

## Research Article

### Hiding Two Binary Images in Grayscale BMP Image via Five Modulus Method

Firas A. Jassim

Department of Computer Information Systems, Irbid National University, Irbid 2600, Jordan

**Abstract:** The aim of this study is to hide two binary BMP images in a single BMP grayscale image. The widespread technique in image steganography is to hide one image (stego image) into another (cover image). The proposed novel method is to hide two binary images into one grayscale bitmap cover image. First of all, the proposed technique starts with transforming all grayscale cover image pixels into multiples of five using Five Modulus Method (FMM). Clearly, any modulus of five is either 0, 1, 2, 3, or 4. The transformed FMM cover image could be treated as a good host for carrying data. Obviously, it is known that the pixel value for the binary image is either 0 or 1. Therefore, by concatenating the two binary images, the composite results are 00, 01, 10 and 11. In fact, these concatenated values could be mapped using simple mapping that assigns a positive integer value such as 1 for 00, 2 for 01, 3 for 10 and 4 for 11. Consequently, a new matrix will be constructed that contains a number varying from 1 to 4 only. Fortunately, the four integer values are the same as the previously mentioned remainders of division by 5, hence, adding these four integers to the transformed FMM cover image. On the recipient side, a reverse process will be implemented to extract the two binary images. In terms of PSNR values, the cover image and the two extracted stego images have acceptable PSNR values, which yields that the proposed method is very efficient in information hiding.

**Keywords:** Binary image, cover image, information hiding, statistical steganography, steganography, stego image

## INTRODUCTION

In light of the energetic expansion of computer network and Internet security, there is a pressing demand to create better ways to protect the confidential information from adversaries. As a result, steganography was innovated as a safeguard for secret and personal information. In fact, steganography is a process of concealing confidential information into any kind of unquestionable host media, such as image, video and audio, which are called cover media (Artz, 2001). Linguistically, the derivation of the word steganography is from a combination of two Greek words. The first word, steganos, means “covered” and graphei means “writing” (Kahn, 1983). Hence, the correct translation of the word steganography is the “covered writing”. The essential process of steganography is to send a secret message such that the cognition of its existence cannot be noticed by any opponent (Provos and Honeyman, 2003).

Steganography and cryptography must be adequately distinguished because they are closely related. As a matter of fact, the basic difference between steganography and cryptography is that, the aim of cryptography is to keep the contents of the message secret. With cryptography, the opponent

knows that there is confidential information inside the cover media. Steganography, on the other hand, aims to preserve the secret existence of the confidential message (Wang and Wang, 2004). Thus, in steganography, the opponent does not perceive that confidential information exists. Occasionally, dispatching an encrypted message will agitate some suspicion, while keeping the secret message unseen will not attract any attention. Dual secrecy might be obtained by combining both steganography and cryptography in the same secret message. In fact, this will make it more difficult for the adversary to dig out the confidential or personal information from the cover media (Abboud *et al.*, 2010).

It is well understood that image steganography is the method of concealing a secret message into a cover image in such a way that only the receiver knows about its existence. Nowadays, digital images have become a commonly used as a cover medium for steganography techniques (Lyu and Farid, 2006). According to Katzenbeisser and Petitcolas (2000) there are multifarious image steganographic techniques. These techniques (categories) can be classified as follows:

- Spatial domain
- Transform domain

- Spread spectrum
- Statistical methods
- Distortion techniques

In spatial domain techniques, the confidential message is embedded into the cover image in a direct manner. Here, the most common and simplest steganographic method is the Least Significant Bits (LSB) method. The LSB technique is one of the most widespread methods for image steganography (Raja *et al.*, 2005). Technically, in the LSB technique, the least significant bits of the image pixels are replaced by the confidential message bits. The human eye cannot notice the confidential information within the cover image (Provos and Honeyman, 2003). Another type of steganographic category is the transform domain techniques. The transform domain steganography technique is used for concealing a large amount of data with high security, good invisibility and no loss of secret message in transforming coefficients of the cover images (Johnson and Jajodia, 1998). Transform domain methods hide messages in significant areas of the cover image, which makes them more robust to attacks. The most frequently implemented transformation methods are the Discrete Cosine Transformation (DCT) (Cox *et al.*, 1996), Discrete Wavelet Transform (DWT) (Xia *et al.*, 1997) and Discrete Fourier Transform (DFT) (Kieu and Chang, 2009). In spread spectrum steganographic techniques, the confidential message is diffused over a broader bandwidth than the minimum demanded bandwidth to send a confidential message. A general framework for spread spectrum steganography was discussed by Marvel *et al.* (1999). In accordance with statistical techniques, the cover image is divided into blocks and the secret message bits are hidden in each block. More precisely, this is done by altering the cover image in such a way that some statistical modifications are made (Katzenbeisser and Petitcolas, 2000).

Eventually, concerning distortion techniques, both the encoder and the decoder must agree on a predefined cover image to hide the secret image within it. The confidential information is stored by cover image distortion (Holub and Fridrich, 2013). In the sender part, the encoder adds some alteration to the cover image as a deformation, while on the recipient side, the decoder checks for the dissimilarities between the original cover image and the distorted cover image to extract the secret message.

### FIVE MODULUS METHOD

The Five Modulus Method (FMM) was first proposed by Jassim (2012). It originated as a method for image compression. Its advantage was to make all the neighbor pixels similar to each other, by decreasing the gap between pixels in the same block.

Subsequently, a more general impression was introduced by Jassim (2013c) as a method for image transformation, which was the k-Modulus Method, or k-MM. The k-MM was just a generalization of the FMM and could be implemented with any positive integer k such that  $k > 0$ . Depending on the required application or process, one can decide on the suitable value for k. Mathematically speaking, it is known that the modulus of any positive integer k is 0, 1, ..., k-1. Indeed, by any deep glance at the k-MM transformed pixels, one can easily notice the distinct pixels that are not multiples of k. After that, by taking their reminder of the division by k to extract the hidden information,



(a) Original Lena (b) FMM transform of Lena

(c) 10-MM transform of Lena

Fig. 1: k-modulus method for image transformation

the hidden information can be obtained in conformity with predefined process or protocol for both sides, which are the sender side and the receiver side.

Moreover, it must be mentioned that, the ocular dissimilarities between the transformed, either FMM or K-MM, are slightly unrecognizable by the human eye, (Fig. 1). According to Jassim (2013c), the visual differences are undetectable by simple eye matching. Therefore, if the transformed cover image was examined by any adversary, then there would be no suspicions at all. Further, the most common error metrics demonstrate that the mathematical differences between the cover and the transformed k-MM images are strongly acceptable when k is less than 10 (Jassim, 2013c).

The FMM operator could be represented as:

$$F[\Phi] = \hat{\Phi} \quad (1)$$

where,

$\Phi$  = The mathematical notation for the original grayscale bitmap image

F = The Five Modulus Method transform operator that can be implemented in accordance with algorithm 1. Lastly, the resulting FMM transform was represented as  $\hat{\Phi}$  :

Table 1: 5x5 random block transformation

Original image	97	104	98	108	104
	106	102	102	103	102
	108	112	101	102	100
	103	97	99	104	104
	104	96	100	103	100
5-MM transform	95	105	100	110	105
	105	100	100	105	100
	110	110	100	100	100
	105	95	100	105	105
	105	95	100	105	100
10-MM transform	100	110	100	110	110
	110	100	100	110	100
	110	110	100	100	100
	110	100	100	110	110
	110	100	100	110	100

**Algorithm 1: Five modulus method transformation:**

**Input:** Grayscale bitmap image ( $\Phi$ ) of size  $N \times M$

**Output:** Five modulus method transform ( $\hat{\Phi}$ ):

1. for  $i \leftarrow 1$  to  $N$  do
2.   for  $j \leftarrow 1$  to  $M$  do
3.     if  $\Phi(i, j) \bmod 5 = 4$  then
4.        $\hat{\Phi}(i, j) \leftarrow \Phi(i, j) + 1$
5.     else if  $\Phi(i, j) \bmod 5 = 3$  then
6.        $\hat{\Phi}(i, j) \leftarrow \Phi(i, j) + 2$
7.     else if  $\Phi(i, j) \bmod 5 = 2$  then
8.        $\hat{\Phi}(i, j) \leftarrow \Phi(i, j) - 2$
9.     else if  $\Phi(i, j) \bmod 5 = 1$  then
10.       $\hat{\Phi}(i, j) \leftarrow \Phi(i, j) - 1$

We now focus on a single iteration of the algorithm to show how the FMM and the 10-MM methods work. As it can be observed from Table 1, a 5x5 random block was chosen to make a simple comparison between the original and the transformed blocks. Clearly, the FMM transform more closely resembles the original block than the 10-MM transform. Thus, these small dissimilarities between original and FMM blocks are too small to affect the final cover image quality and consequently will not affect the Human Visual System (HVS).

As a result, the k-MM transformation is a new born method and needs a lot of research in terms of its efficiency and performance. Recently, it has been inoculated into some image processing fields. The embedding of FMM into JPEG compression technique has been discussed by Jassim (2013b).

Also, in accordance with Jassim (2013a), a novel steganography technique for hiding an image in another image via FMM has been explored. In addition, implementation of FMM to hide text within digital images can be found in Jassim (2013d). As a matter of fact, FMM or k-MM can be utilized as a good carrier for confidential information.

**PROPOSED TECHNIQUE**

**Binary image representation:** Binary images are images that are normally displayed as black and white

pixels only. Apparently, binary values have two possible intensity values: 0 for black and 1 for white (Gonzalez and Woods, 2008). In fact, binary images are often created by thresholding a grayscale or color image. The basic idea of thresholding is to separate the object from the background (Stockman and Shapiro, 2001). As a matter of fact, the main benefit of binary images is the small storage, since it stores one bit per pixel. Binary images are usually suitable for images containing simple graphics, text, or line art. Mathematically speaking, binary images are encoded as two-dimensional arrays and can be clarified by the following formula.

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes:

$$B(x, y) = \begin{cases} 0, & \text{for object} \\ 1, & \text{for Background} \end{cases}$$

**Proposed hiding algorithm:** Formerly, steganography techniques have been implemented in order to hide one stego image into another cover image. But less work has been done to conceal two stego images in one cover image that are of the same size, i.e., both the stego images and the cover image are of the same dimensions (Chakraborty and Bandyopadhyay, 2013). To begin, there must be an explanation for the reason for using grayscale bitmap images. The first reason is that, the bitmap images are extremely suitable for hosting k-MM image transformation (Jassim, 2013c). Indeed, the steady environment for the bitmap image in which it does not change its pixel values during transmission makes it appropriate to preserve FMM specific pixel values from any modification, alteration, or any other distortion process. The second reason is due to the lesser file size for the grayscale bitmap images compared with the color bitmap images. Actually, it is known that, bitmap images are the largest file size in all the commonly defined image formats. Hence, converting the original color bitmap image into a grayscale bitmap image will produce an image approximately one-third of the original file size. Subsequently, in this study, this is the reason of using a grayscale bitmap image. On the other hand stego images must be binary images that consist of black and white sketches.

The basic and simple concept for the proposed algorithm starts with concatenating the two black and white stego images together to create a new matrix. Honestly, the resulted matrix consists of dual combinations of zero and one, which are either 00, 01, 10, or 11. Now, a novel combination criterion has been created as a process of converting each dual combination of zero and one into a positive integer number mapping. This novel mapping can be examined

Table 2: Positive integer transformation for dual binary representation

Binary combination	Positive integer number
00	1
01	2
10	3
11	4

in Table 2. Thence, the newly resulted matrix consists of either 1, 2, 3, or 4 for each of its elements, called the stego matrix. Finally, the transformed FMM cover image and the resulting stego matrix will be added together to construct a new cover image that may be transmitted securely through the channel. On the recipient side, a completely reversed process will be exercised to extract the two stego images. The first thing that the recipient must do is to take the remainder of five for each pixel in the received cover image. Clearly, as stated previously, the resulted matrix pixel values will be either 1, 2, 3, or 4. In conformity with Table 2, a converse process can be easily accomplished to extract the two hidden stego images. Accordingly, the best category to describe the proposed approach is the statistical steganographic techniques.

The mathematical symbolic representation for the two binary images can be examined in the next two formulas:

$$I_1(x_{ij}) = \{x_{ij} : x_{ij} \in [0,1]\}$$

$$I_2(y_{ij}) = \{y_{ij} : y_{ij} \in [0,1]\}$$

for  $i = 0, 1, \dots, N; j = 0, 1, \dots, M$

Presently, we are ready to gather all the predefined facts and symbols in a definitive equation for the transmitted cover image through the channel:

$$\Phi' = \hat{\Phi} + C \tag{2}$$

where, C is the obtained matrix that resulted from the concatenation between the two binary images  $I_1$  and  $I_2$ , which can be expressed as:

$$C = (I_1 \parallel I_2)$$

or (in more details):

$$C(x, y) = \{x \parallel y : \forall x \in I_1, \forall y \in I_2\}$$

where,  $\parallel$  is the mathematical notation for the concatenation operator that was used in this study. As mentioned in section II, Eq. (1),  $\Phi$  is the mathematical representation for the original grayscale bitmap image that can be defined precisely as:

$$\Phi_{ij}(x) = \{x_{ij} : x_{ij} \in [0,255]\}$$

while the transformed image using FMM can be defined as:

$$\hat{\Phi}_{ij}(x) = \{x_{ij} : x_{ij} \in [0,255], x_{ij} \bmod 5 = 0\}$$

It must be stressed that all the images used in this novel steganographic algorithm are of the same dimensions, i.e., both the cover image and the two stego images are belong to the  $Z^{N \times M}$  space.

As described in Table 2, the proposed hiding operator can be plainly expressed as:

$$T[C(x, y)] = \begin{cases} 1, & \text{if } x = 0, y = 0 \\ 2, & \text{if } x = 0, y = 1 \\ 3, & \text{if } x = 1, y = 0 \\ 4, & \text{if } x = 1, y = 1 \end{cases} \tag{3}$$

where,  $x \in I_1$  and  $y \in I_2$ . However, for the sake of clearness, the whole proposed hiding algorithm can be examined in a step-by-step manner in algorithm 2.

Note that,  $\Phi'$  is the ultimate cover image that will be transmitted through the channel, having two confidential black and white images embedded within it. Graphically speaking, both the encoding process and the decoding process can be demonstrated as Fig. 2 and 3, respectively.

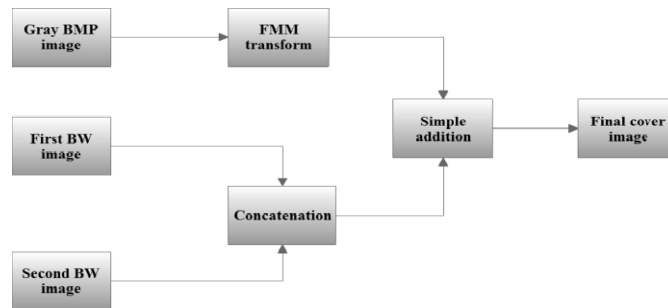


Fig. 2: Encoding of the proposed technique

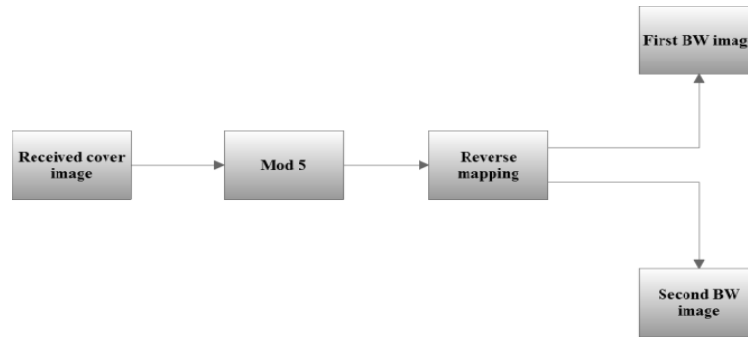


Fig. 3: Decoding of the proposed technique

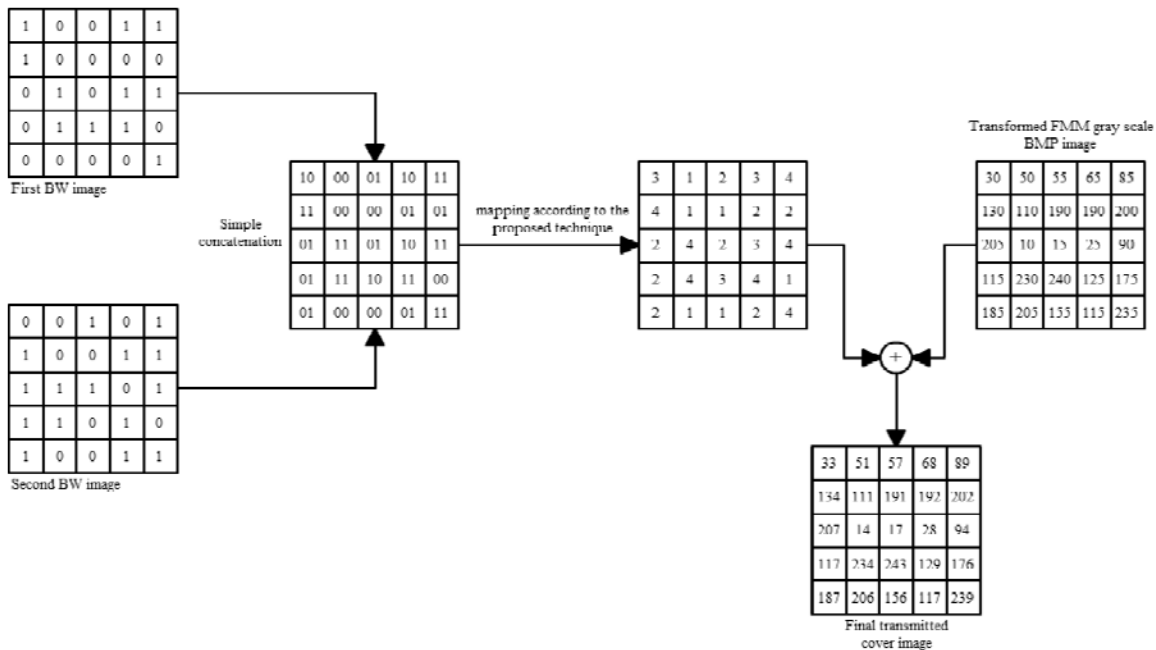


Fig. 4: Encoding process of 5x5 block

**Algorithm 2:** Hiding two black and white images in grayscale bitmap image.

**Input:** Transformed FMM image ( $\hat{\Phi}$ )

**Input:** First black and white image ( $I_1$ )

**Input:** Second black and white image ( $I_2$ )

**Output:** Final cover image ( $\Phi$ ):

1. for  $i \leftarrow 1$  to  $N$  do
2.   for  $j \leftarrow 1$  to  $M$  do
3.     if  $I_1(i, j) = 0$  &  $I_2(i, j) = 0$  then
4.        $\Phi(i, j) \leftarrow \hat{\Phi}(i, j) + 1$
5.     if  $I_1(i, j) = 0$  &  $I_2(i, j) = 1$  then
6.        $\Phi(i, j) \leftarrow \hat{\Phi}(i, j) + 2$
7.     if  $I_1(i, j) = 1$  &  $I_2(i, j) = 0$  then
8.        $\Phi(i, j) \leftarrow \hat{\Phi}(i, j) + 3$
9.     if  $I_1(i, j) = 1$  &  $I_2(i, j) = 1$  then
10.        $\Phi(i, j) \leftarrow \hat{\Phi}(i, j) + 4$

**Illustrative example:** To shed light upon the proposed technique adequately, an illustrative example will be

debated in details as a supporting material. As the commonly quoted proverb says, “A picture is worth more than a thousand words” (Brisbane, 1911). The presented illustrative example will be introduced and discussed strictly in Fig. 4 and 5. For the sake of time, a 5x5 blocks from both cover and stego images will be utilized instead of the entire image array. First of all, a 5x5 blocks from each of the two binary images will be considered. In conformity to Fig. 4, the encoding process can be easily observed. Clearly, two 5x5 blocks have been taken from two arbitrary black and white images. To the rights of them, it can be seen that the newly constructed concatenation matrix. As stated previously, by applying the novel positive integer mapping in Table 2, a fresh matrix will be established that consists of positive integer values that vary from 1 to 4, in particular. Next, we can add this newly constructed matrix to the ready-made FMM matrix of the grayscale bitmap cover image to give birth to an ultimate transmitted cover image.

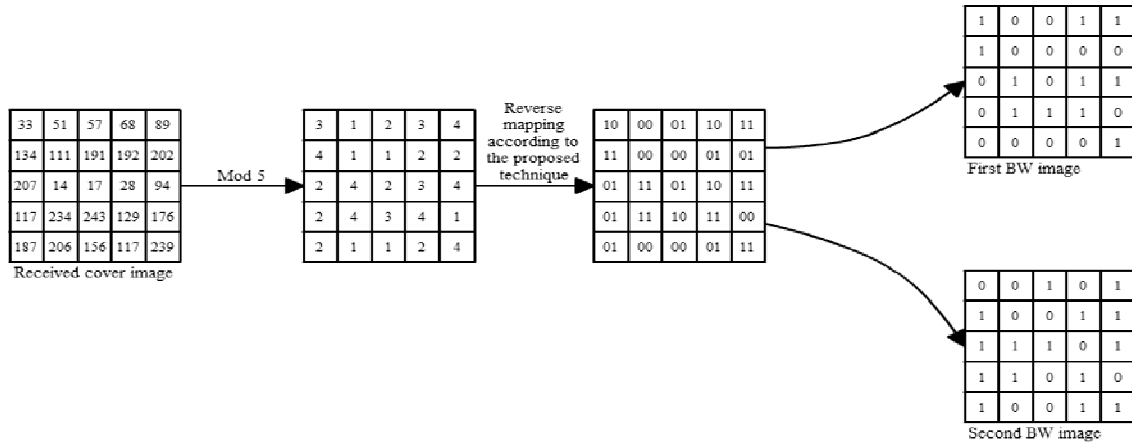


Fig. 5: Decoding process of 5x5 block

The decoding process can be easily perceived in Fig. 5. Initially, the received robust cover image will be divided by five and store its remainder in a fresh matrix, which must consists of a positive integer varying from 1 to 4 exactly. After that, the simple mapping in Table 2 can be applied oppositely to retrieve the original stego concatenated matrix, which can be easily partitioned to put up the two original binary 5x5 blocks that were entered in Fig. 4.

### EXPERIMENTAL RESULTS

In order to demonstrate the enforcement of the proposed steganographic technique, four grayscale bitmap 512x512 test images were utilized as cover images (Fig. 6). Furthermore, three pairs of stego binary images were used as confidential stego images that could be embedded into the previous four cover images (Fig. 7). In this study, the dimensions of the stego images are 512x512, the same dimensions for the cover images. It is not compulsory that the dimensions of the cover and stego images must match. Although the dimensions are not required to be identical, but they must satisfy the following condition:

$$\dim(I_1) \leq \dim(\Phi)$$

$$\dim(I_2) \leq \dim(\Phi)$$

Practically speaking, the ocular results that were earned by applying the proposed technique for image steganography ensure that the sent cover image is highly secured. According to Fig. 8, the Lena image was used as a cover image along with the three pairs of the stego images. Additionally, to consolidate the proposed algorithm, one of the most commonly implemented error metric measures was used, which is the Peak Signal-to-Noise Ratio (PSNR) (Gonzalez and



Fig. 6: Four cover images

Woods, 2008). The higher the value of PSNR, the better the quality of the cover image. The mathematical formula for the PSNR is as follows (Hore and Ziou, 2010):

$$PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}}$$

where, MSE is the abbreviation for Mean Square Error, which is the basic and simplest error measure between two digital images. In this study, MSE was calculated between the original grayscale bitmap image and the final transmitted cover image. The general form for MSE is:

$$MSE = \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M [\Phi_{ij} - \Phi'_{ij}]^2$$

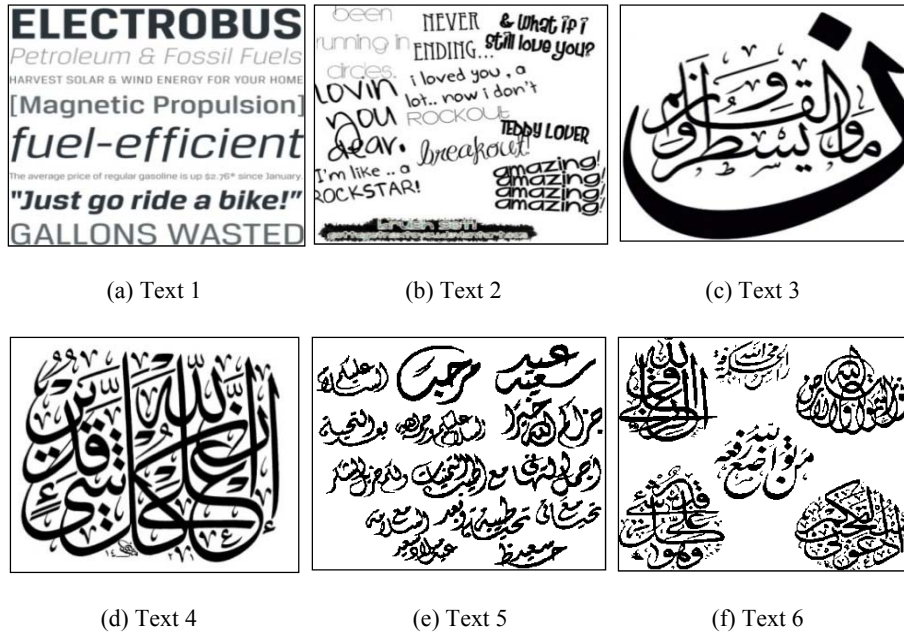


Fig. 7: Three pairs of stego images (first pair, (a) and (b), second pair (c) and (d) and third pair (e) and (f))

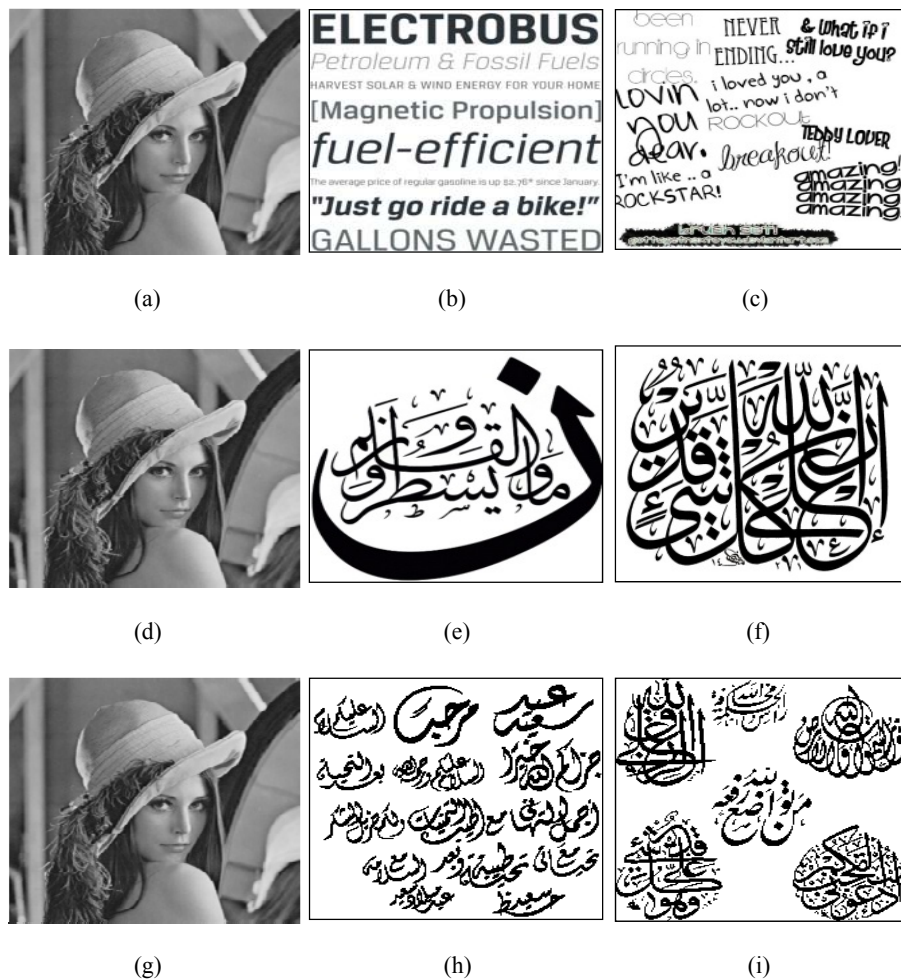


Fig. 8: Received cover image (first column), extracted pair of stego images (middle and last columns)

Table 3: Mean Square Errors (MSE) between original and sent cover images

	First stego pair	Second stego pair	Third stego pair
Lena	14.0889	12.4982	13.9893
Peppers	14.0882	12.5023	13.9879
Boat	14.0429	12.4666	13.9375
Barbara	14.2033	12.6491	14.1288

Table 4: Peak Signal to Noise Ratio (PSNR) between original and sent cover images

	First stego pair	Second stego pair	Third stego pair
Lena	36.4352	36.8855	36.4660
Peppers	35.9697	36.5981	36.1104
Boat	36.6562	37.1733	36.6889
Barbara	36.0441	36.5474	36.0669

The MSE and PSNR values were computed and presented in Table 3 and 4, respectively. In accordance with Barni (2006), the convenient value for the PSNR that could be acceptable varies from 30 and 50. Therefore, our computed PSNR values are tolerable because all the obtained PSNR values are higher than 30. In fact, this outcome implies that the reached PSNR value in this study is neither bad nor excellent. The best word to describe our obtained PSNR value is humble.

It is worth mentioning that, there was no need to calculate the error metrics for the two binary stego images because the extracted binary stego images have zero MSE. In other words, since the transmitted grayscale bitmap cover image does not modify or alter its contents through channel transmission, then the extracted binary stego images are identical to the original embedded binary images.

## CONCLUSION

Nowadays, the widely implemented algorithms for image steganography try to hide one stego image into one cover image. This goal can be achieved by hiding an image either with the same dimensions of the cover image or with lesser dimensions. But in the proposed technique, the hidden information comprises two binary images instead of one image. These two binary images are both of the same dimensions as the cover image. The most important aspect of our study was the high payload of the secret information that could be concealed in the sent cover image. Actually, we can embed two binary images that are the same size as the cover image. Thus, one can say that we have 200% payload of hidden information. Moreover, the sent cover image has tiny dissimilarities from the original cover image. Through the experiment, we could confirm the validity and efficiency of the proposed approach according to the humble PSNR values. Indeed, the suggested algorithm is quite appropriate in hiding line drawings and sketches that consists of black and white only. In our future work, we will investigate the possibility of concealing more than two binary images using k-Modulus Method.

## REFERENCES

- Abboud, G., J. Marean and R.V. Yampolskiy, 2010. Steganography and visual cryptography in computer forensics. Proceedings of the 5th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE '10), pp: 25-32.
- Artz, D., 2001. Digital steganography: Hiding data within data. IEEE Internet Comput., 5(3): 75-80.
- Barni, M., 2006. Document and Image Compression. Taylor and Francis, NY.
- Brisbane, A., 1911. Speakers give Sound Advice. Syracuse Post Standard, pp: 18.
- Chakraborty, S. and S.K. Bandyopadhyay, 2013. A steganography approach to hiding two images using dna microarray. Int. J. Innov. Res. Comput. Commun. Eng., 1(2): 158-162.
- Cox, I.J., J. Kilian, F.T. Leighton and T. Shamoan, 1996. A secure, robust watermark for multimedia. Proceedings of the 1st International Workshop on Information Hiding, pp: 185-206.
- Gonzalez, R.C. and R.E. Woods, 2008. Digital Image Processing. 3 Edn., Prentice Hall, NJ.
- Holub, V. and J. Fridrich, 2013. Digital image steganography using universal distortion. In Proceedings of the 1st ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '13). New York, USA, pp: 59-68.
- Hore, A. and D. Ziou, 2010. Image quality metrics: PSNR vs. SSIM. Proceedings of the 20th International Conference on Pattern Recognition (ICPR), pp: 2366-2369.
- Jassim, F.A., 2012. Five modulus method for image compression. Signal. Image Process. Int. J., 3(5): 19-28.
- Jassim, F.A., 2013a. Hiding image in image by five modulus method for image steganography. J. Comput., 5(2): 21-25.
- Jassim, F.A., 2013b. Image compression by embedding five modulus method into jpeg. Signal. Image Process. Int. J., 4(2): 31-39.
- Jassim, F.A., 2013c. k-modulus method for image transformation. Int. J. Adv. Comput. Sci. Appl., 4(2): 267-271.
- Jassim, F.A., 2013d. A novel steganography algorithm for hiding text in image using five modulus method. Int. J. Comput. Appl., 72(17): 39-44.
- Johnson, N.F. and S. Jajodia, 1998. Exploring steganography: Seeing the unseen. Computer, 31(2): 26-34.
- Kahn, D., 1983. The Codebreakers: The Story of Secret Writing. Macmillan, New York.
- Katzenbeisser, S. and F.A. Petitcolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. 1st Edn., Artech House Inc., Norwood, MA, USA.



- Kieu, T.D. and C.C. Chang, 2009. An image authentication based on discrete Fourier transform. *Fund. Inform.*, 97(4): 369-379.
- Lyu, S. and H. Farid, 2006. Steganalysis using higher-order image statistics. *IEEE T. Inf. Foren. Sec.*, 1(1): 111-119.
- Marvel, L.M., C.G. Boncelet Jr. and C.T. Retter, 1999. Spread spectrum image steganography. *IEEE T. Image Process.*, 8(8): 1075-1083.
- Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. *IEEE Secur. Priv.*, 1(3): 32-44.
- Raja, K.B., C.R. Chowdary, K.R. Venugopal and L.M. Patnaik, 2005. A secure image steganography using lsb, dct and compression techniques on raw images. *Proceedings of the 3rd International Conference on Intelligent Sensing and Information Processing (ICISIP '05)*, pp: 170-176.
- Stockman, G. and L.G. Shapiro, 2001. *Computer Vision*. 1st Edn., Prentice Hall PTR, Upper Saddle River, NJ, USA.
- Wang, H. and S. Wang, 2004. Cyber warfare: Steganography vs. steganalysis. *Commun. ACM*, 47(10): 76-82.
- Xia, X.G., C.G. Boncelet and G.R. Arce, 1997. A multiresolution watermark for digital images. *Proceedings of the International Conference on Image Processing (ICIP '97)*, 1: 548-551.