Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information

Moazzam Hossain, Sadia Al Haque, and Farhana Sharmin
Department of Computer Science and Engineering, International Islamic University, Bangladesh

Abstract: *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Security has always been a major concern since time immemorial. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, digital technology and Internet provide for easy to use cover media for steganography. In order to improve the security by providing the stego image with imperceptible quality, three different steganographic methods for gray level images are presented in this paper. Four neighbors, diagonal neighbors and eight neighbors methods are employed in our scheme. These methods utilize a pixel's dependency on its neighborhood and psycho visual redundancy to ascertain the smooth areas and complicated areas in the image. In smooth areas we embed three bits of secret information. In the complicated areas, variable rate bits are embedded. From the experimental results it is seen that the proposed methods achieve a much higher visual quality as indicated by the high peak signal-to-noise ratio in spite of hiding a larger number of secret bits in the image. In addition, to embed this large amount of secret information, at most only half of the total number of pixels in an image is used. Moreover, extraction of the secret information is independent of original cover image.*

Keywords: *Information security, steganography, data hiding, stego image, cover image.*

Received October 27, 2007; accepted February 11, 2008

1. Introduction

The advent of Internet along with progress made by digital technology gave the world of communication a new dimension. Exchange of digital documents, images, audio and even video via Internet is fast, cheap and simple. This ease of communication brought along with it, problems of security. Digital media are easy to intercept, forge, tamper, copy and distribute illegally. Thus, issues dealing with digital data security and copyright protection are receiving growing attention. Steganography is one such means of achieving security by hiding the data to be communicated within a more innocuous data. The main goal of steganography is higher capacity and security of the confidential message. A typical steganographic system consists of a cover media into which the secret message is embedded. The resultant is called the stego media [6].

So far, many steganographic methods have been proposed [2, 4, 5, 6, 7]. The most common of these is replacing Least Significant Bits (LSB) of the pixels with the secret message. The basic drawback of this method is that all pixels cannot endure same amount of change and hence distortions are more visible. To obtain better visual quality of the stego-image obtained by simple LSB, Chan *et al.* [2] proposed the Optimal Pixel Adjustment Process (OPAP). OPAP is applied on the stego image such that the resulting pixel value is much closer to the original value. Both these methods are non-adaptive. Wu *et al.* [7] have proposed an adaptive method based on inter pixel relationship where the number of secret bits to be embedded is variable. This method greatly enhanced the stego image quality.

In this paper, we proposed three efficient steganographic methods that utilize the neighborhood information to estimate the amount of data to be embedded into an input pixel of cover image without producing perceptible distortions. The neighborhood relationship decides the smooth and complicated areas of an image. Small amount of secret information is embedded into the smooth areas whereas a large amount is embedded into the complicated areas. This is based on psycho visual redundancy in gray scale digital images that edged areas can tolerate greater distortion compared to smooth areas. In our schemes we embed a fixed three bits of information in smooth areas. A variable number of bits are embedded into the edged areas. Though more than half of the total number of pixels of an image is exempted from hiding secret information, where methods discussed in [7] and [8] use almost all the pixels of an image for the same amount of hiding capacity, a significantly higher hiding capacity has been achieved.

2. Proposed Methods

Our proposed methods take advantage of psycho visual redundancy and the dependency of a pixel on its surrounding neighbors. The correlation between a pixel and its neighbors decides whether it is located in smooth area or in complicated area.

2.1. Four Neighbors Method

This method takes into consideration the upper, lower, left and right neighbors of a pixel. The cover image is scanned in a raster scan order considering every second pixel from left to right starting from the second row till the $(N-1)^{th}$ row.

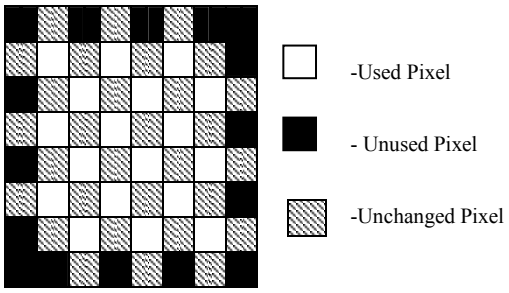

Figure 1. Scanning the cover image for four neighbors method.

In Figure 1, the white pixels represent the pixels into which bits are embedded. The striped pixels remain unchanged. These are the neighbor pixels that decide the amount of secret information to be embedded. The remaining black pixels are unused, that is they do not contribute to the embedding process.

The secret information is a text file. The file is converted into binary prior to the embedding process. The difference value d_i that indicates the smooth or edged region is calculated using the following equation:

$$d_i = (p_{upper} + p_{lower} + p_{left} + p_{right}) /4 - p_i \quad (1)$$

A small value of d_i indicates that the 3x3 region is smooth. When the magnitude of d_i lies between 0-7, the region is considered to be smooth. Only 3 bits of secret data is embedded into pixels that fall in a smooth region. A larger value of d_i implies that our pixel is in an edged or complicated region. Variable rate of secret bits to embed, n, is calculated by

$$n = floor(log_2 |d_i|) \quad (2)$$

n bits of bit stream is extracted from the secret data and converted into its decimal equivalent, say b, and added to lower bound 2^n, to produce new difference value d_i'. d_i' also lies in the same range $[2^n, 2^{n+1} - 1]$ as d_i.

$$d_i' = \begin{cases} 2^n + b, & d_i \text{ is positive} \\ -(2^n + b), & \text{otherwise} \end{cases} \quad (3)$$

Sometimes, the new value of pixel p_i may fall off the boundary of the range [0, 255]. In those cases, the falling off boundary condition for the embedding process is verified as in ref [7]. If a pixel satisfies the condition then it is not used for embedding. Two cases for deciding whether a pixel is in a falling off boundary condition are:

- Case 1: if $d_i >= 8$ and $((p_{upper} + p_{lower} + p_{left} + p_{right})/4) < 2^{n+1} - 1)$, then $p_i = p_i$.
- Case 2: if $d_i < 8$ and $((p_{upper} + p_{lower} + p_{left} + p_{right})/4 + 2^{n+1}) > 256$, then the corresponding stego pixel is the same as the original value.

The corresponding pixel value of the stego image p_i' is then calculated as

$$p_i' = (p_{upper} + p_{lower} + p_{left} + p_{right}) /4 - d_i' \quad (4)$$

Extraction is the reverse of the embedding. The difference value d_i^* is calculated for every white pixel using equation 1. Based on d_i^* the secret information b is obtained.

$$b = \begin{cases} d_i^* - 2^n, & d_i^* \text{ is positive} \\ -(2^n + d_i^*), & \text{otherwise} \end{cases} \quad (5)$$

b is converted into its binary representation which consists of n bits. The falling off boundary condition is also considered to decide whether the pixel contains secret information or not.

2.2. Diagonal Neighbors Method

This method determines the smooth and edged areas in the cover image based on a pixels relationship with its diagonal neighbors.

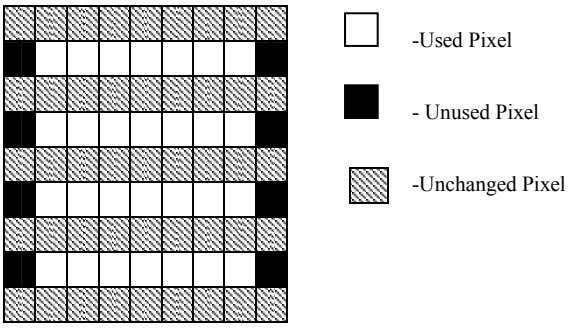

Figure 2. Scanning the cover image for diagonal neighbors method.

The embedding and extraction steps are similar to the Four Neighbors Method. However, the difference value d_i is given as

$$d_i = (p_{upper\text{-}left} + p_{upper\text{-}right} + p_{lower\text{-}left} + p_{lower\text{-}right}) /4 - p_i \quad (6)$$

As in the previous method, three bits of secret information are embedded into the smooth areas and n bits are embedded into the edged areas. Fall off boundary conditions are modified for diagonal neighbors such that a pixel is used for embedding or exempted based on the average of diagonal neighbors.

2.3. Eight Neighbors Method

As the name implies, this method makes use all the eight neighbors of a pixel in a 3x3 region. Hence the smooth and edged areas are much more accurate than the previous two methods. This method results in a stego image with imperceptible quality.

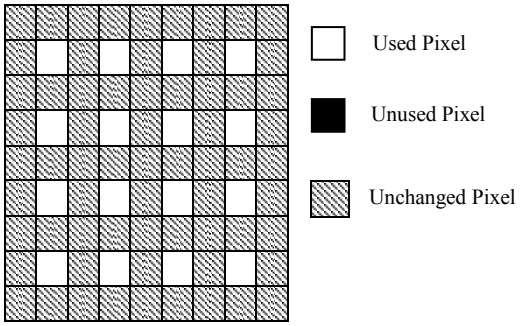

Figure 3. Scanning the cover image for eight neighbors method.

The value of d_i is given by the following equation

$$d_i = (p_{upper} + p_{lower} + p_{left} + p_{right} + p_{upper\text{-}left} + p_{upper\text{-}right} + p_{lower\text{-}left} + p_{lower\text{-}right}) /8 - p_i \quad (7)$$

The remaining steps for embedding are the same as the previous two methods. The fall off boundary condition takes all eight neighbors into consideration. The extraction steps are the same as discussed in the first method except that eight neighbor pixel values are used.

3. Experimental Results and Discussions

In this section, we present the experiments carried out to justify our proposal and discuss the corresponding experimental results along with the future extension of our proposal.

3.1. Experimental Results

Some standard 512 X 512 gray scale images are used as the cover image. A secret message is created to be hidden in the images. We have used the Peak Signal-to-Noise Ratio (PSNR) to measure the quality of the stego images. The larger the PSNR value the smaller the possibility of visual attack by human eye [8].

In Figure 4, four of the standard gray scale images, named Lena, Baboon, Peppers and Tank have been shown. These images can exhibit us how the amount of smooth regions and complicated regions in an image influences the embedding capacity and PSNR. It is seen from Figure 5 that the distortions take place in the stego images due to embedding a large amount of secret message using four neighbors method, are unrevealed to human eye. In addition, the image Baboon is comparatively more complicated than the image Lena because it contains more edge areas where the gray scale variation is very frequent. Thus it has a greater embedding capacity than that of the image Lena.

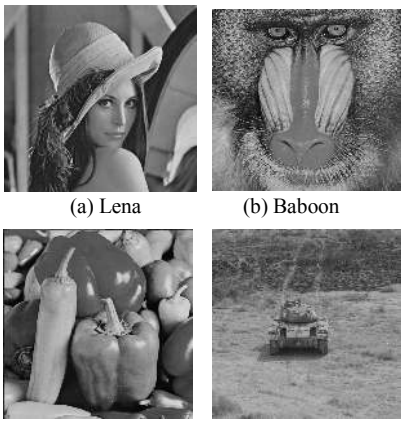

Figure 4. Original cover images.

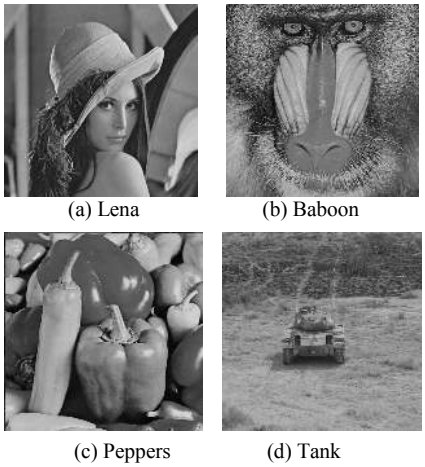

Figure 5. Stego images resulted from four neighbors method.

The data displayed in Table 1 have the same opinion about what discussed in the previous paragraph.

Table 1. The experimental results for the proposed four neighbors method.

Images	Maximum Hiding Capacity (in bits)	PSNR (in dB)
Lena	392208	41.1468
Baboon	435223	36.5154
Peppers	393567	41.0449
Tank	395405	40.7986

Table 2. The experimental results for the proposed diagonal neighbors method.

Images	Maximum Hiding Capacity (in bits)	PSNR (in dB)
Lena	395680	40.6504
Baboon	443165	35.0725
Peppers	395213	40.5709
Tank	405507	39.5107

Tables 2 and 3 illustrate the experimental results for diagonal neighbors method and eight neighbors method respectively.

Table 3. The experimental results for the proposed eight neighbors method.

Images	Maximum Hiding Capacity (in bits)	PSNR (in dB)
Lena	196968	43.9590
Baboon	220575	38.8280
Peppers	197379	43.7135
Tank	199729	43.3911

Moreover, the proposed methods use less than half of the total number of pixels in an image where methods discussed in [7] and [8] use almost all the pixels of an image for the same amount of hiding capacity. For instance, four neighbors method uses only 130048 pixels of the image Lena to hide 392208 secret bits. And in case of the image Baboon, the number of pixels used to embed 435223 secret bits is 129488. It can be added that, the total number of pixels in a 512x512 gray scale image is 262144.

3.2. Discussions

All three proposed methods implemented the adaptive method of steganography, that is, the amount of secret bits to hide is variable. Thus, the quality of stego images is progressively improved.

The first method is four neighbors method, which can hide a large number of secret bits in digital images and can maintain a very good PSNR. The second method, diagonal neighbors method, can hide more bits than four neighbors method. However this is accomplished by sacrificing the PSNR. The PSNR values are slightly less than in four neighbors method, but are still good. In diagonal neighbors Method, the maximum capacity for the same image is much more than in the four neighbors method. The reason is that, pixels are more related to its four neighbors, difference is not so larger and thus they are closed. The difference between the pixel and its diagonal neighbors is slightly larger and so it can hide more bits. The third method that we proposed for steganography is eight neighbors method, where a large number of pixels remain unchanged, but hiding a considerable amount of secret data.

As future works, our secret information can first be encrypted by using any standard encryption algorithm and then embedded. In this way we provide an extra layer of security to our systems. Moreover, unused pixels can be used for embedding. LSB substitution may be used as the method for embedding bits of secret information into the unused pixels. Combining LSB method with our proposed scheme may lead to increased data hiding capacity.

4. Conclusions

We have proposed three novel and efficient steganographic methods to embed secret information into images without producing perceptible distortions. The methods do not require referencing the original image when extracting the embedded data from a stego-image. The method utilizes the neighborhood information to estimate the amount of data that can be embedded into an input pixel of cover image. The pixels in edge areas may embed more data than those in non-edge areas.

Our experimental results have shown that the proposed method provides an efficient way for embedding large amount data into cover images without making noticeable distortions. Moreover, the proposed methods use less than half of the total number of pixels in an image where methods discussed in [7] and [8] use almost all the pixels of an image for the same amount of hiding capacity.

However, the secret message can be distorted if the stego image is changed en route. Introducing flags for detection of any kind of manipulation such as change of a bit due to transmission errors or intruders or image processing operations such as cropping and rotation, can help detect whether the stego image contains the exact information or not. This flag may be a bit in the unused pixels or can be included in the image header.

References

[1] Buchanan M., "Creating a robust form of Steganography," http://etd.wfu.edu/theses/availab le /etd05092004110852/ unrestricted/ Buchanan_ STEM04.pdf, 2006.

[2] Chan K. and Cheng M., "Hiding Data in Images by Simple LSB Substitution," *Computer Journal of Pattern Recognition Letters*, vol. 37, no. 3, pp. 469-474, 2004.

[3] Chang C. and Tseng W., "A Stegangraphic Method for Digital Images Using Side Match," *Computer Journal of Pattern Recognition Letters*, vol. 25, no. 5, pp. 1431-1437, 2004.

[4] Morkel T., Eloff J., and Olivier S., "An Overview of Image Steganography," http://mo.co.za/open /stegoverview.pdf, 2006.

[5] Provos N. and Honeyman P., "Hide and Seek an Introduction to Steganography," http://niels .xtdnet.nl/papers/practical.pdf, 2006.

[6] Sellars D., "An Introduction to Steganography," http ://www. totse.com /en/privacy/ encryption/ 163947. html, 2006.

[7] Wu C. and Tsai H., "A Steganographic Method for Images Using Pixel Value Differencing," *Computer Journal of Pattern Recognition Letters*, vol. 24, no. 6, pp. 1613-1626, 2003.

[8] Wu I., "A Study on Data Hiding for Gray Level and Binary Images," http:// ethesys. lib.cyut .edu. tw/ ETD-db /ETD-search /getfile? URN=etd-0707104- 144705& filename = etd-0707104-144705.pdf, 2006.

Moazzam Hossain received his BSc in computer science and engineering from International Islamic University, Bangladesh and MSc in computer systems engineering from Technical University of Denmark. He was a member of system security group, informatics and mathematical modeling, Technical University of Denmark. His research interests include computer and data security, artificial intelligence, image processing, pattern recognition, and web based applications.

Sadia Al Haque received her BSc in computer science and engineering from International Islamic University, Bangladesh in 2006. She has received scholarships and awards for academic excellence including the Vice Chancellor's Gold Medal for her BSc degree.

Farhana Sharmin received BSc in computer science and engineering from International Islamic University, Bangladesh in 2006. She is currently pursuing Masters of business administration at International Islamic University, Bangladesh. She is an associate member of Institution of Engineers, Bangladesh.