Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Algorithm for Image Steganography Based on Effective Channel Selection Technique

Vijaypal Dhaka*
School of Engineering & Technology
Jaipur National University
Jaipur,India

Ramesh C. Poonia
School of Engineering & Technology
Jaipur National University
Jaipur,India

Yash Veer Singh
School of Engineering & Technology
Jaipur National University
Jaipur,India

Abstract—This paper introduces, a novel steganographic technique for images is proposed which is a type of spatial domain information hiding technique. To hide the secret information in original image or cover image, the effective channel selection technique is used .In the previous image steganographic technique, we hidden the secret data in to the only two, three or four bits or at most five bits of a pixel in a image which produces the poor value of peak signal to noise ratio (PSNR) and high value of root mean square errors (RMSE) which are both the image quality parameters. Proposed technique can embed large data than previous technique and shows the better result for image quality parameter.

Keywords— RGB, Steganography, Image quality parameters (MSE, PSNR), Stego image, Cover image.

I. INTRODUCTION

Steganography means to conceal the existence of a message in such a way no one can see the information in the cover image.

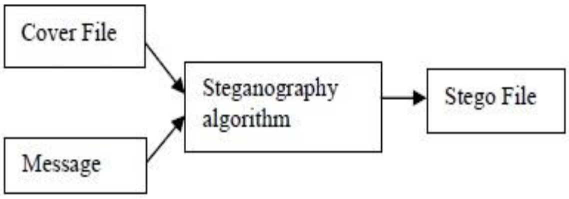

Figure1: Steganography Process

Generally there are two methods to hide the secret information .such as steganography and cryptography. By using the cryptography only data is encoded and appears as unintelligible or random stream of the data to the third party by using substitution and transposition technique but the existence of the message is evident to the hackers and crackers, where as in technique of steganography the existence of the message is not evident. Stego means covered and graphy means writing, thus meaning of steganography in Greek word is “covered writing”. As defined by Cachin [7], steganography is the art and science of communicating in such a way that the presence of a message can not be detected. When cryptography is applied with the steganography on any secret message it becomes more secure and invisible to third party. The existing work done by using LSB techniques such as substitution method for steganography. Steganography is very old method in which Invisible ink, Pin punchers, Character marking, Typewriter correction ribbon methods were used. Around 440 B.C the technique of steganography used by the Histiaeus is that he used his most faithful slave and shaved the head of the slave to hide the information which disappeared when the hair had regrown. There are various techniques of steganography but the images are mostly used to hide or embed the secret information. These types of techniques are known as image steganography techniques. Image steganographic method can be categorized in to two groups [3]: the transform domain technique group and the spatial domain technique group. In the Spatial domain method the intensity values of the pixels of the image are used to hide the information directly, while in the transform domain methods frequency domain of images which are previously transformed, used to embed the information.

II. RELATED WORKS

A. *2k Correction and Edge-Detection Technique for Image Steganography:-*

J.G. Yµ, E.J Yoon Shin and K.Y Yoo(2008) proposed this technique. In this technique contrast sensitivity function (CSF) and just noticeable difference (JND) methods are used. . A mathematical 2k Correction method is used to give the better result in the form of imperceptibility .For example a pixel of cover image is used to hide the secret information and output of the this algorithm is called the stego image, some differences were found between the cover image and the stego image. These differences indicate the quality of the cover image is degraded. 2k Correction method corrects the intensity value of every pixel .If k-bits of the secret data are embedded in the intensity value of the pixel of the image then the technique of addition or *subtraction* 2k is applied to each intensity value of pixel, and finally the corrected intensity value of pixel of the stego image becomes closer to the intensity value of pixel of the original image. Then in the stego-pixel the secret data is not changed. This scheme is better than the previous scheme because more data is embedded than the previous technique and better imperceptibility occurred. This method is an edge detection which only uses 3-bits from MSB. In this technique embedment of the secret data depends on the intensity value which is received from each pixel intensity value whether it is on the other part of the image or it is on the edge. 2k correction mathematical formula is used for this technique which modifies the value of stego pixel closer to the value of the cover pixel.

B. *Least significant Bit (LSB) Scheme:-*

This method is very simple for hiding the existence of the secret message in a cover image. Substitution technique play very important role in the LSB image steganography. In this technique LSB bits are replaced by the secret data which is to be sent. Then the secret message bits become random stream of the data or permuted which are unintelligible to the thirds party. 4 LSB substitutions method which modifies last 4 bits of a LSB of pixel. In LSB technique on average fifty percent bits of the LSB's are replaced. These changes can not perceived by the human eyes.

C. *Pixel-Value Differencing (PVD) scheme:-*

In this technique more data can embed in the edge area with high imperceptibility. To distinguish edge and smooth areas Wu and Tsai proposed a novel staganography technique by using pixel-value differencing (PVD).In general the changing of the edge area can not be distinguished well because this area is very less sensitive to the human eyes. Then in this technique edge area is used to hide the more data than the smooth area.

D. *Wen-Nung Lie and Lie Chang's Technique:-*

Multimedia data such as video,text,audio,image etc can be embedded by using this technique of L.C.Chang and W.N lie in to a host image. Two important properties of the steganographic technique are sufficient data capacity and good imperceptibility. Lie Chang proposed the technique which satisfies both properties [4]. This technique is called Adaptive LSB technique which uses the Human Visual System (HVS).HVS has the two important characteristics: Contrast Sensitivity Function (CSF) & Just Noticeable Difference (JND), Spectral Sensitivity and Masking .The technique of JND is very simple because this is the characteristics of the of HVS and it is used by Li-Chang .It is also known as the luminance difference threshold or the visual increment threshold. In this method the amount of the light is defined JND which is necessary to add to a visual field of intensity value so that this can be distinguished by the background. This technique is used to embed the high capacity data than the other steganographic technique about overall bright images and when the capacity of the embedding the data is increased then has a high distortion on the original image ,but overall dark images does not concern.

E. *LSB Based Image Steganography using secret key*:-

This is the technique based on the image steganography which improves the result compared to the previously defined LSB substitutions techniques and enhances the level of security for the embedded data. This is a new technique which is used to substitute LSB of RGB colour image. In this technique secret information is hidden in the LSB of the cover image by using new security conception where as the hidden information is protected from unauthorized users by using the secret key encryption. In general, the LSB of the image is used to store the secret information in to a specific position. So anyone who knows the retrieval methods can extracts the hidden information. But this technique allows different positions of the LSB of the image to store the hidden information depending upon the secret key. As a result of this technique, it is very difficult to anyone to extracts the hidden information who know the retrieval methods. In this technique various image quality parameters are used to measure the quality of the stego images. This technique changes very small number of bits of the image, so the value of the PSNR gives better result. Finally the result obtained from this technique shows in LSB based image steganography by using secret key which provides better security and the better value of image quality parameter PSNR and MSE than the general LSB based image steganography substitution methods.

F. *Most Significant Bit (MSB) Edge Detection Technique:-*

One model out of several computational models is used for CSF (Contrast Sensitivity function) proposed by Mannon-Sakrison[1]. According to this technique, one is able to satisfy the two functions such as increment of hiding capacity and good imperceptibility when additional secret data is embedded in the pixels of the image of high spatial frequency. Generally, the human eye is very sensitive to throughout pictures of the view, while for fine detail having low sensitivity. Such type of characteristics of HVS is called CSF which is proposed by Mannon-Sakrison.

Edge –Detection Algorithm is used in order to judge any pixel has low spatial frequency or high spatial frequency in a digital image. The most important algorithm for edge detection is called GAP algorithm. In this algorithm we use only three bits from the MSB for the input value of this Edge-Detection Algorithm. Because of this the pixels that are selected from the extracting phase must be equal to the pixels that are selected from the embedding phase. If the pixel value is smaller than first threshold value (88 intensity values) then three bits are embedded in a pixel and judged by using the edge region. Two important steps are used in this technique. In first step, In order to sort out edge-region in the cover image, first of all execute the algorithm of MSB3 Edge-Detection at a cover image. In second step if any intensity value of the pixel is smaller than the value of first threshold value (88 pixel value) and exists on the edge region then in the pixel, embed the three bits of the secret data.

III. Proposed Novel Algorithm For Image Steganography Based On Effective Channel Selection Technique

In this proposed novel algorithm for image steganography based on effective channel selection technique the use of secret key is introduced. In computer graphics images are the group of pixels and each pixel has its own intensity value (0-255) .A pixel is a sample of any image. The intensities values of all the pixels are stored in frame buffer as arrays of values. Any colour image is made up of the combination of three channels which are called Red(R), Green (G) and Blue (B), where the combination of the three colours represents a colour pixel. In this algotithm the bits of the effective channel's (blue channel) pixel were replaced with secret key and the original data bits. Firstly key is converted in to binary form and its binary form is filled in the effective channel or blue channel of the first pixel. After then secret message is converted in to binary form and its binary form is filled in blue channel of the next pixel. According to Hecht (researcher) the blue colour is very less sensitive to the human eyes so blue channel is selected to hide the secret data which is very effective to the visual perception and also to hide the more data than red and green channel. For example, suppose three colour pixels (size of each colour pixel is 24 bits) of the image can be used to hide the message .Suppose the bits of the three original pixels are given below:

(10100010 11001001 10001000) (10100101 01001000 10101001) (11101000 01100111 11001001)

If we want to hide the letter "F" by applying this new image steganographic technique by replacing the blue channel bits of a pixels of the image, which has position 70 in to ASCII character table and having binary number is "01000110" and letter "B" which has an ASCII code 66 and the representation in binary form is "01000010" then the result is of such type

(01000010 11001001 10001000) (01000110 01001000 10101001) (11101000 01100111 11001001)

A. *Embedding Phase the secret data*:-

The process of embedding the secret data is as follows.
Inputs: Text data, secret key and Cover Image.
Outputs: Stego Image.
Procedure:-

a): - Create an array called Pixel-Array in which all the pixels are stored and these pixels are fetched from the original image.

b): Create another array called Character-array in which all the characters are stored and these characters are fetched from the given text file.

c):-Again create another array which is used to store all the characters called Key-Array and these characters are fetched from stego key.

d):-Select the first pixel of the cover image and fetched characters from Key-Array and place these characters in blue channel of first pixel. If more characters are present in Key-array, then blue channel of the next pixel is used to embed rest of the characters of the key-Array, otherwise go to step (e).

e):- To indicate end of the key some symbols are used for terminating .Here the key '0' is used as a terminating symbol.

f):-Each blue channels of the next pixel is used to place the characters from Character-Array by alteration of it.

g):- Repeat step (f) till all the characters from the character-array has been embedded.

h):-Again to indicate the end of the secret data put some terminating symbol.

i):-Finally Obtained the output of the proposed algorithm called stego image that are used to hide the secret data that we input.

*B. Phase of Secret Data Extraction from the Stego Image:-*The process of extraction phase is as follows.

Inputs:-Stego Image File, Secret key.
Output: Secret text data
Procedure:

a) :-Consider three arrays are used . They are Pixel-Array, Key-Array, and Character-Array.

b):-Extract all the pixels from the given stego image and store these pixels in an array called Pixel-Array.

c):-Now, start the process of pixel's scanning from first pixel of the stego image and extract key characters from the blue channel of the pixels and put it in key-Array. Follow step (c) till we get terminating symbols otherwise follow step (d).

d):-If these extracted key matches with the key entered by the receiver, then follow Step (e) otherwise terminate the program by displaying message "key is not matching".

e):-If the key is valid, then again start scanning next pixels and extract secret message character from the blue channel of the next pixels and place it in Character-Array. Follow step (e) till we get terminating symbol, otherwise follow step (f).

f):-Extract secret message from Character-Array.

IV. Final Experimental Result Of Proposed Novel Algorithm Based On Effective Channel Selection Technique

To examine the performance of the proposed new image steganographic technique, first of all steganographic technique applied as a test image to Lena's Image. To measure the quality of the image parameters such as Peak

Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) for an encrypted stego image, different kinds of the result have been calculated with the RGB channels by changing the intensity value of the blue channel to embed the secret data in it. A comparative study with the previous image steganographic technique as shown in the below table. Between two images PSNR measures the peak-signal-to-ratio in decibels. For the quality measurement between the cover image (original image) and the stego image (compressed image) the ratio of difference between image quality parameters (PSNR, MSE) for these images are often used. For the better quality of the stego image the higher value of the PSNR is used. On the other hand the lower difference of the MSE (mean square error) between original image and the stego image shows better quality of the image and also indicate lower error.

To compute the value of the image quality parameter PSNR, first of all the block calculates the value of MSE (Mean Square Error) by using the following the mathematical equation.

$$\mathrm{MSE} = \frac{1}{M*N}\sum_{x=1}^{M}\sum_{y=1}^{N}[x(m,n) - y(m,n)]^2$$

From the above equation x(m,n) and y(m,n) are the two images having size of m*n. Where x is the original image or cover image and y is the stego image or encrypted image.

$$\mathrm{PSNR} = 20\log_{10}\left[\frac{\mathrm{MAXPIX}}{\mathrm{RMSE}}\right]$$

Where RMSE stands for Root Mean Square Error of the image which measures the average sum of thesaurus in each pixel of the stego image or encrypted image and MAXPIX is the maximum value of the pixel. Some changes occur in the value of the pixel caused by encryption algorithm.

$$RMSE = \sqrt{MSE}$$

The below tables shows the comparison of results with various steganographic techniques.

TABLE 1: COMPARISION OF PSNR VALUES FOR LENA'S IMAGE

Steganographic Technique	**PSNR**
LSB3	40.89
Adaptive Number of LSBs	40.36
PVD	41.58
2K Edge Correction	42.09
Proposed Algorithm	51.31

TABLE 2: MSE, RMSE AND PSNR OF LENA'S IMAGE FOR PROPOSED NOVEL ALGORITHM

Cover Image	**MSE**	**RMSE**	**PSNR(db)**
Lena	0.48	0.69	51.31

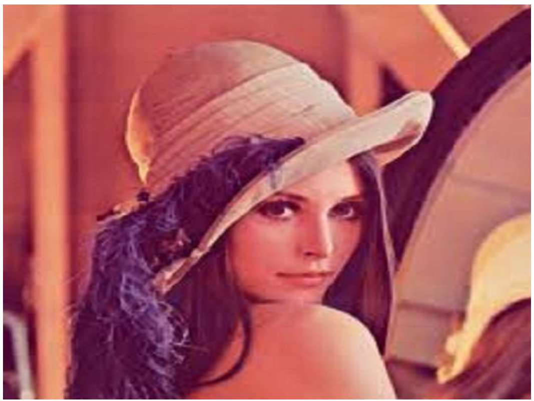

Figure 2(a): Original Lena's Image (512*512)

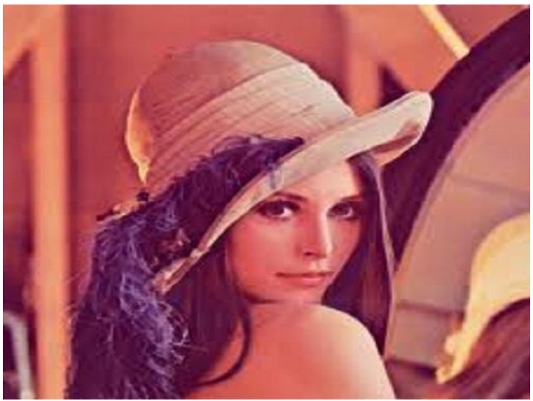

Figure 2(b):Stego Lena's Image(512*512)

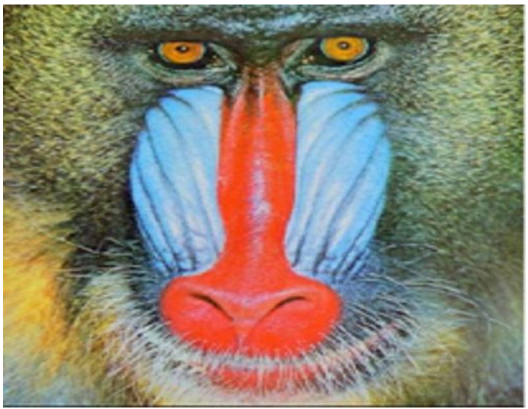

Figure 3(a): Original Baboon's Image (512*512)

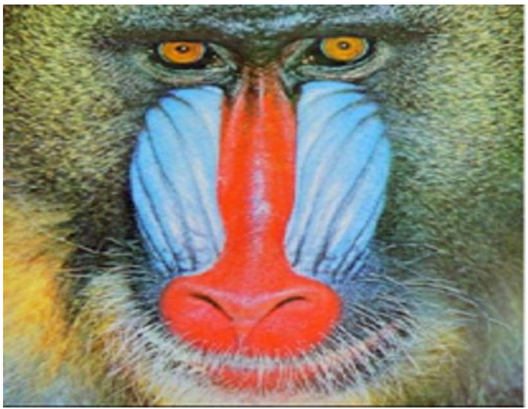

Figure 3(b):Stego Baboon's Image(512*512)

TABLE 3: COMPARISION OF PSNR VALUES FOR BABOON'S IMAGES

Steganographic Technique	**PSNR**
2k Edge Correction	42.03
PVD	37.58
Adaptive Number of LSBs	40.55
LSB3	40.84
Proposed Algorithm	53.89

TABLE 4: MSE, RMSE AND PSNR VALUES FOR BABOON'S IMAGE OF PROPOSED NOVEL ALGORITHM

Cover Image	**MSE**	**RMSE**	**PSNR(db)**
Baboon	0.26	0.52	53.83

Figure 6(a) Animal 1 Original Image (1024*1024)
Figure 6(b) Animal 2 Original Image (1024*1024)
Figure 6(c) Animal 3 Original Image (1024*1024)

Figure 6(a) Animal 1 Stego Image (1024*1024)
Figure 6(b) Animal 2 Stego Image (1024*1024)
Figure 6(c) Animal 3 Stego Image (1024*1024)

TABLE 5: COMPARISION OF PSNR VALUES FOR ANIMAL 1(1024*1024), ANIMAL 2(1024*1024) AND ANIMAL 3 (1024*1024) IMAGES

Cover Image (1024*1024)	**LSB Techniques**	**PVD Techniques**	**PWBBDHA Technique**	**Proposed Algorithm**
	PSNR	**PSNR**	**PSNR**	**PSNR**
Animal1	31.37	29.89	28.46	54.82
Animal2	31.46	29.75	28.51	55.34
Animal3	31.58	29.76	27.54	55.82

TABLE 6: MSE, RMSE AND PSNR VALUES OF ANIMAL l (1024*1024), ANIMAL 2(1024*1024), ANIMAL 3(1024*1024) IMAGES FOR THE PROPOSED NOVEL ALGORITHM

Cover Image (1024*1024)	**MSE**	**RMSE**	**PSNR(db)**
Animal1	0.21	0.46	54.82
Animal2	0.19	0.43	55.34
Animal3	0.17	0.41	55.82

III. CONCLUSION

This paper introduces a proposed a novel algorithm for image steganography based on effective channel selection technique is used in order to hide secret data in cover-image. It is a kind of spatial domain technique. Techniques used so far focuses only on the two or four bits of a pixel in a image,(at most five bits at the edge of an image.) which results less peak to signal noise ratio and high root mean square error i.e. less than 45 PSNR value. Proposed work is concentrated on 8 bits of a pixel (8 bits of blue component of a randomly selected pixel in a 24 bit image), resulting better quality of image. Proposed technique has also used contrast sensitivity function (CSF) and just noticeable difference (JND) Model. Proposed scheme can embed more data than previous schemes [3, 4, 10], and shows better imperceptibility. To prove this scheme, several experiments are performed, and the experimental results are compared with the related previous works. Consequently, the experimental results proved that the proposed scheme is superior to the related previous works. The future work is to extend proposed technique for videos and to modify given scheme to improve image quality by increasing PSNR value and lowering MSE value.

References

[1] J. L. Mannos and D. J. Sakrison. The effects of a visual fidelity criterion on the encoding of images. IEEE Trans. On Information Theory, pages525–536, 1974.

[2] Herodotus, the Histories, and chap. 5 - The fifth book entitled Terpsichore,7 - The seventh book entitled Polyamine, J. M. Dent & Sons, Ltd, 1992.

[3] D. C. Wu and W. H. Tsai. A steganographic method for images by pixel value differencing. *Pattern Recognition Letters*, 24:1613–1626, 2003.

[4] W. N. Lie and L. C. Chang. Data hiding in images with adaptive number of least significant bits based on the human visual system. *Proc. ICIP '99,1:286–290, 1999.*

[5] Joshua R. Smith and Chris Dodge Developments in Steganography. Proceedings of the Third International Workshop on Information Hiding Pages: 77 – 87, 1999.

[6] W. Stallings. *Cryptography and Network Security – principles and practices*. Pearson Education, Inc., 2003.

[7] C. Cachin, "An Information-Theoretic Model for Steganography", Proceedings of 2nd Workshops on Information Hiding, MIT Laboratory for Computer Science, May 1998

[8] Niels Provo and Peter honeyman university of Michigan, Hide and seek –An introduction to steganography, 2003

[9] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham, Steganography and Digital watermarking, 2004.

[10] Jae-Gil Yu, Eun-Joon Yoon, Sang-Ho Shin and Kee-Young Yoo. *A New Image Steganography Based on 2k Correction and Edge-Detection. ITNG* Proceedings of the Fifth International Conference on Information Technology: New Generations Pages 563-568, 2008.

[11] Y. H. Yu, C. C. Chang and Y. C. Hu, *"Hiding Secret Data in Images via Predictive Coding,"* Pattern Recognition, vol. 38, pp. 691-705, 2005.

[12] Y.R. Park, H.H. Kang, S.U. Shin and K.R. Kwon, *"A Steganographic Scheme in Digital Images Using Information of Neighbouring Pixels,"* In International Conference on Natural Computation, pp. 962-967, 2005.

[13] H.C. Wu, N.I. Wu, C.S. Tsai and M.S. Hwang, *"Image steganographic scheme based on pixel-value differencing and LSB replacement methods,"* IEE Proc. Vision Image Signal Process, vol. 152, pp. 611-615, 2005.

[14] C. S. Chan, C. C. Chang and Y. C. Hu , "Image Hiding Scheme Using Modulus Function and Optimal Substitution Table," Pattern Recognition and Image Analysis, vol. 16, pp. 208-217, 2006.

[15] S .K. Moon and R.S. Kawitkar, *"Data Security using Data Hiding,"* International Conference on Computational Intelligence and Multimedia Applications, vol. 4, pp. 247-251, 2007.

[16] C.Y. Yang, *"Color Image Steganography based on Module Substitutions,"* In Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, vol. 2, pp.118-121, 2007.

[17] H.V. Singh, S.P. Singh and A. Mohan, *"A New Robust Method of Hiding Text Characters for Secure Open Channel Transmission,"* International Journal of Computer Science and Network Security, vol. 7 (7), pp. 31-36, July 2007.

[18] Nameer N. EL-Emam, *"Hiding a Large Amount of Data with High Security Using Steganography Algorithm,"* Journal of Computer Science, vol. 3 (4), pp. 223-232, 2007.

[19] S.G.K.D.N. Samaratunge, *"New Steganography Technique for Palette Based Images,"* In Second International Conference on Industrial and Information Systems, pp. 335-340, Aug. 8 – 11, 2007.

[20] J. He, S. Tang and T. Wu, *"An Adaptive Image Steganography Based on Depth-Varying Embedding,"* In Congress on Image and Signal Processing, vol. 5, pp. 660-663, 27-30 May 2008.

[21] J.G. Yu, E.J. Yoon, S.H. Shin and K.Y. Yoo, *"A New Image Steganography Based on 2k Correction and Edge-Detection,"* In Fifth International Conference on Information Technology: New Generations, pp. 563-568, 2008.

[22] E. Hecht, Optics, 2nd Ed, Addison Wesley, 1987.

[23] V. Vijayalakshmi, G. Zayaraz, and V. Nagaraj" Modulo Based LSB Steganography Method 2009"

[24] Piyush Marwah1, Paresh Marwaha, Infosys Technologies Limited, India" Visual Cryptographic Steganography In Images 2010".

[25] Subba Rao Y.V, Brahmananda Rao S.S y, Rukma Rekha N*" Secure Image Steganography based on Randomized Sequence of Cipher Bits 2011".*

[26] Rig Das, Themrichon Tuithung*" A Novel Steganography Method for Image Based on Huffman Encoding 2012".*

[27] Chunfang Yang, Fenlin Liu, Xiangyang Luo, and YingZeng"Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography"2013.