International Journal of Computer Applications Technology and Research
Volume 6–Issue 11, 441-450, 2017, ISSN:-2319–8656

Multi-Level Image Steganography Using Compression Techniques

Mohamed H. Sayed
The National Ribat University
Khartoum, Sudan

Talaat M.Wahby
Sudan University of
Science and Technology
Khartoum, Sudan

ABSTRACT: Steganography is the art and science of writing hidden Messages in such a way that no one, apart from the sender and intended recipient, Suspects the existence of the message. In this research apply Multi-Level Steganography for image steganography was presented. MLS consists of at least two stenographic methods utilized respectively. Two-levels of stenography have been applied; the first level is called (the upper-level), and it has been applied using enhance LSB (secure LSB-L1) image steganography, the secret data in this level is English text, and the cover is Bitmap image, the output is a stego_image called (intermediate image). The second level is called (the lower-level); it has been applied using another enhance LSB (secure LSB-L2) based image steganography. In this level another Bitmap (BMP) image has been used as a cover image and embeds (the BMP image output from level one) as a secure data and generates the new BMP image as stego_image. Lossless data compression technique using Huffman, LZW algorithm and Winrar Application between First and Second level of steganography are applied.

Keyword: steganography, Bitmap, Multi-Level, LSB, Lossless, compression.

1. INTRODUCTION

Security of information is one of the most important factors of information technology and communication. Security of information often lies in the secrecy of its existence and or the secrecy of how to decode it. Cryptography, watermarking and Steganography can be used in information security [1].

Steganography is defined as “the art and science of communicating in a way which hides the existence of the communication”. Methods of steganography have existed for centuries, though with the advent of digital technology, have taken on a new form. Embedding data within the redundancy and noise of media files is among these digital techniques.

Steganography can be classified into image, text, audio and video steganography based on the cover media used to embed secret data. Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different stenographic algorithms exist.

Steganography (from Greek steganos, or "covered," and graphie, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography takes cryptography a step farther by hiding.

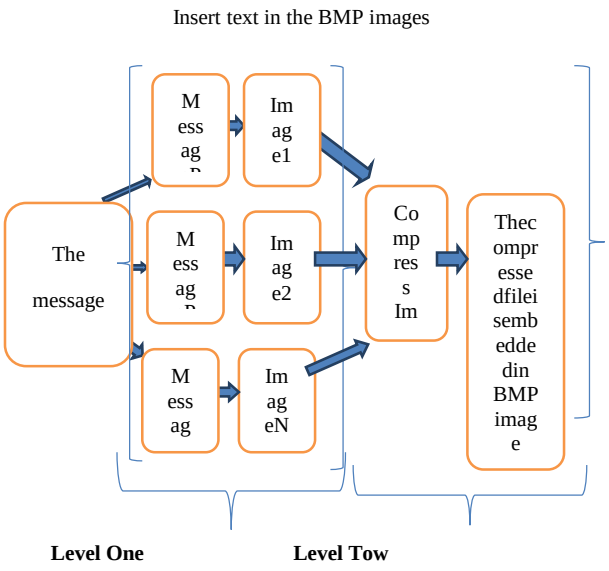


Figure 3.1 shows the proposed algorithm

2. LITERATURE REVIEW

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data, the word Steganography literally means covered or hiding writing as derived from Greek. Steganography has its place in security .It is not intended to replace cryptography but supplement it. Hiding a message with Steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection [2].

Data compression techniques, the file could be reduced in size to, say, 15 KB that makes it easier to store on disk and helps faster transmission over an Internet connection.

Data compression is a process by which a file (Text, Audio, and Video) may be transformed to another (compressed) file, such that the original file may be fully recovered from the original file without any loss of actual information [3]. This process may be useful if one wants to save the storage space. For example if one wants to store a 4MB file, it may be preferable to first compress it to a smaller size to save the storage space. Data Compression is possible because most of the real world data is very redundant. Data Compression is basically defined as a technique that reduces the size of data by applying different methods that can either be Lossy or Lossless. A compression program is used to convert data from an easy-to-use format to one optimized for compactness. Likewise, an uncompressing program returns the information to its original form.

3. PROPOSED METHOD

The proposed method is using multilevel image steganography [4], (two levels) level one will be done by embedding the secret message (text) into cover image (cover one) which is a colored image (BMP image) using Least Significant Bit (LSB) image steganography. And then using key to private message, and finally using compression techniques to compress output result that coming from level one. In level two improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image. Figure 3.1 explain the general overview of the proposed method (embedding process). Steps extracting Process in level one using Modified LSB (secure LSB-L1).

Hide one message in many bitmaps. It is quite similar to writing text across a couple of pages [4]. It means spreading the pixels over multiple images. Figure 3.4 below Shown and more explain:

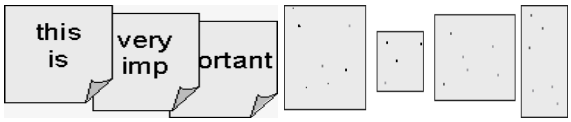


Figure 3.2 spread the information over the images

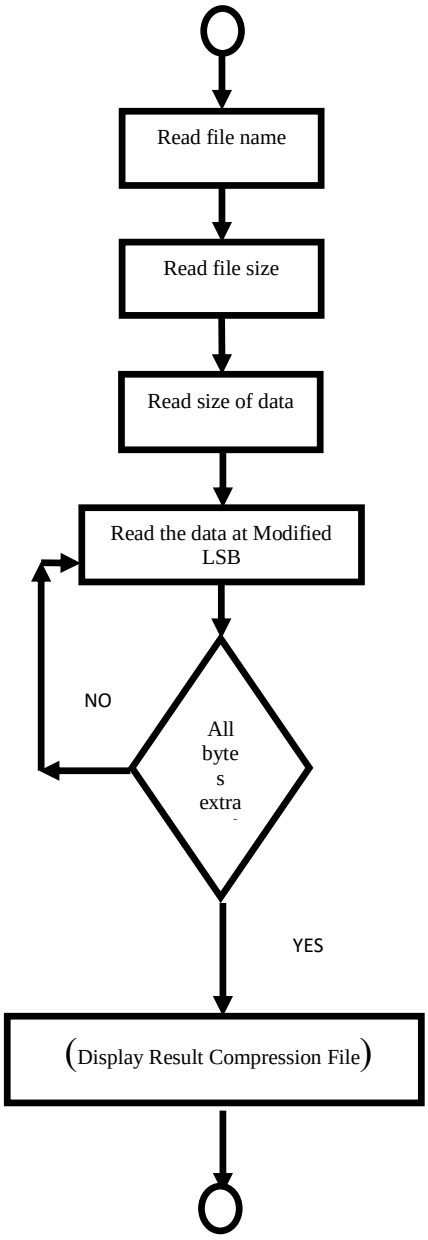
You can send each image in a separate E-mail, post them in different mailboxes, or store them on different discs. The GUI allows selecting carrier bitmaps the same way as selecting key

files. The selection is stored as an array of Carrier Images**.** Larger images can hide more bytes (more pixels) than smaller images.

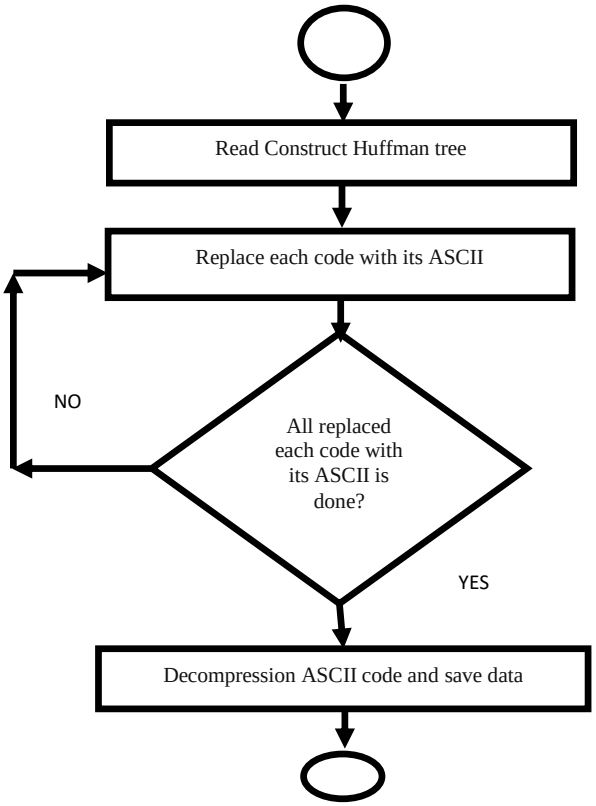
4. PROCESS OF CARRIER UNIT

Now, we start with the first carrier bitmap, loop over the message, hide a number of bytes, and switch to the second carrier bitmap, and so on. Current position in the carrier bitmap Start with 1, because (0,0) contains the message length. At the end, we must save the new images. Each image can be saved using a format (BMP).Steps Embedding Process in level tow using Modified LSB (secure LSB-L2)

Steps extracting Process in level Tow using Modified LSB (secure LSB-L2)



Compression process Using Huffman algorithm



Decompression Process Using Huffman algorithm

5. RESULT

Comparative analysis of multilevel image steganography (secure LSB-L1) and (secure LSB-L2) based image steganography has been done on the basis of parameters like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR).There is a different message size have been used to embed them in different image size in the upper level of image steganography, the first message (first secret message) will be Use is shown in table 5.1

Size Messages	Images in level one	Images in level tow
270 bytes	black-box	Monaliza
4,650 bytes	Red - box	cyber-security
8,232 bytes	White-box	horse

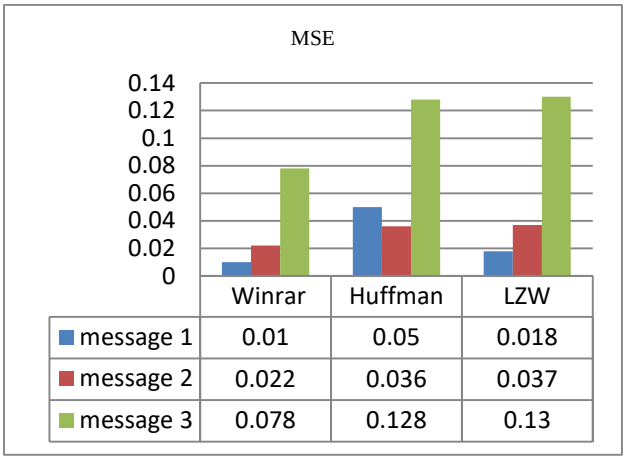
Table 5.1 different image size in the upper level of image steganography

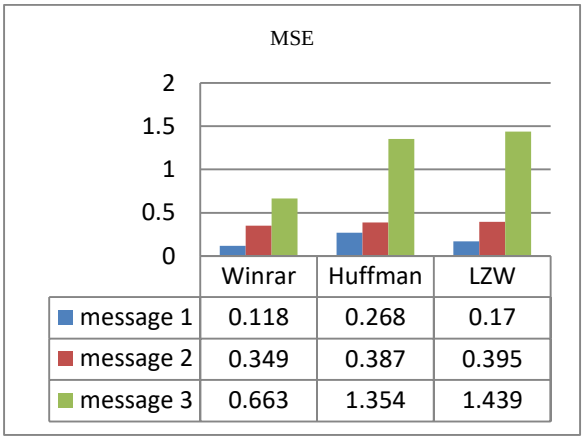
After the upper level (secure LSB-L1) is applied to the above secret messages the output is more than one image. Figure 5.1 Shown and explain level one applied method

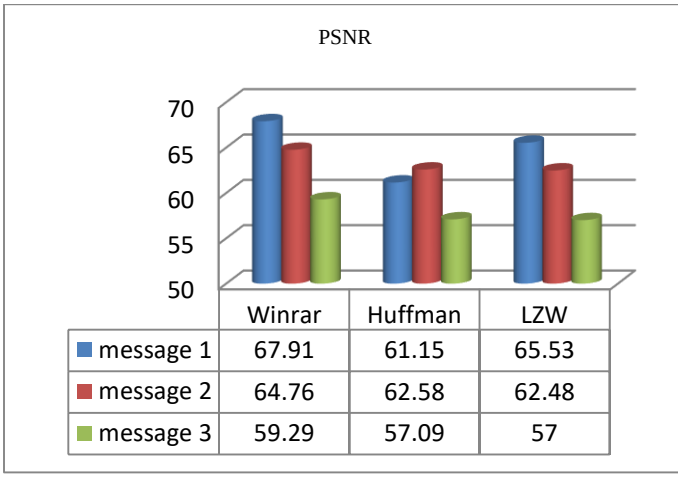
Original Image	Stago-images in level one
	
	
	

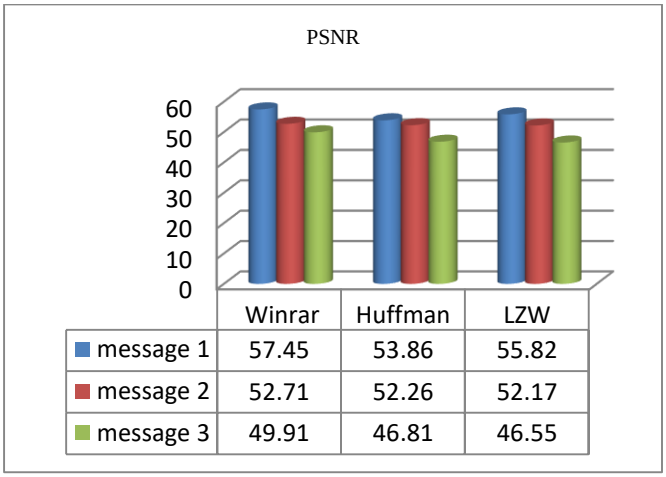
Figure 5.1 explain level one applied method

a below Diagram Shows the experiment results of stego_images and contains the Quality Image parameter values of stego_images above. Figures below is a Diagram showing its Quality Image parameter values (MSE, PSNR) for Monaliza stego-image.



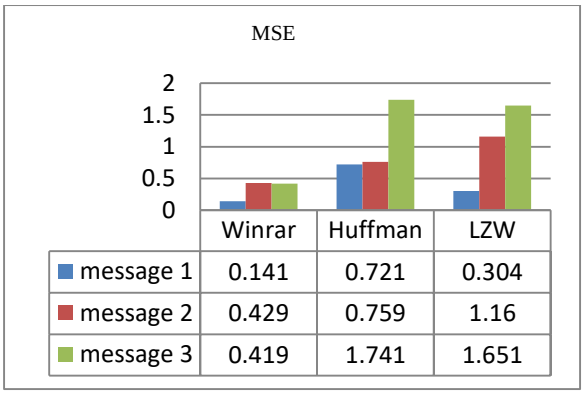


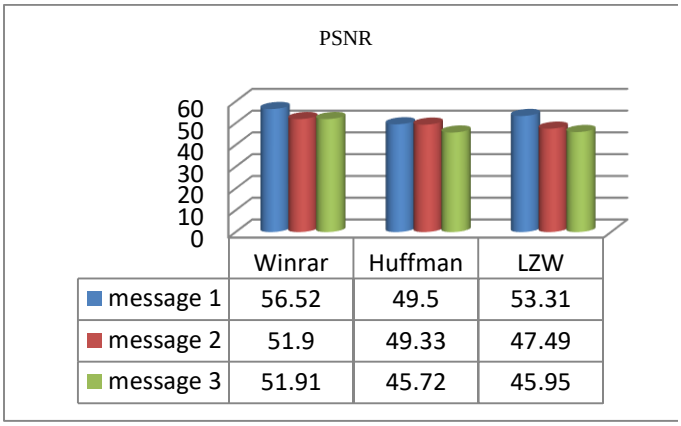




The Second image is the cyber-security stego- image. Figure 4.12 is a Diagram Showing its Quality Image parameter values (MSE, PSNR) for cyber-security stego-image

The third image is the horse stego-image. Figures below shoes the Diagram showing its Quality Image parameter values (MSE, PSNR) for horse stego-image





	Winrar	Huffman	LZW
message 1	56.52	49.5	53.31
message 2	51.9	49.33	47.49
message 3	51.91	45.72	45.95

5.1 Conclusion

The proposed model adds a level of security through the main theme of steganography: "hiding information in plain sight". The cover object usually does not invite suspicion, since it looks similar to the original object to the general observer.

The main objective is applying and improves the way to hide the information division the text on more BMP images.

In this thesis, a new concept for performing hidden secret data, called Multilevel Steganography for image steganography, was presented. MLS consists of at least two stenographic methods are utilized respectively, in such a way that one method (called the upper-level) as a carrier for the second one (called the lower-level).

The proposed method is two levels of image steganography, In the level one uses modified least significant bit (secure LSB-L1) image steganography to hide the secret information into more than one image carrier of the text (at least in 2 images). And that improving hide information by being distributed in more than one image carrier. The last step in this level, adding a key string to secure the information.

While level two employs the algorithm use for Encryption and Decryption in this level provides (secure LSB-L2) using several layers lieu of using only LSB layer of the image. Writing data starts from the last layer (8th or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So, every step we go to upper layer image quality decreases and image retouching transpires.

Multilevel Steganography has potential benefits, as it may enhance the confidentiality of the secret information by using two level image steganography in one the system and add more complexity to the steganography process through applying it in two levels.

Measuring the performance of proposed algorithm has been applied using many experiments and calculate many values of each experiment, the first value is Peak signal to noise ratio (PSNR), this ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality, the second measurement value is Mean Squared Error is the average squared difference between a reference image and a modified image (stego-image). And other calculates values are Normalized Cross-Correlation, Average Difference, Structural Content, Maximum Difference and Normalized Absolute Error.

There are many experiments have been conducted through the different size of secret messages (secret message one, two and three) utilized as a secret data in level one. And compress in one file, then concealed in one BMP image the output is compressed file or (intermediate object) and it's used as a secret data in level two.

5.2 Recommendations

- The proposed method can be used in military applications for secure communications.

- Try to check the result of proposed algorithm using the grayscale image on both levels to compare the performance results.
- Apply another compression technique.
- Apply compression to a text file.

5.3 Future Work

1- Adding Advance encryption algorithm to in the upper level to encrypt the secure text message to increase the security to proposed method.

2- Adding one more level (level Three)

3- Increase the System functionality to hide all other data types like audio, video not only text data and images.

4- Trying to enhance the performance of algorithms in both levels to increase the system capacity.

References

[1] Al-Dieimy, I.I.U, (2002), "Information Hiding In an Open Environment ", Computer Science & Information System (CSIS), University of Technology Malaysia, Malaysia.

[2] Dorothy, E.R, D.K, (2000), "Cryptography and Data Security", IEEE International Symposium on Canada Electronics (ISKE), University of Canada, Canada, Vol.6, p.p 119-122.

[3] P. Jeyanthi, V. Anuratha, "Analysis of Lossless Reversible Transformation Algorithms to Enhance DATA Compression", Journal of Global Research in Computer Science, Volume 3, No. 8, August 2012, p.p 56-62.

[4] Al-Najjar, Atef Jawad. "The decoy: multi-level digital multimedia steganography model." WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering. No. 12. World Scientific and Engineering Academy and Society, 2008.

[5] C. J. S. B, (2002)," Modulation and Information Hiding in Images", Vol. 1174, of Lecture Notes in Computer Science, University of Technology, Springer, p.p 207-226. Clelland, C.T.R, V.P & Bancroft, (1999), " Hiding Messages in DNA Micro Dots ", Proceedings of IEEE International Symposium on Industrial Electronics (ISIE), University of Indonesia, Indonesia, Vol. 1, p.p 315-327.