International Journal of Advances in Image Processing Techniques
Volume 3 : Issue 2 *[ISSN 2372-3998]*
Publication Date : 31 August, 2016

Hiding binary image in a grayscale image using Pixel Matching and Randomization Technique

M.G.Gouthamanaath and Dr. A.Kangaiammal

Abstract - This paper proposes a method of hiding the binary image in a grayscale image. Random numbers could be used to shuffle the binary values of an image. Invert is an operation that complements 0s and 1s of binary image. Pixel matching is a technique that could be used to is also used to extract the binary bits and compare the stego-image with original image. This work aims to generate random numbers with less detectability as well as higher embedding capacity through inverting the binary image. Experiments are made among open source grayscale images and the results with higher Peak Signal Noise Ratio (PSNR) and good visual quality in images obtained.

Keywords – Invert, Pixel matching, Pseudo random number generator, Embedding capacity, grayscale image, Peak Signal Noise Ratio.

I. INTRODUCTION

It is necessary to hide the existence of secret information, instead of changing the format leads to steganography methods. In digital world, steganography plays a key role in secret communication. Text, image, audio and video are the primary carriers in steganography to cart the secret information [4]. Steganography classified into two domains. Spatial domain which inserts the secret data bits in pixel values, whereas in transform domain, transform coefficients are modified to hide the secret information. Spatial domain methods are known for less complexity in its implementation as well as high embedding capacity [1]. Pixel matching reduces the complexity over the structure of the code and fast retrieval of secret information in destination [7].

II. RELATED WORK

A. Pixel matching methods

1. Run length encoding & matrix methods

To overcome the limit in increasing embedding capacity with uncompressed secret information, run length encoding is introduced to decrease the size of the embedding information which leads to high embedding capacity [15].

Dr. A. Kangaiammal
Assistant Professor of Computer Applications,
Government Arts College (Autonomous), Salem -7.

M.G. Gouthamanaath, Full-time Research Scholar
Government Arts College(Autonomous), Salem -7.,

Instead of using single encoding scheme for embedding secret information, in proposed work, two encoding methods introduced. Matrix encoding method for decreasing the secret bits and single digit sum encoding method to find the recurrence relation between the pixel values [2].

2. Genetic algorithm with pixel matching

To obtain second order statistics and tuning vector with optimum values, the genetic algorithm has been introduced in their recommended approach [5]. To find the optimal solution in LSB matching revisited method bipolar system is suggested instead of binary function. The probability of detection of secret information has been reduced in this method [11].

3. Methods with predictive approaches

Improving the pixel matching against correlation attacks on steganography, a method introduced with information table to increase and decrease the pixel values based on the average amount of change made in pixels and also ensures there is no sharp difference between the values of modification among those pixels [19]. To embed large amount of information in an image, less than half of the data bits are embedded and the remaining data will be predicted in destination side. The presence of errors is the limitation of this work. The errors were being reconstructed by noise filters [6].

4. Methods with randomization of bits

After randomization of bits, the values are embedded by adding or subtracting the bits in pixel values [7]. Statistical imperceptibility of the existing methods is resolved by introducing sum and difference covering set [18]. Instead of modifying one pixel, pair of pixels is modified and the correlation between those values will not affect when they are statistically attacked [8]. Remapping of data makes the data retrieval tedious for the intruder who needs to decrypt the secret information [13]. Character value indexing and individual character boundary indexing was introduced with novel randomization algorithm proposed with higher PSNR rate [9]. Pixel Value differencing is combined with pixel indicator technique

in addition to randomization of secret values to get higher PSNR rate has been proposed [10].

B. LSB matching revisited methods

By adding and subtracting the pixel values of cover image by one is the key concept, which leads to high embedding capacity [7]. Avoiding smooth surfaces but choosing the sharp surfaces will ensure more security as a key work in edge adaptive steganography has been proposed with LSB matching revisited (EALSBMR) [17]. Finding the edges with Sobel edge detection algorithm for reducing the difference between cover-image and stego-image is proposed as Sobel edge detection LSBMR (SELSBMR) [20].

C. Algorithm for randomization

True random number generators are always powerful and the unpredictability ratio is higher than the pseudo random number generators, which generates the series through the key values [12]. In order to achieve pseudo random number generator which is as powerful as true random number generator, a new algorithm was proposed. Where cyclic action of random number series is appended by eliminating the reoccurring numbers and finally reaches a unique pseudo random number series and thereby decreasing the probability of detection [9].

III. Proposed Approach

In this proposed algorithm, binary image is embedded into grayscale image with randomization concept and pixel matching technique. If logical 1s in the binary image are higher than the logical 0s then the image is inverted and embedded into a grayscale image based on random number series. Instead of using single random number series, multiple series are generated and combined to form the powerful random number series that rearranges the bits of binary images and embeds in the grayscale image. During extraction at the receiving end, the reverse of above strategy is applied for binary image extraction from the grayscale image. Comparing stego-image with grayscale image the difference is formed as a logical matrix and then rearranged as binary image.

A. Proposed Embedding algorithm

1. Read the binary image and calculate the resolution by m*n (m is height and n is width).
2. Find the number of 1s and 0s in the binary image values

$$\sum_{i=1}^{res}\begin{bmatrix}\mathcal{IF}\ bi(i\equiv 1) & \therefore\ ne=ne+1\\ \mathcal{IF}\ bi(i\equiv 0) & \therefore\ ze=ze+1\end{bmatrix}-(1)$$

$$where\ 1\le i\le res$$

Where ne represents 1, ze represents 0, res represents resolution and bi characterizes binary image.

3. Number of pixels holding the logical 1s are greater than pixels which holds zero, then invert it.

$$\sum_{i=1}^{res}[\mathcal{IF}\ ne>ze\quad n(i)=1-n(i)]\ -(2)$$

$$where\ 1\le i\le res$$

4. Applying pseudo random number generation algorithm [9].

$$\sum_{i=1}^{res}[randy(i)]-\ (3)$$

$$where\ 1\le i\le res$$

Randy represents a random number series by combining several series which is generated through seed series together to form a unique series.

5. Rearrange the logical values by the random number series. By combining the results of equations (2) and (3) equation (4) is formed.

$$\sum_{i=1}^{res}\Big(npv(i)=pv\big(randy(i)\big)\Big)-\ (4)$$
$$where\ 1\le i\le res$$

pv represents unmodified binary image and npv represents modified binary image.

6. Embed the secret data bits among the pixel values of grayscale image.

$$\sum_{i=1}^{res}\begin{bmatrix}\mathcal{IF}\ g(i)\equiv 255\\ \therefore\ g(i)=g(i)-npv(i)\\ \mathcal{IF}\ g(i)\ \neq 255\\ \therefore\ g(i)=g(i)+npv(i)\end{bmatrix}-(5)$$

$$where\ 1\le i\le res$$

g represents the grayscale image and the values of it is decreased by the values of npv values in g written as a stego-image.

B. Proposed Extraction Algorithm

1. Compare the stego-image with original image in the database and store the difference in the loop

$$\sum_{i=1}^{res}\begin{bmatrix}\mathcal{IF}\ sg(i)\neq g(i)\ \therefore sbi(i)=1\\ sg(i)\equiv g(i)\ \therefore sbi(i)\ =0\end{bmatrix}-(6)$$

$$where\ 1 \le i \le res$$

sg represents stego-image, g represents original image and sbi represents rearranged binary image.

2. Generate pseudo random numbers through PRNG algorithm [9]

$$\sum_{i=1}^{res} [randy(i)] - \quad (7)$$

$$where\ 1 \le i \le res$$

3. Extract the secret information from stego-image as equation (8) using (6) and (7)

$$\sum_{i=1}^{res} \begin{bmatrix} k = randy(i); \\ bi(k) = sbi(i); \end{bmatrix} - \quad (8)$$

$$where\ 1 \le i \le res$$

k represents a value of the random number series and bi represents the binary image.

4. To change the binary image into its original form inverts it again using equation (9).

$$\sum_{i=1}^{res} [\mathcal{IF}\ ne < ze \quad n(i) = 1 - n(i)] - (9)$$

$$where\ 1 \le i \le res$$

Original image is successfully extracted from stego-image.

IV. Experiments and Results

A. Visual Quality and Embedding Capacity

Experiments are made on open source images [15]. Images with different resolutions are chosen for finding the Means Square Error (MSE) and PSNR value for proofing improved embedding capacity and good visual quality of the proposed method. The results are shown in Table 1 for eight images for seven different resolutions. The secret image is randomly chosen and embedded into cover images. The proposed work produces greater PSNR values than existing methods as shown in Figure 1. By embedding different capacity of secret image the PSNR rate varies as shown in Table 2. Difference between the two images is represented with binary numbers and produces the bit error ratio.

B. Visual Attacks

Existing methods are implemented with embedding among sharper regions rather than softer regions. It is easily detectable by edge adaptive steganalysis methods. B-Spline fitting method has been proposed with steganalysis that detects through the edge adaptive steganography methods [14].

C. Statistical Attacks

A channel is suspected to be a pathway to stego-images, then this channel is targeted and the images are statistically tested and a correlation study is carried out between the pixels to detect the secret information. Daniel Lerch's method proposed for detection of secret information through pattern-analysis which has got high impact over the methods, that uses unique unprocessed pseudo random numbers [3].

Distinctively, in this proposed work, several random series are generated through a seed series that will make detection process hard to complete. The secret information is added as noise instead of embedding in sharper regions. This method has resistance against histogram attacks as depicted in Figure 1.

D. Comparison between the Existing Methods

The proposed work has been compared with the existing steganography methods such as LSBMR, EASSBMR, SELSBMR and MPMS. In LSB matching steganography the embedding capacity of the cover image has been highly improved. The PSNR rate of all the methods are as shown in Table 3. It is observed that the PSNR of the proposed method is higher than the other existing methods. Furthermore, it is unstated that the proposed approach has overwhelming performance at various hiding capacities. It infers that this approach performs better in overall. Graphical representation of performance in terms of PSNR rate and its histograms are depicted in Figure 2.

TABLE 1. MEAN SQUARE ERROR AND PEAK SIGNAL NOISE RATIO VALUES FOR EIGHT IMAGES WITH SEVEN DIFFERENT RESOLUTIONS

Images		Resolution						
		R1	R2	R3	R4	R5	R6	R7
1	MSE	0.0608	0.0632	0.0898	0.0551	0.0385	0.0405	0.0243
	PSNR	59.97	59.88	58.18	60.39	62.00	61.72	63.84
2	MSE	0.0489	0.0553	0.0022	0.0271	0.0772	0.0720	0.0702
	PSNR	61.23	60.70	74.8056	63.79	59.25	59.55	59.66
3	MSE	0.0293	0.0281	0.0587	0.0992	0.0145	0.0867	0.0240
	PSNR	63.45	63.64	60.44	58.15	66.50	58.74	64.33
4	MSE	0.0196	0.0287	0.0271	0.0691	0.0634	0.0406	0.0441
	PSNR	65.20	63.55	63.72	59.73	60.10	62.04	61.68
5	MSE	0.0250	0.0251	0.0683	0.0725	0.1015	0.0733	0.0722
	PSNR	64.14	64.13	59.78	59.52	58.06	59.48	59.54
6	MSE	0.0941	0.0266	0.0268	0.0179	0.0710	0.1033	0.0903
	PSNR	58.39	63.8830	63.85	65.59	59.61	57.99	58.57
7	MSE	0.0574	0.0645	0.0183	0.0265	0.0278	0.0690	0.0694
	PSNR	60.47	59.9426	65.45	63.82	63.65	59.68	59.70
8	MSE	0.0735	0.0949	0.0721	0.0257	0.0261	0.0259	0.0721
	PSNR	59.45	58.33	59.54	64.02	63.95	63.99	59.54

In Table I, R1-R7 represents various resolutions of the image considered for experiment. The resolutions

are 240x320, 320x200, 352x288, 384x288, 480x320, 640x480 and 800x600.

The open source images 1 to 7 in Table 1 are the images of Apple, Bike, Dragon Fly, Duck, Elephants, Lion, Sunflower and Tulip respectively.

TABLE 2. DIFFERENT EMBEDDING RATES WITH ITS MEAN SQUARE ERROR, PEAK SIGNAL NOISE RATIO AND BIT ERROR FOR 240*320 IMAGES.

Capacity		MSE	PSNR	Bit error
(In %)	In bits			
10	7680	0.0002	83.97	0.0004
20	15360	0.0055	70.69	0.0106
30	23040	0.0094	68.37	0.0183
40	30720	0.0137	66.77	0.0270
50	38400	0.0187	65.43	0.0368
60	46080	0.0240	64.31	0.0480
70	53760	0.0274	63.74	0.0546
80	61440	0.0284	63.59	0.0568
90	69120	0.0289	63.51	0.0578
100	76800	0.0293	63.45	0.0585

TABLE 3. COMPARISON OF OTHER METHODS WITH PSNR VALUES AND EMBEDDING RATE.

Hiding capacity (in bits)	Steganography Techniques	PSNR
8000	**LSBMR**	67.53
	EALSBMR	67.05
	SELSBMR	67.05
	MPMS	71.76
	Proposed work	82.83
16000	**LSBMR**	64.53
	EALSBMR	64.04
	SELSBMR	64.42
	MPMS	67.77
	Proposed work	70.37
24000	**LSMR**	62.77
	EALSMR	62.25
	SELSBMR	62.66
	MPMS	66.98
	Proposed work	68.28
32000	**LSMR**	61.52
	EALSMR	60.99
	SELSBMR	61.38
	MPMS	65.73
	Proposed work	66.55

It is observed that a significant difference of increased PSNR is evinced for the lower hiding capacities and the difference turns closer as the hiding capacity increases. Other methods have varied its PSNR in a non-chronological order. Table 3 and Figure 2 present a clear standing of the proposed approach.

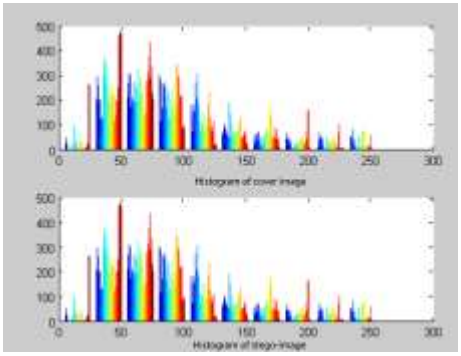

Figure 1. *Comparison of two images by generating its histograms*

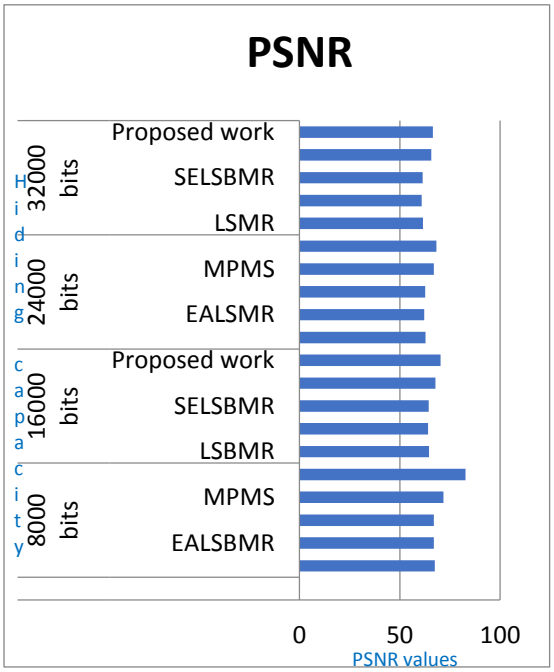

Figure 2. Comparison of other methods with different embedding rate and PSNR values

v. Conclusion and Future Work

In this paper, improvement of embedding capacity and visual quality of the images are highly focused. This two-layered feature makes it hard to detect the secret message behind the grayscale image. Instead of using traditional pseudo random numbers generated series, combined multiple series make it hard to assume the combination. In future, several layers of security can be implemented to enhance this scheme in its prime direction. Further it improves the quality of pseudo random number generation process to achieve high PSNR and security.

References

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc kevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier Signal Processing-2010, pp.727-752.
[2] Arijit Sur, Piyush Goel and Jayantha Mukopadhyay, "A spatial domain steganography scheme for reducing noise", IEEE 2008, pp.1024-1028.
[3] Daniel Lerch-Hostalot and David Megias, "LSB matching steganalysis based on patterns of pixel differences and random embedding", Elsevier 2013, pp.192-206.
[4] Diwedi Samidha and Dipesh Agarwal, "Random image steganography in Spatial domain",IEEE 2013, pp.1-3.
[5] Guangjie Liu, Zhan Zhang, Yuewei Dai and Zhiquan wang, "GA-based LSB-matching steganography to hold second-order statistics", IEEE 2009, pp.510-513.
[6] Huy Nguyen Tien and bac Le, "Noise Reduction Approach for LSB matching revisited",IEEE 2013, pp.76-79.
[7] Jarno Mielikainen, "LSB matching revisited", IEEE Signal processing 2006, pp.285-287.
[8] Ling Xi, Xijian Ping and Tao Zhang, "Improved LSB matching steganography resisting histogram attacks",IEEE 2010, pp. 285-287.
[9] M.G. Gouthamanaath and Dr. A. Kangaiammal, "Multilayered pixel matching steganography using a novel PRNG algorithm and character indexing method", International Journal of Applied Engineering Research 2015, pp.301-307.
[10] M.G. Gouthamanaath and Dr. A. Kangaiammal, "Color Image steganography using combined Pixel value differencing and pixel indicator technique in spatial domain", International Journal of Computer Applications 2015, pp.20-23.
[11] Maryam Mahyabadi, Mahdi Khosravi & Simin Soleymanpour-moghaddam, "Improved pair-wise LSB matching steganography with a new evaluating system",IEEE 2012,pp.982-986.
[12] Roy. S. Wikramaratna, "The centro-invertible matrix: A new type of matrix arising in Pseudo-random number generation", Elsevier 2010, pp.144-151.
[13] Septimiu Fabian Mare, Mirecea Vladutiu and Lucian Prodan, "Decreasing change impact using smart LSB pixel mapping and data rearrangement",IEEE 2011, pp.269-279.
[14] Shunquan Tan and Bin Li, "Targetted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited using B-Spline Fitting",IEEE 2012, pp.336-339.
[15] Tzu-Chuen Lu and Li-Ling Hsu, "The technique of information hiding based on modification function and LSB matching", IEEE 2008, pp.626-631.
[16] Web images accessed from: https://pixabay.com/ accessed on 14-01-2016.
[17] Weiqi Luo, Fangjun Huang and Jiwu Huang, "Edge Adaptive Steganography Based on LSB Matching Revisited",IEEE 2010,pp.201-214.
[18] Xiaolong Li, Tieyong Zeng and Bing Yang, "Improvement of the embedding efficiency of LSB matching by sum and difference covering set", IEEE 2008, pp. 209-212.
[19] Yu Quidong Liu and Xiao-Wei, "A new LSB matching steganographic method based on steganographic information table", IEEE 2009, pp. 360-365.
[20] Zohreh fouroozesh and jihad Al ja'am, "Image Steganography based on LSBMR using Sobel Edge detection", IEEE 2014, pp. 141-145.

About Author(s):

Author-1:

Mr. M.G. Gouthamanaath completed his B.Sc. Computer Science from Periyar University and MCA from Anna University. He is a full-time Computer Science researcher. He has three years of teaching experience. He has published 4 papers in international conferences. His area of interest includes Steganography, Information Security, Mobile Computing.

Author-2:

Dr. A. Kangaiammal received both B.Com. and MCA from Bharathidasan University, Trichy in 1993 and 1996, respectively; M.Phil. (Computer Science) from Manonmaniam Sundaranar University, Tirunelveli in 2001; Ph.D. from University of Madras in 2009 and M.E. Computer Science and Engineering from Salem Vinayaka Missions University in 2010. Her research interest includes E-Learning, Instructional Design and Development, Data and Web Mining, Mobile Computing and Grid Computing. Presently, she is an Assistant Professor of Computer Applications in Government Arts College (Autonomous), Salem-7, Tamil Nadu, India with18+ years of teaching and research experience. She has 12 publications to her credit. She has delivered special lectures for teachers and/or students through FDPs, Conferences, Seminars and Workshops from technical and pedagogical areas.