IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

Text Security using Lossless Portable Network Graphics

Swapnali Patil [1], N. R. Wankhade[2], J. V. Shinde[3]

Student, Comp Dept, Late Sapkal C.O.E., Nashik, India [1]

Asst. Professor, Comp Dept, Late Sapkal C.O.E, Nashik, India [2]

Assoc. Professor, Comp Dept, Late Sapkal C.O.E, Nashik, India [3]

Abstract: Data is an important asset for any individual or organization and must be protected from intruders or hackers. The need to hide data from hackers has existed since ancient times, and nowadays, there are developments in digital media, such as audio, video, images, and so on. To secure secret information, different media methods are used and steganography is one. Steganography hides the data under other data without any differentiable changes. Many individual steganography tools can be used to transfer data securely and, in this report, a new tool is proposed that decreases time and effort. Using this tool, we hide the text in images in one place, so there was no need to have access to multiple tools. This proposed tool developed using the least significant bit (LSB) approach. Steganography is a method of hiding secret messages in a cover object while communication takes place between sender and receiver. Security of confidential information has always been a major issue from the past times to the present time. It has always been the interested topic for researchers to develop secure techniques to send data without revealing it to anyone other than the receiver. There for from time to time researchers have developed many techniques to fulfil secure transfer of data and steganography is one of them. In this paper we have proposed a new technique of image steganography i.e. Hash-LSB with RSA algorithm for providing more security to data as well as our data hiding method. The proposed technique uses a hash function to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image. This technique makes sure that the message has been encrypted before hiding it into a cover image. If in any case the cipher text got revealed from the cover image, the intermediate person other than receiver can't access the message as it is in encrypted form.

Keywords: Cryptography, Steganography, LSB, Hash-LSB, RSA Encryption -Decryption.

I. INTRODUCTION

Globalization has led to the rapid growth of the internet through which consumers can send and receive large amounts of data (e.g., text, audio and images). In modern communication systems, securing data is of utmost importance. Yet sending and receiving secret files over the internet is still insecure, and therefore hiding data in an effective way protects this secret information. Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference.

Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data.

Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction.

II. OBJECTIVE

- Requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings.
- The other goal of steganography is to avoid drawing suspicion to the existence of a hidden message.
- Work on image pixels so we can maintain image quality.
- Robust communication between sender and receiver.

III. LITERATURE SURVEY

Title: Steganalysis Features for Content-Adaptive JPEG Steganography

The basic need of every growing area in today's world is communication. Everyone wants to keep the inside

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

information of work to be secret and safe. We use many insecure pathways in our daily life for transferring and sharing information using internet or telephonically, but at a certain level it's not safe. Steganography and Cryptography are two methods which could be used to share information in a concealed manner.

Cryptography includes modification of a message in a way which could be in digesting or encrypted form guarded by an encryption key which is known by sender and receiver only and without using encryption key the message couldn't be accessed.

But in cryptography it's always clear to intermediate person that the message is in encrypted form, whereas in steganography the secret message is made to hide in cover image so that it couldn't be clearer to any intermediate person that whether there is any message hidden in the information being shared. The cover image containing the secret message is then transferred to the recipient. The recipient is able to extract the message with the help of retrieving process and secret key provided by the sender.

Title: High Capacity Lossless Secure Image Steganography

The needs for steganographic techniques for hiding secret message inside images have been arise. This paper is to create a practical steganographic implementation to hide text inside grey scale images. The secret message is hidden inside the cover image using Five Modulus Method. The novel algorithm is called (ST-FMM. FMM which consists of transforming all the pixels within the 5×5 window size into its corresponding multiples of 5. After that, the secret message is hidden inside the 5×5 window as a non-multiples of 5.

Since the modulus of non-multiples of 5 are 1,2,3 and 4, therefore; if the reminder is one of these, then this pixel represents a secret character. The secret key that has to be sent is the window size. The main advantage of this novel algorithm is to keep the size of the cover image constant while the secret message increased in size.

Peak signal-to-noise ratio is captured for each of the images tested. Based on the PSNR value of each images, the stego image has high PSNR value. Hence this new steganography algorithm is very efficient to hide the data inside the image.

Title: Text Security using Image Steganography

Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. Although related, Steganography is not to be confused with Encryption, which is the process of making a message unintelligible—Steganography attempts to hide the existence of communication.

IV. RELATED WORK

Introduction Model

Steganography derives from the Greek word steganos, meaning covered or secret, and graphy (writing or drawing). On the simplest level, steganography is hidden writing, whether it consists of invisible ink on paper or copyright information hidden in an image file.

Where cryptography scrambles a message into a code to obscure its meaning, steganography hides the message entirely. These two secret communication technologies can be used separately or together—for example, by first encrypting a message, then hiding it in another file for transmission. As the world becomes more anxious about the use of any secret communication, and as regulations are created by governments to limit uses of encryption, steganography's role is gaining prominence.

What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside of them, although there are programs available that can do what is called Steganalysis (Detecting use of Steganography.) The most common use of Steganography is to hide a file inside another file. When information or a file is hidden inside a carrier file, the data is usually encrypted with a key.

▪ Where Hidden Data hides?

It is possible to alter graphic or sound files slightly without losing their overall viability for the viewer and listener. With audio, you can use bits of file that contain sound not audible to the human ear. With graphic images, you can remove redundant bits of color from the image and still produce a picture that looks intact to human eye and is difficult to discern from its original.

It is in those bits that stego hides its data. A stego program uses an algorithm, to embed data in an image file, and a password scheme to allow you to retrieve information.

- What does the project do?
- ▪ Hiding the text message in an image file.
- ▪ Encryption of the same message, so as to support more secure steganography.
- ▪ The decoding of the message, decryption and source message retrieval are its original form.

Technical Model

- Using java.awt.Image, ImageIO.
- The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images.

Encryption Model

- The steganography technique used is LSB coding.
- The offset of the image is retrieved from its header.
- That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

- For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text which user want to encrypt.

Creation of User Space:

- User Space is created for preserving the original file, so that all the modifications are done in the user space.
- In the object of BufferedImage, using ImageIO.read method we take the original image.
- Using createGraphics and drawRenderedImage method of Graphics class, we create our user space in BufferedImage object.
- The text is taken as input and separated in stream of bytes.
- Now, each bit of these bytes is encoded in the LSB of each next pixel.
- And, finally we get the final image that contains the encoded message and it is saved, at the specified path given by user, in PNG format using ImageIO.write method.
- This completes the encoding process.

Decryption Model: -

The decrypt module is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that. Similar to other approaches. NB combine efficiency with reasonable accuracy.

V. PROPOSED SYSTEM

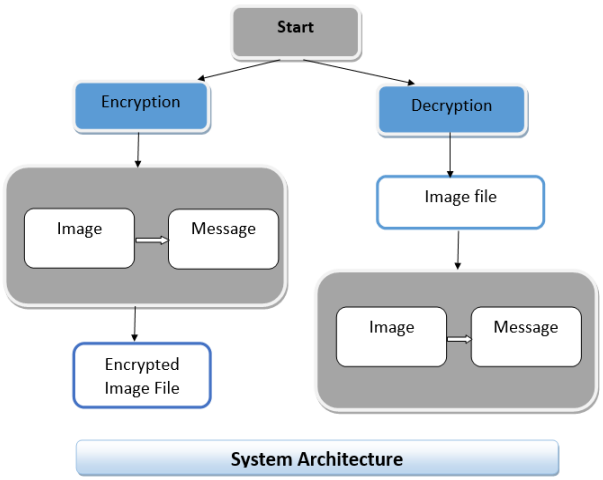

Fig 1 System Architecture

The architecture system itself defines the all scenarios of the image steganography. User first select the input image file then add secrete text message using encryption technique. At receiver side user decrypt the image file using key and get the original message.

Hiding Secret Messages in Digital File: -

Figure 2 describes hiding a secret file in a cover file, we began by selecting a key file and an acceptable cover file. The tool alters and modifies the bits of the cover image to allow the insertion of the secret message in the cover image. After this insertion is completed, a new, acceptable file is generated. This new file is called a stego file.

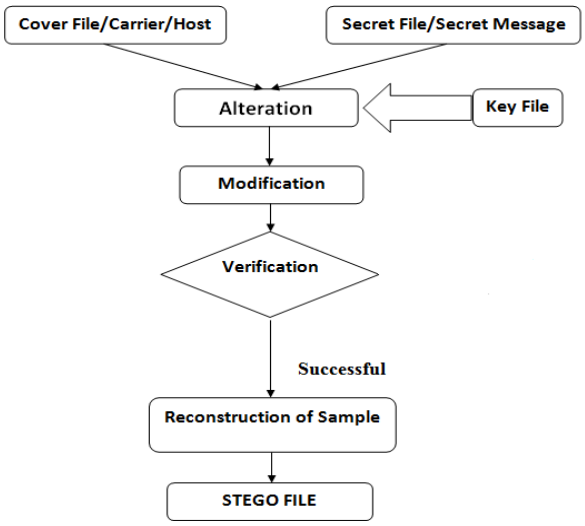

Fig. 3 Encryption process

Secret Message Extraction: -

Figure 3 shows the process of extracting the secret message from the stego file. To extract the secret message, we need the same key file we used to hide the message. We begin by verifying that key file. After verification is successful, the tool extracts the secret message from the cover file.

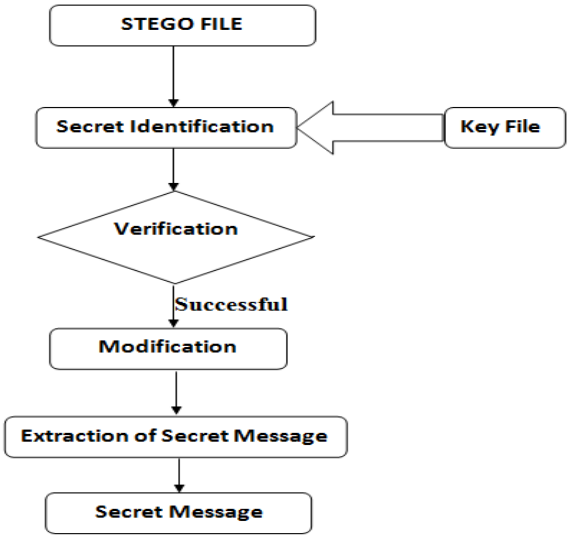

Figure 3 Decryption Process

VI. ALGORITHM

- LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image.
- It is a simple approach for embedding message into the image.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

- The Least Significant Bit insertion varies according to number of bits in an image.
- For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message.
- For 24 bit image, the colors of each component like RGB (red, green and blue) are changed.
- LSB is effective in using BMP images since the compression in BMP is lossless

VII. ALGORITHM WORK

- If we want to hide the data like "Aha!"
- Then we convert the message "Aha!" into ASCII Code and then there equivalent binary code.

A=65 (01000001)
h=104(01101000)
a=97(01100001)
! =33(00100001)

VIII. MATHEMATICAL MODEL

Any steganographic algorithm or simply Stego-algorithm is composed of Stego-Function Ғ and inverse of Stego-Function Ғ-1. Ғ takes Cover-Image C and Information I as input and generates Stego-Image S as the output. At the receiver end the Stego-Image S is fed to decoding algorithm which is mathematically inverse of Stego-Function Ғ(represented as Ғ-1) and produces Information I. These two function along with the entire set of their domain and co-domain form the Steganographic System Ψ (or simply Stego-system).

Mathematically this can be represented as S = Ғ(C, I) and I = Ғ-1
(S) and Ψ = {Ғ, Ғ-1, C, S, I}.

Universal Stego System:
A perfect Depicter of a Stego-Algorithm A same stego-algorithm may operate on different cover images and may insert different information's in them. So any stego system Ψ = {Ғ, Ғ-1, C, S, I} is different for every pair of cover image C and Information I even though the Algorithm of Stego- system Ψ given as Ψ(Algorithm) = { Ғ, Ғ-1} remains the same for all those pairs. So we introduce the concept of Universal Stego System which is Universal Set of all stego systems Ψ = {Ғ, Ғ-1, C, S, I} which have same Stego-Algorithm Ψ(Algorithm) = { Ғ, Ғ-1}. We represent any Universal Stego System by Φ ={ Ғ, Ғ-1, ℂ , 𝕊, 𝕀 } where is set of all cover Images, 𝕊 is set of all stego-images and 𝕀 is set of all Information and stego algorithm of Φ given as Φ(Algorithm) = { Ғ, Ғ-1}. Thus any stego system Ψ = {Ғ, Ғ-1, C, S, I} is an instance of or Universal Stego System Φ = {Ғ, Ғ-1, ℂ, 𝕊, 𝕀}. Mathematically we represent a Universal Stego System Φ as:

$$\Phi = \{Ғ, Ғ^{-1}, ℂ, 𝕊, 𝕀\}$$

{x=x is stego system Ψ = {Ғ, Ғ-1, C, S, I} with stego algorithm { Ғ, Ғ-1}
Stego System Φ = {Ғ, Ғ-1, ℂ, 𝕊, 𝕀} with stego algorithm { Ғ, Ғ-1}}

Where,
ℂ = {C:C is the set of Cover Images}
𝕊 = {S: S is the set of Stego Images}
𝕀 = {I: I is the set of all Information}
Ψ = {Ғ, Ғ-1, C, S, I} and Ψ ∈ Φ

Problem Description: -
Let the system be described by S,
S = {I,ERP,DRP,K,R}
Where,
I = Input
ERP= Encryption Process
DRP = Decryption Process
K = Secrete Key
R = Result

IX. CONCLUSION

Steganography is useful for hiding messages for transmission. One of the major discoveries of this investigation was that each steganographic implementation carries with it significant trade-off decisions, and it is up to the steganographer to decide which implementation suits him/her best. Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

REFERENCES

[1] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key", International Conference on Computer and Information Technology (ICCIT), Pages No. 286 – 291, 22-24 Dec., 2011.
[2] Kousik Dasgupta, J. K. Mandal, Paramartha Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, Issue No. 2, April, 2012.
[3] Mamta Juneja, Parvinder Singh Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", International Conference on Advances in Recent Technologies in Communication and Computing, Pages No. 302 – 305, 27-28 Oct., 2009.
[4] Swati Tiwari, R. P. Mahajan, "A Secure Image Based Steganographic Model Using RSA Algorithm and LSB Insertion", International Journal of Electronics Communication and Computer Engineering (IJECCE), Vol. 3, Issue No. 1, 2012.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 12, December 2016

[5] N. F. Johnson, S. Jajodia, "Steganography: seeing the unseen", IEEE Computer, Vol. 31, Issue No. 2, Pages No. 26 - 34, Feb., 1998.
[6] Wien Hong, Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", IEEE Transactions on Information Forensics and Security, Vol. 7, Issue No. 1, Pages No. 176 - 184, Feb., 2012.
[7] Amr A. Hanafy, Gouda I. Salama, Yahya Z. Mohasseb, "A Secure Covert Communication Model Based on Video Steganography", Military Communications Conference, IEEE, Pages No. 1 – 6, 16-19 Nov., 2008.
[8] R. Chandramouli, N. Memon, "Analysis of LSB based image Steganography techniques", International Conference on Image Processing, Vol. 3, Pages No. 1019 – 1022, 07 Oct 2001-10 Oct, 2001.
[9] Weiqi Luo, Fangjun Huang, Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol. 5, Issue No. 2, Pages No. 201 – 214, June, 2010.
[10] Ross J. Anderson, Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, Issue No. 4, Pages No. 474 – 481, May, 1998.
[11] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, Tong-Yee Lee, "A High Capacity 3D Steganography Algorithm", IEEE Transactions on Visualization and Computer Graphics,Vol. 15, Issue No. 2, Pages No. 274 – 284, March-April, 2009.
[12] Nicholas Hopper, Luis von Ahn, John Langford, "Provably Secure Steganography", IEEE Transactions on Computers, Vol. 58, Issue No. 5, Pages No. 662 – 676, May, 2009.