Image Steganography using Variable-Rate LSB Approach

Hemshikha Joshi[1] Rahul Agarwal[2]
[1]M.Tech Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Engineering College Bikaner, Rajasthan, India

Abstract— Information and communication technology has grown rapidly and internet is the most popular communication medium nowadays. As the demand of more secure transmission has increased, so different steganography approaches have been proposed. In this paper we also present and evaluate my contribution to design the novel approach for image Steganography and named it as variable-rate approach. In this paper three image steganography methods with variable rate of embedding are proposed. A new algorithm is described for hiding a secret image in the least significant bits of a cover image. This method supports both type of images color and gray scale image. How many LSB hides the secret information is decided by the exclusive-or (XOR) operation of a pixel's neighbor. Experimental results show that the algorithm generally hides images without significant changes to the cover image, where the results are sensitive to the smoothness of the cover image.

Key words: Image Steganography, Least Significant Bit, Exclusive-Or Operation

I. INTRODUCTION

With the rapid growth of Internet technologies digital media can be transmitted conveniently over the network. So there is a need to protect data during transmission. Steganography is a technique for information hiding. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious. Steganography is all about creating a form of secret communication between two parties and it is a complement of cryptography. In this paper, a new algorithm is presented to hide information in the least significant bits (LSBs) of image pixels. The algorithm uses a variable number of hiding bits for each pixel, the number of variable bits depends on the xor of the neighbour pixels. The amount of visible degradation is expected to be higher for smooth areas, so the number of hiding bits is chosen to be proportional to the exclusive-or (XOR) of the pixel's neighbours[1], [2]. Analysis showed effectiveness of the algorithm in minimizing degradation while it was sensitive to the smoothness of cover images.

II. BACKGROUND AND RELATED WORK:

Surveys of different steganography techniques were presented in previous work. When an image is chosen to be used for hiding information, it is called a cover image. A cover image containing the secret information is called a stego image. Steganography can be categorized into four categories: audio, video, image and text. For hiding information usually Least Significant Bit (LSB) method is used [3], [4]. In the LSB method the 8th bit of every byte of the carrier file is substituted by one bit of the secret information. This method works fine in the image carriers because if the least significant bit is changed from 0 to 1 or vice versa, there is hardly any change in the appearance of the color of that pixel. Instead of hiding a fixed number of bits in the LSBs of each pixel, one can also embed different number of bits in LSBs of different pixels based on pixel value range calculation. In general if the pixels are located in edge areas they can tolerate larger changes than those in smooth areas.

Wu and Tsai proposed a pixel value differencing method, where a cover image is partitioned into non overlapping blocks of two consecutive pixels [5], [6]. A difference value is calculated from the value of the two pixels in each block. Secret data is covert into a cover image by replacing the difference values of the two pixel blocks of the cover image with similar ones, in which bits of embedded data are included. Zhang and Wang found that pixel value differencing steganography is vulnerable to histogram based attacks and proposed a modification for enhanced security. Chang and Tseng employed two sided, three sided and four sided side match methods. The two sided side match method uses the side information of the upper and left neighbouring pixels in order to make estimates. The three sided side match method uses upper and left neighbouring pixels, and one of the other neighbouring pixels. The four sided side match method uses the upper, left, right and below neighbours. Chang et al. proposed a three way pixel value differencing method. Zhang et al. proposed a pixel value differencing technique by using the largest difference value among the other three pixels close to the target pixel to estimate how many secret bits will be embedded into the pixel. Generally, the related previous work did not focus on hiding images inside other images. In addition, related image steganography research was usually limited to either gray scale or Red-Green-Blue images. The new algorithm of this paper handles hiding different images inside other images of various types.

III. PROPOSED WORK: THE HIDING ALGORITHM

Least Significant Bit image steganography is most commonly used algorithm in which least bit is replaced with MSB of secret message. Here algorithm uses a variable number of LSBs from each pixel of the cover image for hiding. A gray scale image consists of only one color matrix. A Red-Green-Blue (RGB) color image consists of three matrices representing the three color. The number of bits chosen from each pixel color (red, green, and blue) is different. The actual number of bits changes according to neighbourhood information of each pixel color. The number of bits used for hiding is chosen to be proportional to the neighbours' XOR value for each pixel color entry.

Pixels that are reside on the boarder of cover image not used for the hiding information, so almost 50% of pixels are used for hiding the values. The algorithm for hiding image shown in figure 1.

In this algorithm stegoC may be stegoR, stegoG or stegoB represent as red, green or blue color matrix. Each

color is treated separately. But in the gray scale image stegoC describe as single color matrix. In this method we do not hide information at the boarder of the image. The XOR is computed for the value of each one of these pixels' four neighbours: left, right, above, and below as shown in figure 2. This comparison measures the smoothness of the pixel's neighbourhood so that the number of hiding bits can be determined.

Row = 2

While (row ≤n-2) and (the secret image is not finished)

Col = 2 + (row MOD 2)

While col ≤ m-2

x = stegoC (row-1, col) xor stegoC (row+1, col) xor stegoC (row, col-1) xor stegoC (row, col+1))

If x ≤ α

NumLSBs = 1

Else

NumLSBs = ceil(x/2)

Endif

Replace LSBs of stegoC (row, col) with the next numLSBs bits

From the secret image

Col = Col + 2

Endwhile

Row = Row + 1

Endwhile

Fig. 1: Hiding Algorithm

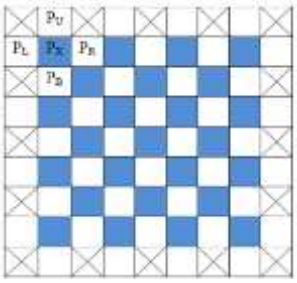

Fig. 2: neighbourhood pixel's for xor computation

If the XOR value is less than a given threshold α, only one LSB is used for hiding. Otherwise, the number of LSBs (numLSBs) used will be the ceiling of one-half of the XOR value. In the implementation of this paper, α was set to 9 and the maximum number of LSBs used for hiding in any pixel color was 4. The extraction process searches each of the three color matrices (Red, Green, and Blue), going through all lines and every other column as in the hiding procedure. The number of bits used for hiding in an entry, stegoC (row, col), is also determined by examining x; the XOR of the four neighbours as in the hiding process. All extracted hidden values are concatenated and grouped into bytes to form the original secret image.

IV. RESULTS AND ANALYSIS:

The algorithm was applied different images of different types and sizes for hiding. The sizes of these secret images ranged from 55*110 to 175*148 pixels. Three different cover images were used: Office (3001*2375 pixels) and koala (2560*1920). The analysis of the results focus on two aspects: difficulty to detect the hidden image existence in the stego image and sensitivity to the smoothness of the cover image. Recall that only non-adjacent pixels are used for hiding. These are approximately 50% of the pixels in the image.

Figure 3 and 4 shows one sample secret image (Penguin), which is 148*175 pixels, and the two cover images. Figure 5 shows the three stego images where each of them is hiding a copy of the Penguin image. As seen in the figures, the difference between the original images and the stego images is not visible to the human eye. The peak signal-to-noise ratio (PSNR) values were the highest for the koala cover image. This cover image has mostly smooth areas, which caused the algorithm to choose only one bit for hiding in each of 84.6% of the pixel entries used for hiding, as seen in TABLE I.

Fig. 3: Secret images

Fig. 4: cover images (office and koala image)

Fig. 5: Stego images (office and koala image)

COVER IMAGE	PSNR (db)	1 bit %	2 bit %	3 bit %	4 bit %
Office	62.701	84.6	11.3	2.9	1.2
Koala	65.104	36.9	32.0	27.1	4.0

Table 1: Result for the Penguin Test Image

V. CONCLUSION

The performance of various steganographic methods can be rated by the three parameters: security, capacity, and imperceptibility. The steganographic methods proposed in this paper are very secure as variable number of bits are hidden in different target pixels. Test results represent that the new algorithm keeps the hidden image difficult to recognize, as shown by the high PSNR and correlation values for stego images. The algorithm must hide less information in images containing more smooth areas to keep avoiding detection. This indicates that hiding in such images would be a poor choice.

VI. FUTURE WORK

The presented algorithm may be modified easily to work with more security. Sometimes due to noise and degradation the LSB of pixels are destroyed because of this we lost our originality of secret message so we can hide secret information in 5, 6, and 7 bit of pixels of cover image by using same approach.

REFERENCES

[1] Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf "Hiding an Image inside another Image using Variable-Rate Steganography" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No. 10, 2013

[2] G. Chhajed, K. Deshmukh and T. Kulkarni, "Review on binary image steganography and watermarking," Int. J. Comput. Sci. & Eng. vol. 3, no. 11, pp. 3645-3651, 2011.

[3] A. Hmood, H. Jalab, Z. Kasirun, B. Zaidan and A. Zaidan, "On the capacity and security of steganography approaches: An overview," J. Appl. Sci., vol. 10, no. 16, pp. 1825-1833, 2010.

[4] A. Pradhan, D. Sharma and G. Swain, "Variable rate steganography in digital images using two, three and four neighbor pixels," Indian J. Comput. Sci. & Eng., pp. 457-463, 2012.

[5] Zhang, X.; Wang, S. (2004): Vulnerability of Pixel Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security, Pattern Recognition Letters, vol.25, pp. 331-339.

[6] Kim, K. J.; Jung, K. H.; Yoo, K.Y. (2008): Image Steganographic Method with Variable Embedding Length, International Symposium on Ubiquitous Computing, pp. 210-213.

