A Novel Steganography Method for Hiding BW Images into Gray Bitmap Images via k-Modulus Method

Firas A. Jassim
Management Information Systems Department
Faculty of Administrative Sciences
Irbid National University
Irbid 2600, Jordan
Email: firasajil@yahoo.com

***Abstract*—This paper is to create a pragmatic steganographic implementation to hide black and white image which is known as stego image inside another gray bitmap image that known as cover image. First of all, the proposed technique uses k-Modulus Method (K-MM) to convert all pixels within the cover image into multiples of positive integer named k. Since the black and white images can be represented using binary representation, i.e. 0 or 1. Then, in this article, the suitable value for the positive integer k is two. Therefore, each pixel inside the cover image is divisible by two and this produces a reminder which is either 0 or 1. Subsequently, the black and white representation of the stego image could be hidden inside the cover image. The ocular differences between the cover image before and after adding the stego image are insignificant. The experimental results show that the PSNR values for the cover image are very high with very small Mean Square Error.**

Keywords*—*Image steganography, Information hiding, Security, k-Modulus Method.

I. Introduction

Recently, there has been great interest in image steganography and its implementation in the filed of information security. The word steganography has been originated from the Greek words stegos which means covered and graphia which means writing. Actually, the word steganography refers to the process of concealing secret data into any kind of media such as image, video, or audio [12]. The essential concept in every data hiding method is the feebleness of human perception such as vision, listening, and hearing. It must be differentiated between steganography and cryptography because both of them are used to hide secret data. The basic dissimilarity between steganography and cryptography is that cryptography focuses on preserving the contents of the message confidential. In the other hand, steganography concentrates on preserving the existence of a message confidential at the first place [13]. Hence, if the notion is to conceal the existence of the secret message, then the method of steganography is preferred [13]. Also, it must be differentiated between steganography and watermarking because of the common confusion between them. The essential difference between steganography and watermarking is the absence of an adversary. In watermarking there is an active adversary that would try to forge the watermarks. On the contrary, in steganography there is no such an active adversary [4]. Recently, there are several methods have been proposed for image based steganography by many authors. The simplest and the most common method is the Least Significant Bit (LSB) which replaces the least significant bits from the right of a pixel to hide the information [6]. Furthermore, there are wide manifold techniques with their own pros and cons were developed in steganography. Many authors have researched the method of hiding information inside image via steganographic technique [3][16][15]. Also, an excellent theoretical background about steganography could be found in [2].

The organization of this article is as follows: In section II, a brief discussion about k-Modulus Method was presented. The proposed steganographic technique was discussed in Section III. In addition, experimental results and conclusions are presented in Sections IV and V, respectively.

II. k-Modulus Method

The first origination of k-Modulus Method was as an image compression method that was proposed by [7]. The basic concept of Five Modulus Method is to transform the whole pixels inside the original image into multiples of five. After that, a generalization of Five Modulus Method was established and named k-Modulus Method (k-MM) where k is any positive integer [6]. The k-Modulus method as an image transformation method proven its ability to mimics the original image before the transformation. In other words, the human eye can not differentiate between the original image and the transformed k-Modulus Method image, fig 1.

Actually, k-Modulus Method transform could be considered as a suitable carrier to convey data inside. The conveyed data could be hidden inside the non-divisible integers of k. Therefore, any pixel that is not divisible by k with reminder zero, this implies that there is hidden information in this pixel and so on. Since the aim of this research is to hide black and white images inside gray image, then the demand for two binary representations is arise. Therefore, choosing k is equal to two is compulsory for two reasons. The first reason is to hide binary data as 0 or 1. The second reason is that whenever there is an increase in k, the transformed image could be distorted. Hence, the best expedient that could be used to preserve the original pixel values as could as possible.

As the topic of k-Modulus method considered as a new born topic, it has many applications is image processing field. According to [9], the embedding of k-Modulus Method into JPG image format to increase the compression ratio was discussed. Moreover, in accordance to [10], increasing the compression ratio in PNG file format was also obtained by the assistant of k-Modulus Method. Finally, the implementation of k-Modulus Method in steganography in two approaches. The first approach, is by hiding text in an image using Five Modulus Method which was discussed by [11]. The second approach which was researched by [8], was the first seed to hide small size image into another larger image.

(a) Original Lena (b) Transformed Lena

Fig. 1: k-Modulus Method Transformation (k=2) with PSNR=50.7787

III. Proposed Steganography Technique

As mentioned previously, k-Modulus method could be treated as a robust host to convey information. The proposed technique starts with transforming the original image into gray scale image. This step is to reduce image size because the color bitmap image is three times higher in size than gray scale image with the same dimensions. Hence, in this research, a gray scale bitmap image could be used as a cover image. The resulted gray scale bitmap image is now ready for the k-Modulus Method transformation with k=2, as mentioned in the previous section. Now, the numerical values for all the pixels within the gray scale bitmap image are of multiples of two. Mathematically speaking, the reminder of dividing any positive integer number by two yields either zero or one. Fortunately, this may be treated as a robust host to accommodate images with binary representation, i,.e. black and white images. Concerning stego (secret) image, it must be a binary (black and white) image. Obviously, the black and white images are the images that consist of zeros and ones. Till this step, two images were constructed which are the cover gray scale bitmap image and the stego black and white image. The final step consists of adding the cover and the stego images together. The resulted image pixels are either multiples of two or multiples of two plus one. If the reminder of the pixel is zero, then it is treated as zero representation, otherwise it is one. hence, one can easily extract the hidden secret black and white image. The reason for choosing black and white image in the proposed steganographic technique is to hide images that contain an essential information such as maps and geometric line. Now, an illustrative example will be discussed to clarify the proposed technique.

Firstly, an arbitrary 10×10 block from Lena gray scale bitmap image will be considered as a cover image, table I. Secondly, the k-Modulus method transformation will be applied to the 10×10 block, tableII. Thirdly, a random 10×10 block from any black and white image will be used as a stego image, table III. Finally, the addition of the cover and stego images could be presented in table IV. Clearly, the resulted block could be divisible by two and produces two reminders which are zero and one. Obviously, the resulted reminders could be formulate the stego (secret) image exactly.

TABLE I: 10×10 Block from Original Lena image

93	95	100	96	98	100	101	97	99	102
96	95	92	100	94	97	97	93	102	106
97	99	98	101	98	98	95	96	99	100
96	95	95	96	100	97	98	97	100	103
100	95	98	97	100	104	98	97	101	101
92	97	93	100	99	98	99	96	101	102
98	96	95	94	99	101	97	100	102	103
95	94	96	98	101	102	95	101	105	100
101	98	99	100	92	104	101	102	105	105
100	100	105	103	102	99	98	100	103	104

TABLE II: 10×10 Block from Transformed Lena image

92	94	100	96	98	100	100	96	98	102
96	94	92	100	94	96	96	92	102	106
96	98	98	100	98	98	94	96	98	100
96	94	94	96	100	96	98	96	100	102
100	94	98	96	100	104	98	96	100	100
92	96	92	100	98	98	98	96	100	102
98	96	94	94	98	100	96	100	102	102
94	94	96	98	100	102	94	100	104	100
100	98	98	100	92	104	100	102	104	104
100	100	104	102	102	98	98	100	102	104

TABLE III: 10×10 Block from black and white Gadeer (Stego) image

1	1	1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0
1	1	1	1	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0

TABLE IV: 10×10 Block obtained by adding Gadeer to Lena

93	95	101	96	98	100	100	96	98	102
97	95	93	100	94	96	96	92	102	106
97	99	99	101	98	98	94	96	98	100
97	95	95	97	100	96	98	96	100	102
101	95	99	97	100	104	98	96	100	100
93	97	93	101	98	98	98	96	100	102
99	97	95	94	98	100	96	100	102	102
95	95	97	98	100	102	94	100	104	100
101	99	98	100	92	104	100	102	104	104
101	100	104	102	102	98	98	100	102	104

On the sender side, the sender will send the constructed cover image that was presented in table IV. On the receiver side, the recipient will divide the whole image by two and store the reminder in a new array. The resulted array is exactly the stego black and white image. It must be mentioned that, the reason for using bitmap is that, bitmap image does not modify its structure since it is a lossless compression technique. In other words, there was a need to preserve the constructed image values exactly. Therefore, a lossless method of compression was proposed. On the contrary, if lossy compression was used instead of lossless then a completely different results will be obtained. In fact, lossy compression does not be appropriate for the proposed technique because it is irreversible. In other words, one can not retrieve the original pixels when using lossy compression. Hence, JPG compression is not suitable for the proposed steganographic techniqe.

IV. Experimental Results

In this section, both a practical and visual evidences have been implemented to support the proposed technique. Actually, the proposed technique in this article has been implemented to four 512×512 test images with different spatial and frequency characteristics as cover images, fig. 2. Since the proposed technique hide stego image with the same size of the cover image, then six 512×512 black and white stego (secret) images, fig. 3. According to [5], two error measures have been utilized to evaluate the differences between the original and the cover images. The first error measure is the widely and simplest one which is the mean square error (MSE) that can be expressed as:

$$MSE = \frac{1}{NM}\sum_{x=1}^{N}\sum_{y=1}^{M}[f(x,y)-g(x,y)]^2 \qquad (1)$$

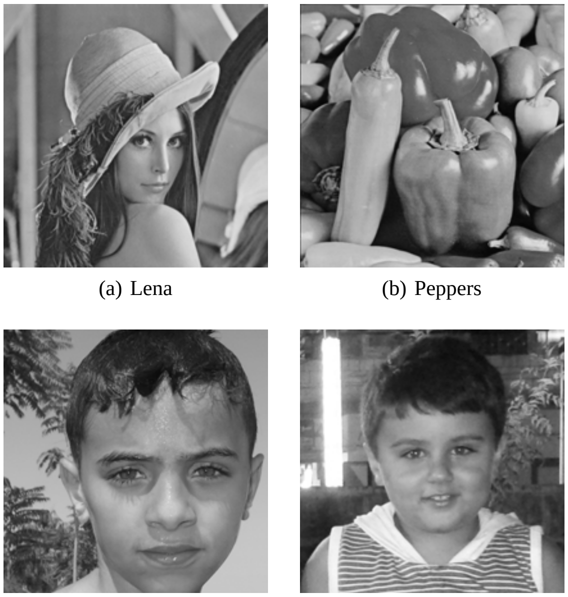
The second error metric is the peak signal to noise ratio (PSNR) which is the most preferable measure that computes the dissimilarities between images in most of the image processing fields [5]. The mathematical formula for the PSNR is as follows:

$$PSNR = 20 \cdot log_{10}\frac{MAX}{\sqrt{MSE}} \qquad (2)$$

The computed error metrics for the proposed technique have been evaluated and introduced in tables V and VI, respectively. Clearly, the mean square error values in table V seem to be very small which implies the closer the values between the original and the constructed cover images. This may consolidate the claim about the proposed technique in which that there are almost tinny dissimilarities that can not be distinguished by the human eye. Hence, any adversary can not notice or even feel that the cover image contain any secret information. Additionally, the PSNR values have been calculated and presented in table VI. The higher the value of PSNR, the more quality the stego image will have. In accordance to [1] [14], the reasonable range for the acceptable PSNR values are between 30 and 50. Therefore, the computed PSNR values are highly tolerable because all the computed PSNR values are higher than 50. Consequently, this support the proposed technique to hide black and white image confidentially in any gray bitmap images.

V. Conclusion

In this paper, a novel confidential steganographic technique was proposed. The essential conclusion that comes from the proposed technique is the high confidentiality and conceal ability to the embedded information inside the cover image. However, the proposed technique is very suitable in sending black and white images like diagrams, line chart, secret maps, etc. Moreover, the file size for the original image will remain constant even after embedding the secret stego image inside. This is one of the important benefits of the proposed technique that helps not to suspect about the cover image and its contents by any adversary. practically, experiment results have demonstrated that the proposed technique produces high PSNR values that makes no doubt that the suggested steganographic technique does not affect the cover image at all.



(a) Lena (b) Peppers

(c) Saif (d) Aws

Fig. 2: Four cover Images

TABLE V: Mean Square Error

	Lena	Peppers	Saif	Aws
Gadeer	0.4977	0.4999	0.4977	0.4980
Noon	0.4993	0.4996	0.4992	0.4918
Text1	0.4996	0.5004	0.4992	0.4945
Text2	0.4988	0.4990	0.4994	0.4924
Mask5	0.4981	0.5000	0.4984	0.4945
Barcode	0.5001	0.5006	0.5003	0.5016

TABLE VI: PSNR values for the cover images

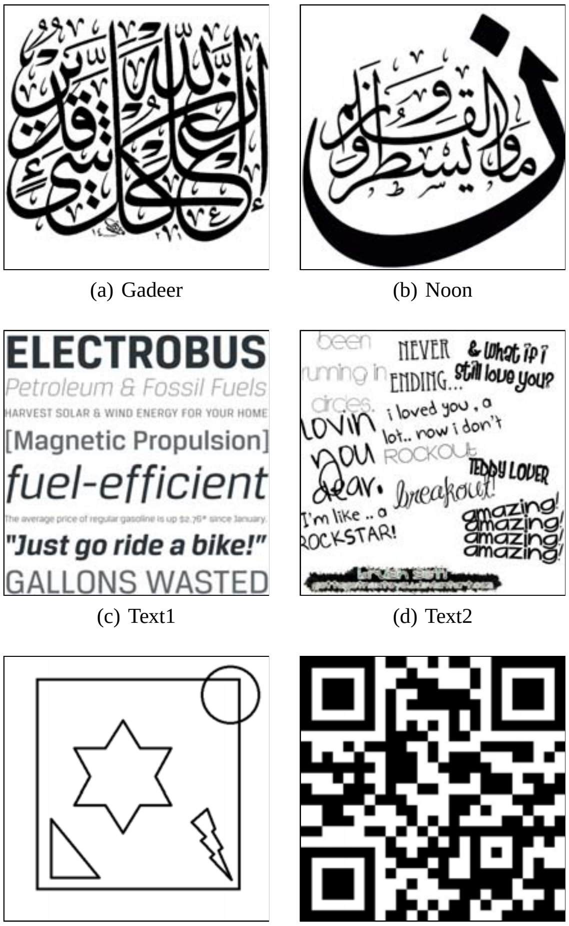
	Lena	Peppers	Saif	Aws
Gadeer	50.8132	50.4329	50.9543	51.1589
Noon	50.7993	50.4355	50.9416	51.2131
Text1	50.7967	50.4282	50.9411	51.1894
Text2	50.8038	50.4400	50.9392	51.2075
Mask5	50.8099	50.4315	50.9484	51.1891
Barcode	50.7926	50.4268	50.9318	51.1270

References

[1] M. Barni, *Document and Image Compression*. Taylor & Francis, 2006.

[2] C. Cachin, "An information-theoretic model for steganography," *Inf. Comput.*, vol. 192, no. 1, pp. 41–56, Jul. 2004.

[3] C. C. Chang, J. Y. Hsiao, and C. C. S., "Finding optimal least significant bit substitution in image hiding by dynamic programming strategy," *Pattern Recognition*, vol. 36, pp. 1583–1595, 2003.

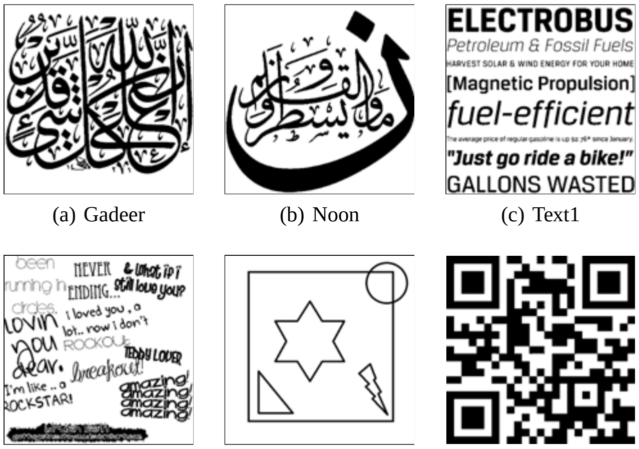


(a) Gadeer (b) Noon

(c) Text1 (d) Text2

(e) Shapes (f) Barcode

Fig. 3: Six stego Images



(a) Gadeer (b) Noon (c) Text1

(d) Text2 (e) Shapes (f) Barcode

Fig. 4: Extracted stego images from Lena as a cover image

[4] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Review: Digital image steganography: Survey and analysis of current methods,” *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[5] R. C. Gonzalez and R. E. Woods, *Digital image processing*, 3rd ed. Prentice Hall, 2008.

[6] F. A. Jassim, “k-modulus method for image transformation,” *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 2, pp. 267–271, 2013.

[7] F. A. Jassim, “Five modulus method for image compression,” *Signals and Image Processing: An International Journal*, vol. 3, no. 5, pp. 19–28, 2012.

[8] F. A. Jassim, “Hiding image in image by five modulus method for image steganography,” *Journal of computing*, vol. 5, no. 2, pp. 21–25, 2013.

[9] F. A. Jassim, “Image compression by embedding five modulus method into jpeg,” *Signals and Image Processing: An International Journal*, vol. 4, no. 2, pp. 31–39, 2013.

[10] F. A. Jassim, “Increasing compression ratio in png image by k-modulus method for image transformation,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 45–52, 2013.

[11] F. A. Jassim, “A novel steganography algorithm for hiding text in image using five modulus method,” *International Journal of Computer Applications*, vol. 72, no. 17, pp. 39–44, 2013.

[12] N. Johnson and S. Jajodia, “Exploring steganography: Seeing the unseen,” *IEEE Computer Society*, vol. 31, no. 2, pp. 26–34, 1998.

[13] H. Wang and S. Wang, “Cyber warfare: Steganography vs. steganalysis,” *Communications of the ACM*, vol. 47, no. 10, 2004.

[14] S. Welstead, *Fractal and Wavelet Image Compression Techniques*. SPIE, 1999.

[15] A. Westfeld, “F5-a steganographic algorithm high capacity despite better steganalysis,” *Lecture Notes in Computer Science*, vol. 2137, pp. 289–302, 2001.

[16] P. C. Wu and W. H. Tsai, “A steganographic method for images by pixel-value differencing,” *Pattern Recognition Letters*, vol. 24, pp. 1613–1626, 2003.