International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Improved Edge Based Steganography Scheme for GrayScale Images in Spatial Domain

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

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

[2] Department of Electronics, Walchand Institute of Technology, Sholapur, 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 improved edge based steganography scheme embeds the secret information in the edge regions of the images without disturbing the smooth region. Generally the regions located at the shaper edges present more complicated statistical features and are highly dependent on image contents. So it is more difficult to observe changes at sharper edges than those in smooth regions. When embedding rate increases remaining edge regions 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: LSB-based steganography, PVD

1. 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.

To avoid the internet fraud the encryption and decryption are being done along with steganography. The main steps in this system are.

1) Encryption of secret message
2) Embedding of encrypted message
3) Extraction of encrypted message
4) Decryption of encrypted 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.

2. 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) PVD

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. The larger the difference between the two pixels, the 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].

3. Proposed Scheme

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 pairs having more difference value are selected, for that a threshold value is set. Threshold value defines the difference between two consecutive pixels. When the threshold value T is set all 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

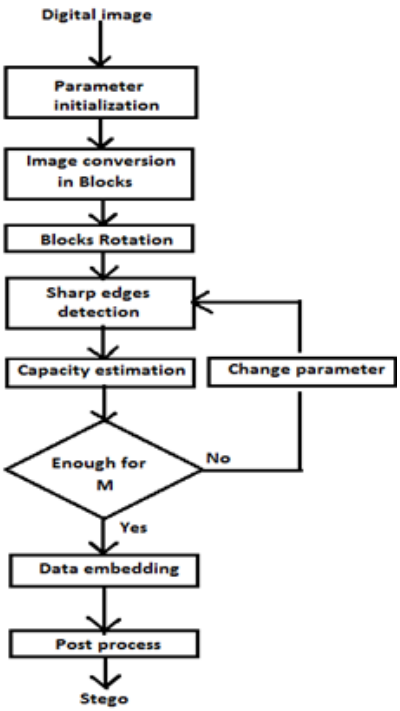

Figure 1: Data embedding process

The fig 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. Then the image is divided in number of blocks. Then the blocks are rotated by random degrees. So that a new image is formed. 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

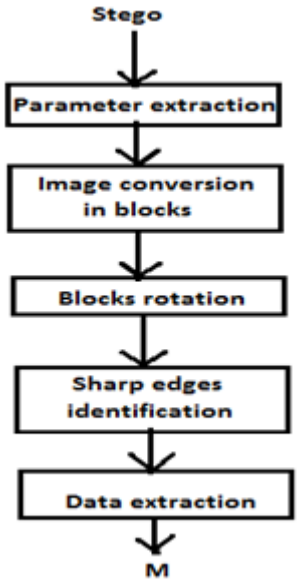

Figure 2: Data extraction process

The fig 2. shows the flow diagram for data extraction. The scheme first extract some parameters from the stego. Based on these parameters the embedding positions can be identified. Then the image is divided in blocks and then blocks are rotated based on parameters. Then the sharp edges are identified. Then the data is extracted completely.

4. Data Embedding and Data Extraction Algorithm

a) Data Embedding

1. Convert the color image in gray scale image.
2. Divide the cover image into non overlapping blocks of Bz*Bz pixels.
3. Each small block, we rotate it by a random degree (0,90,180,270).
4. The resulting image is rearranged as a row vector by raster scanning.
5. The vector is divided into embedding units with every two consecutive pixels (Xi,Xi+1) , where i=(1,3,...,mn-1).
6. Region selection can be determined as follows.

Let EU(t) be the set of pixel pairs whose absolute differences are greater than or equal to a parameter t.

EU(t)={(Xi,Xi+1)| |Xi-Xi+1| >= t, for every (Xi,Xi+1) € V}.

Then we calculate the threshold T by

T=arg max {2 *|EU(t)| >= |M|}.

Where, |M| is the size of the secret message, and |EU(t)| denotes the total number of elements in the set of EU(t).
7. Performing data hiding.
8. we perform the data hiding according to the following four cases.

Case 1: LSB(Xi)=mi & f(Xi,Xi+1)=mi+1
then (Xi',Xi+1')=(Xi,Xi+1)

Case 2: LSB(Xi)=mi & f(Xi,Xi+1)!=mi+1
then (Xi',Xi+1')=(Xi,Xi+1+r) where r=(-1,+1)

Case 3: LSB(Xi)!=mi & f((Xi)-1,Xi+1)=mi+1
then (Xi',Xi+1')=((Xi)-1,Xi+1)

Case 4: LSB(Xi)!=mi & f((Xi)-1,Xi+1)!=mi+1
then (Xi',Xi+1')=((Xi)+1,Xi+1)

where mi and mi+1 denote two secret bits to be embedded.

9. After data hiding, the resulting image is divided into Bz X Bz nonoverlapping blocks. The blocks are then rotated by a random number of degrees . The process is very similar to Step 3 except that the random degrees are opposite. Then we embed the two parameters (T, Bz) into a preset region which has not been used for data hiding.

b) Data Extraction
We first extract the side information, i.e., the block size Bz and the threshold T from the stego image. We then do exactly the same things as Step 1 in data embedding.

The stego image is divided into Bz*Bz blocks and the blocks are then rotated by random degrees.

The resulting image is rearranged as a row vector V. Finally, we get the embedding units by dividing into nonoverlapping blocks with two consecutive pixels. We travel the embedding units whose absolute differences are greater than or equal to the threshold T according to a pseudorandom order ,until all the hidden bits are extracted completely.

5. Results of Proposed Scheme

This section presents some experimental results to show effectiveness of proposed method. The proposed method deals with the gray images of size 512*512 of standard data set obtained from internet.

The proposed scheme uses sharp edges to embed the data by adjusting threshold T. when T is 0 all embedding units will be available for data hiding in this way we can achieve 100% embedding capacity.

The proposed method embeds the secret bits along the edge regions. With the embedding rate less than 35% the smooth regions in the image are more preserved based on human visual system characteristics.

6. Conclusion

In this paper we have proposed an improved edge Based Steganography Scheme to preserve the statistical and visual features in cover images, the proposed novel scheme which first embeds the secret message into the sharper edge regions adaptively according to a threshold determined by the size of the secret message and the gradients of the content edges. Therefore, the subjective quality of stegos would be improved based on the human visual system (HVS) characteristics.

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).
[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.