STEGANOGRAPHY WITH LSB BINARY ADDITION

[1]G. Naga Raju, [2]Dr. P.V.Rama Raju, [3]P.Sai Priyanka, [4]M. Mohan Krishna, [5]M.S.V.Sravya,[6] N.Hema Sai Kumar
[1]Professor & HOD, [2]Asst. Professor, [3, 4, 5, 6]BTech Students
Department of ECE, SRKR Engg college(A), Bhimavaram, India.

Abstract: ***Steganography is the process used for security purposes where human perception cannot follow the data in cover image. It is the practice of concealing a file, message, image, or video within another file, message, image, or video. All of these also try to remove three challenges of steganography i.e. robustness, imperceptibility and capacity. This proposed technique meets these three challenges very efficiently. Here the secret data are not directly embedded within the cover file. The intensity of cover pixel are adjusted in such a way so that at the receiver side the actual target bits are extracted from stego image by performing binary addition. This also performs binary addition among desired number of bits selected from LSB and the two LSBs of the result of binary addition are considered as the interpretation of two target data bits. The maximum change in the intensity value is nominal and is mostly not depends on the number of LSB layer chosen for binary addition. Since the actual data are not hidden thus intruders cannot get it by just using the concept of standard LSB extraction technique. Even though they are able to know the binary addition technique used here even then also don't get the actual target bits without knowing the number of LSB layers involved for binary addition.***

Key Words: Steganography, LSB addition, Robustness, Cover pixel.

I. INTRODUCTION

Today, Information Security, the practice of defending information from unauthorized access, use, modification, recording or destruction, becomes an important security issue with the rise of Internet. Cryptography is a method used for encrypting messages to maintain the secrecy of a communication procedure for a long decade[1]. But besides keeping the message secret, it is often necessary to keep the very existence of the message under wraps. Steganography, a new technique for security wraps secret data into a carrier file in such a stealthy way which avoids the arousing of an eavesdropper's suspicion. Now this data hiding technique has been proposed as one of the promising techniques for the purposes of authentication, fingerprinting, security, data mining, and copyright protection. It is originated from Greek words *Steganós* (Covered), and *Graptos* (Writing) which literally means "cover writing", provides data security by hiding the very existence of the secret information[2].

The Least significant bits are replaced in cover pixels but in a normal image not in Gray scale image[3]. Steganography meets three different challenges: Imperceptibility, Robustness, and Capacity. Imperceptibility refers hiding data in such a way so that it cannot deviate the perceptibility of cover media. Robustness of the secret data refers to preventing eavesdroppers from recovering the secret data until and unless they can able to sense the very existence of it. Capacity, the third one means how much data can be embedded without hampering imperceptibility of cover media. Although these three are much related to each other but they should meet within the steganography without disturbing the other[4]. The use of Least significant bits and pixels can be used in steganography[5]. In our proposed work we try to meet imperceptibility by independently choosing the LSB layer as well as increase the capacity of stego media. At the same time the robustness of the secret data is met by not embedding the actual data within the cover media directly.

II. ROBUSTNESS

All Least Significant Bit (LSB) steganography is popular and simple approach to embed information within an image[6]. The LSB-based technique is the simple one and it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced[7]. It is more imperceptible technique but the capacity of stego media is very poor as well as robustness is very low. To improve robustness as well as capacity in the work we consider three channel of cover image for hiding data where one channel is considered as indicator channel. They divide the image in 4 sub images then use either default (i.e. red color) or user defined pixel indicator channel in zigzag manner[8]. The robustness of steganography techniques is increased either by considering higher LSB Layer or without hiding the actual data or by hiding the data in a robust region. The basic idea to replace the LSB of the cover image with the bits of the messages to be hidden without destroying the property of the cover image significantly.

III. PROPOSED METHOD

Steganography is the process of inserting a secret message within an image in such a way so that no intruder can even feel its existence. Here our objective is to hide a secret text document within a grey scale image in such a way so that actual target bits are not embedded within the stego image for increasing robustness. For doing this the cover pixel values are adjusted in such a way so that at the receiver side the result of binary addition gives the target secret bits.

Embedding of target data:

The embedding of target data is done on two stages - first the adjusted values are placed in their particular bucket then binary addition is used for hiding data within the cover pixels. Each character of the secret text that is to be embedded is converted to its 7 bit ASCII before start processing. Then we decide the value of n which is the number of bits from LSB of cover pixel involved for binary addition.

Bucketing of adjusted values:

In this proposed work n (n>2) bits from LSB of cover pixels are considered for binary addition. If the two least significant bits of this addition result are considered then the four combinations are 00, 01, 10 and 11.The higher order bits of binary addition are ignored here. These combinations have a relation with the number of 1 present within the considerable n bits during binary addition. Table 1 show this relationship between the binary addition and the number of 1 involves within this addition.

Table 1: Relationship between binary addition and number of 1's involved within this addition

No. of 1's within the considerable n (n>2) bit binary	Two LSB's of binary addition result	No. of 1's within the considerable n (n>2) bit binary	Two LSB's of binary addition result
0	00	5	01 (101)
1	01	6	10 (110)
2	10	7	11 (111)
3	11	8	00 (1000)
4	00 (100)		

Table 2: Four buckets for considering 4 LSB's for addition

Bucket Class	4 bits from LSB are considered for binary addition
	Numbers 0 to 15
00	0,15
01	1,2,4,8
10	3,4,6,9,10,12
11	7,11,13,14

If the number of bits of cover pixel involved for binary addition is n so 0 to 2n- 1 different combination are possible in this case. Now these decimal values are con-verted in binary and then arranged in their specific bucket by counting number of 1s in this binary string. The buckets are prepared according to two LSBs of binary addition result and are named according to the two bit combinations of binary. Table 2&3 shows the bucketing result for n=4 and n=6.

Table 3: Four buckets for considering 6 LSB's for addition

Bucket class	6 Bits from LSB are considered for binary addition
	Numbers 0 to 63
00	0,15,23,27,29,30,39,43,45,46,51,53,54,57,58,60
01	1,2,4,8,16,32,63
10	3,5,6,9,10,12,17,18,20,24,31,33,34,36,40,47,48,55,59,61,62
11	7,11,13,14,19,21,22,25,26,28,35,37,38,41,42,44,49,50,52,56

Embedding using Binary Addition:

In this proposed work the embedding technique does not embed the target data directly into the pixel but the desired bits in cover pixels are modified in such a way so that at the receiver side binary addition results of these bits gives the actual data bits. First the target cover pixels are converted to their binary equivalent of 8 bits, then the binary addition of n (n > 2) desired number of bits from LSB are calculated. After that two target bits are compared with the two least significant bits of addition result, then the desired n bits are adjusted if required. If two target bits are same with the 2 LSBs of binary addition result then there is no change is made. If these are not same then the adjustment is required. For doing this adjustment first the particular bucket are chosen based on the two target bits. Then the closest value from this bucket is selected to modify n considerable LSBs for addition so that in receiver side result of binary addition of this n number of desired bits gives the actual target bits. Since each of the buckets is arranged in ascending order the binary search technique is applied for choosing the closest value.

Let "01001110…" this target bit string is to be inserted and n = 4 LSBs of cover pixels are considered for binary addition. Suppose two target bits are embedded within a cover pixel of intensity value 18910 (10111101_2). The 4 bit binary addition from LSB of its 8 bit representation is 1101_2 (1310). Now binary addition is performed among these 4 bits (1 + 1 + 0 + 1 = 11) and the last two bits of this addition result (i.e. 11_2) is compared with the two target bits (012). These are not similar. Thus the 4 bits (1101_2 or 1310) is replaced with the closest value of '01' bucket and here it is 1000_2 (810). Now 18910 (10111101_2) is replaced with 18410 (10111000_2).In this proposed technique since 7 bit ASCII of the character is considered and 2 bits of target text are embedded at a time. So the size of the target bit stream should be even, if it is not then make it even by padding 0 at the end. The target string length and the desired number of bits used for binary addition are inserted at the beginning of the stego image by using same binary addition concept.

Extraction of target data

At the receiver side first the string length and the numbers of bits (n > 2) involved for binary addition are extracted then the target hidden data are extracted using binary addition. During each iteration, first the pixel intensities are converted to their corresponding 8 bit binary. Then the binary addition is performed among the n (n >2) LSBs and the two least significant bits of summation result are obtained. Let, extracted value of n is 4 and a stego pixel value is 18410 (10111000_2). The 4 bit from LSB of 10111000_2 is 1000_2. Now the last two bit of binary addition result of 1000_{2andar} 01 (1 + 0 + 0 + 0 =01). This 01 is the target secret bit extracted at the receiver side. This entire procedure continues until the recipient extracts the entire target bit stream sent by the sender and store these results. Now these pair of bits are concatenated to make the target bit stream. Then each of the 7 bits are cut and converted to their corresponding ASCII. The corresponding target text is generated from these ASCII.

IV. PROPOSED ALGORITHM

Algorithm for Embedding:

Step 1: Take an image and a text as input. Convert the text into binary.
Step 2: Convert the text into binary.
Step 3: Store the target string length as well as the value of n within the cover image.
Step 4: Place the values within the range 0 to 2n-1 into its particular bucket.
Step 5: Consider the last n bit of cover pixels of the image and perform binary addition.
Step 6: Now take the pair of bits of the message and compare it with the two LSBs of addition result.
Step 7: If the binary addition value is same with the last two message bits then nothing is needed to be done, otherwise the n bits will be adjusted by the closest value of particular bucket.
Step 8: Repeat step 4 to step 6 for embedding all target bits.
Step 9: Send the stego message to the receiver side.
Step 10: End

Algorithm for Extraction:

Step 1: Take the stego image as input.
Step 2: Consider the last n bits (confirm by sender) of each target pixel of the stego image and perform binary addition.
Step 3: Two LSBs of addition result are considered as the bits of secret data putting from the end.
Step 4: Now concatenate 7 bits each and convert them to their corresponding decimal value.
Step5: Write it into another file as a form of characters and form the target message.
Step 6: End

In our proposed technique the bits of the cover images are not replaced by the actual target data bits, only the bits of the cover images are adjusted in such a way so that at the receiver side the result of the binary addition gives the target bits. Here the binary addition technique is also used for embedding two target bits at a time and we consider two least significant bits of summation for the interpretation of target data. Since two target bits are embedded at a time so from capacity point of view these proposed technique is two times better than the standard LSB technique.

The actual target bit is not embedded within the cover pixel here thus if any intruder can able to understand the existence of hidden message then also he cannot get it by using LSB technique concept on any bit position. If that unauthorized person already knows the application of binary addition in this proposed work then also he cannot get the actual data by applying binary addition approach without knowing how many LSBs are involved for this addition. For example if the stego pixel is 10110110_2 and 3, 4, 5, 6, 7, 8 any number of LSBs are considered for binary addition then the results of two least significant bits of summation are not same in all cases which is shown in Table 3. So our proposed technique is efficient from robustness point of view.

The maximum change in pixel intensity is independent of number of considerable bits for embedding which makes our proposed technique more imperceptible. If value of n is greater than 2 i.e. any number of Least Significant bits more than 2 is involved for performing binary addition the maximum change is 7 for all cases. Each time the bucket of four pairs 00, 01, 10 and 11 are form before embedding. During the adjustment always the nearest values from the particular bucket is chosen. If the four buckets form by considering any number of bits (always greater than 2) are examined then we show that the smallest values are 0, 1, 3 and 7 (in decimal) for bucket 00, 01, 10 and 11 respectively.

Table 4: Two LSB's of addition result by considering different number of bits from LSB

No. of bits consider for binary addition	Bits considered for addition	Result of two least significant bits of summation
3	10110110	10
4	10110110	10
5	10110110	11
6	10110110	00
7	10110110	00
8	10110110	01

Four buckets by considering 4 and 6 LSBs for binary addition are shown in Table2&3 and if the 4 least significant bits are considered then the maximum change (value 7) in pixel intensity value is occurred when say last four bits is 010 (i.e.00002) and the target bit pair is 112 or vice versa. In this situation we need to adjust last four bits of cover pixel by the nearest value of 11 bucket i.e. by 710 (i.e. 01112) to get 112 at the receiver side only by binary addition of 4 LSBs. This discussion is true for any number of bits (should be greater than 2) considered for binary addition.

V. RESULTS

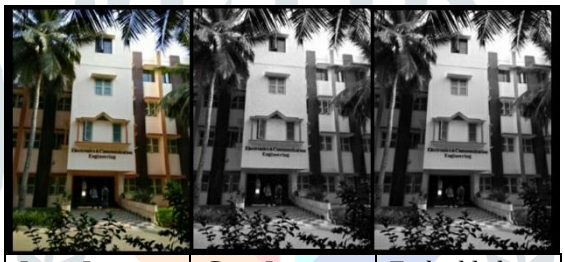
The original input image given is first converted into an image in gray scale and embedded with text in it. This image on reception is again processed to give the input image and the text separately. Text can be of any size. The embedded image does not show much difference hence not allowing the eavesdroppers to find the hidden text. Figure 1 gives the images of example 1 and Figure 2 gives the images of example 2.Figure 3 gives the images of example 3.

Input image	Gray image	Embedded image

Figure1: Images of Example1

Input image	Gray image	Embedded image

Figure2: Images of Example2



Input Image	Gray Image	Embedded image

Figure3: Images of Example3

VI. CONCLUSION AND FUTURE SCOPE

Steganography becomes a most trustworthy security technique in today's communication world. Different techniques are available in this field for providing security and they can try to meet three challenges of steganography by their own. But the technique discussed in this paper meets three challenges of steganography more efficiently. It meets imperceptibility issue by ensuring that the maximum number of changes in intensity value is independent of number of LSB layer chosen for binary addition. It is robust in the sense that the actual target bits are not embedded within the cover pixel to get the stego image. It is two times capacitive than standard LSB technique for steganography. The capacity can also be increased by considering three target bits at a time instead of two. But in this case maximum change in pixel intensity value becomes more (since the number of chosen bits always greater than 6) which affect imperceptibility issue. The future scope of steganography is with the rapid advancement of smart mobile devices the need to protect valuable proprietary information has generated a plethora of new methods and technologies. The new techniques provide hybrid solutions that combine the cryptography with the best of steganography.

VII. REFERENCES

[1] Petitcolas FAP, Anderson R J, Kuhn MG. Information Hiding - A Survey. In Proc. IEEE, vol. 87, no. 7, pp. 1062-1078; July 1999.

[2] Provos N, Honeyman P. Hide & Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine, pp 32 -44; 2003.

[3] Dr.P.V.RamaRaju,G.Naga Raju, P.Rama Krishna: Image encryption after hiding(IEAH) technique for colour images.

[4] Artz D. Digital Steganography: Hiding Data within Data. IEEE Internet Computing Journal; June 2001.

[5] Dr.P.V.RamaRaju,G.Naga Raju,T.AnveshGandhi : RGB Image Steganography using Zigzag Pixel Indicator and Scan Techniques.

[6] Nguyen BC, Yoon SM, Lee HK. Multi Bit Plane Image Steganography. IWDW, LNCS, vol. 4283, pp. 61–70; 2006.

[7] G.NagaRaju,M.Veeramanikanta,V.Sreelekha, Mubashirunnisa,Y.ManojKumar: Hiding and encrypting binary images using a different approach.

[8] Mahimah P, kurinji R. Zigzag pixel indicator based secret data hiding method.In proc. Of IEEE international conference on computational intelligence and computing research;2013.

[9] Bashardoost M, Sulong GB, Parisa G. Enhanced LSB Image Steganography Method By Using Knight Tour Algorithm, Vigenere Encryption and LZW Compression. International Journal of Computer Science; 2013.

[10] Himakshi, Verma HK, Singh RK, Singh CK. Bi-Directional pixel-value differencing approach for RGB Color Image. In Proc. of IEEE Sixth International Conference on Contemporary Computing (IC3), pp. 47-52; 2013.

[11] Agham V, Pattewar T. A Novel Approach Towards Separable Reversible Data Hiding Technique. In Proc. of IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 771-775; 2014.

[12] Hamid N, Yahya A, Ahmad RB, Al-Qershi OM. Characteristic region based image steganography using Speeded-Up Robust Features technique. In Proc. IEEE International Conference on Future Communication Networks (ICFCN 2012), pp. 141-146, Iraq; 2012.

[13] Datta B, Bandyopadhyay SK, Kedia A. High Imperceptible Data Hiding using Remainder Method. International Journal of Computer Applications, Vol. 95, No.18, pp. 12-19 ; June 2014.

[14] Luo W, Huang F, Huang J. Edge Adaptive Image Steganography Based on LSB Matching Revisited. IEEE Transactions on InformationForensics and Security, Vol. 5, No. 2; June 2010.

[15] Rawat D, Bhandari V. A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. International Journal of Computer Applications, Vol. 64, No. 20; February 2013.