International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A Steganography Scheme For Information Hiding In higher Gradient Pixel Pairs

Dr. R. R. Dube[1], M.A. Lalkot[2], Dr. R. J. Shelke[3]

[1] *Department of Electronics & Telecommunication, Walchand Institute of Technology, Solapur, Maharashtra, India*

[2] *Department of Electronics, Walchand Institute of Technology, Solapur, Maharashtra, India*

[3] *Department of Electronics, Walchand Institute of Technology, Solapur, Maharashtra, India*

ABSTRACT

The steganography algorithms are most popular in spatial domain. However in most existing algorithms the information used to embed in any region in spatial domain without considering any relationships of the image content. There for some structural asymmetry exists in those images which have smooth regions like sky, even when the size of information is small. There for this leads poor visual quality and low security based on some analysis and extensive experiments. The steganography scheme for information hiding in higher gradient pixel pairs embeds the secret information in the pixel pairs of higher gradient of the images without disturbing the smooth region. Generally the regions located at the pixel pairs of higher gradient present more complicated statistical features and are highly dependent on image contents. So it is more difficult to observe changes at pixel pairs of higher gradient than those pixel pairs of lower gradient. When embedding rate increases remaining pixel pairs of lower gradient can be released for information hiding by changing some parameters. so that it will achieve more embedding capacity also enhances the security as compared to existing approaches such as typical least significant bit based approaches and PVD based methods. The new scheme also improves the visual quality of stego images.

Keywords – Edge Adaptiveness, LSB Matching Revisited, PVD, Spatial Domain, Security

I. INTRODUCTION

In any communication system there is always a risk that anyone is listening the talk. The internet is not different than that, it also faces the same kind of risk. The midpoint attacks are those who are related to third party listening. The aim of the third party is to record all the shared secret information between two computers (client and server) and miss use it. So to avoid that kind of attack we had the concept of encryption and decryption. But today only encryption and decryption is not sufficient, because there are many attackers available who can easily decrypt the secret information.

Today steganography became very popular. Steganography is the art and science of invisible communication. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. The carrier file formats used by steganography are text, images, audio/video and protocol. But amongst those carrier file formats digital images are most popular because of their frequency on internet.

The main steps in this scheme are.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A. Embedding of message

B. Extraction of embedded message

There are many spatial domain steganography algorithms such as LSB based PVD based available but still there are some risks. Whenever the secret message embedded without considering the relationship between image contents the flat and smooth regions get contaminated. The proposed scheme makes the detection hard than the existing approaches. the proposed scheme uses the edge regions of digital image for embedding the secret message while keeping the smooth and flat regions as they are. When embedding rate increases more edge regions can be released for embedding without disturbing the smooth regions. In that way we can achieve high embedding rate.

II. DIFFERENT APPROACHES

A. LSB replacement is a well-known steganography method. In this embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudorandom number generator (PRNG). As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganography algorithms, such as the Chi-squared attack, regular/singular groups (RS) analysis , and sample pair analysis [4] [7].

B. LSB matching (LSBM) employs a minor modification to LSB replacement. If the secret bit does not match the LSB of the cover image, then +1or -1 is randomly added to the corresponding pixel value. Statistically, the probability of increasing or decreasing for each modified pixel value is the same and so the obvious asymmetry artifacts introduced by LSB replacement can be easily avoided. Therefore, the common approaches used to detect LSB replacement are totally ineffective at detecting the LSBM [10].

C. A popular type of steganography algorithms in the spatial domain. However, in most existing approaches, the choice of embedding positions within a cover image mainly depends on a pseudorandom number generator without considering the relationship between the image content itself and the size of the secret message. Thus the smooth/flat regions in the cover images will inevitably be contaminated after data hiding even at a low embedding rate, and this will lead to poor visual quality and low security based on our analysis and extensive experiments, especially for those images with many smooth regions. The LSB matching revisited image steganography with an edge adaptive scheme can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image [8].

D. The PVD is a pixel value differencing method. The basic idea of PVD-based approaches is to first divide the cover image into many no overlapping units with two consecutive pixels and then deal with the embedding unit along a pseudorandom order which is also determined by a PRNG. Larger the difference between two pixels, larger the number of secret bits that can be embedded into the units. To a certain extent, existing PVD-based approaches are edge adaptive since more secret data is embedded in those busy regions [9].

III. PROPOSED METHOD

The proposed scheme uses the sharp edge regions of the grayscale images. For detecting the sharp edges in the grayscale images all the pixels are divided in the groups. Each group consists of two pixels. Then the pixel pairs

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

of higher gradient are selected, for that a threshold value is calculated. Threshold value defines the difference between two consecutive pixels. When the threshold value T is calculated the no. of pixel pairs are selected according to that threshold value. The threshold value depends on the size of secret message. If the size of secret message changes, the threshold is set such that edges are sufficient to embed message M. After edge detection for message M the secret bits are embedded in least significant bits of even odd pixels.

A. Data embedding

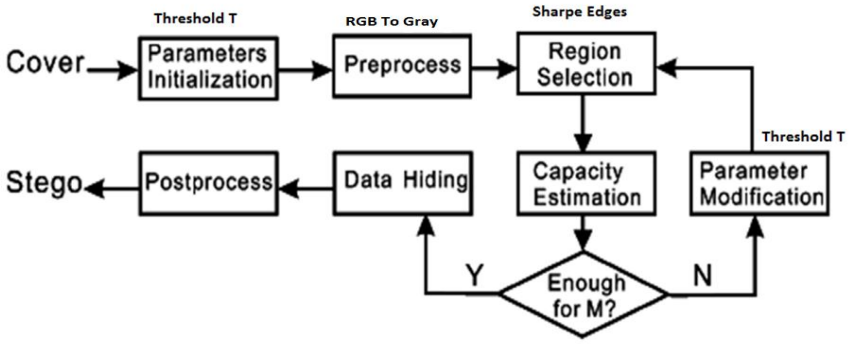

Figure 1: Data embedding

The figure 1 shows the flow diagram of proposed scheme. The scheme first initializes some parameters which are used for image processing, capacity estimation and region selection for the given image. The image is divided into non overlapping embedding units. So that a new image will form. Then the sharp edges are detected by initializing the threshold value. Then the capacity is estimated for given message. If the capacity is not enough for embedding the data, the threshold value T is changed until edges are enough to embed all the data. Then the data embedding is done. After data embedding some post process are done on the image.

B. Data extraction

Figure 2: Data extraction

The fig 2 shows the flow diagram for data extraction. The scheme first extracts some parameters from the stego. Based on these parameters the embedding positions can be identified. Then the data is extracted completely.

IV. DATA EMBEDDING AND DATA EXTRACTION ALGORITHM

A. Data Embedding

1. Convert the color image in gray scale image.

2. The image is divided into non overlapping embedding units with every consecutive pixels (x_i, x_{i+1}), where $i = 1,3,....mn-1.$

3. For given message M, the threshold T for region selection is determined as,

$$T = \{2 \times |EU(t)| \geq |M|\}$$

Where $EU(t) =$ set of pixel pairs whose differences are greater than or equal t.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

$|M|$ = size of secret message.

4. Performing data hiding according to the following four cases.

Case 1: $LSB(x_i) = m_i \;\&\; f(x_i, x_{i+1}) = m_{i+1}$

$$(x_i', x_{i+1}') = (x_i, x_{i+1});$$

Case 2: $LSB(x_i) = m_i \;\&\; f(x_i, x_{i+1}) \neq m_{i+1}$

$$(x_i', x_{i+1}') = (x_i, x_{i+1} + r);$$

Case 3: $LSB(x_i) \neq m_i \;\&\; f(x_i - 1, x_{i+1}) = m_{i+1}$

$$(x_i', x_{i+1}') = (x_i - 1, x_{i+1});$$

Case 4: $LSB(x_i) \neq m_i \;\&\; f(x_i - 1, x_{i+1}) \neq m_{i+1}$

$$(x_i', x_{i+1}') = (x_i + 1, x_{i+1});$$

Where $f(x_i, x_{i+1}) = LSB(\lfloor x_i/2 \rfloor + x_{i+1})$

$$f(x_i - 1, x_{i+1}) = LSB(\lfloor x_i - 1/2 \rfloor + x_{i+1})$$

$$r = \pm 1$$

m_i And m_{i+1} denotes two secret bits to be embedded, (x_i, x_{i+1}) denotes pixel pair to be embedded, (x_i', x_{i+1}') denotes pixel pair after embedding.

5. Then the parameter T embedded into a preset region which has not been used for data hiding

B. Data Extraction

1. First the side information T is extracted from stego.

2. The image is divided into non overlapping embedding units with every consecutive pixels (x_i, x_{i+1}), where $i = 1,3,....mn-1$

3. Region identification is done according to threshold value T. Those pixel pairs whose absolute difference value is greater than or equals to T those pixel pairs will be selected for extraction. Extraction is done according to formulas,

$$w_i = LSB(x_i')$$

$$w_{i+1} = LSB(\lfloor x_i'/2 \rfloor + x_{i+1}')$$

Where w_i and w_{i+1} are secret bits after extraction.

V. RESULTS AND DISCUSSIONS

A. Mean Square Error (MSE)

The mean square error can be calculated according to given formula,

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} [I(x,y) - I'(x,y)]^2$$

The following are the results for mean square error for different methods and for different embedding rates,

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

Embedding Rate	MSE-Image-Buildings (400×400)		
	AE-LSB	LSB	PROPOSED
10%	1.9211	0.048406	0.020763
20%	2.7981	0.0901	0.042188
30%	3.8022	0.13049	0.063525
40%	4.7121	0.16461	0.083994
50%	5.35	0.19638	0.10728

Table 1:MSE values for different method

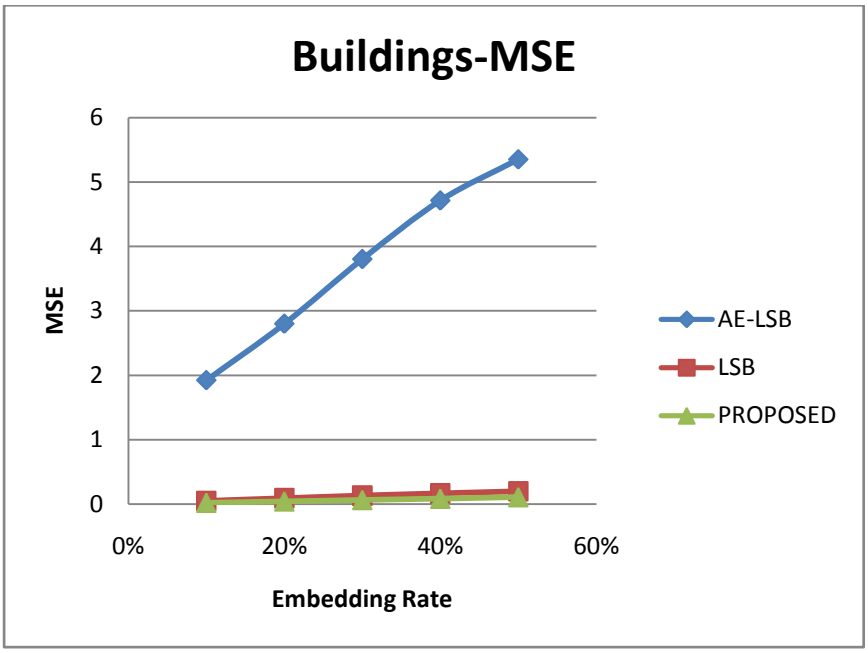

Figure 3: the graph embedding vs. Mean Square Error

The above result shows the purposed method has low mean square error values as compared to other methods.

B.PSNR (Peak signals to noise ratio)

The PSNR can be calculated according to given formula,

$$PSNR = 20 * \log 10(255/sqrt(MSE))$$

The following are the results for PSNR for different methods and for different embedding rates,

Embedding Rate	PSNR-Image-Buildings (400×400)		
	AE-LSB	LSB	PROPOSED
10%	45.2952	61.2818	64.958
20%	43.6622	58.5836	61.879
30%	42.3304	56.9749	60.1014

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

40%	41.3987	55.9662	58.8883
50%	40.8473	55.1998	57.8256

Table 2: PSNR values for different methods

The above result is for PSNR value the PSNR value defines a quality of image. The value for the PSNR is depends on the value of mean square error. When mean square error decreases PSNR value improves. When original image and stego image are identical then mean square error is zero hence the value of PSNR is infinite. The above table 2 shows values for PSNR. Proposed method has improved values as compared to other methods. And the following figure 4 shows graph for embedding rate vs. PSNR.

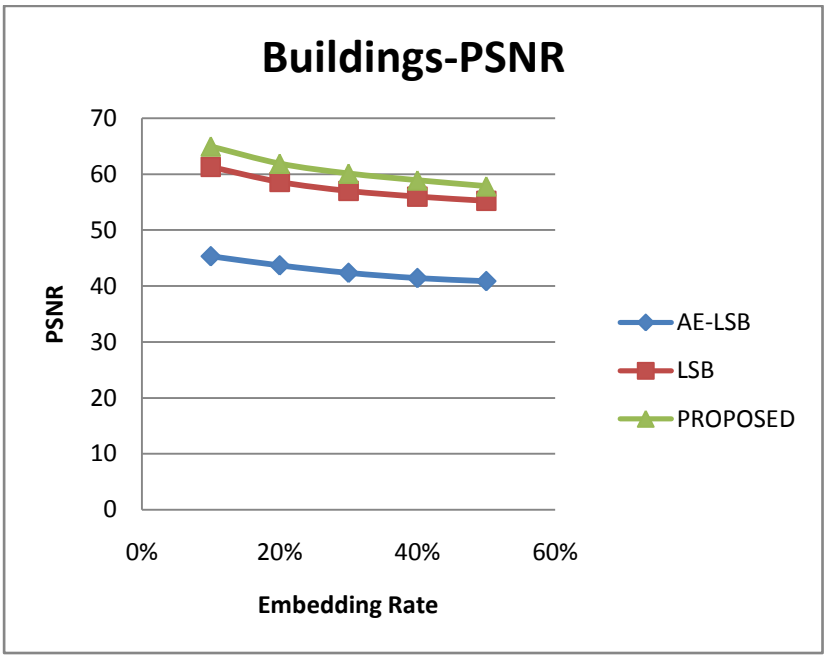

Figure 4: Graph for PSNR embedding rate vs. PSNR

The figure 4 shows graph for PSNR value for different methods.

C .WPSNR (Weight PSNR)

The PSNR can be calculated according to given formula,

$$WPSNR = 10 * \log 10 \frac{\max(x)^2}{\|NVF(x'-x)\|^2}$$

The following are the results for WPSNR for different methods and for different embedding rates,

Embedding Rate	WPSNR-Image-Buildings (400×400)		
	AE-LSB	LSB	PROPOSED
10%	35.2815	75.086	77.0064
20%	31.8949	71.5226	73.9641
30%	29.4737	69.1768	72.1169
40%	28.1813	67.6801	70.8109
50%	27.51	66.4688	69.6932

Table 3: WPSNR values for different methods

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

The difference between the PSNR and WPSNR is that the WPSNR is unlike the PSNR. The PSNR value is independent of the positions of embedding and the WPSNR is depends on the positions of embedding in the image. The weighting for changes in higher gradient pixel pairs is low than the weighting for changes in the lower gradient pixel pairs. When the information is embedded in higher gradient pixel pairs then the value of WPSNR will improve. When the information is embedded in lower gradient pixel pairs then value of WPSNR will decrease. The above table shows values for WPSNR. It is observed that the values for WPSNR are improved for proposed method as compared to other method.

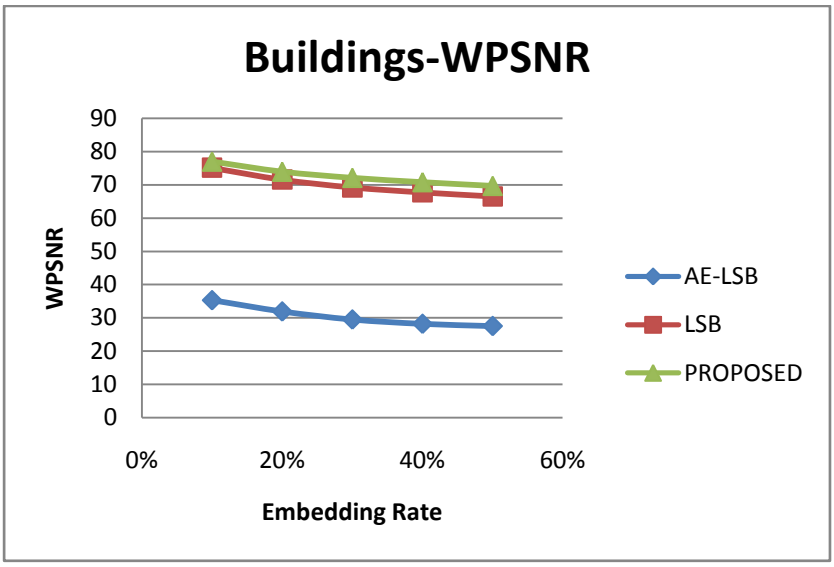

Figure 5: graph for WPSNR for different methods

VI. CONCLUSION

There usually exist some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the LSB of stego images becomes more random, and according to analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. To preserve the statistical and visual features in cover images, the proposed novel scheme which first embeds the secret message into the higher gradient pixel pairs adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. The experimental results shows that both visual quality and security of stego images are improved significantly compared to other existing methods.

REFERENCES

[1] Akhil P. V., Akbersha K. E. ‘ Pixel Pair Matching’ (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727 Volume 16, Issue 1, Ver. IV PP 76-80 (Jan. 2014).

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[2] Dr. Madhu Sandilya, Dr. Meenu Chawla, 'Spatial Domain Image Steganography based on Security and Randomization' (IJACSA) Vol. 5, No. 1, 2014.

[3] Saiful Islam, Mangat R. Modi and Phalguni Gupta, 'Edge-based image steganography' EURASIP Journal on Information Security 2014.

[4] Mamta Juneja, Parvinder Singh Sandhu, 'Improved LSB based Steganography echniques for Color Images in Spatial Domain' International Journal of Network Security, Vol.16, No.4, PP.366-376, July 2014.

[5] Arvind Kumar, Km. Pooja, 'Steganography- A Data Hiding Technique' International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010.

[6] Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, 'Edge Adaptive Image Steganography Based on LSB Matching Revisited' IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2, JUNE 2010.

[7] Shailender Gupta, Ankur Goyal, 'Information Hiding Using Least Significant Bit Steganography and Cryptography'I.J.Modern Education and Computer Science, 2012.

[8] Unik Lokhande, A. K. Gulve, 'Steganography using Cryptography and Pseudo Random Numbers' International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014.

[9] J. K. Mandal and Debashis Das, 'Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain' International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[10] Guangjie Liu, Zhan Zhang and Yuewei Dai, ' Improved LSB-matching Steganography for Preserving Second-order Statistics, JOURNAL OF MULTIMEDIA, VOL. 5, PAGE NO. 5, OCTOBER 2010.