Coalesced Technique in Steganographic Images Using Encoded Conversion for Augmented Security

Jagan Raj J
Ph.D Research Scholar, Dept. of Computer Science,
Thiruvalluvar Govt. Arts College, Rasipuram, Tamil Nadu, India
Email: jae.jaganraj@gmail.com
Dr. C. Kavitha
Asst. Professor, Dept. of Computer Science,
Thiruvalluvar Govt. Arts College, Rasipuram, Tamil Nadu, India
Email: kavithachellappan@yahoo.com

Abstract- Information security is major concern now a days as number of users using internet are increasing and information getting shared every second. This has also increased the cyber-crime and threat for the information being shared. Two important techniques being used for information security are steganography and cryptography. Encoding the secret test into another form is called Cryptography and it is basically secret writing; on the other side Steganography is hiding a data. In this article, a hybrid technique is introduced by combining the cryptography, compression and Steganography properties. This proposed algorithm works on spatial domain, which also use the space efficiently.

Keywords- Steganography, Cover image, Encryption, compression.

1. INTRODUCTION

In the last few years information security has become one of the critical issues in communication system. With the passage of time, requirements for security have been changing tremendously. Before the emergence of computer and network communication facilities, information security was primarily provided by physical and administrative means. But with the introduction of computer, distributed systems and the use of internet, automated tools are needed to protect information stored on the computer and measures are also needed to protect the data during their transmission also. There are various forms of security attacks which demands high level of security.

Steganography is the scientific discipline of covert communication by concealing information in another media. It refers to the process of hiding the presence of the secret message. It is an art of covert writing. It does not keep the message secret but it provides the secrecy of the message. Steganography hides a secret message from the third party. It does not arouse an eavesdropper's attention. According to Dictionary.com- "Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message". The Steganography term is deducted from the Greek words "stegos" implying "cover" and "grafia" implying "writing" and literally means "Cover writing" [1]. Any steganography technique must satisfy a no. of requirements- the integrity of the secret message which is embedded in stego-object must be accurate; the alteration in the stego-object should not be detected by the naked eye; choice of stego-object must be dependent on the size of secret message to be hidden and last but not the least we must always presume that malicious person knows that steganography is being used (that the stego-object is carrying some secret message).

A typical Steganography system consists of following elements:

A. Cover Object (C)
B. Secret Message (M)
C. Stego Object (S)

A. Cover Object

In Steganography, cover objects are those in which we hide secret message. The cover object can be any files like images, audio, videos, text. The most used cover object for hide information is image.

B.Secret Message

In Steganography, the secret message is the message to be hidden in cover object. The secret message can be images, text messages etc.

C. Stego Object

The stego object is generated after hiding the secret message in cover image. After that stego object is transmitted and then at receiver side processing is done on stego object to retrieve message from it.

The first step in steganography is to pass both the secret message and the cover message ie., the image file, into the encoder. In the encoder, protocols will be implemented to embed the given secret message into the media file. The type of protocol to use will depend on what kind of information you are trying to embed and where you are embedding it in. For example, you can use an image protocol to embed information inside any image file. A key is often needed in sender's end for embedding process. This can be a public or private key, so that you can encode the secret message with your own private key and then the recipient can decode it using his/her public key. When embedding the information in this way, you can reduce the chance of a third party attacker getting hold of the stego object and decoding the same to find out the secret message. In general, the embedding process inserts a mark in an object.

Having passed through the encoder, a stego image will be produced. A stego image is the original cover object with the secret information embedded inside in it. This object should or always look identical to the cover object as otherwise a third party attacker can see embedded information. Having produced the stego image, it will then be sent through some communications channel, such as secure copy, ftp or email to the intended recipient for decoding. The recipient will decode the stego object in order to view the secret information. The decoding process is simply the reverse of encoding process followed. It is the extraction of secret data from a stego image.

In the decoding process, the stego image is fed in to the system. The private or public key can decode the original key that is used during the encoding process is also needed so that the secret information can be decoded in receiver's end. It depends on the encoding technique, where sometimes the original cover object is also needed during the decoding process. Otherwise, there may be no way of understanding or extracting the secret message from the stego image. Once decoding process is completed, the secret message embedded in the stego-image can then be extracted and seen. The generic decoding process again requires object, S. The result will be either the retrieved secret message from the object or indication of the likelihood of M being present in image C. Different types of robust marking systems use different inputs and outputs. A formula for this process can be:

Cover Object (C) + Secret message (M) = Stego-Object (C)

The typical flow of a steganography process is as mentioned in figure-1

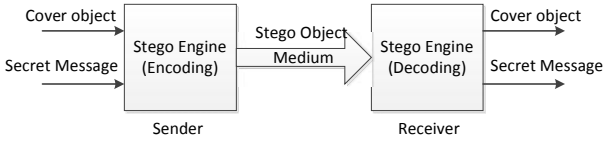

Fig.1: Encoding and decoding in steganography

CATEGORIES OF STEGANOGRAPHY

Various categories of steganography are listed below [2] [3] [4]

Text Steganography

In text steganography, text is used as cover object. It hides secret message behind the other text file. It is done by modifying the text or by modifying some features of text components. Different methods used are line-shift coding, word-shift coding and feature coding. Text steganography was very much used in ancient times, but today these techniques have become obsolete. It is also known as linguistic steganography.

Image Steganography

In image steganography, images are used as cover object. It hides secret messages into digital images. It makes use of the weakness of HVS as it cannot detect any variation in luminance part of color pixels. There are different algorithms for different file formats of images. These are Least Significant bit (LSB) insertion, Masking and Filtering etc. JPEG, PNG, GIF (Graphics Interchange Format) etc. are the file formats for images which are used.

Audio Steganography

In this, digitized audio signal is used for embedding secret message which produce modification of binary sequence order of the corresponding audio file. By inserting non-hearable tones in audio signal used as cover object data is embedded. Audio steganography exploits the weaknesses of the human auditory system (HAS). It exploits psycho acoustical masking phenomenon (makes a weak tone unperceivable in the existence of a strong tone) of HAS. HAS cannot identify some variations in the sound waves. The methods used are LSB coding, Spread Spectrum, Echo hiding etc. MPEG, MP3 etc. are the file formats for audio which are used.

Video Steganography

In video steganography, video is used as cover object. Since videos are aggregation of images and sounds, that is why many of these techniques can be implemented on video files also. The advantage of concealing secret information in video is the fact that it is a moving flow of images and sounds and a huge amount of information can be concealed inside a video. Any noticeable change might remain unobserved by humans because it is an uninterrupted flow of information. AVI (Audio Video Interleave), MPEG, DIVX, and MP4 etc. are the file formats for video which are used.

Protocol Steganography

It is the process of hiding information in network control protocols that are used in network transmission. It is also known as network steganography. Steganography can be used on the covert channels which exist in the OSI network model layers. Network protocols used in the mechanism are TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol) etc.

The techniques including image steganography, audio steganography, video steganography and protocol steganography are collectively known as technical steganography.

2. RELATED WORKS

Many researchers have been done till now in the field of steganography. Many papers on the recent researches and developments in the field of steganography were studied. The literature survey basically provides a way to investigate for research and gives an idea of what has been done till date. A succinct review based on the study of these papers related to our work is as follows.

Diwedi Samidha et al. [5] described several image steganography techniques in spatial domain. Along with existing techniques like LSB, layout management schemes and replacing only l's or only zero's, some more methods like replacing intermediate bit, raster scan principle, random scan principle, color based data hiding and shape based data hiding are also proposed. These new techniques are based on random selection of pixels for data hiding considering many parameters of an image like physical location and intensity value of pixel, etc.

Sourabh Chandra et al. [6] proposed a symmetric key cryptographic algorithm which is content based. This algorithm included binary addition operation for encrypting the plain text and circular shift operation and folding method for making the key secure. This algorithm posed a difficulty for opponent to decrypt the key and text.

Amrit Pal Singh et al. [7] developed an improved method for image based steganography using LSB technique. It is based on by slicing the three planes of RGB image and then hiding the data into each plane based on color sensitivity by using LSB technique. It resulted in high embedding capacity and better image quality. Its PSNR value was better than previous steganographic methods. Embedding Recovery

YogitaBirdi et al. [8] proposed a method in steganography for secure communication. First, data is encrypted and then embedded using raster scan technique. This method made use of the Raster Scan Principle of displaying an image on CRT (Cathode Ray Tube) display. In this pixels have been hidden in the cover image in left to right and right to left manner. This made data extraction difficult for the opponent.

Motivation

Due to advancement in technology the number of attacks increases on internet so data security required so in this paper proposed a hybrid technique for data security by using cryptography and steganography properties. We took the motivation from literature work papers they work on variable block size and data hiding in different ratios so it's difficult to Steganalysis of data.

Proposed Algorithm

Encoding algorithm

Compress the secret message as compressed text using Lempel-Ziv-Welch losless algorithm. Let M be the secret message, LZW compresson algorithm and Tc compressed text

LZW(M) = Tc

Encrypt the compressed text as encrypted text using asymmetric cryptograpic algorithm. Let Tc be the compressed text, ASC asymmetric cryptography, Kpu be the public key

ASM(Tc,Kpu) = Te

Convert Te to binary format and find the cardinality for the output

|Te |=Rb

Generate random numbers for empbedding encrypted text, Let Rbbe number of random numbers required, RE Random engine, Srshared random seed, Pl is pixel list

RE(Rb,Sr)= A, where A is {(a) : a A,n(a)=|Te |}

Generate stego object using proposed random LSB technique by storing length of the bits to read in first 8 bits, Let Osbe stego object f(x,y) is the function that embeds the value in cover object, where x is Rbi and ai

f(Rbi,ai)= Os,

whereRbi Rb,A is {(a) : ai A,n(a)=|Te |}

Send the stego object in network

Decoding algorithm

Read first 8 bits from Stego object's LSB and store the result as Sr

Generate random number list, A for encrypted text, using Sr, shared random seed of size Rb

RE(Rb,Sr) = A, where A is {(a) : a A,n(a)=|Te |}

Take the LSB of each element in A and generate the bit patterns for encrypter text Te from Os

f(Os,ai) = Te

Decrypt the encrypted text using asymmetric cryptograpic algorithm. Let Tc the compressed text, ASC asymmetric cryptography, Kpr be the private key

ASM (Te,Kpr) = Tc

Generate the secret message from compressed text using Lempel-Ziv-Welch losless algorithm. Let M be the secret message, LZW compresson algorithm and Tc compressed text

LZW (Tc) = M

Results and Comparison

Below are the space utilization comparison of Secret text (M) using tradiional LSB algorithm and the proposed algorithm for various secret texts [9], [10] and [11]

A. With existing LSB algorithm

Table.1.No. of LSB required for sample files using traditional LSB technique

File Name	Original size of Message (M) (in bytes)	No of LSB positions required for Message in Stego object (in bytes)
lzw-intro.txt[9]	4060	4060
lzw-decoding.txt[10]	1068	1068
Afaf-Meleis.txt[11]	9732	9732

B. With proposed algorithm

Table.2 No of LSB required for sample files using proposed technique

File Name	Original size of Message (M) in (bytes)	No of LSB positions required for Message in Stego object (in bytes)	No of LSB required for Message Length storage in Stego object (in bytes)	Total LSB position required for proposed algorithm (in bytes)
lzw-intro.txt	4060	4060	8	4068
lzw-decoding.txt	1068	1068	8	1076
Afaf-Meleis.txt	9732	9732	8	9740

Result comparison

Space utilzation comparison between traditional LSB and proposed technique for secret message in Stego Objecct

File Name	No of LSB positions required for Message in stego object (in bytes)	Total LSB position required for proposed algorithm (in bytes)	Efficiencyof space utilization in stego object by proposed algorithm
lzw-intro.txt	4060	2507	38%
lzwdecoding.txt	1068	782	27%
Afaf Meleis.txt	9732	5743	41%
Average efficiency acquired (in %)			35%

6. CONCLUSION

Based on the series of the test results and observations gathered, it shows that the researchers were able to hide a secret message in stego object with constraint on the available LSB requirement. The enhanced LSB technique described in this project helps to successfully hide the secret data into the cover object without any distortion. Steganographic secrecy results are best when selecting the proper mechanisms. However, the stego medium which seems innocent enough may, upon further investigation, actually broadcast the existence of embedded information development in the area of covert communications and steganography will continue. Proposed mechanism of steganography will ensure the reduced space utilization in the stego object, by which more payload of secret message can be embedded.

REFERENCES

[1] G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551, April 1955.

[2] H. Gupta, Prof. R. Kumar, and S. Changlani, “Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method”, International Journal of Emerging technology and Advanced Engineering(IJETAE), vol. 3,no. 6, pp. 212–214, June 2013.

[3] S. Suri, H. Joshi, and V. Minocha and A. Tyagi, “Comparative Analysis of Steganography for Coloured Images”, Intrnational Journal of ComputerSciences and Engineering(IJCSE), vol. 2, no. 4, pp. 180–184, 2014.

[4] B. Madhuravani, D. S. R. Murthy, P. B. Reddy and K. V. S.N. R. Rao, “Strong Authentication Using Dynamic Hashing and Steganography”, IEEE International Conference on Computing, Communication and Automation(ICCCA), pp. 735–738, 2015.

[5] D. Samidha and D. Agrawa, “Random Image Steganography in Spatial Domain”, IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System(ICEVENT), pp. 1–3, 2013.

[6] S .Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, “Content Based Double Encryption Algorithm Using Symmetric Key Cryptography”, Procedia computer Science International Conference on Recent Trends in Computing(ICRTC), vol. 57, pp. 1228–1234, 2015.

[7] A. Singh and H. Singh, “An Improved LSB Based Image Steganography Technique for RGB Color Images”, IEEE International Conference on Electrical, Computer and Communication technologies, pp. 1-4, 2015.

[8] Y. Birdi and Harjinder Singh, “Raster Scan Technique for Secure Communication in Steganography”, International Journal of AdvancedResearch in Electrical, Electronics and Instrumentation Engineering, vol.4,no.6,pp.5174–5179,2015.

[9] lzw-intro.txt,https://en.wikipedia.org/wiki/Lempel%E2%80%93Ziv%E2%80%93We lch#Algorithm

[10] lzw-decoding.txt, https://en.wikipedia.org/wiki/Lempel%E2%80%93Ziv%E2%80%93Welch#Decoding

[11] Afaf-Meleis.txt,https://en.wikipedia.org/wiki/Afaf_Meleis

[12] Jagan Raj.J and Prasath.S, “Enhancing the data security and data integrity in steganographed images by store bit randomization”,International Journal of Innovative Technology and Creative Engineering, vol.5, no.12,2015.

[13] Jagan Raj J and Prasath S. Article: Validating Data Integrity in Steganographed Images using Embedded Checksum Technique. IJCA Proceedings on National Conference on Research Issues in Image Analysis and Mining Intelligence NCRIIAMI 2015(1):5-8, June 2015.