High Capacity Image Steganography using Secret Key for Medical Information

T. Somassoundaram* and N. P. Subramaniam

1Department of Electronics and Communication Engineering, Sathyabama University, Chennai – 600119, Tamil Nadu, India; somsthy2005@gmail.com
2Department of EEE, Pondicherry Engineering College, Pillaichavadi, Pondicherry – 605014, Tamil Nadu, India; npsubbu@pec.edu

Abstract

The skill of thrashing the information and storing in an invisible form is referred as Steganography. The study targets to characterize the better security using RGB for image imparting. The proposed steganography algorithm uses Hybrid SPIHT DEFLATE algorithm to reduce the number of bits and increase the capacity of the thrashed information. An intense layer of RGB channel is selected for adding the compressed information. Concurrently, the position value is calculated on the specified secret key. The cover image is pixelized on the specific channel environment and thrashed information. The proposed approach is screened on the Brain medical image. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are the performance metrics evaluated in the proposed approach. The results prove that the thrashing of data in an intense layer renders minimized vulnerability over unintentional attacks.

Keywords: High Capacity Image Steganography, Hybrid SPIHT DEFLATE Algorithm, Medical Electronics, Steganography

1. Introduction

In the modern world, Communication plays a vital role in the field of Information Technology. The confidential information should highly protect before transmitting over any public channel. As the confidential information increases, the complexity level of protecting the information also increases. Protecting the information becomes easier in case of sharing the secret key under same public channel. In remote communication, the World Wide Web (WWW) acts as public channel which is handier.

The major factor in public channel is the security. Virtual Private Networks (VPN) acts as a communication bridge among the users for sending confidential information. The networks in VPN build by the Internet. If any intruder accesses the VPN network, then it is capable of accessing the whole network. So, a secured communication channel is necessitated for the data transmission. The art of Cryptography is the best remedy for the securing the data over insecure channel. Several cryptographic techniques are available to obtain a secured communication. Still, there is a lack of security using cryptographic techniques. A major disadvantage is the limitations that have been enforced by the government.

The sensible information is protected from unofficial users by the steganography techniques. The process of thrashing the information is known as steganography. In open systems, internet security and privacy is the major part. In digital media, the confidential information is thrashed. In compare to Cryptographic techniques, steganography provides higher security. The steganography targets to secure the transmission and also to thrash the data. The reason behind the data thrashing is to eliminate the unofficial users from the existence of message.

The communication medium in stego is the image files in a précised resolution form. The best type of image file is to thrash the information inside of cover medium is a 24 bit BMP images. The communication security is enhanced by adding a secret message into digital image. It is very useful for altering the unwanted image pixel. The
difference between cover image and stego image is higher; the task of discovering the thrashed data from the stego image is quite complicated for the attackers.

The cover image utilizes the RGB channel for carrying the data. The secret information and its key are used in one of the three channels. The LSB of blue and green components will determine the position value in the deeper layer of channels to thrash the data. The secret key and channel environment is used to extract the data from stego image.

The image steganography has gained much attention among the users for its high embedding functionalities. LSB substitution is the easiest method used for the thrashing of data. There are seven different methods in image steganography discussed in\textsuperscript{7} namely stego1 bit, stego2 bit, stego3 bit, stego4 bit, stego color cycling, stego PRNG and stego3fridrich. These steganographic methods are simple to use in inﬁxing and eliciting the process. The screening of a message in 24 bit of single LSB of RGB bytes is used by Stego 1 methods. The original representation of the image is not extremely altered. The other methods like Stego 1, Stego 2, Stego 3 and Stego 4 utilizes 2,3,4 LSB of RG bytes of 24bit for data embedding.

The color values of an image are cycled to hold down the information using stego color cycle technique. In\textsuperscript{8}, the cover image is splitted into non-collapsing parts of the pixels which is known as pixel value differencing. The difference between two pixels of a block is calculated. This difference value is replaced with the conﬁdential information; in which data is embedded. But it lacks in supporting histogram based attacks\textsuperscript{9} when any alteration is done. Different schemes such as two_sided, three_sided and four_sided is introduced in\textsuperscript{9}. Anyhow\textsuperscript{10} and\textsuperscript{11} suffer from boundary problem. The color intensity value of a pixel using stego-based techniques is introduced in\textsuperscript{9}. A single channel is represented as the pivot channel. Based on pivot channel, the data is thrashed. The last two bits of pivot channel are used for detecting whether the data bits are thrashed in other channels\textsuperscript{7}.

In\textsuperscript{9}, the LSB oriented steganography technique is studied. The data thrashing is embedded with the use of secret key of green or blue channel. It also minimized the security and more inclined to the unofficial attacks. Again, this is enhanced with better information security in\textsuperscript{9}. The act of LSBs alteration of the cover image in LSB embedding directs to the commodity to discover that stego is used. Due to less robustness and easily detecting the thrashed data in high storage power\textsuperscript{14}. The random key generation in data thrashing technique for video image is studied in\textsuperscript{12}.

The random RGB pixel is embedded with the thrashed data using encryption key.

Reversible Steganography method using dynamic key generation for the medical images is proposed in\textsuperscript{13}. Patient information is thrashed inside the medical images with the help of key. The key is dynamically generated by graph\textsuperscript{3} coloring and pixel count of color image. The intention of this study is to avoid thinking that the conﬁdential information exists in stego ﬁles. The analysis of stego image may detect some image and also discover the existence of thrashed messages inside the images.

2. Proposed Method

The working nature of the novel approach is supplied in Figure 1.

2.1 Pre-Processing of Secret Information

The Brain image is taken for illustration for thrashing. Firstly, the Brain image is compressed using the Hybrid SPIHT-DEFLATE algorithm proposed in\textsuperscript{14} to reduce the total number of bits. The Brain image is decomposed using Multi-Wavelet transform and then the coefﬁcients are encoded using the Hybrid SPIHT-Deflate algorithm. The total number of bytes of the compressed image is greatly reduced; thus leads to minimal bandwidth required for transmission. The reverse process is carried out to reconstruct the original Brain image.

In the proposed architecture, the thrashed information consists of two parts – Header and Data as shown in Figure 2. First three bytes of the thrashed information is allocated to header part and the rest is followed by the compressed data. The ﬁrst byte of the header part consists
of the total number of bytes thrashed, and the next two bytes consists of the dimension of the thrashed information. The compressed medical information is converted into 1D and then packed into the data part of the proposed data frame. On reconstructing the thrashed information, the extracted data is reconstructed using the dimension obtained from the second and third byte of the header.

### 2.2 Information Thrashing and Recovery

The substitution technique modifies the LSB bits in a usual manner. This is very useful for expressing the thrashed messages. In some cases, the thrashed messages are collapsed in the lower layer of the LSB that leads to transition distortions attacks. The proposed technique is splitted into three matrices and shown in Figure 3. These three matrices represent the Red, Green and Blue value of the pixels. An intense layer of blue or green or red contains the embedded bits of a message. The approach is difficult to discover the information and minimized the vulnerability over the public channel. The limited pixel is used for substitution process. The position of substitute bit and the pixel of a host image are used for selecting and determining the R or G or B bits. The position value is estimated for host bit (h) and message bit (m). If the value is equal, then the message is thrashed. If it is not equal then it is not selected for data thrashing. The proposed steganography techniques are shown in Figure 4 and Figure 5.

#### 2.2.1 Information Hiding Technique

The two important things to thrash the information are the cover image and message image. The cover image is splitted into three matrices such as red, green and blue. The message is formed by the 1D array of binary representation. Then the length of the array is used for predicting the value of secret key. The samples of 1bit of three matrices are counted and those three positions in the sample are measured. The bit of calculated position in B channel is checked with message bit. If they are equal then the LSB of blue is set as 1 and green as 0 to clearly indicate the channel as B.

The estimated position of bits in G channel is checked with the message bit. If they matches, then the LSB of blue bits is set as 0 and 1 to LSB of green bits. The estimated position in R channel is checked with the message bit. If they are equal, then 0 is set as LSB of blue and green to denote as R channel. Then the data is sorted using single channel. The priority is given as Blue, Green or Red. If value 1 is set as LSB of blue or green then there is no data thrashing of the message. In case of not equating with any bit value, then it is added in any intense layer of Red, Green and Blue. It is not easily visible to the human eye even in changes of position value of the LSB. The action is performed until the data is thrashed completely.

#### 2.2.2 Information Recovery Technique

The thrashed information is recovered using stego-image and secret key. The matrices are obtained by dividing the stego-image. The blue and green channels of LSB are used for data thrashing. Again, it is used for identifying secret bit of the blue and green channel. The blue and green channel get X-ORed and if the value is 1 the secret bit is thrashed, if the value is 0 there is no data or it is present in the red channel. According to the value of $b_i$ and $g_i$, the exact position of the pixel is identified and the hidden...
data is obtained with help of secret key. The position of the bit is stored in 1D array. Thus the process is continued till the hidden message bits are picked to store. Every 8bit is stored in 1D array and it is separated and converted into the message information which is sent by the sender.

3. Experimental Results

The efficiency of the proposed approach is proved and carried out using Subjective an Objective quality of the proposed approach. A GUI was developed using MATLAB R2013a. Quality metrics used in the paper is discussed below.

3.1 Subjective Quality

Subjective quality is evaluated by the presence of the medical diagnostic information in the recovered thrashed information and the visual appearance of the stego image. The medical information as message bit is thrashed into the cover image using the proposed approach. According to the proposed method the message image Figure 7 is concealed into the cover image Figure 6. The message is embedded into the cover image to form stego-image. The stego-image is shown in Figure 8 which is very nearest to the cover image. The thrashed data is extracted from the stego-images using the secret key.

The proposed approach is highly secure due to data embeds in variable position and the vulnerability to the unofficial attacks is minimized. The complexity of stego-analysis arises in selecting the pixel, channel and position estimation. The high percentages of pixels are used for information hiding that indicates the data capacity. From Figure 6 and Figure 8 are looking exactly same as their corresponding original cover images.

3.2 Objective Quality

The objective quality metrics used in the paper is discussed below. The objective qualitative measure is evaluated based on Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE)\(^\text{15}\).

- Mean Square Error (MSE) is the cumulative squared error between the compressed image and the original image given using Equation (1). Peak Signal to Noise Ratio(PSNR) is the peak of the measured error given using Equation (2)

\[
\text{MSE} = \frac{\sum \sum (r_{ij} - x_{ij})^2}{M \times N}
\]
Experiment: The objective evaluation is carried out for the pre-processed thrashed information. Table 1 depicted the evaluation of the proposed algorithm for various medical Brain images taken up for the illustration. From Table 1, the size of the thrashed information is greatly reduced.

4. Conclusion

The pixel and channel for substitution is selected by the bit value of the substitution position and message bit. The position of substitution in the channel is determined by the status of selected channel and value of the secret key. The ambiguity in selecting pixels and channel will thus increase complexity of stego-image analysis. The use of secret key gives a way to secure the information from unofficial users. Thus, the proposed algorithm greatly reduces the aggregation of bytes thrashed in to the cover image which proportionately reduces the CPU time consumed on the overall process. Thus, the proposed method is used to thrash medical information in the cover image increasing the robustness and providing high capacity stego-image quality.

5. References

1. Gollman D. Computer Security. 3rd ed. New York, USA: John Wiley and Sons Publishers; 1999. p. 201.
2. Curran K, Bailey K. An evaluation of image based steganography methods. Multimedia Tools and Applications. 2006; 30(1):55–88.
3. Wu DC, Tsai WH. A steganographic method for images by pixel value differencing. Pattern Recognition Letters. 2003; 24(10):1613–26.
4. Zhang X, Wang S. Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognition Letters. 2004; 25(3):331–9.
5. Chang C, Tseng HW. A steganographic method for digital images using side match. Pattern Recognition Letters. 2004; 25(12):1431–7.
6. Parvez MT, Gutub AA. RGB based variable-bits image steganography. Proceedings of IEEE Asia Pacific Services Computing Conference; Yilan. 2008. p. 1322–7.
7. Kaur M, Gupta S, Sandhu PS, Kaur J. A dynamic RGB intensity based steganography scheme. World Academy of Science, Engineering and Technology. 2010; (47):1170–3.
8. Karim SMM, Rahman MS, Hossain MI. A new approach for LSB based image steganography using secret key. Proceedings of 14th International Conference on Computer and Information Technology (ICCIT 2011); Dhaka. 2011. p. 286–91.
9. Juneja M, Sandhu PS. An improved LSB based steganography technique for RGB color images. 2nd International Conference on Latest Computational Technologies (ICLCT’13); Coimbatore. 2013. p. 10–4.
10. Xi L, Ping X, Zhang T. Improved LSB matching steganography resisting histogram attacks. Proceedings of the IEEE International Conference on Computer Science and Information Technology; Chengdu. 2010. p. 203–6.
11. Zamani M, Manaf AA, Ahmad RB, Zeki AM, Abdullah S. A genetic-algorithm-based approach for audio steganography. World Academy of Science, Engineering and Technology. 2009; 54:360–3.
12. Somassoundaram T, Subramaniam NP. High performance angiogram sequence compression using 2D Bi-orthogonal multiwavelet and hybrid SPIHT and DEFLATE algorithm. Indian Journal of Science and Technology. 2015 Jul; 8(14):1–6.
13. Somassoundaram T, Subramaniam NP. A hybrid scheme on medical image compression using SPIHT and Deflate technique. IJERT. 2014; 3(5):2317–22.