IJIRR

International Journal of Information Research and Review
Vol. 04, Issue, 01, pp.3549-3553, January, 2017

Research Article

NEW TECHNIQUE OF STEGANOGRAPHY BASED ON LOCATIONS OF LSB

Orooba Ismaeel Ibraheem Al-Farraji

Al-Nahrain University, College of Medicine, Baghdad-Iraq

ARTICLE INFO

Article History:

Received 25th October, 2016
Received in revised form
22nd November, 2016
Accepted 20th December, 2016
Published online January, 30th 2017

Keywords:

Steganography,
LSB,
Image,
Secret Message,
Cover image,
Techniques,
Steganography,
Hiding data.

ABSTRACT

Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. This paper purposed an image based steganography that uses Least Significant Bit (LSB) techniques in new method that is hide locations of LSB that be equal with bits of characters in secret text.

INTRODUCTION

Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion (Jesus Olguin, 2016). Steganography is a branch of information hiding technology which encompasses applications for protection against detection and protection against removal such as copyright protection for digital media, watermarking, fingerprinting and data embedding. In these applications, information is hidden within a host data set, which is intentionally corrupted in a covert way, so that it could be sent secretly to an intended receive (Mohamed Sameh Hassanein, 2014). Steganography is classified into 3 categories (Sumathi et al., 2013),

- Pure steganography where there is no stego key. It is based on the assumption that no other party is aware of the communication.
- Secret key steganography where the stego key is exchanged prior to communication. This is most susceptible to interception.
- Public key steganography where a public key and a private key is used for secure communication (Sumathi et al., 2013).

Steganography can used for almost all digital file formats, but the formats those are with a high degree of redundancy are more suitable. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object's use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily [Falesh, 2014].

Steganography Techniques

Steganography is an area in which many studies and intensive research have been carried out. There are several different methods and algorithms of hiding data in different types of files [George Abboud, 2010]. Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security.

- Image Steganography: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to

Corresponding author: OroobaIsmaeel Ibraheem Al-Farraji,
Al-Nahrain University, College of Medicine, Baghdad-Iraq.

hide the information (Mehdi Hussain, Mureed Hussain, 2013).

- Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields (Handel, 1996).
- Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats (Sherly, 2010).
- Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc for steganography (Jayaram, 2011).

•Text Steganography: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code [Falesh et al., 2014] and etc is used to achieve information hiding (Mehdi Hussain and Mureed Hussain, 2013).

Image Steganography

With billions of images moving on the internet each year, it is safe to say that digital image steganography is of real concern to many in the security field (Mohanish et al., 2016). Digital images could be used for a number of different types of security threats. In the corporate world, the sending of a harmless looking bitmap file could actually conceal the latest company secrets. JPEG files could be used in defense organizations to conceal and guard deep secrets (Deepika Sharma, 2013).The use of digital images for steganography makes use of the weaknesses in the human visual system. The human visual system has a low sensitivity towards random pattern changes and luminance. The human eye is incapable of discerning small changes in color or patterns and because of this weakness, text or graphic files can be inserted into the carrier image without being detected. Each graphic image is made up of pixels. Each pixel's color is determined by the numerical value that it is assigned, ranging from 0 to 255. The typical digital image is made up of either 8 bit (256 colors) or 24 bit (true color, 8 bits each for red, green and blue) pixels (Shamim Ahmed Laskar, 2012).

What is an image?

An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (Mohanish U.Bhojane, 2016). The pixels in an image are displayed horizontally row by row.

The number of bits in a color scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current color schemes is 8, meaning that there are 8 bits used to describe the color of each pixel (corresponding to 2^8 = 256 colors). Monochrome and grayscale images use 8 bits for each pixel and are able to display 256 different shades of gray. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color (Frery, 2013).

The Proposed System

The Proposed research aims to develop an improved steganography approach which is Adaptive LSB Method for color images with higher imperceptibility/quality, large capacity/payload and better in robustness/resistance to attacks. As well as text messages can be hidden in new method that is hide the locations of LSB that equal bits of secret text in another place of cover image and use a special key. The key is being the first location where I start hide the locations of LSB that be equal the bits of secret text.

The proposed system comprises of two components:

- Embedding Module
- Extracting Module.

Embedding Module

Embedding is the process of divided the cover image in two parts and start comparison the bits of secret text with LSB in first part if be equal save the locations of LSB after end of comparison start hide the locations in second part of image and the location that start hide in it will be the key and I chose it randomly.

The operations of Embedding

- Input the secret text/image files that to be hidden in the cover image.
- convert the secret text in binary code and save in array1
- Select the cover image (JPEG file) from list of stored Image files and the text files.
- Split the image in two parts and save the part1 in array2 and save part2 in array3.
- Start compare between the secret text (array1) and part1 from image(array2)
  - Compare the first two bits with least significant bits of part (image) in array 2 with the first two bits of secret text.
  - if two bits of text equal two LSB of part1(image) in array2 then save the location of LSB (row, column) in array4 .
  - If two bits of text not equal two LSB of part1 (image) in array2 then go to LSB in next pixel and continues in comparison until find LSB equal two bits of character.
  - Take new two bits from the secret text and go to step a until end of the secret text
- In the end of operation 4 became all bits in the secret text has LSB equal with it and its location saved in array4.
- Convert array4 to binary code and hide it in array3 part2 of image.

- The first location that will start hide in it will be the key.

Back the two parts of image together and back the cover image save in it locations of LSB that equal the secret text.

Extracting Module

Extracting is the process of getting the embedded message from the stego image.

The main algorithm for the embedded stage is as follow:

- Input the key and stego-image .
- Split the stego-image in two parts
- Extracting locations of LSB that equal secret text from part2 and start with location that equal the key.
- 3- Save LSB only that locations in part2 in array
- Convert array of locations to Ascii system then to character (secret text)

The Algorithm of the Proposed System

The following steps describe the algorithm:

Algorithm 1: Convert secret text to binary code
Input: Secret Text
Output: Array of binary code

Step1-input text

Step2- convert text to Ascii code

Step3 – convert Ascii code to binary code

Step4 – save in array1

Step5- End

Algorithm 2: Split the Image
Input: Image
Output: Two Arrays of binary code

Step1- Open Image Operation

This operation will open the image file and save header in a file and save the palette value of body in another file.

Step2- Split the body of the image file in two parts

This operation will split the body image in parts to use one part in comparison and second part in hiding.

Step3- save the value of pixel of part1 in array2save the value of pixel of part2 in array3

Step4-End

Algorthim3: Find the position
Input: Array2, Array1
Output: Positions of pixel that equal to ASCII code of text image

Step1- Find the position operation this operation is done by read part1 of image array2

Step2- Compare array1 (binary of secret text)

Step3- for I = 1 to length of array1 step2

Read array1
For j = 1 to length of array2 step 8
Read array2
If array1[I] = array2[j+6] and array1[I+1] = array2[j+7] then
Array4[I] =j+6
Array4[I+1]= j+7
end if
next j
next I

Step4- end

Algorithm 4: Substation

Input: Array4, Array3

Output: Array3 after hide Array4 within

Step1- for i= 1 to length of array4

Read array4

For j = Key to length of array3 step 8

Array3[j+6]=array4[I]

Array3[j+7]=array4[I+1]

Next j

Next i

Step 2- end

Algorithm5: extraction stego-image
Input: Array2, Array3
Output: stego-image

Step1- back array2 to file

Step2- back array3 to another file

Step 3- merge the two files to extract palette

Step 4 – back header to palette to extract stego-image

Step 5- end

Extracting The Secret Text

The operation of extracting

- Split the stego-image in two parts and save the part1 in array5 and save part2 in array6.
- extract the location from array6 and save in array7
- According to array7 extract secret text from array5

The Algorithms of Extracting

The following steps describe the algorithm:

Algorithm 1: Split the Image
Input: Image
Output: Two Arrays of binary code

Step1- Open Image Operation

This operation will open the image file and save header in a file and save the palette value of body in another file.

Step2- Split the body of the image file in two parts

This operation will split the body image in twoparts.

Step3- save the value of pixel of part1 in array 5 and part2 in array6

Step4-End

Algorithm 2: extract text secret from cover image
Input: array6
Output: Two Arrays of binary code

Step1- for i= 1 to length of array6 step 8

For j= 1 to length of secret text

```
Array7[j] = array6[i+6]
Array7[j+1] = array6[i+7]
Next j
Next i
```

Step2- for m= key to length array5

```
        Read Array5[m] =
Read Array7[m]
        If Array5[m] = m then
          For n= 1 to length of secret text
Array8[n] = Array7[m]
Next n
         Next m
```

Step3- convert array8 to asci code theto text

Step4 – print secret text
Step 5 - end

Step3- save the value of pixel of part1 in array 5 and part2 in array6

Step4-End

RESULTS AND DISCUSSION

We have conducted several experiments to examine the effectiveness of proposed algorithm. We choose the cover image of buildings, people and vehicles and images to hide various text. All the images and taken from real world data. Proposed system is tested on more than 50 images with different text for data hiding. System is giving 94% accurate results.

Conclusion

There are several types of algorithms for steganography. Each type of algorithms has its own advantages and limitations. No method can provide fully perfect solution.

Each type of solution has robustness to some type of attacks but is less resilient to some other types of attacks. Main focus of the current research in hide locations. In case of practical application, choice of solution type actually depends on the nature of application and requirements. The proposed method uses LSB Method to optimize the strength of steganographic process. The imperceptibility and robustness of proposed method shows better performance in comparison to other approaches in practice. Accuracy of the system evaluated to be 94% which shows considerably good improvement over the existing approaches.

REFERECSES

Deepika Sharma, PawaneshAbrol, "Digital Image Tampering – A Threat to Security Management", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 10, October 2013

Eduardo Gelbstein, Ahmad Kamal, "Information Insecurity", A survival guide to the uncharted territories of cyber-threats and cyber-security, 2002

Frery, AC. 2013. "Image Data Formats and Color RepresentationImage Data Formats and Color Representation, Introduction to image processing.

George Abboud, Jeffrey Marean, Roman V. Yampolskiy, "Steganography and Visual Cryptography in Computer Forensics", Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010.

Handel, T. &Sandford, M., Hiding data in the OSI network model, Proceedings of the 1st International Workshop on Information Hiding, June (1996).

Jayaram P, Ranganatha H R, Anupama H S, "INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

Jesus Olguin, "Steganography... what is that?", https://www.trustwave.com/Resource , September 19, 2016 .

Manpreet Kaur, Vinod Kumar Sharma, "Encryption based LSB Steganography Technique for Digital Images and Text Data", IJCSNS International Journal of Computer Science and Network Security, VOL.16 No.9, September 2016.

Mehdi Hussain ,Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013

Mohamed Sameh Hassanein, "Secure Digital Documents Using Steganography and QR Code", A thesis submitted for the degree of Doctor of Philosophy, November, 2014.

Mohanish, U. Bhojane, Yash, P. Mangrulkar, Koutuk, A. Mundada, 2016. "Encoding and Decoding of Secret Message in an Image", Satellite Conference ICSTSD 2016 International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26.

Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, "Comparison of different techniques for Steganography in images" , International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 2, February 2014.

Shamim Ahmed Laskar, KattamanchiHemachandran, 2012. "High Capacity data hiding using LSB Steganography and Encryption", International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December.

Sherly, A. P., Amritha P P, "A Compressed Video Steganography using TPVD", International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010.

Sumathi, C.P., Santanam, T. and Umamaheswari, G. 2013."A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

****