ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

The R2 Bit Algorithm for Information Hiding In Images (R2BA)

Dr. V. Nanda Kumar
Programmer Selection Grade, Computer Centre, School of Computer Science at Alagappa University, Karaikudi, Tamilnadu, India

Abstract*—Internet transmissions help distribution of large multimedia data. Unauthorized access to such digital data is a primary concern. Communication networks and data availability on the internet poses many challenges. Individuals and companies seeking confidentiality of information look towards Steganography as a solution. Steganography based communication can prevent leakage of information, since, Steganography hides the secret message in communication by covering it. Steganography takes advantage of old Steganographic techniques like null ciphers and coding in image and helps protect privacy. This trend of electronic communications with a genuine need to conceal messages from curious eyes is another reason for the resurgence of Steganography. Steganography can be used in military and intellectual property or applications that need to hide a message within another object ensuring the hidden message is not visible to an observer. Existing Steganographic systems are decodable and stronger systems offer a small capacity for Steganographic messages. A simple approach towards hiding secret text in images in communications over the network is proposed in this paper.

***Index Terms*— Steganalysis, Steganography, Stegos, Information Hiding, Image with text.**

I. INTRODUCTION

Steganography is science of writing hidden messages where only the intended recipient knows the existence of the message. Though Steganography is related to cryptography, it is not the same. Steganography is hiding the existence of a message whereas cryptography rearranges or scrambles a message. The prime goal of Steganography is to pass on a secret message without others knowing the existence of a secret message. [1] Has been in use for 2500 years. Data with the hidden messages are called Steganos or Stegos. Steganography has a variety of techniques for hiding messages in media like invisible inks, digital signatures and microdots. Modern digital Steganography encrypts data and inserts them using special algorithms which may add or modify the original file. Multimedia data can be edited and delivered error free over computer networks. Digital media distribution is also a worry to the digital content owners. The data can be easily copied and the intellectual rights of copyright owners need protection. Visible Watermarking of the digital content is a solution followed by many and includes embedding information about the owner or brand. Steganography relies on hiding message in multimedia data as an acknowledgement in secret communication between Steganography can also be thought of as a method of encryption that hides data in a graphic or an audio file. It replaces unused or insignificant bits of the media with the secret data. The messages are sometimes encrypted and then a cover text is modified to contain the encrypted message. The characteristics of a cover text can be manipulated to carry the hidden message and the recipient alone can recover the message and decrypt it. important confidential information can be stored ,their access limited, Transmission in an encrypted form to keep away intruders during transit of the files. Larger the cover message, easier to hide information. A 24-bit bitmap will carry three color values (red, green, and blue) of each pixel. This paper presents a method in which the text to be hidden is split into two bit fractions and added to the pixel data of the image with a little noise. The data is embedded as a part of the image. The software used to code is again used to reverse the process, keeping the guesses to decode away from the message. Existing Steganographic scheme and steganalysis schemes are also discussed, confirming the applicability of the proposed scheme. The performance is validated against standard Steganographic attacks.

II. STEGANOGRAPHY METHODS

Recent Steganographic software are becoming effective in hiding information in image, audio or text files. A very generic description of the Steganographic process can be visualized as covering medium plus hidden data plus stegokey (if any). The cover medium is the file in which the data will be hidden and to increase the complexity, the data can be encrypted called the stegokey. The result is also known as the stego medium which is typically image or audio files. Steganography used in computers can be of three forms. In the first, text files hide text, the second is hiding voices or audio in other audio files. The third form is hiding text in images. Steganography can be achieved using various methods like Substitution, Transformation, Domain Spread, Statistical Distortion, Cover generation. The techniques must satisfy a number of requirements to apply Steganography correctly. It is important for a Steganography technique to ensure that the integrity of the embedded information inside the stego object is maintained and not altered in any way, thus maintaining the principles of Steganography. Also the covering medium should not have a noticeable change or visible to a third party, resulting in an attempt to extract the Stegos. Fig. 1 depicts the general process of Steganography.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

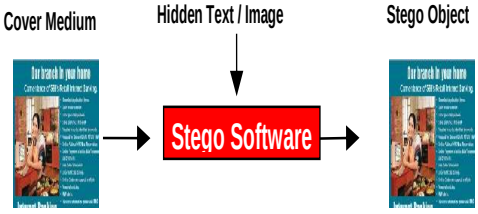

Fig. 1 - Generic Process of Steganography

A. *Textual Steganography*

There are many ways of hiding messages in text. [7], like Open space, Line shift, Word shifting and many more which alter the characteristics of formatting or the characters. It has to be altered in a way not visible to the naked eye but possible to decode using a computer. Margaret Thatcher, then Prime Minister of England had word processors programmed spacing the words to trace disloyal ministers [8]. To re-quote a known example of textual Steganography is a German spy's message during World War II said "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects for pretext embargo on by-products, ejecting suets and vegetable oils." Translates to "Pershing sails for NY June 1" [16].

- **Line Shifting:** The lines inside the document are shifted up or down by a small fraction i.e. 1/200th of an inch based on a codebook (a set of rules specifying the parts of the document to be changed). The shifted lines are detectable only to the computer when it measures the distance between the lines. Shifting a line up or down can represent a single bit, 0 or 1 and a number of bits can be embedded using the whole document.
- **Word Shifting:** The word shift is based on the same principle as the line shifting technique. The codebook specifies the words to be shifted and the shift left can be a 0 and shift right can be 1. For Example in the sentence "*The quick brown fox jumps over the lazy dog*", words are shifted in any one direction by .5 points, results in "*The quick brown fox jumps over the lazy dog*" and encodes 01000001 not visible to the naked eye.
- **White Space:** Another way of hiding data in text is to manipulate the white space to store bits. As an example the code can be a fixed amount of white space at the end of the sentence to signify a 1 or 0. SNOW is a program which uses this technique is [9]

B. *Spread Spectrum*

Used by the military since the 1940s, encodes data as a binary sequence which resembles sounds. The noise can be recognised only be a receiver with the correct key. The signals are also hard to intercept or jam.

C. *Audio File Steganography*

Information can be hidden in the Layer III encoding of an mp3 file [10]. There are many applications offering information hiding in audio formats like .wav, .avi, etc. They actually attach the hidden information to the end of a file such as Camouflage [11].

D. *Image Steganography*

There are many applications for Steganography on images [12]. Watermarking is very simple but widely used technique for watermarking images. A pattern is added to an existing image typically a logo which distorts the underlying image. In Figure 2 the portrait is watermarked with the university logo.

Fig 2. Watermarking on Images

III. RELATED WORK

A. *The LSB*

Least Significant Bit Image Hiding method is an easy way of hiding information in images. It uses least significant bits of each pixel of an image to hide the most significant bits of another image. It belongs to the Image domain group and more susceptible to damage. If the rgb values of a pixel are R(1 0 1 0 1 0 1 0), G(0 1 0 1 0 1 0 1), B(1 1 0 0 1 1 0 0) then LSB would be R(1 0 1 0 1 0 1 0), G(0 1 0 1 0 1 0 1) and B(1 1 0 0 1 1 0 0). The last bit is known as the least significant bit (LSB). The seven bits preceding the LSBs have enough information and when the to be hidden data's bits are substituted into the least significant bits (LSB's) location it will have literally no effect on the images [14]. For Example Alphabet "A" can be hidden in the first eight bytes of a 24-bit image (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001) will result in (00100110 11101001 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001). This method is good for equal images. If one image has more room quality is sacrificed. This technique is easy to find and recover the hidden data [13].

B. *PVD*

Pixel-Value Differencing (PVD) scheme: Alterations in the edges of an image cannot be distinguished so easily, while changes in the smoother areas can be. Based on this fact, Wu and Tsai proposed a Steganography technique the pixel-value differencing (PVD) method to distinguish edge and smooth areas, where the PVD technique could embed more data in the edges.

IV. PROPOSED STEGANOGRAPHY SCHEME (R2BA)

Any image is an array of numbers representing luminosity of various points or pixels. The images vary in size based on their width and height. The pixels are dots of the image in

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

width by height matrix. Each pixel takes 24 bits or three bytes of information to represent as an image and can be used to hide information. In the proposed scheme, a new method of hiding is used based on an algorithm. Since each pixel is combination of three components(R, G, and B), the Red component is used to hide the information. Any pixel value of red which has a decimal value of sixteen is used to hide the message. The entire message is split into equal 2 bit values and embedded into the red pixel value of an image. This is carried on till the end of the image. The message length is also embedded into the image using the software. The same software has to be used at the receiving end, decode the image and extract the message. Text Encryption and Decryption are depicted in Figures, Fig. 3 and Fig. 4 respectively.

C. R2BA Encoding/Decoding Algorithm

```
/*calculate the no of bytes where the message can be hidden
*/
  For I = 1 to length of the pixel bits
            If Red color then
               If binary value < 16 then
                    Hidebytescount=hidebytescount+1
              End if
            End if
         Next I

/* convert Message to Binary bits */
 For j = 1 to messagelength
    Messagebitsarray = messagebitsarray+bits(message(j))
Next j

/* Embed Message in Image Pixel Data */

       For I = 1 to len(Messagebitsarray) step two // Taking
two bits at a time
           For j = 1 to length of the pixel bits
              If Red color then
                If binary length < 4 then
                     Updated Red Pixel Value = "01"+
Messagebitsarray(i)+ Messagebitsarray(i+1)+Red Pixel
Value
               End if
             End if
          Next j
       Next I

  /* Extract Message from Image Pixel Data - R2BA
Extraction Algorithm*/

        For j = 1 to length of the pixel bits
              If Red color then
                If binary length < 4 then
                     Messagebitsarray = Messagebitsarray
+Bit(3) of  Red Pixel Value)+bit(4) of Red Pixel Value
               End if
             End if
          Next j
```

D. Secret Text Embedding phase

Inputs: Image file and text
Output: Text embedded image
Procedure:
Step 1: Extract the pixels of the image and store it in an array.
Step 2: Convert text box text into binary bits and store them in an array.
Step 3: Loop through all the pixels of the image to check if the Red value <= 16.
Step 4: If the value of Red in RGB is <=16 create a new value of R as "01"+Two bits of the Message Array + Old Red Value and rewrite the pixel value.
Step 5: Repeat step 3 till all the bits of the character array have been embedded.
Step 6: Write the new Image

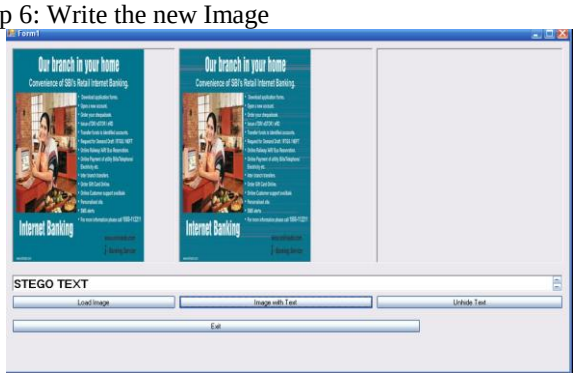

Fig. 3 - Text Encryption

E. Message Extraction phase

Inputs: Embedded image file
Output: Secret text message and Covering Image
Procedure:
Step 1: Extract the pixels of the stego image and store it in an array.
Step 2: Loop through all the pixels of the image to check if the first two bits of Red value = "01".
Step 3: If step 2 is true then extract the 3rd and 4th bit of the red and store it in a bit character array and rewrite the Red pixel value with the last four bits.
Step 4: Repeat step 2 till all the bits of the character array have been retrieved.
Step 5: Write the new Image
Step 6: Combine 8 bits of the character bit array retrieved and extract the text

Fig. 4 - Text Decryption

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 2, August 2013

V. STEGANALYSIS

Steganalysis is discovery of hidden files. Current steganalysis programs discover and remove contents that are sometimes required like watermarking. Scientists and researchers keep trying methods to detect information hidden fin files. Governments contract technology Organizations or Universities to research on algorithms to retrieve information that is hidden from digital, audio and video files. [15] Steganography software's have their own unique signatures on files. Once the signature is identified, mathematical equations or expressions can be developed and used with other files to compare or trace the deviations. If a software program is used on a file, it is most likely to leave its digital fingerprint which an algorithm could detect. In steganalysis a detector would analyse the image and determine the possibility of a Steganographic fingerprint before creating a report. Steganalysis can also be classified for destruction of the message. If a secured technique is developed, there is an effort to develop an opposing technique. The security achieved is high and third parties may trace the disturbance and not the cause. Since only two bits are replaced and that too selectively not randomly, it is difficult to get back the original message or hidden message without the software**:**

VI. CONCLUSION AND FUTURE SCOPE

This paper proposed Steganography for exchanging messages and further emphasizes data hiding in images. Encoding algorithms manipulate binary files, voice, text, etc. R2BA can be applied in watermarking, fingerprinting, detection of unauthorized or illegally copied material. The strength of security level achieved in R2BA is very high and third parties will not be able to get back the original hidden information without the software or how it works.

REFERENCES

[1] http://searchsecurity.techtarget.com/definition/steganography.

[2] Singh, Simon, "The Cipher of Mary Queen of Scots" URL:www.arch.columbia.edu/DDL/cad/A4513/S2001/r9/

[3] "The Science of Secrecy, Steganography" URL:www.channel4.com/plus/secrecy/page1b.html, Singh, Simon, The Cipher of Mary Queen of Scots" URL:www.arch.columbia.edu/DDL/cad/A4513/S2001/r9/.

[4] Counterintelligence News and Developments, Volume 2, June 1998 "Hidden in Plain Sight Steganography" URL:www.nacic.gov/pubs/news/1998/jun98.htm.

[5] "Classical Steganography, Cardano Grille" URL:http://library.thinkquest.org/27993/crypto/steg/classic1.shtml

[6] Home & Garden Television, "Clues in the Quilts" URL:http://www.hgtv.com/HGTV/project/0,1158,CRHO_project_7305,00.html

[7] Braynov Svet, "Secure Sockets Level, Steganography" URL: ww.cs.buffalo.edu/~sbraynov/lectures/lecture6_pdf.pdf

[8] Anderson, Ross "Stretching the Limits of Steganography" URL:www.cl.cam.ac.uk/ftp/users/rja14/stegan.ps.gz

[9] M. Kwan, The Snow Home Page, http://www.darkside.com.au/snow/index.html, March 2001

[10] Petitcolas, Fabien A. P. "mp3stego" URL:www.cl.cam.ac.uk/~fapp2/steganography/mp3stego

[11] CamouflageSoftware.com "Camouflage" URL:http://www.camouflagesoftware.com

[12] Tannenbaum, Andrew S. "Steganography Demo for Modern Operating Systems", 2nd ed. URL: www.cs.vu.nl/~ast/books/mos2/zebras.html

[13] M. D. Swanson, B. Zhu and A. H. Tewfik, "Robust Data Hiding for Images", IEEE Digital Signal Processing Workshop, pp. 37-40, Department of Electrical Engineering, University of Minnesota, www.assuredigit.com/tech_doc/more/Swanson_dsp96_robust_datahiding.pdf, September 1996

[14] Machado, Romana, "How Stego Online Works", http://www.stego.com/howto.html

[15] Wetstone Technology, Inc., "What You Can't See Can Hurt You…, The Dangers of Steganography", http://www.wetstonetech.com/technicalpapers.htm

[16] Steganography AndDigital Watermarking, © 2004, Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham.

AUTHOR'S PROFILE

Dr.V. NANDA KUNMAR is presently working as Programmer Selection Grade, Computer Centre, School of Computer Science at Alagappa University, Karaikudi, Tamilnadu.He 18+ years of teaching experience. He has presented and published research papers in more than 7 international journals. His research areas include Cryptography, Green Computing and Networking. He has guided more than 50 Post graduate students. He finished his Master of computer Science at alagappa University, Master of Philosophy at Bharathidasan University and his Doctorate at Alagappa University