Volume 6, Issue 2, February 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Communication by Reversing Each Message Bit & using 2-2-2 LSB Image Steganography

Dipti P Kulkarni, Prof. Vanita D Jadhav
Computer Science and Engineering, SVERI's COE Pandharpur, Pandharpur, Maharashtra, India

Abstract-Today there is more use of internet for communication .There are many possible attacks that will capture our information and misuse it or change information .if we want to send important message then for secure communication we are using steganography.This paper give information about 2-2-2 LSB image steganography method with stego-key as number of bit (or pixel)to store size of message.This method hides large number of data.In this method we use 24-bit color image.This method first reverse each message bit &then hides message bits in 7^{th} &8^{th} bit of each Red(R),Green(G),Blue(B) color component of all pixel.

Keywords: Cryptography, Steganography.

I. INTRODUCTION

we can secure communication by using cryptography or steganography.In cryptography we encrypt message by using different encryption algorithm.But in steganography we hiding message behind cover object.steganography means hiding information and cryptography means protecting information.In this paper we using steganography technique means except sender and receiver, another person don't know existence of the message in cover object .there are different types of cover object (e.g. audio ,video,text,image) .In this paper we are using cover object as image because image having more redundant bit to hide secret message .redundent bit means if we change these bit then there is no change in cover object.In this we using 24-bit color image as cover object.

II. RELEVANT WORK

Mehdi Hussain and Mureed Hussain in [1]has given information about Survey of Image Steganography Techniques. In this paper give information about need of Steganography. This paper gives main types of Steganography depending on the Types of the cover objects i.e it may be
Image Steganography:In this important data is hide behind cover object (i.e image)this is known as image steganography.
Network Steganography: When data is hide behind network protocol such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography.
Video Steganography:Video Steganography is a technique to hide any kind of files or information behind digital video . Video (combination of pictures) is used as cover object for hidding information.
Audio Steganography:When taking audio as a cover object for information hiding it is called audio steganography.
Text Steganography:General technique in text steganography, such as number of tabs, white spaces, capital letters etc is used to hide information.
This paper tells which factors need to be consider in image Steganography i.e(High capacity,Perceptual transparency, Robustness, Temper Resistance, Computation Complexity) .image Steganography Technique devided into two types Spatial domain,Transform domain, again these two technique devided into different techniques
Tahir Ali, Amit Doegar in [2]has given information about "A Novel Approach of LSB Based Steganography Using Parity Checker". Pixel of 24-bits image has three color components i.e R, G, B of 8-bits each. In this method it collects the LSB of three color components and makes a group of three bits. Then sequence of these three bits may be even number of 1's or odd number of 1's. If the sequence of three bits contains even number of 1's then it is called as even parity else it is called as odd parity. To embedd message bit is depends on the message bit and the parity generated by the LSB of each color components .The main aim of the proposed method is to increase the size of the message to be embedded with the image and also make the technique difficult to the other person to detect the presence of secret but authorized person know about secret
Tanmoy Halderet , Sunil Karforma, Rupali Mandalal in [3] in this paper they compared and analyzed two most popular steganographic algorithms LSB (least significant bit)-replacement and PVD (Pixel value differencing) from spatial domain, which are widely used to hide secret E-governance information. In this paper discussed, compared and analyzed those two algorithms.In this paper they given detail information about PVD.
Dr. MaheshKumar, MuneshYadav in [4] This paper contain image steganography Using frequency domain.By this method more security is maintained than other method since the hidden data/image cannot be extracted without knowing decoding rules. DWT operations provide sufficient secrecy.

Hamdan Lateef Jaheel and Zou Beiji in [5] In this paper they combined two steganography algorithms those two are JSteg and OutGuess algorithms , in this the benefits of characteristics and features of both algorithms is used to enhance the protection level for important images. In this method, the secret information (image) is first hide inside another image using JSteg algorithm and the resultant stego-image is further hidden inside a final image using OutGuess 0.1 algorithm. In this due to combination of two algorithms it is difficult to extract secret message. But in this method must considered the choice of a good image size and type. In this method it hide the secret image and best tried that image could go unnoticed.This paper given Results that is the capacity and PSNR for images proved that approach is a good and acceptable steganography system. The method given in this paper is based on JPEG images

Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf in [6]this paper gives information about Hiding an Image inside another Image using Variable-Rate Steganography.In this method how many number of bits used for hiding is depend on according to pixel neighborhood information of the cover image. It uses exclusive –or (XOR)of a pixels neighbors which give information of smoothness of the neighborhood. If XOR value is high it indicate that less smoothness so more bits can be used & there is no degradation of the cover image. The results are given in this paper show that the algorithm generally hides images without degradation of the cover image, but the results are sensitive to the smoothness of the cover image

Jagruti Salunkhe, Sumedha Sirsikar in [7] This paper gives information about review and comparative analysis of various available methods for PVD. An more information of Steganographic methods that uses PVD is given.In this paper different methods are combined so it improve hiding capacity and image quality.

III. PROPOSED TCHNIQUE

A. Embedding process

In this method we take 24-bit color image which hide our message,then we calculate message size that is total number of character or total number of byte .Then we convert message size in binary, &embed it in p bits in image using LSB of Gcomponent of each pixel,this p bits is key i.e. known to sender & receiver then we convert our message into bit stream using 8-bit ASCII code and change each message bit(i.e if message bit is zero then change it by one &if message bit is one then change it by zero).Then we embed message bits in 7^{th} &8^{th} bits of each color component R,G,B of 24-bit color image.consider for example a grid for 3 pixel of 24 bit image can be as follows

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000 we want to embed 200 then first
we change each message bit & we get binary representation as 00110111 & then we embed each two message bits in 7^{th} ,8^{th} bit of RGB color component of each pixel in above 3 pixel.

(00101100 00011111 11011101)
(10100111 11000100 00001100)
(11010010 10101101 01100011)

Embedding algorithm

1. Get message to be embedded
2. Calculate size of message (number of character or byte)
3. assume p=number of pixel to store size of message(stegokey)
4. convert size of message in bit format using p bits &convert message into bit stream using 8- bits ASCII code & then change each message bit(i.e. if message bit is zero then change it by one &if message bit is one then change it by zero) 5.I=1
6. embed bit of size in G LSB component of Ith pixel
7. I=I+1
8. if(I<=p)then goto step 6 else goto step 9
9. let N is length (i.e total number of bits)
10. n=0(it is taken for comparision)
11. collect 7^{th} ,8^{th} bit of R component of Ith pixel
12. get two message bit
13. embed bit in 7^{th},8^{th} bit of R component of Ith pixel
14. n=n+2
15. if (n<N)then goto step 16else goto step 27
16. collect 7^{th} ,8^{th} bit of G component of Ith pixel
17. get two message bit
18. embed bit in 7^{th},8^{th} bit of G component of Ith pixel
19. .n=n+2
20. if (n<N)then goto step 21else goto step 27
21. collect 7^{th} ,8^{th} bit of B component of Ith pixel
22. get two message bit
23. embed bit in 7^{th},8^{th} bit of B component of Ith pixel
24. n=n+2

25. if (n<N)then goto step 26else goto step 27
26. I=I+1&goto step 11
27. END

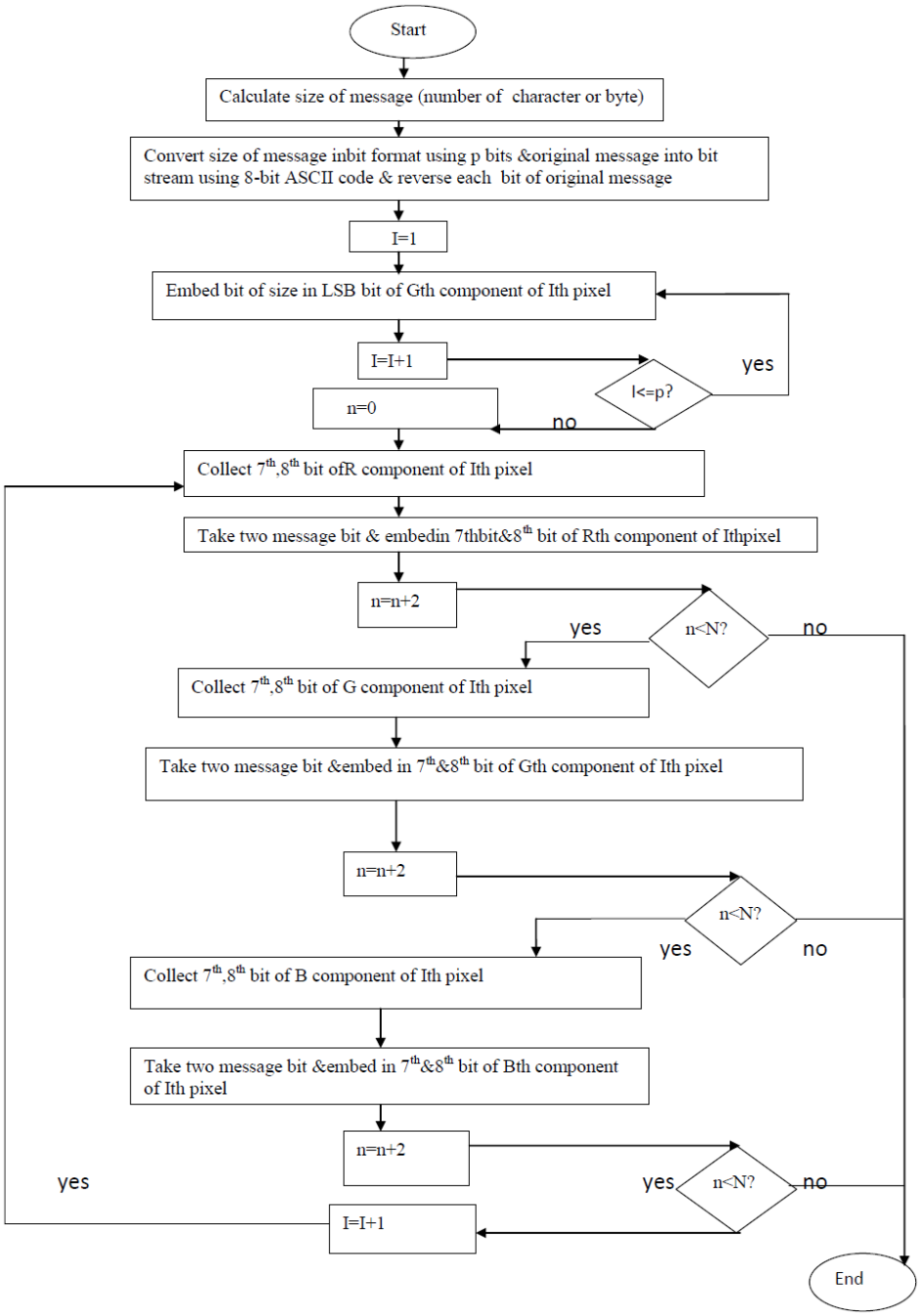

Fig 1 Flowchart for embedding message

B. Extraction process

In this method we first calculate size of message by taking LSB bit of Gth component of P pixel then we take two bit 7^{th},8^{th} of RGB each component of each pixel then we reverse each message bit i.e if message bit is zero then change it by one and if message bit is one then change it by zero then convert it into original message.

Extracting algorithm

1. get stego image ,I=1
2. collect LSB bit of G component of Ith pixel
3. I=I+1
4. if (I<=p)then goto step 2else goto step 5
5. convert message in digit &N=digit*8
6. n=0
7. collect 7^{th} ,8^{th} bit of Rcomponent of Ith pixel
8. n=n+2

9. if (n<N)then goto step 10else goto step 17
10. collect 7^{th} ,8^{th} bit of Gcomponent of Ith pixel
11. n=n+2
12. if (n<N)then goto step 13else goto step 17
13. collect 7^{th} ,8^{th} bit of Bcomponent of Ith pixel
14. n=n+2
15. if (n<N)then goto step 16else goto step 17
16. I=I+1&goto step 7
17. recieve bit stream &change each message bit ((i.e. if message bit is zero then change it by one &if message bit is one then change it by zero) & change it into original message
18. END

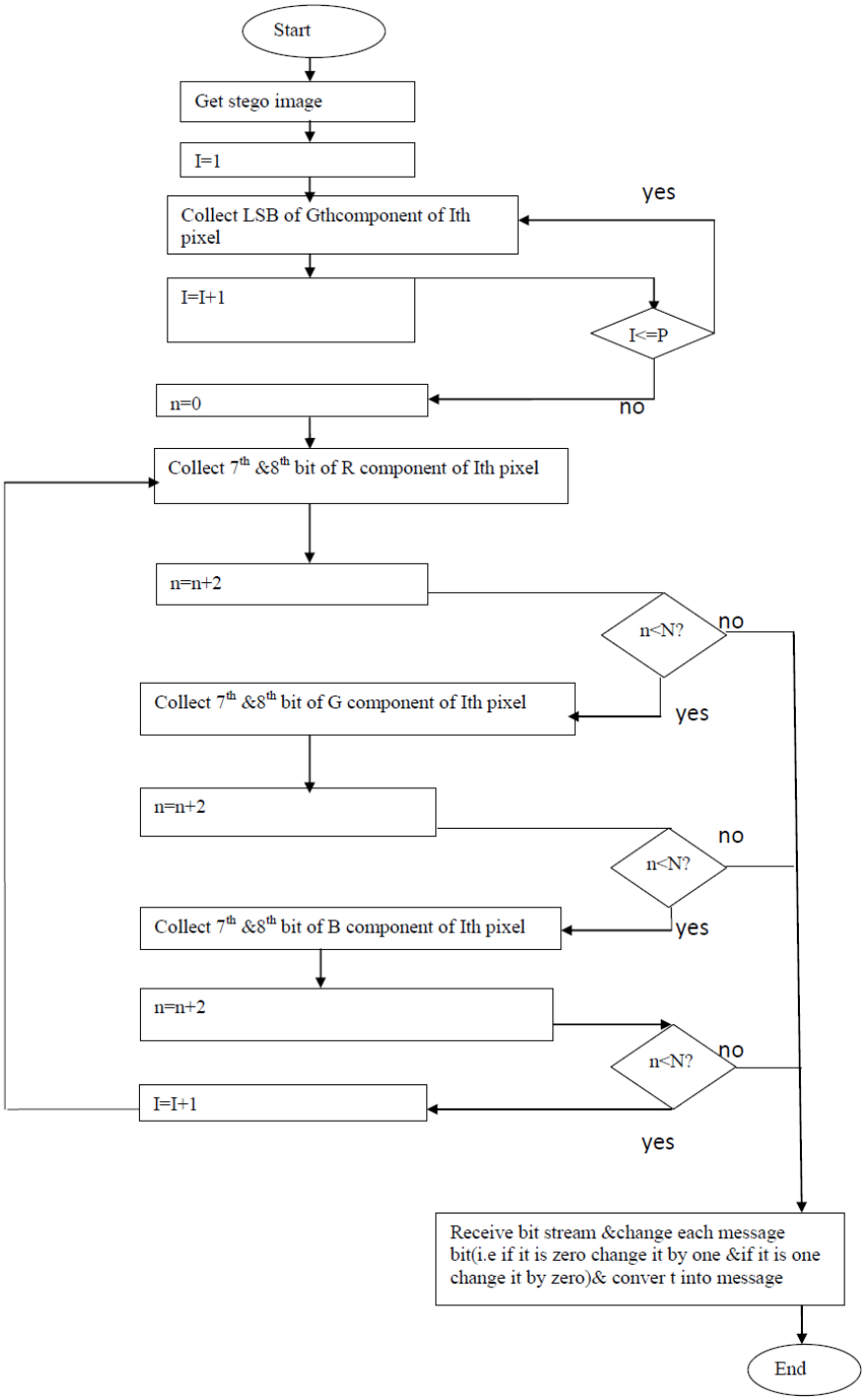

Fig 2 Flowchart for extraction of hidden message

IV. CONCLUSIONS

By this method we can increase size Of message but if extracting algorithm &stegokey known then another person can easily get message.By this method stego image look same as cover image.i.e. there is no degradation of cover image .this method is simple.

REFERENCES

[1] Mehdi Hussain and Mureed Hussain ,"A Survey of Image Steganography Techniques", International Journal of Advanced Science and TechnologyVol.54 May, 2013.

[2] Tahir Ali, Amit Doegar, "A Novel Approach of LSB Based Steganography Using Parity Checker" ,International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X ,Volume 5, Issue 1,January 2015.

[3] Tanmoy Halder, Sunil Karforma, Rupali Mandal, "Analysis of Least-Significant-Bit and Pixel-Value-Difference Steganography, an E-Governance Data-Security Issue", International Journal of Advanced Research inComputer Science and Software Engineering , IJARCSSE Volume 4, Issue 8,August 2014 ISSN: 2277 128X.

[4] Dr. MAHESH KUMAR, MUNESH YADAV, "Image Steganography Using Frequency Domain", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 3, ISSUE 9, SEPTEMBER 2014 ISSN 2277-8616.

[5] Hamdan Lateef Jaheel and Zou Beiji, "A NOVEL APPROACH OF COMBINING STEGANOGRAPHY ALGORITHMS" , INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 8, NO. 1, MARCH 2015 .

[6] Abdelfatah A. Tamimi, Ayman M. Abdalla, Omaima Al-Allaf, "Hiding an Image inside another Image using Variable-Rate Steganography" ,IJACSA International Journal of Advanced Computer Science and Applications,Vol. 4, No. 10, 2013.

[7] Jagruti Salunkhe, Sumedha Sirsikar, "Pixel Value Differencing a Steganographic method: A Survey" ,international Journal of Computer Applications (0975 –8887)International Conference on Recent Trends in engineering & Technology -2013(ICRTET'2013).

ABOUT AUTHOR

Miss. Dipti P Kulkarni is student of Master of Engineering in Computer Science and Engineering. She has completed her Bachelor of Engineering in Information Technology from Solapur University .

Prof. Vanita D Jadhav is currently working as Assistant Professor in SVERI's COE Pandharpur. She has completed Master Technology in Computer Science and Engineering. She guided and published number of projects.

