International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 5, July - 2012

Embedding of Text in Image – A case of High Security Steganography

R.Srinivas [1], D.Sivaraja Kumar [2]
[1] Assoc Professor, [2] Final M.Tech Student
[1]Dept of Computer Science and Engineering,
[2] Dept of Computer Science and Engineering
[1]Aditya Institute of Technology And Management – Tekkali, Srikakulam.
[2]Aditya Institute of Technology And Management – Tekkali, Srikakulam.

ABSTRACT

A steganographic method of embedding textual information in an image file with high security is presented in this paper.In the proposed technique, first the Image file is pixelled and then an appropriate bit of each pixel is altered to embed the textual information. As a steganographic approach the perceptual quality of the host image quality was not to be degraded.

Keywords-**Cover object, Secret Message, Data Embed, Data Extraction, Human Visual System (HVS), Stego-object, Steganography.**

I. INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding important data in digital media and it is an art of sending hidden data or secret messages over a public channel so that a third party cannotdetect the presence of the secret messages. The goal of steganography is different from classical encryption, whichseeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages.

Steganography is generally understood to deal withelectronic media rather than physical objects. Steganography become more important as more people join the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages.There have been numerous proposals for protocols to hide data in channels containing images , video , audio and even typeset text . This makes sense for a number of reasons.First of all, because the size of the information is generally quite small compared to the size of the data in which it must be hidden (the cover text), electronic media is much easier to manipulate in order to hide data and extract messages. Secondly, extraction itself can be automated when the data is electronic, since computers can efficiently manipulate the data and execute the algorithms necessary to retrieve the messages. Electronic data also often includes redundant, unnecessary and unnoticed data spaces which can be manipulated in order to hide messages.

Steganography is the art and science of hidingcommunication.In this workmainly an Image file can be used as a host media to hide secret message with high security using RSA secret Keys without change in the file structure and content of the Image file. Because degradation in the perceptual quality of the cover object may leads to change in the cover object which may leads to the failure of objective of steganography.

II.ASSUMPTION AND SCOPE

It is theart of discovering and rendering useless covert messages. The goal ofsteganalysis is to identify suspected informationstreams, determinewhether or not they have hidden messages encoded into them, and, ifpossible, recover the hiddeninformation. Steganography based on hiding the secret datainto electronic media like image, audio, video and text. For example, an image contains various pixel values. A common image size is 640 × 480 pixels and 256colors (or 8 bits per pixel). Such an image could contain about 300 kilobits of data. Digital images are typically storedineither 24 bit or 8 bit files. A 24 bit image provides themostspace for hiding information. A data – embedding technique into an image file can be based on masking , bit modification , LSB based methodbased on lifting wavelet transform etc. Embedding text into an image file LSB modification creates animperceptible change in the host image file.

A steganography system, in general, is expected to meet three key requirements namely, imperceptibility ofembedding, exact recovery of embedded data, andlarge payload (payload is the bits that get delivered to the end user at the destination) . In a steganographyframework, the technique for hiding the secret message isunknown to unauthorized persons other than the who is the sender and the receiver. Mainly steganographic technic should posses the following desired characteristics :
High Securable: a person should not be able to extract the covert datafrom the host medium without the knowledge of the generatedsecret keys used in the extracting procedure.
Imperceptibility: the medium after being embedded with the Secret message should be indiscernible from the original

medium.One should not become suspicious of the existence of thecovert data within the medium.
Large capacity: the maximum length of the secret message thatcan be embedded should be as long as possible.
Resistance: the covert data should be able to survive when thehost medium has been manipulated, for example by some lossy compression scheme .
Exactdata extraction: the extraction of the secret data from themedium should be exactly and true.

Mainly the goal of steganography is to provide securecommunication like cryptography. Here don't confused steganography with cryptography, Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden.. In cryptography, the system is damaged when the unauthorizedperson can open the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message.

III.RELATED WORKS

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not posses the right keys. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called stego-image is obtained.
Stego-image selected as a host medium in the extraction process to extract the secret message in the stgeo-image. In this work RSA keys used for protecting message data with high security. RSA keys has been used in this work at the time of embedding and as well as extraction process. By using RSA keys the secret message able to read only sender and receiver, other persons not able to read the message without knowing the generated private keys.Using the public key and encryption algorithm, everyone can encrypt a message. The decryption key is known only to authorized parties

The goal of steganography is covert communication. So, a fundamental requirement of this steganography system is that the hider message carried by stego-media should not be sensible to human beings. In case of hiding information in image embeds data with modification of the pixel value image quality cannot perceived by the human visual system(HVS).All these steganographic techniques deal with a fewcommon types of steganography procedure depending on thequality of the host media. That means the cover object which will be used to hidethe secret message.

A human visual system model (HVS model) is used by image processing, video processing and computer visionexperts to deal with biological and psychological processes that are not yet fully understood. It is common to think of "taking advantage" of the HVS model to produce desired effects. Examples of taking advantage of an HVS model include colour television. Originally it was thought that colour television required too high a bandwidth for the then available technology. Then it was noticed that the colour resolution of the HVS was much lower than the brightness resolution; this allowed colour to be squeezed into the signal by chroma subsampling. Another example is image compression, like JPEG. Our HVS says that we cannot see high frequency detail so in JPEG we can quantize these components without a perceptible loss of quality.

Two properties of the HVS dominantly used insteganographic techniques are frequency masking and temporal masking . The concept using the perceptual holes of the HVS is taken from wideband video coding (e.g. MPEGcompression) . In the compression algorithms, the holesare used in order todecrease the amount of the bits needed to encode image quality, without causing a perceptual distortion to the coded image. On the other hand, in the information hiding scenarios, masking properties are used to embed additional bits into an existing bit stream, again without generating visual noise in the image sequence used for data hiding.

IV.DESIGN METHODOLOGY

In this work, an image file with ".jpeg" extension has been selected as host file. Most files are JPEG format.JPEG is used in a number of image file formats. JPEG is the most common image format used by digital cameras and other photographic image capture devices; along with JPEG it is the most common format for storing and transmitting photographic images on the World Wide Web. These format variations are often not distinguished, and are simply called JPEG.

To do that, first one needs to know the file structure of the image file then apply the transformation of host file. Transformation image divided into four equal parts (i.e LL_1,LH_2,HL_3,HH_4),LL_1 image having wanted pixels or approximation pixel and remaining all are unwanted pixels. In this work LH_2 pixels has been selected because it has unwanted pixel values. Modification on the wanted pixel values may effect on the image quality. The pixels that represents the whole data image. Every pixel value representing with the binary values and every binary values have basic two parts, i.e. MSB And LSB. While embedding data, one can't deal with the MSB values. In this paper embedding on the only LSB values with secret message of binary value.

A program has been developed which can read the image file bit by bit and stores them in a different file. Then start with the LSB field to modify them to embed textual information. For example, if the word "message" has to be embedded into an image file one has to embed the binary values of the word “message” into the image pixel value.Consider the following TABLE:

TABLE I
Letters with ASCII values and corresponding binary values

Letter	ASCII Value	Corresponding binary values
m	109	01101101
e	101	01100101
s	115	01110011
s	115	01110011
a	097	01100001
g	103	01100111
e	101	01100101

From the above TABLE, the word “message” into the host image file actually the corresponding 8 bit binary values have to be embedded into the LSB field of that image file.

V.BLOCK DIAGRAM

5.1.EMBEDDING OF DATA

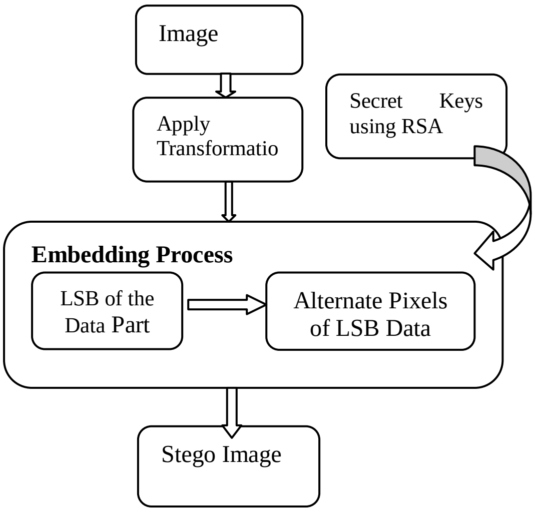

Figure-1: Embedding Of Secret Message

5.2. EXTRCTING OF DATA

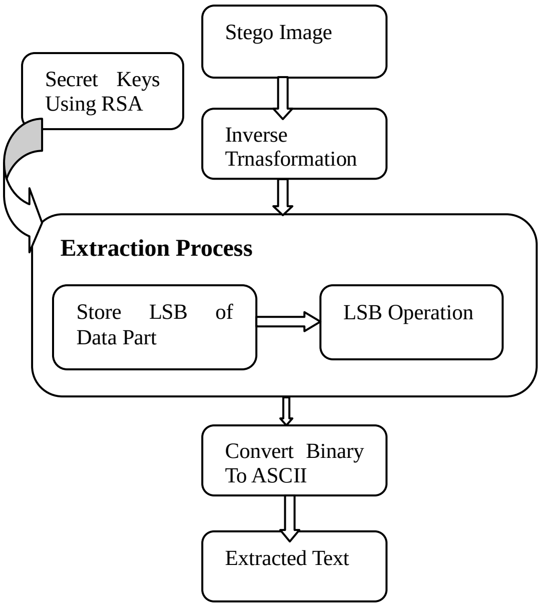

Figure-2: Extraction Of Secret Message

From the above block diagrams fig.1 shows the process of embedding secret message into the host image. From the fig.1 select the host as image file and apply the transformation then read the selected sub image in transformation image and read the pixel values first. Select the first pixel values and embed with the message data at the same time give the secret key using RSA. From the fig.2 select the stego image form the embedded process and apply the inverse transformation then extract the original message from the extraction process using same as LSB method using in the embedded process. Before the embedding process it will ask the generated secrete keys using RSA algorithm, these keys are known only sender.

VI.ALGORITHM

To develop this algorithm multiple bits of each pixel of the file have been changed or modified to insert secret data in it. It has also been observed the degradation of the host image file after modification of the bits. In this work the bit modification was done by 4 bits LSB method, 4 bit change in LSB gave the best result. Thus, data can be embedded according to the following algorithm.

6. 1 . Algorithm (Embedding process)

- Select the host as image file with “.jpeg” extension.
- Apply the transformation of selected host image file.
- Start from a suitable position of the pixel value and convert it to the binary form.
- Edit the least significant bit with the data that have to be embedded and enter the secrete key .

- Take every pixel and change the least significant bit to embed the whole message.

The data extraction algorithm at the receiver’s end follows the same logic as the embedding algorithm.

6.2. Algorithm (For Extracting of Data)

- Select the Stego image as host image file.
- Apply the inverse transformation of selected stego image.
- Start from the suitable pixel position of stego-image ..
- Give the generated keys in the extraction process.
- Check every pixels and store the LSB bit operation and extract the binary values message data.
- Convert the binary values to decimal to get the ASCII values of the secret message.
- From the ASCII find the secret message.

VII.EXPERIMENTATIONAND RESULTS

An image file named “sun.jpg” has been selected for this experiment apply the transformation on the host image and checking the binary values of each pixel. Give the encryption keys at the time of embedding process by using RSA algorithm.

The data embedding with LSB modification has been started with the selected pixel value of the binary value.In any Image pixel value is in between 0 to 255. If the data embedding process is started first and second pixel values are90, 96 (As per the TABLEII data) then the LSB value of the firstpixel value is 90(As per the TABLE data) should be modified and make it all four bits of LSB is Zero. If the binary value of the corresponding pixel is “01011010” then LSB four bits should be 0000. From TABLE I it can be observed that to embed the letter “m”, the sender has to embed the binary value “01101101”. It has two fields first four is MSB and last four is LSB. In this embedding process last four bits of data embedded with the pixel value 90’sLSBand MSB of the message data four bits embedded with the 96thpixel value of LSB. As per the Table II data letter “m” embedding with pixel values of “90”, “96” and letter “e” embedding with the “92”,”94” of LSB four bits.

TABLE II
Pixels of image file with values before and after embedding

Pixel Value	Binary values of corresponding pixel	Binary value to be embedded	Binary values after modification
90	01011010	1101	01011101
96	01100000	0110	01100110
92	01011100	0101	01010101
94	01011110	0110	01010110

According to the same logic remaining consecutive Letters of the word “message” is embedded in the file “sun.jpeg.”

Embedding of secret message into the existing binary values of the pixel values with binary values causes a minimal change in the image file “sun.jpeg” that remains almost imperceptible to anyone Other than the sender.

When it comes to the point of data extraction at the receiver’s end, the extraction algorithm has to be followed: First select the stego object file as host image and apply inverse transformation then change the image into binary format that has come from the source as stego-object. Start from pixel value is 90(As per the TABLEII data), check the least significant bit, and perform the LSB operation as well as embedding process. Check every pixel to collect the whole messages. Like 96th, 92nd, 94th and so on. After getting all the bitsand combine the message of LSB and LSB in 8 bit form then convert the binary values to decimal to get back the ASCII from which the text can be retrieved.

Here at the time extraction process give the generated decryption secret keys by using RSA algorithm. Without giving proper keys used in the extraction process the secret message cannot exctract.The whole retrieval process can be depicted with the following TABLE more thoroughly:

TABLE III
Extraction of data from image file

Pixel Value	Binary Values with embedding secret data	LSB bit operation
90	01011101	1101(LSB)
96	01100110	0110(MSB)
92	01010101	0101(LSB)
94	01010110	0110(MSB)

From theTABLE, it is clearly observed that after getting 01101101 in the extraction process it is converted into the equivalentdecimal that is 109, the ASCII of “m”. Thus “m” is retrieved. Like the same way, the next letters also have been retrieved and hence the complete word “message”.

VIII.CONCLUSION

A steganographic method hiding secret data into a host image file using the 4bit LSB method and providing more security has been presented in this paper. A procedure has been developed in which the data field is edited to embed intended data into the image file. To proceed with this, quality of the image has been checked perfectly because a minimal change in the pixel values may leads to a corruption of whole image file.

In this algorithm, starting from the first pixel value is 90 and every pixel has been modified to embed textual information. How the performance is affected by changing different bit fields has not been reported in this work. However a rough study was made to see how the changing of a specific bit field creates degradation in the host image file and in which point it leads to perceptible change in the visual image quality to any other third party other than the sender or receiver. It was noticed that changing the least significant bit of the bytes gave the best results and giving a secret keys at the time of embedding and extraction of secret message is protected a message with high security.An image file with size 952 KB has been used. The maximum text file size that can be embedded in this image file without degrading the file structure can be traced through a survey.

The main goal of this work was embedding of text into image as a case of High Security steganography using RSA Secret keys.By using RSA secret keys providing high security for steganography. This is the more advantage of this work .Without knowing the generated secret keys the hacker doesn’t extract the secrete message from the embedding data. The generated secret keys is known only sender. So by using secret keys more advantage of this work. The two primary criteria for successful steganography are that the stego image resulting from embedding is perceptually indistinguishable from the host image file, and the embedded message is recovered correctly at the receiver. In test cases the text-based data has been successfully embedded to the image file to visualize in what extent the target has been achieved.

REFERENCES

[1]. Kharrazi, M., Sencar, Husrev T., and Memon, N., "Image Steganography: Concepts and Practice", WSPC, April 22, 2004.

[2]. Stefan Katzenbeisser, Fabien A. P. Petitcolas, "Information Hiding Techniques f or Steganography and Digital Watermarking". Boston, Artech House, pp. 43 – 82. 2000.

[3]. K. Matsui and K. Tanaka. Video-steganography. In: IMA Intellectual Property Project Proceedings, volume 1, pp 187-206, 1994.

[4]. N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer, vol. 31, no. 2, pp. 26-34, IEEE, Feb. 1998.

[5]. S.S. Agaian, D. Akopian, O. Caglayan, S. A. D'Souza, "Lossless Adaptive Digital Audio Steganography," In Proc. IEEE Int. Conf. Signals, Systems and Computers, pp. 903-906, November 2005.

[6]. Mohammad Pooyan, Ahmed Delforouzi, "LSB-based Audio Steganography Method Based on Lifting Wavelet Transform", International Symposium on Signal Processing and Information Technology, IEEE, 2007.

[7]. C. C. Chang, T. S. Chen and H. S. Hsia, "An Effective Image Steganographic Scheme Based on Wavelet Transform and Pattern- Based Modification", IEEE Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003.

Author's Profile

D. Sivarajakumar
Pursuing M.Tech. in Computer science and engineering Stream at Tekkali AITAM, Srikakulam (Dist) A.P. India. as a part of his academic project and research, he developed this concept of High Security stegonography. With the never ending and extraordinary support from the guide and coauthor of this paper Prof. R.Srinivas he completed this thesis. Sivarajkumar567@gmail.com, Contact No. 9618358042

R.Srinivas have received M.Tech from Andhra University. Presently he is working as an Associate Professor in CSE Department, AITAM College. His areas of interest are Data Mining and Image Processing.