iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** II **Month of publication:** February 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue II, February 2018- Available at www.ijraset.com

Data Encryption and Hiding Model depends on Time in Steganography

V.Raja[1], G.Kalpana[2]
[1]*Department of Computer Science*
[2]*Department of Computer Application S.R.M Institute of Science and Technology, Chennai, India*

Abstract: ***In this paper, we are presenting a new secured method for data hiding technology. In this technology sender information will be hidden to an image. Image will be selected by user and it will be converted into bits. Finally the sender information will be embedded into an image which depends upon the sending time value. The hiding of data into Image/audio/video is called Steganography. The change due to the embedding of sender information in the image is very low. This method is more secured as it is difficult to detect the information and hence this technology performs more secured data transmission.***

Keywords: Steganography–Watermarking – reversible data hiding. R.G.B – Red, Green, Blue L.S.B – Least Significant Bit.

I. INTRODUCTION

Before entering into Steganography, we would like to introduce multimedia. Multimedia is a combination of image, audio, video, text and animation. In the above multimedia forum we can embed the message in a secret way. [1],[3],[18],[19]. While comparing, cryptography and Steganography are related, there is a difference between the two. Cryptography [17],[12],[14] is used to scramble messages so that they cannot be understood. It does not hide the fact that the message exists. Steganography conceals the fact that the message exists by hiding the actual message in another [13][16].

II. INTRODUCTION TO STEGANOGRAPHY

There are a large number of Steganography methods that most of us are familiar with ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication[20][21]. With computers and networks, there are many other ways to hide information such as: Covert channels (e.g., Loki and some distributed denial of service tools use the Internet Control Message Protocol, or ICMP, as the communications channel between the "bad guy" and a compromised system). [5].

Hiding files in "plain sight" (e.g., to “hide" a file with an important sounding name in the c:\winnt\system32 directory?)

Null ciphers (e.g., using the first letter of each word to form a hidden message in an otherwise innocuous text)

Steganography today, however, is significantly more sophisticated than the examples above suggest, allowing a user to hide large amounts of information [14][15]within image and audio files. These forms of Steganography [16][13][3] often are used in conjunction with cryptography so that the information is doubly protected; first it is encrypted and then hidden so that an adversary has to first find the information (an often difficult task in itself) and then decrypt it. [8]

There are a number of uses for Steganography besides the mere novelty. One of the most widely used applications is for so called digital watermarking.[12] A watermark, historically, is the replication of an image, logo, or text on paper stock so that the source of the document can be at least partially authenticated. A digital watermark can accomplish the same function; as graphic artist, for example, might post sample images on the web site complete with an embedded signature so that he can later prove their ownership [4][6][13] in case others attempt to portray their work as their own.

Data hiding techniques can be applied in military, industrial and distance medical treatment applications. Intelligence agents may use this technique to deliver information to an agency. In long distance medical treatment applications, a patient’s x ray may be sent to a remote medical center with private information such as the patient’s name, treatment data, and so on. Data hiding [21][20][19] can be classified into two categories. The first category is irreversible data hiding, in which the secret message is extracted without restoring the cover image.

The second category is reversible data hiding, in which the secret message is extracted from the embedded image, and the original image is also completely restored. The reversibility of data hiding techniques is an important property in medical treatment and military industrial applications.[11]

III.STEGANOGRAPHY METHOD

Steganography is an art of hiding messages inside some harmless carriers to shelter the communication. One of the popular Steganography techniques is replacement of least significant bits (L.S.B) in digital signal because of its extreme simplicity. [9]

The following formula provides a very generic description of the pieces of the Steganography process:

Cover medium + hidden data = stego medium

In this context, the cover medium is the file in which we will hide the hidden data. The resultant file is the stego medium (which will, of course be the same type of file as the cover medium). The cover medium (and thus the stego medium) is typically image or audio files[14][15][19][3]. In this article, we will focus on image files.[2][4][8]

Before discussing how information is hidden in an image file, it is worth a fast review of how images are stored in the first place. An image file is merely a binary file containing a binary representation of the color or light intensity of each picture element (pixel) comprising the image.

Images typically use either 8bit or 24bit color. When using 8bit color, there is a definition of up to 256 colors forming a palette for this image, each color denoted by an 8bit value. A 24bit color scheme, as the term suggests, uses 24 bits per pixel and provides a much better set of colors. In this case, each pixel is represented by three bytes, each byte representing the intensity of the three primary colors, red, green, and blue (RGB) respectively. The Hypertext Markup Language (HTML) format for indicating colors in a web page often uses a 24bit format employing six hexadecimal digits, each pair representing the amount of red, blue, and green respectively. The color orange, for example, would be displayed with red set to 100% (decimal 255, hex FF), green set to 50% (decimal 127, hex 7F) and no blue (0), so we would use "#FF7F00" in the HTML code.

The size of an image file, then, is directly related to the number of pixels and the granularity of the color definition. A typical 640x480 pixel image using a palette of 256 colors would require a file about 307 KB in size (640 • 480 bytes), whereas a 1024x768 pix high resolution 24bit color image would result in a 2.36 MB file (1024 • 768 • 3 bytes).

To avoid sending files of this enormous size, a number of compression schemes have been developed over time, notably Bitmap (BMP), Graphic Interchange Format (GIF), and Joint Photographic Experts Group (JPEG) file types. Not all are equally suited to Steganography, however.[10]

GIF and 8bit BMP files employ what is known as lossless compression, a scheme that allows the software to exactly reconstruct the original image. JPEG, on the other hand, uses lossy compression, which means that the expanded image is very nearly the same as the original but not an exact duplicate. While both methods allow computers to save storage space, lossless compression is much better suited to applications where the integrity of the original information must be maintained, such as Steganography. While JPEG can be used for stego applications, it is more common to embed data in GIF or BMP files. [4]

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24bit color, the amount of change will be minimal and indiscernible to the human eye.[6][8][9].As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:

R	G	B
10010101	00001101	11001001
10010110	00001111	11001010
10011111	00010000	11001011

Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden):

101101101

If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following

R	G	B
10010101	00001100	11001001
10010111	00001110	11001011
10011111	00010000	11001011

Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs. [8]

This description is meant only as a high level overview. Similar methods can be applied to 8bit color but the changes, as the reader might imagine, are more dramatic. Grayscale images, too are very useful for Steganography purposes. One potential problem with any of these methods is that they can be found by an adversary who is looking. In addition, there are other methods besides LSB insertion to insert hidden information[11][12][5][6].

Without going into any detail, it is worth mentioning steganalysis [13],[11][17], the art of detecting and breaking Steganography.

One form of this analysis is to examine the color palette of a graphical image. In most images, there will be a unique binary encoding of each individual color. If the image contains hidden data, however, many colors in the palette will have duplicate binary encodings since, for all practical purposes, we can't count the LSB. If the analysis of the color palette of a given file yields many duplicates, we might safely conclude that the file has hidden information.

But what files would one analyze. Suppose a person decides to post a hidden message by hiding it in an image file that he/she posts at an auction site on the Internet. The item being auctioned is real so a lot of people may access the site and download the file; only a few people know that the image has special information that only they can read. And we haven't even discussed hidden data inside audio files. Indeed, the quantity of potential cover files makes steganalysis a Herculean task.[12][16]

IV. THE PROPOSED TECHNIQUE

We apply this method to exchange the information between the sender and receiver.

A. Data Mixing [Sender end]

1) Select the image
2) Get the sender information from the user.
3) The given message will be converted to ASCII value.
a) Msg : HIDE AND SEEK
b) ASCIIvalue: 72736869326578683283696975
c) Finally calculate the no of bits required to store the information.
d) Nbr72736869……696975
e) Binary value 01110010….01100101 for Nbr.
4) Convert the image into rgb cube array value
a) The selected image will be converted into numbers. It depends upon the pixel color.
b) Eg: Pixel is Red, and then the value is RGB 255 0 0
5) The sending time of the image from sender to receiver plays a major role in this data hiding technology
  i) A ⟶ B Suppose the time is 10:12 Sum of the digits of the time = 1+0+1+2=4. Binary value of sum of time= 4 = 0100.
6) Initially the first 5 pixels (or) 15 bytes are utilized to store the information.
  5 Pixels occupy 15 bytes
  1 Pixel occupies 3 bytes RGB
  5 Pixels = 5*3=15 Bytes
  15 Byte will be split up into 11 Byte + 4 Byte
  The first 11 bytes LSB are used to store the calculated value of no of bits required to store the user information. The next 4 bytes LSB are used to store the binary value of the sum of time.
7) The sender information embedding process will be started at the 6th pixel.
a) In that pixel, we take 3 byte information (RGB) value
b) Each byte L.S.B of RGB is used to embed a single bit of user information.
c) The next pixel will be select as follows:
    np=CPP+TV
    np: Next pixel
    CPP. Current pixel position [9]
    TV. Time value
d) In that position (np) the next 3 bits of information will be embedded.
e) Similarly the remaining information will be embedded into the image in the same manner.

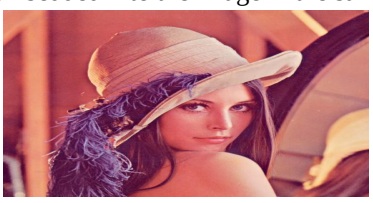


Fig 1 : Sample Leena image

36	Electric Lime	#CEFF1D	(206, 255, 29)	1990		Fluorescent.
37	Fern	#71BC78	(113, 188, 120)	1998		
38	Forest Green	#6DAE81	(109, 174, 129)	1958		
39	Fuchsia	#C364C5	(195, 100, 197)	1990		
40	Fuzzy Wuzzy	#CC6666	(204, 102, 102)	1998		
41	Gold	#E7C697	(231, 198, 151)	1949		Metallic.
42	Goldenrod	#FCD975	(252, 217, 117)	1958		
43	Granny Smith Apple	#A8E4A0	(168, 228, 160)	1993		
44	Gray	#95918C	(149, 145, 140)	1949		
45	Green	#1CAC78	(28, 172, 120)	1903		
46	Green Blue	#1164B4	(17, 100, 180)	1949	1990	
47	Green Yellow	#F0E891	(240, 232, 145)	1949		
48	Hot Magenta	#FF1DCE	(255, 29, 206)	1972		Fluorescent.
49	Inchworm	#B2EC5D	(178, 236, 93)	2003		
50	Indigo	#5D76CB	(93, 118, 203)	2000		
51	Jazzberry Jam	#CA3767	(202, 55, 103)	2003		
52	Jungle Green	#3BB08F	(59, 176, 143)	1990		

Fig 2 : Sample RGB Color Table

B. DATA EXTRACTION (RECEIVER END):

1) Receive the image from a sender
2) Read first five pixels values from the imge
3) Each pixel has 3 byte of information.
4) Each byte L.S.B gives a single bit of sender information.
5) 5 pixel= 5*3= 15 byte=> 15
6) Sender Information = 15 bits 15 Bits
7) 15 Bits = 11 + 4
8) Depending upon the time value the receiver will easily pick the next pixel to read the data
9) Repeat the same until message received.

V. CONCLUSION

The proposed method depends upon the time value. On account of safety measure this is obviously better than the simple data hiding technique. In this method receiver should know the information about hiding technique. At the same time the method gives more security for the user information.

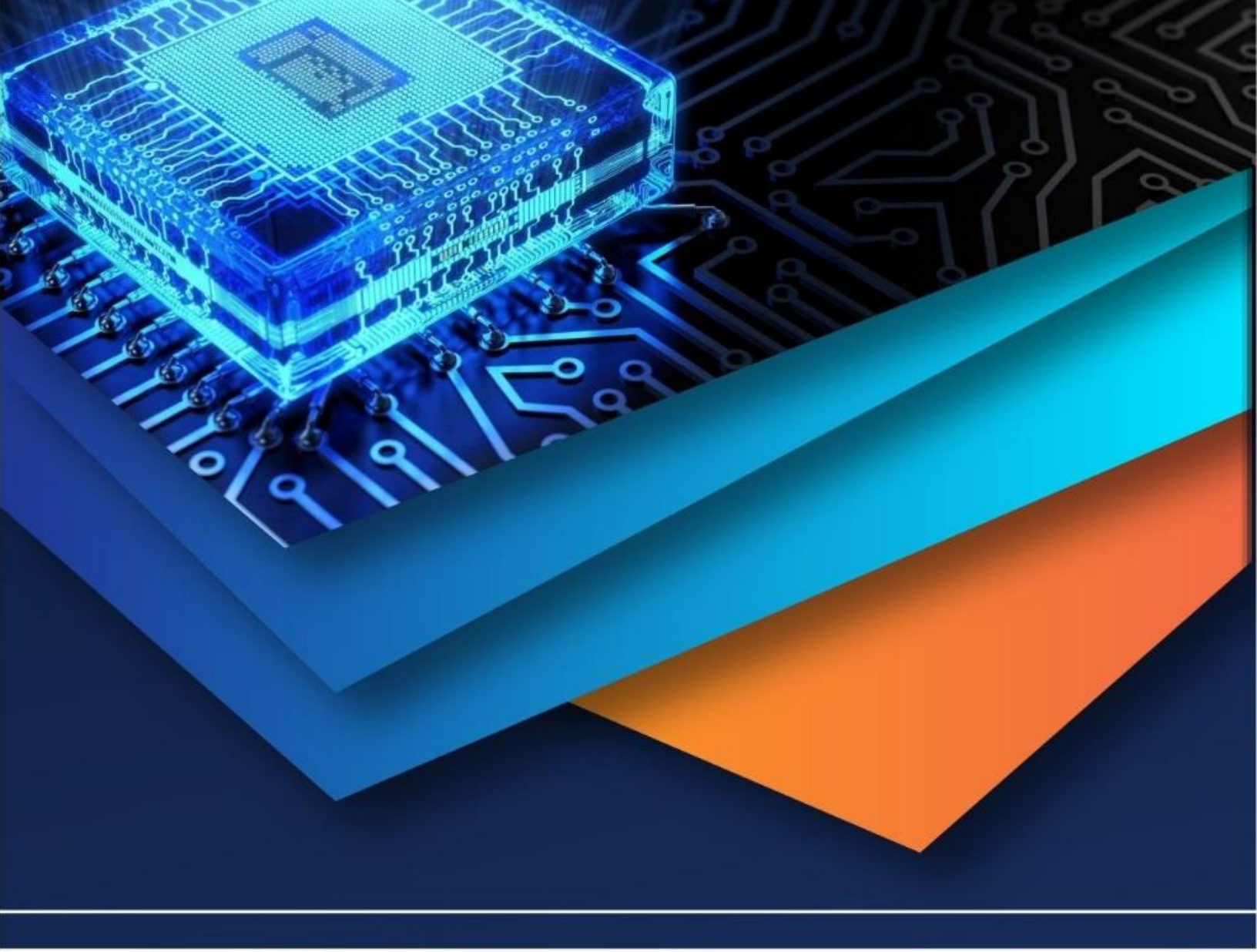
VI. FUTURE ENHANCEMENT

We would like to enhance the proposed system to store the user information in the rgbcube array's diagonal elements and implemented in matlab code. We would like to improvise user can store more data. In data security point of view, we would like to find a encryption algorithm to encrypt the user data, it provide high security.

REFERENCES

[1] Chan, C.-K., Cheng, L.-M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition.
[2] Chen, W.-J., Chang, C.-C., Le,T.H.N. (2010). High payload Steganography mechanism using hybrid edge detector. J. Expert System. Applications.37, (4), pp. 3292–3301
[3] Wang, R.-Z., Lin, C.-F., Lin, J.-C. (2001). Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition.
[4] Wu, D.-C., Tsai, W.-H. (2003). A steganographic method for images by pixel value differencing. Pattern Recognition Letter.
[5] Khodaei, Faez.(2011). New adaptive steganographic method using least significant-bit substitution and pixel-value differencing.IET image processing.
[6] Yang, C.-H.(2008). Inverted pattern approach to improve image quality of information hiding by LSB substitution.Pattern Recognition.
[7] Frank Y. Shih. (2007). digital Watermarking and steganography fundamentals and techniques. CRC Press.
[8] Andrew, "Steganalysis of embedding in two Least significant bits", IEEE transaction on information forensics and security, vol 2 Mar –07. Greory Kipper. (2004). investigator's guide to steganography. auerbach publication. WaiChi. (2010). Techniques and application of intelligent multimedia data hiding. Springer.
[9] Lee, I.S.[IShi], Tsai, W.H.[WenHsiang], "Data Hiding in Binary Images with DistortionMinimizing Capabilities by Optimal Block Pattern Coding and

Dynamic Programming Techniques", IEICE (E90D), No. 8, August 2007, pp. 11421150.
[10] Ingemax cox, matthewmiller and tonkalker "Digital watermarking and Steganography",Morgan Kanfman series in multimedia information system ,USA ,2008.
[11] Ali Bani. (2008). A new Steganography approach image encryption exchange by using the least significant bit insertion. IJCSN.
[12] Stefan katzen beisser and Fabien a.p petitcoals. (1999). Information hiding techniques for Steganography and digital Watermarking. Artech house books.
[13] Zhang XP, Wang SZ. (2006). Efficient steganographic embedding by exploiting modification direction. IEEE Communication Letter.
[14] Hong W, Chen TS.(2012).A novel data embedding method using adaptive pixel pair matching. IEEE Trans Information Forensics Security.
[15] Lan TH, Tewfik AH. (2006). A novel high-capacity data-embedding system. IEEE Trans Image Process.
[16] Greory Kipper , "investigator's guide to steganography"auerbach publication , 2004
[17] peter wayner disappearing cryptography Morgan Kanfman series in multimedia information system ,USA ,2009.
[18] USC-SIPI image database - http://sipi.usc.edu/database/
[19] https://www.economictimes.indiatimes.com.
[20] https://www.gartner.com/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY