Advanced 3-DES Block Based LSB Algorithm for Image Steganography

Shreyank N. Gowda
RVCE, Bangalore

Abstract

Steganography is a technology of hiding information of any type, by using some medium as a cover. Image steganography is steganography done using an image as the cover medium. This algorithm takes the entire text and encrypts it first using the Triple Data Encryption Standard Algorithm (3-DES) and then takes this data as one block, and based on an input 'n' breaks this text down to 'n' blocks. It then takes 'n+1' images in random, and performs Least Significant Bit(LSB) algorithm on these images using one image per block. These images are sent in random order after the encrypted text is concealed in them. This ensures enhanced security due to the randomness of the algorithm along with the encryption security provided by the 3-DES algorithm. After this a hash table is created which is used to keep hold of the correct sequence of the 'n' blocks. This hash table is later concealed in the 'n+1'th image, called the hashing image. Due to the random nature that images are sent security is enhanced for the data. Results show two important things, firstly that since we use more than 1 image we can hide a larger amount of data in comparison to a standard LSB which uses a single image. Secondly, since the text is broken down, each image uses a smaller amount of text to conceal and this increases the Peak Signal to Noise Ratio (PSNR) value for each image showing that this algorithm is more advantageous than the standard LSB.

1. Introduction

Steganography is a method to hide information of some type, i.e. text, videos, images, etc. using some medium as cover. The word steganography is obtained from the Greek Language using two words. The first word is steganos which means to being concealed or covered and the second word graphein which means writing.

Steganography and cryptography are both methods used to hide data but they do not infer to the same thing. Cryptography encrypts some information and sends that information without doing anything to hide that information. So one look at an encrypted text attracts attention of the attacker and it becomes obvious that some text is being hidden.

Steganography however does not attract attention to itself as an object of scrutiny since the attacker does not know that there is the possibility of some information being hidden.

Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

The most basic algorithm for steganography is the Least Significant Bit (LSB) algorithm. In this algorithm the least significant bit of each pixel is modified to accommodate one character from the plain text. This algorithm is easily broken down and any information being hidden using this can be obtained by an attacker.

This paper will deal with an algorithm that uses LSB as its base and enhances the security of the algorithm. The paper looks to combine cryptography and steganogrpahy to aid the objective of both: securing data.

To understand LSB algorithm consider an example, a grid for 3 pixels of a 24-bit image can be as follows: 00101101 00011100 11011100 10100110 11000100 00001100 11010010 10101101 01100011 When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows: 00101101 00011101 11011100 10100110 11000101 00001101 11010010 10101100 01100011.

3-DES is similar to the standard DES algorithm, it is actually the DES algorithm implemented using 3 different keys to enhance the security level of the algorithm.

The original DES cipher's key was of size 56 bits and was generally sufficient when that algorithm was designed, but the availability of now increasing computational power has made brute-force attacks feasible.

Triple DES provides a relatively simple method by increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

2. Background

In In [1] the author tries to convey the idea of using a texture as the cover image to hide data. Since a texture is a set of pixels that repeat itself it becomes much easier to hide data. However a texture shows a

high indication of information being hidden and is hence more vulnerable to attacks.

In [2] the authors suggest using more than 1 image for hiding data and show that this method provides a huge boost to the security. This is also the method we enhance by using a cryptographic algorithm.

In [3] the authors use a mapping technique called non-linear chaotic mapping. The data to be hidden is first embedded onto a scrambled image. The cover image is simultaneously subject to Discrete Wavelet Transform. This image is later embedded along with the scrambled image. This method can hide large amount of data, but should the map be obtained its extremely easy to obtain the information.

In [4] the authors suggest a method of hiding data using either of the RGB colour channels. Since an image has 3 channels modifying any one channel shows that there is not much change in terms of the image visually to the human eye. However, this method cannot be used for large images.

In [5] the authors propose the use of the Blowfish algorithm to enhance security of data before the use of the steganography algorithm.

In [6] first Huffman encoding is done on the data and then the data is broken down to blocks. Simultaneously DCT is performed on the cover image. LSB is then modified using Huffman values obtained. Maintaining the Huffman codes are very important since loss of Huffman codes means loss of data. Also, computation time for this method is extremely large.

In [7] dual layer of security to the data is provided, for the first layer it is by using the standard Least Significant Bit method and for the second layer it involves using the Advanced Encryption Standard Algorithm. Steganography does not replace the encryption of data, instead it provides extra security feature to it.

In [8] the message desired to be hidden is embedded in only the blue part of the RGB channel. Results showed that this enhanced the security level of the image as visual distortion was not visible.

In [9] the secret data is taken and firstly hidden by using the Vigenere encryption method to increase the standard of protection of the data. Next, the Lempel Ziv Welch (LZW) technique is used to compress the data to hide its actual capacity. Afterwards, the extended knight tour algorithm is implemented where each bit stream of the data is made to spread out on the image. This enhances the robustness of the given image.

In [10], the author proposes the use of Diffie-Hellman algorithm to select the pixel positions for embedding information.

In [11], a steganography algorithm was designed based on discrete cosine transform, Arnold Transform and Chaotic System. The chaotic system is made to generate a random sequence for spreading data in frequency band Discrete Cosine Transform coefficient of the cover image. The secret data is further scrambled using the Arnold Cat Map which further enhances the security feature. The recovery process is doing the same method in reverse process.

In [12] the authors suggest an algorithm that increases the security of the Caesar Cipher algorithm without increasing the time complexity too much.

3. Proposed Method

At the senders' side, first the data to be hidden is collected. This is subject to encryption using 3-DES algorithm. It is then broken down to a desired number of blocks. For example, if a 1024 character set of data is taken, it is converted to a new amount of data say 1000 characters using the encryption algorithm and if then it is broken down to 4 blocks we obtain 4 blocks with 250 characters each. After the breaking down of data is done to 'n' blocks, 'n+1' images are chosen in a random order from a set of 'm' images where m>n+1.

The 'n' blocks are then encoded into 'n' images using standard LSB algorithm. After this encoding is done the 'n' images are sent in random order. This enhances the security of the data.

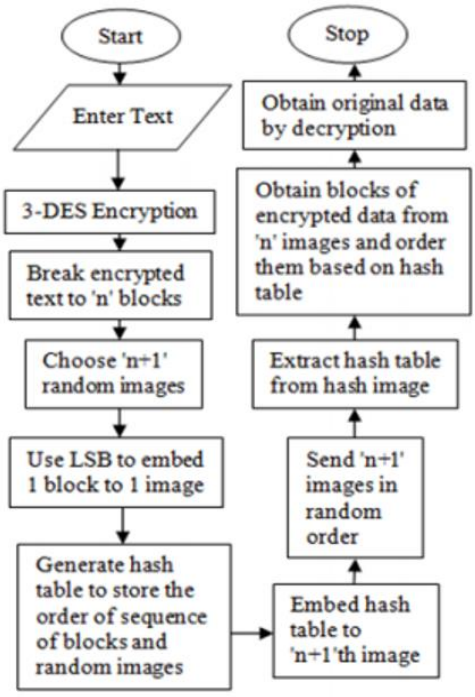

Figure 1. Flowchart of Proposed Method

However, a problem occurs, since we have to maintain the correct sequence of data. To overcome this problem, we use a hash table which contains the sequence number of the block and the image which is storing it.

Figure 1 shows the flowchart of the proposed method. This is then embedded using LSB into the remaining single image and is also sent by the sender. This last image is called the hash image. Once the receiver receives this set of images, he first obtains the hash table out of the image that contains the hash table. Once he obtains the hash table he can order the images to receive the correct order of information. He orders the images, then collects out individual data and then merges all the data collectively to obtain the initial information. The random sending of data enhances the chaos factor and hence makes it more difficult to obtain the information even if the images are received by some intruder. The proposed algorithm provides many advantages over the standard Least Significant Bit Algorithm, mainly with respect to size and Peak Signal to Noise Ratio (PSNR), but also in terms of security due to the use of a pre-existing encryption algorithm. The entire algorithm is executed in Python using OpenCV.

4. Experimental Results

To test the strength of the algorithm following tests were done in comparison to the standard Least Significant Bit Algorithm [9]:

1) to check the maximum size of a text file that could be hidden.
2) time of execution needed for both algorithms
3) Peak Signal to Noise Ratio for original to new image.

Table 1 represents the results for the experiment conducted for determining maximum size of file that can be hidden. It can be concluded from the results that the maximum size can be increased when using the block based algorithm instead of the standard one.

The explanation for that is quite simple, since for the block based algorithm we use more images, more pixels are available for applying standard LSB, this allows more information to be hidden and hence the block based algorithm gives better outcome in this case.

Table 1. Result of determining maximum size that can be hidden

S.No	Input Size	Output for LSB	Output for advanced 3-DES	'n'
1	320x240	512kB	2048kB	4
2	1280x780	2MB	8MB	4

Table 2 represents the results for the experiment conducted to determine the time needed for execution of the algorithm in comparison with the standard LSB algorithm. As can be seen from the table time taken to execute the standard LSB is lesser. The explanation for this is that extra time is needed for breaking the text to blocks and also for generating a hash table and further storing that hash table in an image. The variation in time is not too much however and is tolerable. In fact, it can even be seen when we use a 512 kB file as input to be hidden then the difference in execution of time is negligible. Also, it is very important to remember that in practical cases files of up to 100kB are hardly used for hiding these types of information. Hence this algorithm proves very useful.

Table 2. Time of execution

S.No	Input Size (Image Size, Text size)	Output for LSB	Output for Advanced 3-DES	'n'
1	1280x780, 1kB	0.5 secs	1.472 secs	1
2	1280x780, 10kB	1.265 secs	2.338 secs	4
3	1280x780, 100kB	8.327 secs	10.27 secs	4
4	1280x780, 512kB	40.111 Secs	43.372 secs	8

Table 3 presents the results of Peak Signal to Noise Ratio, between the pre-algorithm image to the post-algorithm image. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the most used error metrics to compare image compression quality. The MSE represents the cumulative squared error that is between the compressed and the original image, whereas, PSNR represents a measure of the peak error. This is used to indicate the maximum difference between the images. The Peak Signal to Noise Ratio is the difference between corresponding pixel values of the pre-algorithm to post-algorithm image. This is done using MatLab. The higher the value of PSNR the lesser is the difference in quality of the image. For the block based algorithm, average PSNR value is taken of all n+1 images. Figure 2 (a) is the original image and Figure 2 (b) is the image obtained after the execution of the block based algorithm.

Table 3. PSNR value determination

S.No	Input Size (Image Size, Text size)	Output for LSB	Output for Advanced 3-DES (Avg)	'n'
1	1280x780, 1kB	77.15	83.51	4
2	1280x780, 10kB	71.14	78.42	4
3	1280x780, 100kB	63.25	68.76	4
4	1280x780, 512kB	51.23	64.47	8

Figure 2 (a) Original Image (b) Image after execution

As can be seen the changes are hardly visually perceptible which ensures that the changes can hardly be noticed, thus increasing the security of the algorithm.

5. Conclusion

Following conclusions can be drawn on the basis of the execution and eventual comparison between Least Significant Bit Algorithm and the Block based algorithm:

- The block based algorithm can hide more amount of data.
- The block based algorithm needs relatively more time for execution. However for text files large in size the difference in time is not much.
- The amount of space needed for block based algorithm is more since we need more than just the 1 image to execute the algorithm.
- PSNR value is higher for the block based algorithm, indicating difference in original to secret image is not much.
- Security is more for the block based algorithm since it increases the chaos factor due to the random nature of the algorithm.

6. References

[1] Wu, K.C. and Wang, C.M., 2015. Steganography using reversible texture synthesis. IEEE Transactions on Image Processing, 24(1), pp.130-139.

[2] Gowda, S.N. and Sulakhe, S., 2016, April. Block Based Least Significant Bit Algorithm For Image Steganography. Annual Int'l Conference on Intelligent Computing, Computer Science & Information Systems (ICCSIS-16).

[3] Thenmozhi, S. and Chandrasekaran, M., 2013, January. A novel technique for image steganography using nonlinear chaotic map. In Intelligent systems and control (ISCO), 2013 7th international conference on (pp. 307-311). IEEE.

[4] Parvez, M.T. and Gutub, A.A.A., 2008, December. RGB intensity based variable-bits image steganography. In Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 1322-1327). IEEE.

[5] Gowda, S.N., 2016, October. Using Blowfish encryption to enhance security feature of an image. In Information Communication and Management (ICICM), International Conference on (pp. 126-129). IEEE.

[6] Nag, A., Biswas, S., Sarkar, D. and Sarkar, P.P., 2010. A novel technique for image steganography based on Block-DCT and Huffman Encoding. arXiv preprint arXiv:1006.1186.

[7] Gowda, S.N., 2016, December. Advanced dual layered encryption for block based approach to image steganography. In Computing, Analytics and Security Trends (CAST), International Conference on (pp. 250-254). IEEE.

[8] Gupta, S., Gujral, G. and Aggarwal, N., 2012. Enhanced least significant bit algorithm for image steganography. IJCEM International Journal of Computational Engineering & Management, 15(4), pp.40-42.

[9] Bashardoost, M., Sulong, G.B. and Gerami, P., 2013. Enhanced LSB image Steganography method by using knight Tour algorithm, Vigenere Encryption and LZW compression. IJCSI International Journal of Computer Science Issues, 10(2), pp.221-227.

[10] Gowda, S.N., 2016, November. An advanced Diffie-Hellman approach to image steganography. In Advanced Networks and Telecommunications Systems (ANTS), 2016 IEEE International Conference on (pp. 1-4). IEEE.

[11] Singh, S. and Siddiqui, T.J., 2012. A security enhanced robust steganography algorithm for data hiding. IJCSI International Journal of Computer Science Issues, 9(3), pp.1694-0814.

[12] Gowda, S.N., 2016, September. Innovative enhancement of the Caesar cipher algorithm for cryptography.In Advances in Computing, Communication, & Automation (ICACCA)(Fall), International Conference on (pp. 1-4). IEEE.

[13] Kamdar, N.P., Kamdar, D.G. and Khandhar, D.N., 2013. Performance evaluation of lsb based steganography

for optimization of psnr and mse. Journal of information, knowledge and research in electronics and communication engineering, 2, p.505.

