptography we find that steganography conceals the existence of the secret message [7], but cryptography attempts to conceal the content of the secret message. On the other hand steganalysis concerns with identifying stegogrammes that contain a secret message. Steganalysis does not however consider the successful extraction of the message which is usually a requirement for cryptanalysis. Steganalysis begins by identifying any artifacts that exist in the suspect file as a result of embedding a message. None of the steganographic techniques that are known today achieve perfect security [8], and this means that they all leave signs of embedding in the stegogramme. This gives the steganalyst a good chance to identify whether a secret message exists or not.

Another type of information hiding is digital watermarking [9], which is the process that embeds a watermark or label into a multimedia object.

In this paper we propose a new steganography technique for hiding messages with minimum delectability by steganalysis techniques. To achieve the intended goal, the secret message is subjected to two phases of compression before embedding: in the first phase, the message is compressed by removing the weak words and replacing some expressions with their commonly used abbreviations. In the second phase, the resultant compressed message is further compressed using the Huffman lossless compression technique. Finally, the compressed secret message is embedded into the cover image based on the modulus three of

[*] Corresponding author.
E-mail addresses: abdelhamid.attaby@feng.bu.edu.eg (A.A. Attaby), monmursi@yahoo.com (M.F.M. Mursi Ahmed), asammak@feng.bu.edu.eg (A.K. Alsammak).
Peer review under responsibility of Ain Shams University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.asej.2017.02.003
2090-4479/© 2017 Ain Shams University. Production and hosting by Elsevier B.V.

the difference between DCT coefficients of the cover image during JPEG compression process.

Most of the related steganographic techniques concentrate on the area in which the secret message will be hidden and neglect the way of hiding. As a result of this they use LSB as the technique of hiding which increases the manipulation percentage on the cover image. In this paper, we introduce a new hiding technique named DCT-M3 which is more efficient and have less manipulation on the cover images than standard LSB.

2. Steganographic techniques

Many research papers are introduced to survey the different image Steganography techniques used to hide information into images [10–14]. Steganographic techniques can be classified into three categories, spatial domain, frequency domain and other compression type techniques.

– Spatial domain techniques

The spatial domain techniques use the pixel gray levels and their color values directly for encoding the message bits. The mostly used spatial domain techniques are:

- Least Significant Bit (LSB)

One of the earliest stego-systems were those referred to as Least Significant Bit Substitution techniques, so called because of how the message data (m) is embedded within a cover image (c). LSB techniques can be classified into two different embedding schemes: sequential and random.

Sequential embedding often means that the algorithm starts at the first pixel of the cover image C0,0 and embeds the bits of the secret message data in order at the least significant bit of the pixel value until there is nothing left to embed [15–17].

Random embedding scatters the locations of the values that will be modified to contain the bits of the message data. The main reason for the random approach is to make things a little trickier for the steganalysts that are looking to determine whether the image is a stegogramme or not [18,19]. Manjula and Danti [20] introduced a hash based LSB insertion technique to embed a secret image into a color cover image. Another algorithm based on different size image segmentations (DSIS) and modified least significant bits (MLSB) is introduced by Al-Shatanawi and El. Emam [21]. The DSIS algorithm is used to generate set of non-uniform segments to embed a secret image randomly. Mondal and Pujari [22] presented a new image steganography scheme in which both the secret message and the cover image are divided into a number of small and equal sized segments. A new pseudo-random sequence generator function is used to generate a pseudo-random sequence to embed segments of secret message into the segments of the cover image.

- Bit Plane Complexity (BPC)

Zhang et al. [23] proposed a new spatial domain steganography technique which uses an image as the vessel data and embed secret messages in the bit-planes of the vessel. The cover image is divided into blocks and classified into information and noisy blocks, and then the secret data is hidden into noisy blocks because the naked eye can't observe noisy areas.

- Histogram-based data hiding

Wei Su et al. [24] proposed a novel reversible data hiding algorithm in which a reversible hiding scheme is proposed to utilize the histogram of the pixels of the cover image. The algorithm shifts the part of the histogram between the peak point and the minimum point to the right side to create a space for hiding secret data. In these histogram-based data hiding schemes, the maximal hiding capacity is dependent on the number of pixels in the peak point of the histogram.

- Pixel Value Differencing (PVD)

In which the cover image is segmented into non overlapping blocks of two consecutive pixels pi and pi + 1. After calculating the difference value di = pi – pi + 1, the data is embedded into these differences by adjusting the pixel values to the specific difference. Blocks with small difference value are located in flat areas and blocks with high difference value are located in the sharp edged areas. Thus, we can embed more data in edged areas than smoothed ones because of the properties of human vision. This idea is introduced by Wu and Tsai [25].

- Gray Level Modification data (GLM)

Potdar and Chang [26] proposed a new technique to hide data by changing the gray level values of the gray scale image pixels called Gray Level Modification technique. The scientific support of this technique is the mapping of binary data within the spatial domain of the image by modifying gray level values of the pixels. They showed how using the concept of odd and even numbered gray values can be used to map binary data. Modifying the gray level values by one unit would not change the image statistics to a great extent. It is a one-to-one mapping between the binary data and the selected pixels in an image and the complexity of the algorithm is of the order O(n).

– Frequency domain techniques

Hiding secret messages in the spatial domain can easily be extracted by unauthorized user and it can be detected by visual attacks. On the other hand hiding data in frequency domain of JPEG images has benefits of good invisibility, high security without loss of secret messages.

- Steganographic in the DCT domain

In which the image is converted into the DCT domain in 8 × 8 blocks such that the color values of the image pixels switch from pixel values to DCT coefficients. In order for the values to be presented as whole numbers, each 8 × 8 block is quantized according to a quantization table (normal or altered quantization table). Fig. 1 shows the JPEG process.

J-Steg [28] and JPHide [29] are the two basic JPEG steganographic methods that use LSB embedding technique. JSteg embeds the secret message sequentially into the cover image by replacing the LSBs of quantized DCT coefficients with the secret message bits. JPHide modifies the LSB and second least significant bit-plane. OutGuess [30] embeds the secret message by scattering the embedding locations over the entire image according to a PRNG (pseudorandom number generator) on image c derived using seed k. F5 is introduced by Westfeld [31] using the same technique in OutGuess but it embeds the secret message bits by decreasing the absolute value of the coefficient by one. Yet Another Steganographic Scheme (YASS) [32] divides an input image in spatial domain into blocks with a fixed large size known as the big blocks (or B-blocks). Then it selects an 8 × 8 embedding host block (or H-block) randomly with a secret key for performing DCT within each B-Block. Then it encodes the secret data by error correction codes. Finally, after performing the inverse DCT to the selected H-blocks, the whole image is compressed and distributed as a JPEG image.

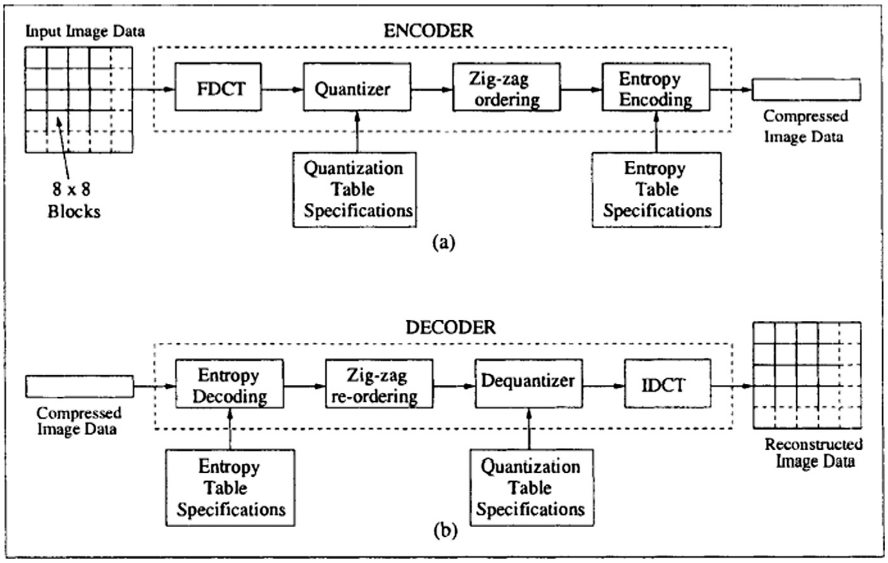

Fig. 1. JPEG compression process (a) compression, (b) decompression [27].

- Steganographic in the DWT domain

These techniques work exactly like the techniques that hide data in DCT coefficient but instead of hiding the secret messages into DCT coefficients, the Discrete Wavelet Transform or Discrete Fourier Transform is used as embedding regions as introduced in [33].

- Steganographic in the DFT domain

Naoum et al. [34] presents an enhanced image Steganography system based on discrete wavelet transformation and resilient Back-propagation neural network.

- Steganographic in the Contourlet domain

Sun and Guo [35] introduced a novel image steganography based on contourlet transform and hill cipher. The cover image is decomposed with contourlet transform and one of the subbands is selected to embed the secret data. Then hill cipher is applied to encrypt the secret message.

– Compression-based Hiding Techniques

A lot of non-traditional techniques have been proposed that are not using neither spatial domain of the pixel values nor the frequency domain, instead they use other regions of an image file to embed secret messages.

- Compression algorithm technique

Wang and Wang [36] proposed an algorithm in which the data-embedding is integrated with an image-compression algorithm of JPEG. For example, the steganographic tool Jpeg-Jsteg takes a loss-less cover-image and the message to be hidden to generate a JPEG Stego-image. In the coding process, DCT coefficients are rounded up or down according to individual bits to be embedded.

- Vector Quantization

Chang et al. [37] and Yang et al. [38] used the Vector Quantization indices to hide secret messages in which the secret data is embedded into the unused code space of compressing the image.

3. The proposed methodology DCT-M3

As more and more techniques of hiding information (Steganography) are developed, the methods of detecting the use of steganography (Steganalysis), also advance. Most steganography techniques change the properties of the cover source which increases the probability of detecting the changes. The proposed technique introduces a new algorithm for embedding the secret message by trying to minimize the changes in the cover image properties.

To minimize the changes in the cover work we introduced two ideas, the first one is compressing the secret message as long as possible by the current compression techniques, the second idea is using a new hiding technique DCT-M3 which uses the modulus 3 as a base factor for hiding not the traditional LSB technique which uses the modulus 2 as a base factor.

Fig. 2 shows a framework of the proposed DCT-M3 technique. It starts with the compression phase which compresses the secret message in three levels. Then the secret message is embedded into the cover image using DCT-M3 embedding algorithm; during the embedding phase. In the extraction phase, on the receiver side, the DCT-M3 extraction algorithm is used to extract the embedded message.

– Preparing the secret message

The message length is one of the factors affecting the degree of detecting the presence of hidden message. For this reason, we will try to shorten the input message as much as possible to minimize the number of modifications created by the embedding algorithm. The preparation process consists of three steps; the first step concerns with replacing the most commonly used phrases with shorter ones. The second step removes the weak words from the message in such a manner that doesn't affect the meaning of the input message. The third step compresses the output of the previous two steps using Huffman compression algorithm.

- Message Shortening

The most commonly used phrases are replaced with shorter ones by using a look up table prepared for this purpose. The entries of the table are collected from social media as well as the commonly used abbreviations. Table 1 shows a sample of the collected phrases along with their abbreviated form.

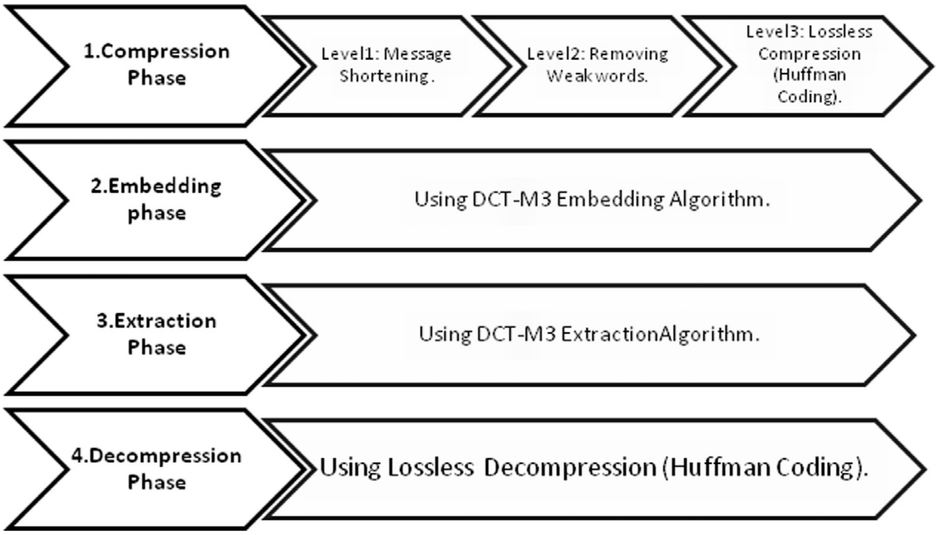
1.Compression Phase
Level1: Message Shortening.
Level2: Removing Weak words.
Level3: Lossless Compression (Huffman Coding).
2.Embedding phase
Using DCT-M3 Embedding Algorithm.
3.Extraction Phase
Using DCT-M3 ExtractionAlgorithm.
4.Decompression Phase
Using Lossless Decompression (Huffman Coding).

Fig. 2. A framework of the proposed algorithm.

- Removing weak words

English is a stress-time language which means that content words such as nouns and principal verbs are stressed, while structure words such as articles, helping verbs, etc are not stressed. In this step, the weak words such as (the, in, be, with, etc.) will be removed from the message.

Table 1
Samples of abbreviated phrases.

Abbreviation	Phrase	Abbreviation	Phrase
Anytng	Anything	Mob	Mobile
Asl	Age, sex, location	md	Managing director
2wimc	To whom it may concern	ldr	Long distance relationship
Atw	At the weekend	xlnt	Excellent
Ax	Across	Wassup	What's up

- Lossless compression (Huffman coding)

The resultant message from the previous steps is compressed using the lossless compression Huffman coding. We choose Huffman coding to compress the secret message as Huffman coding is an optimal prefix code and it is the most commonly used technique in entropy coding.

We used in our algorithm a fixed Huffman coding table based on the English language frequencies shown in Fig. 3 based on a sample of 40,000 words and the frequencies of letters.

– Embedding and extracting algorithms

The embedding algorithm has three inputs, a cover image, a seed K and the message generated from phase 1. The extracting algorithm has the stego-image and seed K as inputs and generates the secret message as output. Fig. 4 shows an overview of the proposed steganography system.

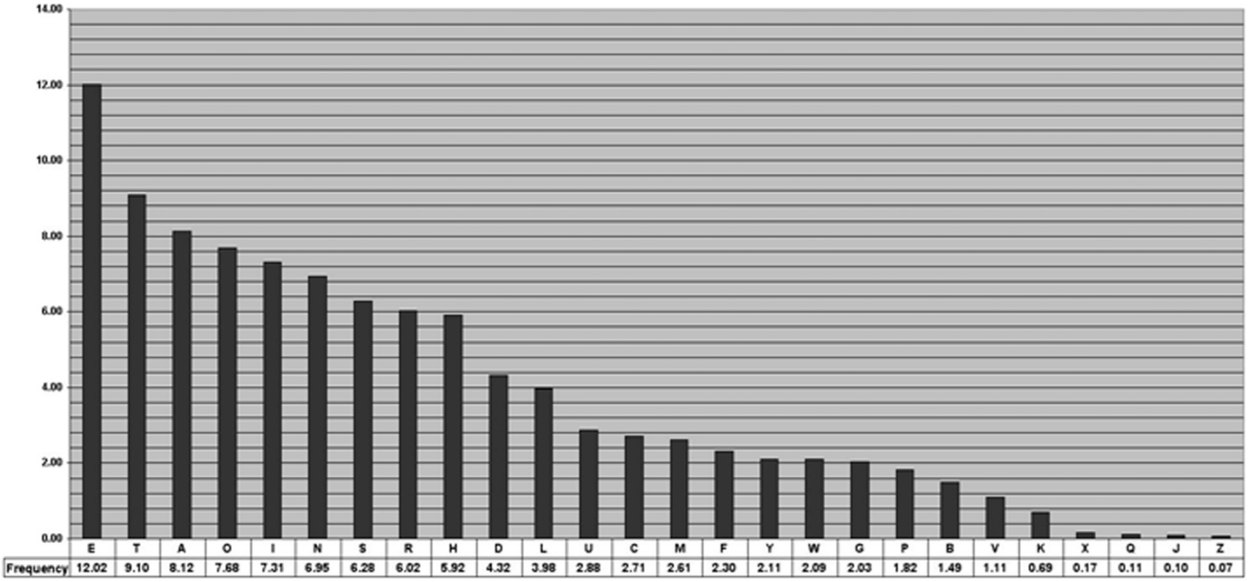

Fig. 3. The frequencies of the letters of English language [39].

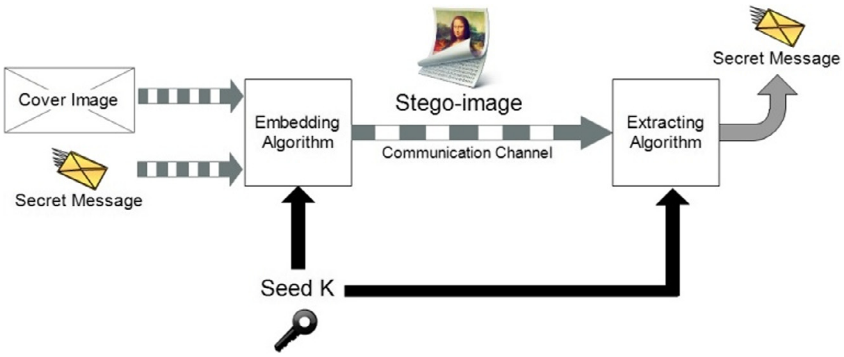

Fig. 4. An overview of the proposed steganography system.

Table 2
Embedding algorithm action table.

DCT coefficients difference% 3 =	First DCT coefficient	Sub-message bits	Action
Zero	Even	00	No change
		01	Add 1 to the first DCT coefficient or subtract 1 from the second DCT coefficient
		10	Subtract 1 from the first DCT coefficient or add 1 to the second DCT coefficient
		11	(Subtract 1 from the first DCT coefficient and subtract 1 from the second DCT coefficient) OR (add 1 to the first DCT coefficient and add 1 to the second DCT coefficient)
	Odd	00	(Subtract 1 from the first DCT coefficient and subtract 1 from the second DCT coefficient) OR (add 1 to the first DCT coefficient and add 1 to the second DCT coefficient)
		01	Add 1 to the first DCT coefficient or subtract 1 from the second DCT coefficient
		10	Subtract 1 from the first DCT coefficient or add 1 to the second DCT coefficient
		11	No change
One	Even	00	Add 1 to the second DCT coefficient
		01	No change
		10	Add 1 to the first DCT coefficient or subtract 1 from the second DCT coefficient
		11	Subtract 1 from the first DCT coefficient
	Odd	00	Subtract 1 from the first DCT coefficient
		01	No change
		10	Add 1 to the first DCT coefficient or subtract 1 from the second DCT coefficient
		11	Add 1 to the second DCT coefficient
Two	Even	00	Subtract 1 from the second DCT coefficient
		01	Subtract 1 from the first DCT coefficient or add 1 to the second DCT coefficient
		10	No change
		11	Add 1 to the first DCT coefficient
	Odd	00	Add 1 to the first DCT coefficient
		01	Subtract 1 from the first DCT coefficient or add 1 to the second DCT coefficient
		10	No change
		11	Subtract 1 from the second DCT coefficient

Table 3
Extracting algorithm table.

DCT coefficients difference % 3 =	First DCT coefficient	Sub message
Zero	Even	00
	Odd	11
One	Don't Care	01
Two	Don't Care	10

The embedding algorithm can be summarized as:

1. Get the binary representation of the whole secret message after removing the unnecessary words and compression (According to the preparing phase).
2. Split the binary representation into groups of two bits (Pairs).
3. Convert the RGB color layers of the cover image into three different components (Y, Cb and Cr).
4. Convert the image into transform domain by transforming the pixel data into $8 * 8$ block DCT coefficients.

Table 4
Dataset of secret messages.

No	Secret message	Message length
M1	Hence it is that is almost a definition of a gentleman to say he is one who never inflicts pain. This description is both refined…	646 Character
M2	The Road is one of the great fundamental institutions of mankind. Not only is the Road one of the great human institutions because it is fundamental to social existence, but also because…	840 Character
M3	Poetry is the language of the imagination and the passions. It relates to whatever gives immediate pleasure or pain to the human mind.	134 Character
M4	The first and most important principle to be observed in constructing a paragraph is that of UNITY. Just as each sentence…	509 Character
M5	The second principle of paragraph construction is Order – that is, logical sequence of thought or development of the subject…	291 Character

5. Generate randomized sequence with seed K using pseudo random method.
6. Choose a fixed place of two DCT coefficients which will be altered to embed the message (Avoid the DC component of each DCT coefficients block).
7. Within each block of 64 coefficients embed only two bits (Pair) as follows:
   - Compute the difference between non-overlapping pair of AC coefficients which are selected before.
   - Change DCT coefficients values based on the original values and the message bits according to Table 2.
8. Complete the embedding until the message bit stream is finished.
9. Restore original sequence of the DCT blocks using the seed K.
10. Quantize the image using a quantization table.
11. Re-order the values using Zig-Zag ordering.
12. Use Huffman lossless compression coding to compress the image.

The extracting algorithm can be summarized as:

Table 5
Dataset of cover images.

No.	Image name	Image	Image size
1	Lena.jpg		512 * 512
2	Baboon.jpg		512 * 512
3	Preppers.jpg		512 * 512

1. Convert the stego-image into transform domain by transforming the pixel data into 8 ∗ 8 block DCT coefficients.
2. Generate randomized sequence with seed K using pseudo random method.
3. Within each block of 64 coefficients extract two bits (Pair) according to Table 3.
4. Concatenate the extracted sub message pairs to get a stream of bits.
5. Uncompressing the stream of bits to get the original message.

4. Experimental results and discussion

Several experiments are carried out to evaluate the efficiency of the proposed algorithm. The following subsections describe the testing dataset, steganalysis tools, and evaluation measures used during the evaluation process.

– The dataset

The dataset used in our experiments consists of two parts; the first part contains five secret messages with different lengths, from 134 to 840 characters, as shown in Table 4. The second part of the dataset contains three standard test images with different levels of details, low, medium, and high, as shown in Table 5. These images are commonly used in image processing research area and will be used in our experiments as cover images in which the secret messages will be hidden.

– Steganalysis tools and experiments

Fifteen experiments will be carried out to evaluate the performance of the proposed algorithm compared to the most commonly used steganography technique LSB. Each experiment will embed one of the test messages into one of the cover images. These experiments are carried out using a steganalysis tool; Stegdetect. Table 6 summarizes the results of these experiments. The results show that the Stegdetect tool succeeded to detect the presence of hidden message in 10 experiments out of 15 using the LSB algorithm. While it failed to detect the presence of the hidden messages in any experiment using our DCT-M3 algorithm. These results are due to fact that the proposed algorithm is unknown for the current steganalysis tools. Also, the proposed DCT-M3 embeds the secret message with minimum changes in the cover image. The number of changes in DCT coefficients using the DCT-M3 algorithm is lower than that caused by the LSB algorithm. Table 7 summarizes the changing probabilities of DCT coefficients using LSB and DCT-M3 algorithms.

Table 6
Steganalysis testing results summary.

Cover image	Secret message	Embedding algorithm	Detection tool Stegdetect
Lena.jpg	M1	DCT-M3	FALSE
		LSB	TRUE
	M2	DCT-M3	FALSE
		LSB	FALSE
	M3	DCT-M3	FALSE
		LSB	FALSE
	M4	DCT-M3	FALSE
		LSB	TRUE
	M5	DCT-M3	FALSE
		LSB	TRUE
BabooFalse.jpg	M1	DCT-M3	FALSE
		LSB	TRUE
	M2	DCT-M3	FALSE
		LSB	TRUE
	M3	DCT-M3	FALSE
		LSB	TRUE
	M4	DCT-M3	FALSE
		LSB	FALSE
	M5	DCT-M3	FALSE
		LSB	FALSE
Preppers.jpg	M1	DCT-M3	FALSE
		LSB	TRUE
	M2	DCT-M3	FALSE
		LSB	TRUE
	M3	DCT-M3	FALSE
		LSB	FALSE
	M4	DCT-M3	FALSE
		LSB	TRUE
	M5	DCT-M3	FALSE
		LSB	TRUE

Table 7
Changing probabilities of DCT coefficients.

Steganography technique	Probability of changes in DCT coefficients		
	No changes	Change in 1 coefficient	Changes in 2 coefficients
LSB	25%	50%	25%
DCT-M3	25%	66.7%	8.3%

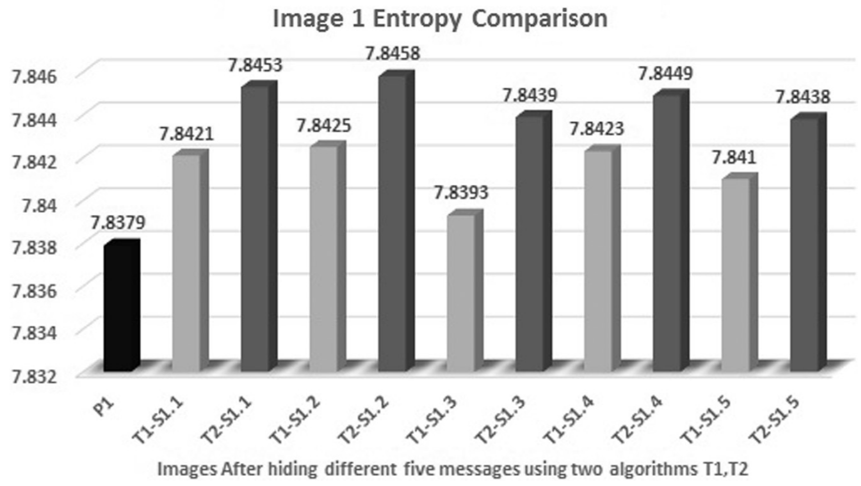

Fig. 5. Entropy comparison before and after hiding different messages using the proposed technique (T1) and LSB technique (T2) into lena.jpg image.

Table 8
MAE, MSE and SNR values of stego-images hidden using the proposed technique (T1) and LSB technique (T2) into lenga.jpg image.

	MAE	MSE	SNR
T1-S1.1	0.845340729	2.9324913	58418.29402
T2-S1.1	1.373382568	4.65518951	36800.03545
T1-S1.2	1.117469788	3.88476563	44098.19167
T2-S1.2	1.485157013	5.36602402	31925.15326
T1-S1.3	0.180862427	0.63803101	268499.7086
T2-S1.3	0.762817383	2.28845215	74858.95619
T1-S1.4	1.156082153	3.98982239	42937.0339
T2-S1.4	1.116016388	3.47024155	49365.76801
T1-S1.5	0.652404785	2.23894501	76514.22369
T2-S1.5	0.939044952	2.70823288	63255.68987

Table 9
MAE, MSE and SNR values of stego-images hidden using the proposed technique (T1) and LSB technique (T2) into baboon.jpg image.

	MAE	MSE	SNR
T1-S2.1	0.841804504	2.86935425	58338.10042
T2-S2.1	1.365066528	4.68689728	35715.02987
T1-S2.2	1.094421387	3.76851654	44418.71874
T2-S2.2	1.430622101	5.08929825	32891.11153
T1-S2.3	0.175003052	0.61193848	273544.944
T2-S2.3	0.755813599	2.2674408	73824.49702
T1-S2.4	1.371196747	4.8233757	34704.46563
T2-S2.4	1.095466614	3.40071106	49222.84585
T1-S2.5	0.768253326	2.7109108	61747.76258
T2-S2.5	0.955856323	2.76852417	60462.78306

Table 10
MAE, MSE and SNR values of stego-images hidden using the proposed technique (T1) and LSB technique (T2) into preppers.jpg image.

	MAE	MSE	SNR
T1-S3.1	0.846576691	2.92754745	53348.24444
T2-S3.1	1.318805695	4.47018814	34938.01879
T1-S3.2	1.097190857	3.78382874	41275.52492
T2-S3.2	1.454032898	5.23020172	29861.08865
T1-S3.3	0.178562164	0.62955093	248080.8285
T2-S3.3	0.765312195	2.29593658	68024.31666
T1-S3.4	1.366184235	4.81438065	32440.2096
T2-S3.4	1.287658691	4.18836212	37288.9241
T1-S3.5	0.77696228	2.73566437	57090.16029
T2-S3.5	0.957069397	2.76894379	56404.0043

– Evaluation measures

JPEG steganography adds another type of distortion to stego images in addition to that added by image compression. Therefore, many evaluation measures are used to measure the performance of the perceived stego image. Shannon's entropy is used to evaluate the randomness of stego-images and it is compared versus cover images to be used as an estimate of image steganography [40].

MAE (Mean Absolute Error), MSE (Mean Square Error), SNR (Signal to Noise Ration) and PSNR (Peak Signal to Noise Ratio) are used to evaluate the imperceptibility of stego-images and to measure the difference between cover images and stego-images.

- Shannon's Entropy

Shannon's entropy can measure the randomness of the data in an image. If bits are too disorderly steganography may be suspected. We used MATLAB built-in entropy function to evaluate the entropy of each image of the 30 stego-images stated in the previous section. The summary of entropy comparisons for the first image (lena.jpg) is shown in Fig. 5. The figure shows that the entropy of the image before hiding any secret message was 7.8379 (P1) then the entropy increased after hiding different secret messages into the image using two different techniques T1 (DCTM3) and T2 (LSB). It is clear that the first technique T1 always affect the image with less entropy than the second technique T2. For example, the entropy of the image S1 when hiding the secret message no 1 using the first technique T1 is 7.8421 while it reaches 7.8453 when hiding the same secret message into the same image but using the second technique T2. Overall, the proposed algorithm always produce stego-images with an entropy less than or equal to the entropy of stego-images produced by LSB technique which gives an indicator for less manipulations.

- MAE, MSE and SNR

We applied MAE (Mean Absolute Error), MSE (Mean Square Error) and SNR (Signal to Noise Ratio) to test images and compared the results of the proposed algorithm with LSB algorithm. Tables 8–10 show the results of MAE, MSE and SNR for lena.jpg, baboon.jpg and preppers.jpg respectively.

The results of Tables 8–10 show that the proposed algorithm produces better results than LSB technique in almost all stego-images. For example, the values of MAE and MSE of T1-S1.1 which indicates the difference between the original image S1 and the

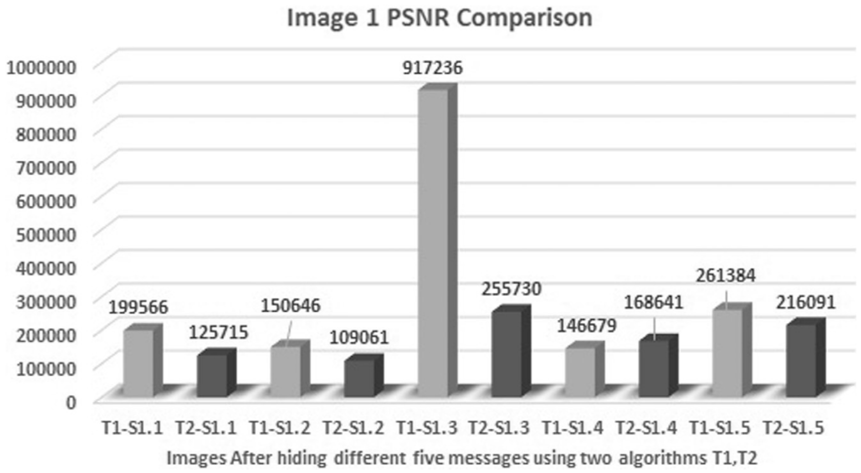

Fig. 6. PSNR comparison of stego-images after hiding different messages using the proposed technique (T1) and LSB technique (T2) into lena.jpg image.

stego-image after hiding the secret message no 1 using the first technique T1 are 0.8453 and 2.93249 respectively. When hiding the same message into the same image but using the second technique T2 (LSB), the values are 1.373 and 4.655. This indicates that much manipulations are performed on the image in the LSB technique. The previous results prove that the proposed algorithm is more efficient than LSB technique as it satisfies lower MAE & MSE and higher SNR.

- PSNR (Peak Signal to Noise Ratio)

The results of comparing PSNR of stego-images produced by the proposed algorithm and LSB technique is shown in Fig. 6 for lena.jpg image. For example, the value of PSNR of T1-S1.1 which indicates the ratio between the original image S1 and the stego image after hiding the secret message no 1 using the first technique T1 (DCT-M3) is 199566. When hiding the same message into the same image but using the second technique T2 (LSB), the value is 125715. This demonstrates that the LSB technique produces more changes on the image than that produced by the proposed technique. It proves that our proposed DCT-M3 algorithm gives higher values of PSNR than that of LSB algorithm.

5. Conclusion

The steganographic capacity and imperceptibility represent the most important aspects of any steganography technique. This paper proposes a novel steganography technique to enhance the stego image quality as well as increasing the steganographic capacity. The introduced method relies on minimizing the secret message as much as possible before embedding. Then the proposed algorithm DCT-M3 is applied to embed the shortened message based on the modulus three of the difference between DCT coefficients of the cover image during JPEG compression process. Fifteen experiments are carried out to evaluate the performance of the proposed algorithm. The results prove that the proposed algorithm reduces significantly the number of changes in the cover image while embedding messages with different lengths. On the basis of above analysis, we can conclude that the DCT-M3 algorithm gives better results compared to the most commonly used steganography LSB technique.

References

[1] Marvel Jr, Boncelet C, Retter C. Spread spectrum image steganography. IEEE Trans Image Process 1999;8:1075–83.

[2] Memon N, Chandramouli R. Analysis of lsb based image steganography techniques. In: Proceedings of IEEE ICIP; 2001.

[3] Morimoto N, Bender W, Gruhl D, Lu A. Techniques for data hiding. IBM Syst J 1996;35:313–6.

[4] Doerr G, Dugelay JL. Security pitfalls of frameby-frame approaches to video watermarking. IEEE Trans Signal Process Suppl Secure Media 2004;52:2955–64.

[5] Gopalan K. Audio steganography using bit modification. In: Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), vol. 2; 6–10 April 2003. p. 421–24.

[6] Davida G, Chapman M, Rennhard M. A practical and effective approach to large-scale automated linguistic steganography. In: Proceedings of the information security conference; October 2001. p. 156–65.

[7] Anderson R, Petitcolas F. On the limits of steganography. IEEE J Select Areas Commun (J-SAC), Special Issue on Copyright and Privacy Protection 1998;16:474–81.

[8] Cox I, Miller M, Bloom J, Fridrich J, Kalker T. Digital watermarking and steganography, 2nd ed. Morgan Kaufmann Publishers; 2007. ISBN: 978-0-12-372585-1.

[9] Mohanty S. Digital watermarking: a tutorial. Indian Institute of Science, Bangalore - 560 012; 1999.

[10] Kutade P, Bhalotra P. A survey on various approaches of image steganography. Int J Comput Appl 2015;109(3). January.

[11] Prajapati H, Chitaliya N. Secured and robust dual image steganography: a survey. Int J Innovative Res Comput Commun Eng January 2015;3(1).

[12] Kalaivanan S, Ananth V, Manikandan T. A survey on digital image steganography. Int J Emerg Trends Technol Comput Sci 2015;4(1). January-February.

[13] Hussain M, Hussain M. A survey of image steganography techniques. Int J Adv Sci Technol 2013;54(May).

[14] Shelke F, Dongre A, Soni P. Comparison of different techniques for Steganography in images. Int J Appl Innovation Eng Manage 2014;3(2). February.

[15] Celik MU, Sharma G, Tekalp AM, Saber. Reversible data hiding. In: Proceedings of IEEE international conference on image processing. Rochester, NY; 2002 p. 157–160.

[16] Ker AD. Steganalysis of embedding in two least-significant bits. IEEE Trans Inform Forensics Secur 2007;2(1):46–54.

[17] Li X, Yang B, Cheng DF, Zeng. A generalization of LSB matching. IEEE Signal Process Lett 2009;16(2):69–72.

[18] Yu Lifang, Yao Zhao, Ni Rongrong, Li Ting. Improved adaptive LSB steganography based on chaos and genetic algorithm. EURASIP J Adv Signal Process 2010;2010. doi: http://dx.doi.org/10.1155/2010/876946.

[19] Shreelekshmi R, Wilscy C, Madhavan V. Cover image preprocessing for more reliable LSB replacement steganography. In: Proc. of International Conf. on Signal Acquisition and Processing; 2010. p. 153–56.

[20] Manjula G, Danti Ajit. A novel hash based least significant bit (2-3-3) image teganography in spatial domain. Int J Secur Privacy Trust Manage (IJSPTM) 2015;4(1). February.

[21] Al-Shatanawi O, Emam N. A new image steganography algorithm based on mlsb method with random pixels selection. Int J Netw Secur Its Appl (IJNSA) 2015;7(2).

[22] Mondal A, Pujari S. A novel approach of image based steganography using pseudorandom sequence generator function and DCT coefficients. Int J Comput Netw Inform Secur 2015;3:42–9.

[23] Zhang H, Zhang X, Li-jun LI. A new BPCS steganography against statistical analysis. J. Hunan Univ. (Nat. Sci.) 2007;34(4):68–72.

[24] Ni Z, Shi YQ, Ansari. Reversible data hiding. IEEE Trans Circ Syst Video Technol 2006;16(3):354–61.

[25] Wu DC, Tsai WH. A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett. 2003;24:1613–26.

[26] V. Potdar, E. Chang, Gray level modification steganography for secret communication. In: IEEE International conference on industrial informatics INDIN. Berlin, Germany; 2004. p. 355–368

[27] Acharya T, Tsai P. JPEG2000 standard for image compression: concepts, algorithms and VLSI architectures.

[28] Derek Upham. Jsteg; 2008.

[29] Allan Latham. Jphide; 2008.

[30] https://packages.debian.org/sid/utils/outguess.

[31] Andrew Westfeld. F5-a steganographic algorithm: high capacity despite better steganalysis. In: Proceedings of the 4th information hiding workshop, LNCS, vol. 2137; 2001. p. 289–302.

[32] Sarkar A, Solanki K, Manjunath BS. Yass: Yet another steganographic scheme that resists blind steganal- ysis. In: Proceedings of the 9th information hiding workshop, vol. 4567 of LNCS. Sprinnger; 2007. p. 16–31

[33] Al-Ataby A, Al-Naima F. A modified high capacity image steganography technique based on wavelet transform. Int Arab J Inform Technol 2010;7:358–64.

[34] Naoum R, Shihab A, AlHamouz S. Enhanced image steganography system based on discrete wavelet transformation and resilient back-propagation. Int J Comput Sci Netw Secur 2015;15(1). January.

[35] Sun S, Guo Y. A Novel Image Steganography Based on Contourlet Transform and Hill Cipher. J Inform Hiding Multimedia Signal Process 2015;6(5). September.

[36] Wang S. Cyber warfare: steganography vs. steganalysis. Communications of the ACM; 2004. p. 76–82

[37] Chang CC, Thai SN, Lin. A reversible data hiding scheme for VQ indices using locally adaptive coding. J Visual Commun Image Represent 2011;22:664–72.

[38] Yang CH, Wu SC, Huang SC, Lin. Huffman-code strategies to improve MFCVQ-based reversible data hiding for VQ indexes. J Syst Softw 2011;84(3):388–96.

[39] http://www.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html.

[40] Franco S. Mathematics behind image compression; 2014.

Abdelhamid A. Attaby. Teaching Assistant in the Electrical Engineering Department, Faculty of Engineering (Shoubra), Benha University. He received his M.Sc. and BSc degrees from Faculty of Engineering (Shoubra), Benha University In 2015, and 2009 respectively. His research interests are in the areas of Computer networks, Computer Security, and Image Processing.

Mona F.M. Mursi. Professor Emeritus in the Electrical Engineering Department, Faculty of Engineering (Shoubra), Benha University. She received her Ph.D. and M.Sc. degrees from the University of Missouri, USA and the B. Sc. from Cairo University. In 1972, 1969, and 1965 respectively. She is ex-Head of the Electrical Engineering Department in Benha University as well as Professor and ex-Head of the Computer Applications Department, College of Computers and Information Science, King Saud University, Riyadh. She was also an Assistant Professor at the EE Department, Faculty of Engineering, Cairo University. She worked in industry in USA for several years in engineering design and technical management in the area of small to large scale computer systems and instrumentation. In Egypt she worked as computer consultant for computer companies. Her research interests are in the areas of Microprocessor design, Computer Architecture, and Computer Security.

Abdelwahab Alsammak, is an associate professor in the Electrical Engineering Department, Faculty of Engineering (Shoubra), Benha University. He is the head of Computer Systems Engineering program. He got his Ph. D., M.Sc. and B.Sc. from Zagazig University in 1992, 1987, 1982 respectively. He works also as the consultant of the Egyptian Universities Portal Project, Ministry of Higher Education, Egypt since 2012. His research interests include Artificial Intelligence, Natural Language Processing, Data Mining, and Software Engineering.