International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

A Novel Technique for Secure, Lossless Steganography with Unlimited Payload

[1]Swati Balbhadra, [2]Jageshwar Shrivas, [3]Rohit Miri

[1] Mtech Scholar, CSE Department, Dr.C.V.Raman university, Chhattisgarh, India
[2] Assistant Professor, CSE Department, Dr.C.V.Raman university, Chhattisgarh, India
[3] HOD, CSE Department, Dr.C.V.Raman university, Chhattisgarh, India

---

Abstract- Steganography is a technique by which any message can be hiding and cannot be seen by necked eyes. It is a very good way by which a message can be prevent from being seen or discovered. Cryptography is distinguished from Steganography in which messages are not completely masked but remain ambiguous by rushing it. By following cryptography technique the hidden messaging cannot be completely prevented from discovered by any third element. Security has a lot of importance and application in various fields. It is a measure of human carelessness in order to gain the latest technology. Still can be compressed, steganographic embedded and digital watermarked for any transformations. In this paper we have proposed some advanced techniques for finding and analysis of steganographic encapsulate content. Here we put the both statistical and pattern classification techniques which provide us reasonable distinguished schemes for finding encapsulate content of different levels. Our calculations are depends on a some statistical properties of bit strings and wavelet coefficients of image pixels. These measures may have serious effect on human perception to the use of application. As we know that cryptography and steganography are the two different approaches in security, we have tried to combine them. It should be noted that both requirements can also be satisfied solely through cryptographic means. Symmetric key cryptography makes use of single key for encryption and decryption of data. In the proposed approach to dual security we make use of DES (Data Encryption Standard) Algorithm for first phase of encryption and Audio steganography for the second phase of encryption. It's a unique way to draw attention to symmetric key encryption methods such as DES and Audio steganography with LSB implementation.

KEYWORDS: **-** steganography**,** LSB. Images. Pattern organization techniques, perception, patterns, Data Encryption.

1 INTRODUCTION

In steganography, the message which is needed to be sent is masked in such a way that an unauthorized person would not know whether any secret communication is occurring or not. Hidden messages inside digital transporters has become famous ([1,2]). An extreme rise in demand and consumption of multimedia has reacted in data hiding techniques for files like audio (.wav), images. Digital images are first performable source for hiding message. The process of hiding in formation is called an embedding. Least Significant Bit (LSB) embedding is the most commonly used steganographic technique. In LSB wrapping, the LSBs of unprocessed images are replaced with the message bits [3, 4]. The contain of embedding (the number of bits embedded) referred to as level, is given as the Percentage of the total amount of pixels. Steganalysis will analyze whether a given data, contains any secret message covered into it. We will be focus on steganalysis of images. Natural images have few statistical properties. These get disturbed due to steganographic operations. A steganalyst inspect this fact by analyzing the images. We offer some new effective techniques for identify and analysis of steganographic encapsulate content. Our approach is to fuse various techniques together viz. statistical, pattern recognition techniques, run length, transform coding techniques, and also encryption techniques. Using our proposed measures, we present that with statistical and pattern classification techniques, we will achieve distinguished schemes for identifying embedding at different stages. Hear methodologies are based on a few statistical characteristics of bit strings and wavelet coefficients of image pixels.

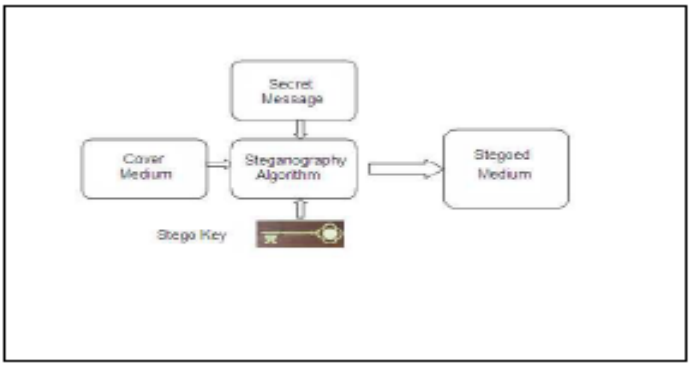

Figure:1 Typical Steganography Model

1.1 Digital Images

To store an image on computer, it is divided into small parts called pixels. The value of intensity of these pixels is stored for three basic colors as an image on computer. '.bmp', '.pnm' is some file formats to store such images, which are uncompressed file formats for images. These images have a lot of repetition. Also the loss of small information in pixel intensity is not visible by the human eye. So there is presence of compression techniques like jpeg for images. The compression techniques will try to de-correlate the repetition and may also introduce some loss of information [5, 6, 7]..

1.2 LSB Steganography for Uncompressed images

One simple and yet effective method of steganography is LSB replacement. As men- tioned, small perturbation in pixel intensity is not detected by an eye; these techniques take advantage of it by changing the LSB of a few pixels. The algorithm used will decide

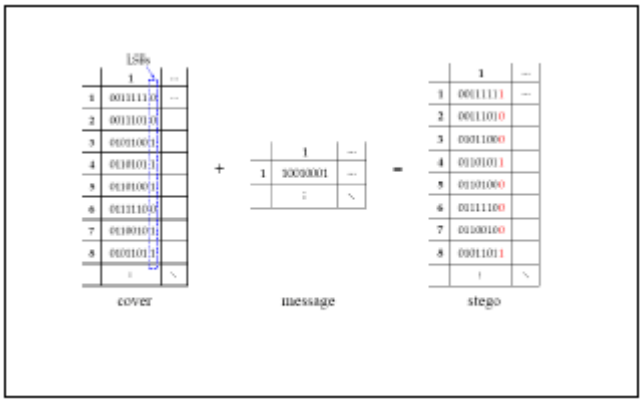

Figure:2 LSB Steganography

Which pixels in an image to be modified. Some algorithm will pick the pixels in image at regular interval depending upon image size and message size. Sophisticated stegano- graphic software viz. S-Tools [7], CSA-Tool [8] can add further layers of complexities, such as distributing messages in a pseudo-random way and encrypting messages. The disadvantage of such schemes is that lousy compression techniques cannot be applied on such images after the process of embedding as information is hidden in LSBs which are highly susceptible to change. This technique is explained in Fig. 2. One byte of the message, the middle one in the Fig. 2.is embedded into the LSBs of eight consecutive pixels in the cover image by modifying the eight LSBs of the eight pixels in the cover image to the same as those in the message, right in figure.

1.3 LSB Steganography for JPEG images

For compressed image formats (e.g., JPEG), LSB insertion is performed on the compressed data, for instance, the quantized DCT coefficients in a JPEG image. Similar to embedding in raw pixels, LSB insertion on the compressed data stream introduces.

II. RELATED WORK

D. AlaaTaqa, A.A.Zaidan, B.B.Zaidan, "New framework for high securedata hidden in the MPEG,JPEG,PNG using AE Sand DES encryption and decryptions technique ", 2009 .

It uses a combine approach between cryptography and steganography.In this method a Secret key steganography and AES (Advanced Encryption Standard) method is used for hiding secure data . by this technique we can hide large amount of data.

E. Kirti Upreti, Kriti Verma, Anita Sahoo, "Variable bits secure system for color images", 2010 .

Proposed approach taken for identification like variable byte and bits. In this method the secret message is converted into two types of the plain texts and the two cipher texts generated by using RSA and IDEA algorithms. This approach is the idea in image steganography, where variable number of bits of encrypted data can be stored in Data channel and their number in Indicator channel and the use of both channels ensure minimum distortion .by this method very high capacity with minimal distortions is obtained.

F. Subba Rao Y.V, Brahmananda Rao S.S, RukmaRekha N, "Secure image steganography based on randomized sequence of cipher bits"2011 .

Proposed the use of random cipher bits for secured image steganography. In this author generates the random sequence of cipher bits using an L.F.S.R (Linear Feedback Shift Register) and select the random sequence approximate same as the image and then embed these random them. The strong point of our approach is that there is no one to one mapping between a cipher text and an image. The drawback of the given approach is hiding large data in single image.

G. SosS.agaian, RavindranathC.cherukuri, Ronnie sifuentes, "A new secure adaptive steganographic algorithm using Fibonacci numbers",2006 .

Proposed the algorithm based on Fibonacci bit-planed decomposition and T-order statistics. the T-order statistics enables the embedding of classified data in noisy portions of an image and the Fibonacci bit-plane decomposition enables the decomposition of an image based on Fibonacci numbers creates more number of bit planes. The advantage of the given approach is the enhancement of the technique.

H. Wen-Jan Chen, Chin-Chen Chang, T-Hoang Ngan Le, "High payload steganography mechanism using hybrid edge detector", 2010

Proposed a steganography process. It was based on the LSB steganography mechanism and a hybrid edge. The hybrid edge detector works on two stages .initially it is applied on the cover image and then the classified message is embedded in the edges of the image using same technique (LSB). By this a better quality of image can be produced. But the capacity is limited on the edges of the cover image.

I. Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "RG intensity based variable bits image steganography", 2008 .

Proposed an algorithm for RGB image steganography, in this, the values of R, G and Bare used to decide the number of bits . one of the three channels is used as the indicator and data stored on either of the two channels other than indicator. lower color component can store higher number of bits. It offers very good capacity

J. K. Pramitha, Dr. L. Padma Suresh, K. L. Shunmuganathan, "Imagesteganography using mod-4 embedding algorithm based on imagecontrast", 2011 [17]

Given a new technique based on image contrast for gray scale images. In this process group of 2x2 blocks of spatially adjacent pixels is selected as the valid block for embedding the private message and then modulo for operation is applied on each valid block . secret message is encrypted by RSA encryption algorithm . the given approach also increases capacity of the secret data .

Vinay Pandey1, Manish Shrivastava2, Medical Image Protection using steganography by crypto-image as cover Image, ***International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)Volume-2 Number-3 Issue-5 September-2012.***

Fast and secure transmission is very much needed in today scenario,. In this paper we propose a new technique to cipher an image for secure transmission. Our research is focused on image cryptography, data hiding and steganography. One of the methods to encrypt binary images is by using watermarking technique the watermarking is used to embed invisibly message inside the image. To embed the encrypted image in the patient information we have used a watermarking technique .it shares a secret into a number of shares so that only a pre determined group of share holders reveals the secret whereas the secret reconstruction is impossible for any unauthorized set of shareholders. Visual cryptography is a kind of secret sharing in which the secret reconstruction can be done only by the HVS .In previous method owner encrypts the original unprocessed image using an encryption key and then a data hider attaches additional data into the encrypted image using. a data-hiding key But to decrease transmission time the data compression is necessary .in recent years a new difficulty is trying to merge in a single step, compression, an decryptions and data hiding . Few solutions have been proposed recently to combine image encryption and compression.. Since the entropy of encrypted image is maximal, the wrapping step, considered like noise, is not possible by using regular data hiding algorithms. A new plan is to apply reversible loss less data hiding algorithms on encrypted images by removing the embedded data before the image decryption. But if the key leaks ten the intruder can encrypt or decrypt message to resolve this problem we use steganography by using crypto-image of other medical image so we finds that the other encrypted image covers the embedded image

III.PROBLEM IDENTIFICATION

The goal is the hidden communication. So, a basic necessity of this steganography system is that the hidden message should not be visible to human beings. The other purpose of steganography is to avoid drawing intuition to the existence of a hidden message. This approach has become famous recently.

The various problems are handled by steganalysis.

Security of Hidden Communication: The hidden data should not be visible both perceptually and statistically so as to avoid the suspicions. Size of Payload: Steganography requires a large amount of wrapping capacity. needed for higher payload and secure communication are very conflicting. Depending on the specific application, a tradeoff has to be looked after.

1. A used security tools based on steganography techniques.
2. To explore methodology of hiding data record using encryption module of this project
3. To extract techniques of getting confidential data using encryption and decryption module.
4. Identified by wrapping algorithm
5. Detection of presence of hidden message in cover signal
6. Prediction of location of hidden message bits
7. Estimation of secret key used in the embedding algorithm

   Steganography occasionally is used when encryption is not allowed to use. Or it is used to supplement encryption part. An encrypted file can still hide information by means of steganography, so even if the encrypted file is decode, the hidden message is invisible.

IV. PROPOSED APPROACH

We made schemes for LSB Steganalysis under following assumptions [11, 12].

1. The hidden message contains approximately equal number of positive and negative.

2. The embedded bits are uniformly distributed in an image.

3. LSB changing technique is used by the steganography technique.

For I experiments, we used different type of images that contain important hidden information. These are images taken with a Nikon Coolpix camera at full 8M resolution with important of different images save unmeasured format. Different images are crop to get 800x600 images without doing image step by step operations processing. Let,

I = {I: j = 0, 1, 2 . . . 14} be the set of natural simple up colored images.

K: The initial LSB embedding represent given image. I.e. k% LSB's of an image had been upgrade by steganographic operations technique.

Ski: The Start Image that is an image. I with k% embedding.

(K is the unknown to be detected.)

I: The force wrapping level.

Ski: An image I with k% original embedding and I% forced embedding.

IV. RESULT

TABLE I. STEGO-IMAGES (.BMP) OF SIZE (WIDTH × HEIGHT × LENGTH)

TABLE II. RECORDED RESULTS OF PERFORMANCE EXPERIMENTS

	Classic-LSB Technique			Proposed LSB Technique		
Stego-Image	*Butterfly*	*Garden*	*Girls*	*Butterfly*	*Garden*	*Girls*
Length of Secret Message (Characters)	1000	1000	2000	1000	1000	2000
Number of LSB Changed	1972	4001	8081	1508	2987	5760
Signal to Noise Ratio (SNR) of the Stego-Image	51.930	50.107	51.377	53.115	51.890	53.360
Time of Hiding Operation (Second)	0.047	0.140	0.421	3.76	7.005	60.372
Time of Extracting Operation (Second)	0.110	0.125	0.421	0.109	0.124	0.421

The GUI has adjustable provisions for setting phase and setting the frequency of cycles. It shows the input x-ray image in two formats original grayscale and negative of that image. The transformed result that image. Have plot in x scale and y scale .the wraping of value for the thread in were best finding were noted.

V. CONCLUSION

This is to boost the performance of the Classic-LSB image steganography technique was present in this paper. The LSB image steganography technique was advised to break the long message into small divisions. Then hide the short divided message in different parts in the pixels of the stego-

image. The purpose of this technique is to reduce the amount of LSB that has been changed from the pixels of the stego-image and hence very difficult to be attacked by HVS. The recorded results showed that the proposed LSB image steganography technique increases security of the secret message hidden in the stego-image. That is done by decreasing the number of LSB. The limitation of the proposed LSB is in the long hiding time that is spend during the thorough search to locate the best matching required for large size stego-image.

VI.APPLICATION

Steganography can be used when we need to hide data. The main reason for hiding data is to prevent unauthorized persons from being aware of the existence of a message.

1. Steganography can be used to hide secrets of a company or plans of a new invention. With the help of steganography, we can send out trade secrets without anyone at the company being aware and hence prevents corporate espionage.

2. Steganography can be also used to hide secret data and copyright information.

VII. FUTURE WORK

The ridge let transform is very stable with respect to steganographic operations, we may infer that one should used for digital water marking purposes, this transform would lead to robust watermarking schemes.

Apart from this point segmented LSB is more secure than the classical LSB.

REFERENCES

[1]Cheddad, J. Condell, K. Curran, & P. Kevitt, (2010). Digital image steganography- survey and analysis of current methods. Signal Processing, 90, 727–752. doi: http://10.1016/j.sigpro.2009.08.010

[2] Adnan Gutub, Ayed Al-Qahtani, &Abdulaziz Tabakh. (2009). Triple-A: secure RGB image steganography based on randomization. AICCSA, IEEE/ACS International Conference on Computer Systems and Applications, Rabat, Morocco, 400-403, doi: http://doi.ieeecomputersociety.org/10.1109/AICCSA.2009.5069356

[3] Kaur, R. Dhir, & G. Sikka. (2009). A new image steganography based on first component alteration technique. International Journal of Computer Science and Information Security (IJCSIS), 6, 53-56. http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf

[4] Alvaro Martin, Guillermo Sapiro, &Gadiel Seroussi. (2005). Is Steganography Natural. IEEE Transactions on Image Processing, 14(12), 2040-2050. doi: 10.1109/TIP.2005.859370

[5] Bhattacharyya, A. Roy, P. Roy, & T. Kim. (2009). Receiver compatible data hiding in color image. International Journal of Advanced Science and Technology, 6,15-24. http://www.sersc.org/journals/IJAST/vol6/2.pdf

[6] EE. Kisik Chang, J. Changho, & L. Sangjin. (2004). High Quality Perceptual Steganographic Techniques. Springer. 2939, 518-531. doe: 10.1007/978-3-540-24624-4_42, http://www.springerlink.com/content/c6guuj5xnyy4wj3c/

[7] C. Kessler. (2001). Steganography: Hiding Data within Data. An edited version of this paper with the title "Hiding Data in Data". N.F. Johnson, & J. Suhil. (2006). Exploring Steganography: Seeing the Unseen. Computing Practices. http://www.jjtc.com/pub/r2026.pdf

[8] P.Mohan Kumar, &D.Roopa (2007). An Image Steganography Framework with Improved Tamper Proofing. Asian Journal of Information Technology, 6(10), 1023-1029. ISSN: 1682-3915. http://medwelljournals.com/abstract/?doi=ajit.2007.1023.1029

[9] Po Yuch Chen, & Hung Ju Lin. (2006). A DWT Based Approach for Image Steganography. International journal of Applied Science and Engineering, 4(3), 275-290. http://www.cyut.edu.tw/~ijase/2006/4-3(Microsoft%20Word%20-%20010-009-6).pdf

[10] Ran-Zan Wang, &Yeh-Shun Chen. (2006). High Payload Image Steganography Using Two-Way Block Matching. IEEE Signal Processing letters, 13(3), 161-164. doi: 10.1109/LSP.2005.862603

[12] Ross J. Anderson & Fabian A.P. Petit colas. (1998). On The Limits of steganography. IEEE Journal of selected Areas in communication, 16(4), 474-481. Special Issue on Copyright and Privacy protection. ISSN 0733-8716. http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf

[13] SorinaDumitrescu, &Xiaolin (2005). A New Framework of LSB Steganalysis of Digital Media. IEEE Transactions on Signal Processing, 53(10), 3936-3947. doi: 10.1109/TSP.2005.855078

[14] Xinpeng Zhang, Shuozhong Wang, &Zhenyu Zhou. (2008). Multibit Assignment Steganography in Palette Images. IEEE Signal Processing Transactions, 15, 553-556. doi: 10.1109/LSP.2008.2001117

[15] Sukhpreet Kaur, Summit Kaur (2010). A Novel Approach for Hiding Text Using Image Steganography. (IJCSIS) International Journal of Computer Science and Information Security, 8(7), October. http://www.scribd.com/doc/40763180/A-Novel-Approach-for-Hiding-Text-Using-Image-Steganography

.

