A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images

Ankit Chaudhary[1], J. Vasavada[1], J.L. Raheja[2], Sandeep Kumar[3], Manmohan Sharma[3]

[1]BITS Pilani, RJ India
ankitc.bitspilani@gmail.com, h2010451@bits-pilani.ac.in

[2]CEERI/CSIR Pilani, RJ India
jagdish@ceeri.ernet.in

[3]Pilani, RJ India
{kumarsandeep.bits, manmohan.manu}@gmail.com

Abstract

This paper proposes an improved steganography approach for hiding text messages in lossless RGB images. The objective of this work is to increase the security level and to improve the storage capacity with compression techniques. The security level is increased by randomly distributing the text message over the entire image instead of clustering within specific image portions. Storage capacity is increased by utilizing all the color channels for storing information and providing the source text message compression. The degradation of the images can be minimized by changing only one least significant bit per color channel for hiding the message, incurring a very little change in the original image. Using steganography alone with simple LSB has a potential problem that the secret message is easily detectable from the histogram analysis method. To improve the security as well as the image embedding capacity indirectly, a compression based scheme is introduced. Various tests have been done to check the storage capacity and message distribution. These testes show the superiority of the proposed approach with respect to other existing approaches.

Keywords- *Keyless Steganography, Lossless RGB Images, Hash Based Embedding, Information Hiding*

1. INTRODUCTION

Steganography is a technique used to transmit a secret message from a sender to a receiver in a way such that a potential intruder does not suspect the existence of the message. Generally this is done by embedding the secret message within another digital medium such as text, image, audio or video. The terms cryptography and steganography are often used synonymously although they are essentially distinct. In cryptography, a plain message is encrypted into cipher text and might look like a meaningless jumble of characters whereas in case of steganography, the plain message is hidden inside a medium that looks quite normal and does not provide any reason for suspecting the existence of a hidden message. Using steganography, we need to take care about the resource utilization, the space requirements and the level of security. In addition, the quality of the cover object i.e. digital medium is important after using it for steganography.

Electronic steganography approaches use digital processing techniques for hiding and detecting embedded information. In case of image steganography, the secret message is transmitted embedded within a digital image called a *cover* image. Once the message is embedded within the image, it is referred to as a *stego* image. In a keyless steganography approach the sender includes only the information and does not include any cryptography algorithm. Therefore, the reliability and the security are totally dependent on the efficiency of the steganography algorithm itself. In this paper a keyless steganography algorithm applicable for lossless image formats like BMP, PNG or TIF, is proposed. Attempts are made to improve the storage capacity while incurring minimal quality degradation of the image. Security is enhanced by distributing the message throughout the image. The organization of the paper is as follows: section 2 discusses the related works, section 3 describes the proposed algorithm, section 4 provides details about the experimentations and results while section 5 discusses the overall conclusion and future scopes. This work is extension of our previous work [3].

2. RELATED WORK

The most widely used technique to hide data is the usage of the LSB. Although there are several disadvantages to this approach, it is relatively one of the easiest to implement. This method uses bits of each pixel in the image, it is necessary to use a lossless compression format otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. Least Significant Bit replacement embeds fixed-length secret bits into the least significant bits of pixels by directly replacing the Least Significant Bits of each byte of the cover image with the secret message bits. Some stegno analysis methods will identify the pixel difference in the host image very easily [6]. For a 24 bit image, 3 bits can be stored in each pixel. To the human eye, the resulting stego image looks almost identical to the cover image. A random LSB insertion method in which secret message is spread out among the image data in a seemingly random manner [11]. This is an efficient approach but changes to the MSB bits can degrade the image quality substantially.

One of the best keyless steganography approaches is the Pixel Indicator Technique (PIT) algorithm proposed by A. Gutub [4] where a color channel is used as a pixel indicator and the other two channels are used as for message embedding. The main drawback is that one of the channels cannot be used to store the actual message. To increase the capacity, usage of 2, 3 or 4 are proposed in [7]. A heuristic based approach for information embedding in the form of multimedia objects or text using steganography is proposed in [1]. In [10], the least significant bit (LSB) of each pixel is modified sequentially. In [2] the authors have proposed a steganographic technique by mixing with it cryptography to increase the security layer. There are other approaches available using Discrete Cosine Transformation (DCT) and Wavelet Transform (WT) [5].

3. PROPOSED APPROACH

The proposed approach is described in different sections as follows.

3.1 Motivation and Overview

The main motivation of the proposed work is to overcome the shortcomings of the techniques suggested in [9], which is an improvement of Pixel Indicator Technique (PIT) proposed in [4]. The process can be made efficient by considering only a single function i.e. randomization, instead of calculating K1 and K2. There is another shortcoming with the approach suggested in [9] that K1 and K2 calculations are dependent upon image size and message length. Our approach also takes care of distribution of the message over the cover image, as an improvement of not storing the message bits within the cover image in contiguous pixels only in the upper portion of the image [4]. Additionally the proposed work also attempts to increase the security level by introducing a text message compression at the first level, which indirectly increases the embedding capacity of the image.

3.2 Indicator Values

The first step towards the random distribution of the message in image is using indicator values. In the current work, we use MSB bits of Red, Green and Blue channel as pixel indicator values instead of utilizing an entire channel as in [4], which is suggested in [9]. The MSBs indicate in what sequence the message is hidden using the LSBs. In addition to this, this scheme is applied after applying compression to the original message. Therefore it would be make it extremely difficult to break, even after suspicion of the message within an image.

In this scheme the MSB remains unchanged when an LSB of a byte is utilized for storing a message. The sequences of LSB bits containing the message are indicated in Table 1. For example if the MSB code of channels is 001, then the message hiding LSB sequence is RGB, but if the MSB is 100, then the message hiding sequence becomes BGR. This scheme enables us to fully utilize all the LSBs of every channel of the cover image to store the hidden message and hence improve its capacity. Moreover the varying indicator values introduce a security aspect as it becomes increasingly difficult to decode the message even if its presence is suspected. We are not changing the scheme suggested for Indicator values in [9].

Table 1. Indicator Values

MSB bits of Red, Green and Blue channel sequentially	Sequence of channel's LSB bits where the message bits needs to be Hidden
000	Red, Green and Blue (RGB)
001	Red, Green and Blue (RGB)
010	Red, Blue and Green (RBG)
011	Blue, Red and Green (BRG)
100	Blue, Green and Red (BGR)
101	Green, Red and Blue (GRB)
110	Green, Blue and Red (GBR)
111	Green, Blue and Red (GBR)

3.3 Message Distribution

Instead of storing the message only in the upper portion of the image in contiguous pixels, as in [4], there is a technique proposed to distribute the message over the entire image in [4]. There is a key-number generated which indicate the gap value between two pixels containing the message to be hidden. This key-number K2 is computed based on *MessageLength* and image dimension i.e. *ImageWidth* and *ImageHeight* of the cover image. K2 is an integer which indicates the gap between pixels which contain the actual hidden information i.e. the information is inserted after every K2 pixels. The potential drawback with this is: the message distribution within the image is fixed in order. i.e. information is inserted after every K2 no. of pixels.

The proposed approach is based on randomization and hashing with respect to the MSBs of the channels, to skip R numbers of bytes. R is a generated random numbers based on the seed value S given to a random numbers algorithm. To illustrate the procedure, a XOR operation between the LSB bits of the cover image and the stego image indicate the pixels which have changed. The message is seen clustered towards the upper portion of the stego image, while for the scheme indicated in [9], the results for the proposed approach where the message is seen to be distributed with skipping K2 bytes after storing information once [9]. The result for the proposed approach, where the message is distributed randomly (with respect to MSBs) after storing information once, is better than the above two approaches.

3.4 Image Quality

While using steganography, image quality is one of the most important issues because, degradation in image quality suggests directly towards ‘something embedded in the image’. The quality of an image is degraded by changing the bits of an image to store information. As the number of LSB bits used to store the message increases, the quality of the stego image correspondingly degrades more. To limit this degradation the proposed approach uses stego-1 bit LSB [7] which implies that we are storing 1 message bit/channel, however we can use maximum of four Least Significant bits of each channel from an image. This improves the quality compared to the algorithm proposed in [4] where two LSB bits are used for the purpose. The other improvement in the image quality is due to randomization, i.e. not all the image bytes are used for the embedding purpose.

3.5 Message Encoding Process

The message encoding process is summarized below:

Input: Cover Image, Secret Message File.
Step1: Take as input the cover image, message/file to be hidden.
Step2: Compress the original secret file. (Output: .zip file)
Step3: Store the compressed file within the cover image (using the indicator values specified in Table 1).
Step4: Calculate the random number R and skip R no. of bytes.
Step5: Repeat steps 3 and 4 till the message embedding is not over.
Output: Stego Image.

3.6 Message Retrieving Process

The message retrieving process is summarized below:

Input: Stego Image.
Step1: Take the stego image as an input.
Step2: Retrieve the message from the image by generating random number R and skipping R bytes every time, using the table indicator values.
Step3: The output would be a compressed text file (.zip). By uncompressing the file, we would get the original text message file.
Output: Secret Message.

4. EXPERIMENTAL RESULTS

We resort to a number of statistical measures, to verify the superiority of this approach. Different sizes of messages inserted to different cover images. Table 2 shows the analysis with respect to embedding capacities of different algorithms. Figure 1 shows the original image and the Figure 2 is after inserting the secret text. The sample image contains more than 1 KB data. It is clear that, the change in image after embedding the data is not visible in the image, by bared eyes.
Here, '*Y*' in Table 2 represents '*embedding is possible*' and '*N*' represents '*embedding is not possible*'. It can be seen from the Table 2 that the embedding capacity of the suggested approach is comparable to the approach suggested in [9]. In our approach, although randomization tries to distribute message more, compression in the first step would compress the original message, increasing the embedding capacity of the image indirectly. One important thing to note here is, the cover image size should not be affected after embedding. However, padding based approach increases the image size by message size after embedding.

Figure 1: Original Image

Figure 2: Stego Image

5. CONCLUSIONS

In this paper we have proposed an improved steganography approach for hiding text messages within lossless RGB images. The objective of this work is to increase the security level and improve the storage capacity while incurring minimal quality degradation. As future improvements we want to compress the message and then store the data to increase the capacity further. We also want to insert any message both text and image at the same time (might be in PDF format or WORD format). We would also like to improve our algorithm by keeping in mind the robustness issue.

6. ACKNOWLEGEMENT

This research is being carried out at Central Electronics Engineering Research Institute (CEERI), Pilani. Authors would like to thank Director, CEERI for his active encouragement and support.

Table 2. Embedding Capacity

Algo \ MsgSize	10 B	1 KB	100 KB	1 MB	3 MB	5 MB	7 MB
Simple LSB	Y	Y	Y	Y	Y	Y	N
Padding Based Approach#	Y	Y	Y	Y	Y	Y	Y
PIT	Y	Y	Y	N	N	N	N
Ref-10 (max = 2.2MB)	Y	Y	Y	Y	N	N	N
Suggested Approach (max = 3.8MB)	Y	Y	Y	Y	Y	N	N

**considering imagesize = 800*600*

7. REFERENCES

[1] Bandyopadhyay, S.K., Bhattacharyya, D., Das, P., Mukherjee, S., Ganguly, D., A secure scheme for image transformation, In Proceedings of 9th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Phuket, Thailand, Aug. 06-08, 2008, pp. 490-493.

[2] Bhattacharyya, D., Das, P., Bandyopadhyay, S.K., Kim, T., Text steganography: a novel approach. International Journal of Advanced Science and Technology, Vol. 3., Feb 2009, pp. 79-86.

[3] Chaudhary, A. and et al., "An Algorithmic Approach to Intrusion Detection", Proceedings of 4th IEEE International Conference on Advanced Computing and Communication Technologies (ICACCT 2010), Panipat, India, 30th Oct, 2010, pp. 742-748.

[4] Gutub A. A., Pixel indicator technique for RGB image steganography, Journal of Emerging Technologies in Web Intelligence, Vol. 2, Issue 1, Feb 2010, pp. 56-64.

[5] Khare, A., Kunari, M, Khare P., Efficient Algorithm For Digital Image Steganography, Journal of Information Science, Knowledge and Research in Computer Science and Application, Oct 2010, pp. 1-5.

[6] Johnson, N.F., and Jajodia, S., Exploring steganography: Seeing the unseen, IEEE Computer Magazine, Vol. 31, Issue 2, Feb 1998, pp. 26-34.

[7] Neeta, D., Snehal, K., Jacobs, D., Implementation of LSB steganography and its evaluation for various bits, In Proceedings of 1st International Conference on Digital Information Management, Bangalore, India, Dec 6, 2006, pp. 173-178.

[8] Raheja, J.L., Manasa M.B.L., Chaudhary, A., Raheja, S., ABHIVYAKTI: Hand Gesture Recognition using Orientation Histogram in different light conditions, Proceedings of the 5th Indian International Conference on Artificial Intelligence (IICAI-11), Tumkur, India, 14-16 Dec, 2011, pp. 1687-1698.

[9] Roy, S. and Parekh, R., A Secure Keyless Image Steganography Approach for Lossless RGB Images, In Proceedings of ACM ICCCS, Rourkela, Odhisha, India, Feb 11-12, 2011, pp. 573-576.

[10] Singh, M., Singh, S.B. and Singh L.S.S., Hiding encrypted message in the features of images, International Journal of Computer Science and Network Security, Vol. 7, Issue 4, April 2007, pp. 302-307.

[11] Sutaone, M.S. and Khandare, M.V., Image based steganography using LSB insertion technique. In Proceedings of International Conference on Wireless, Mobile and Multimedia Networks, Mumbai, India, Jan 11-12, 2008, pp. 146-151.