A Novel Approach For Image Steganography In Spatial Do-Main Using Last Two Bits of Pixel Value

Rajkumar Yadav *rajyadav76@rediffmail.com*
UIET, M.D.University,
Rohtak, 124001, India

Ravi Saini *ravisaini1988@rediffmail.com*
UIET, M.D.University,
Rohtak, 124001, India

Gaurav Chawla *chawla.gaurav17@gmail.com*
UIET, M.D.University,
Rohtak, 124001, India

Abstract

In this present study a new method for insertion of message in an image is proposed. We have used last two bits of pixel for insertion and retrieval of message. This method is an improvement over earlier methods like Least Significant Bit (LSB) method [2], 6th and 7th bit method [5] and 6th, 7th and 8th bit method [6]. Our method provides us optimal solution in case of chances of message insertion at a pixel location such that the change at a pixel value does not exceed range from +1 to -1 which is negligible to human eye.

Keywords: LSB Method, Cryptography, Steganography, Pseudo Random Number Generator.

1. INTRODUCTION

Steganography is the art and science of hiding information by embedding data into cover media. The term originated from Greek roots that literally mean “covered writing” [1]. The field of Steganography is very old. Throughout history, many steganography techniques have been documented, including the use of cleverly-chosen words, invisible ink written between lines, modulation of line or word spacing and microdots [2, 3, 4]. Usually the secret information is concealed by the use of an innocuous cover as to not arouse suspicion if hostile agents discover the cover. As an example, the cover text:-“I’m feeling really stuffy. Emily’s medicine was not strong enough without another febrifuge.” hides the sentence “Meet me at Nine” if the reader retains the second letter of each word in sequence [11].

Steganography can also be achieved by embedding secret data in an unsuspecting medium like image, video or audio in such a way that the human-perceived quality of the unsuspecting medium is not altered [12]. The idea was first described by Simmons in 1983 [7]. More comprehension theory of steganography is given by Anderson [8]. Steganography is different from cryptography which is about concealing the content of message whereas steganography is about concealing the existence of the message itself [9]. Images provide excellent carriers for hiding information and many different techniques have been introduced [10].

The most popular and oldest technique for hiding data in digital image is LSB technique [2]. One of the major disadvantage associated with LSB technique is that intruder can change the LSB of all image pixels. In this way, hidden message can be destroyed but the change in

image quality is in the range of +1 to -1 at each pixel position.[5] designed the algorithm which uses 6^{th} and 7^{th} bits of pixel value for message insertion. It removes the disadvantages of LSB techniques but it has also one disadvantage. The disadvantage is that the chance of message insertion at pseudo random location at first chance is only 49%. Batra et *al*. [6] gives an algorithm which uses 6^{th}, 7^{th} and 8^{th} bit for message insertion. This technique increases the chances of message insertion at pseudo random location at the first chance up to 85.93%. Our method uses the last two bits of pixel value and it increases the chances of message insertion at pseudorandom location at first chance up to 100% which is optimal solution.

2. DESCRIPTION OF PROPOSED METHOD

We have used the last two bits of pixel value for insertion and retrieval of message. We can insert 0 at a pixel value if last two bits of pixel value are 00 or 10. If the last two bits of pixel value, are not 00 or 10 by adding or subtracting 1 at that pixel value for insertion of 0. Similarly, we can insert 1 at a pixel value if last two bits of pixel value are 01 or 11. If the last two bits of pixel value are not 01 or 11 then we try to make them 01 or 11 by adding or subtracting 1 at that pixel value for insertion of 1. Now, at the retrieval end, if the last two bits of pixel value are 00 or 10 then 0 is the message bit else 1 is the message bit. The insertion process is shown in figure 2 (a) and retrieval process is shown in figure 2 (b).

The intruder can change the LSB of all the pixel values in our method also as in case with LSB method. But in case of our method if intruder changes LSB's of all pixel values then at some locations the change in pixel values would be +2 or -2 which will be visible to human eye. This situation indicates that something goes wrong in the middle (i.e. between sender and receiver). So, in this age the sender retransmit the stego image once again.

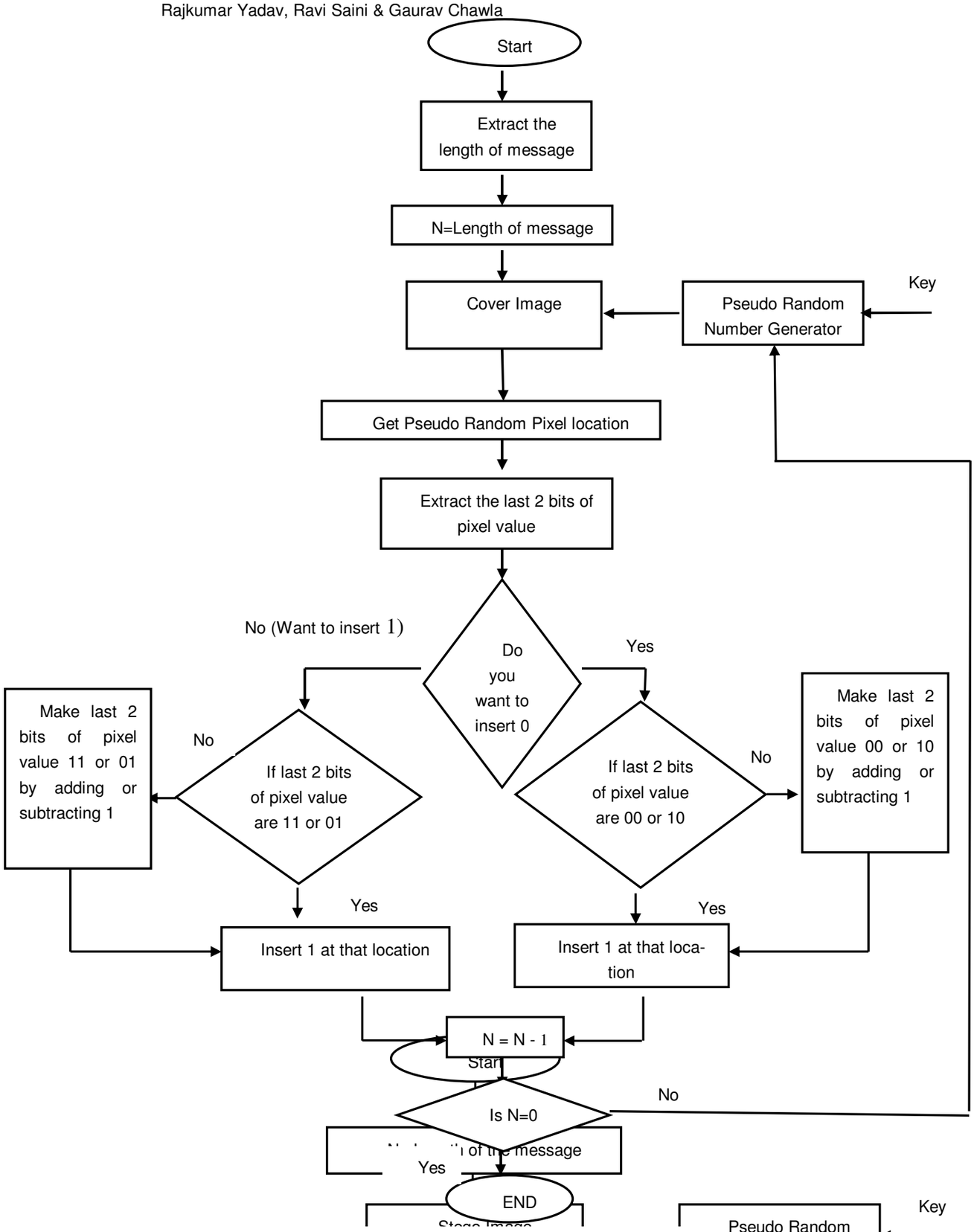
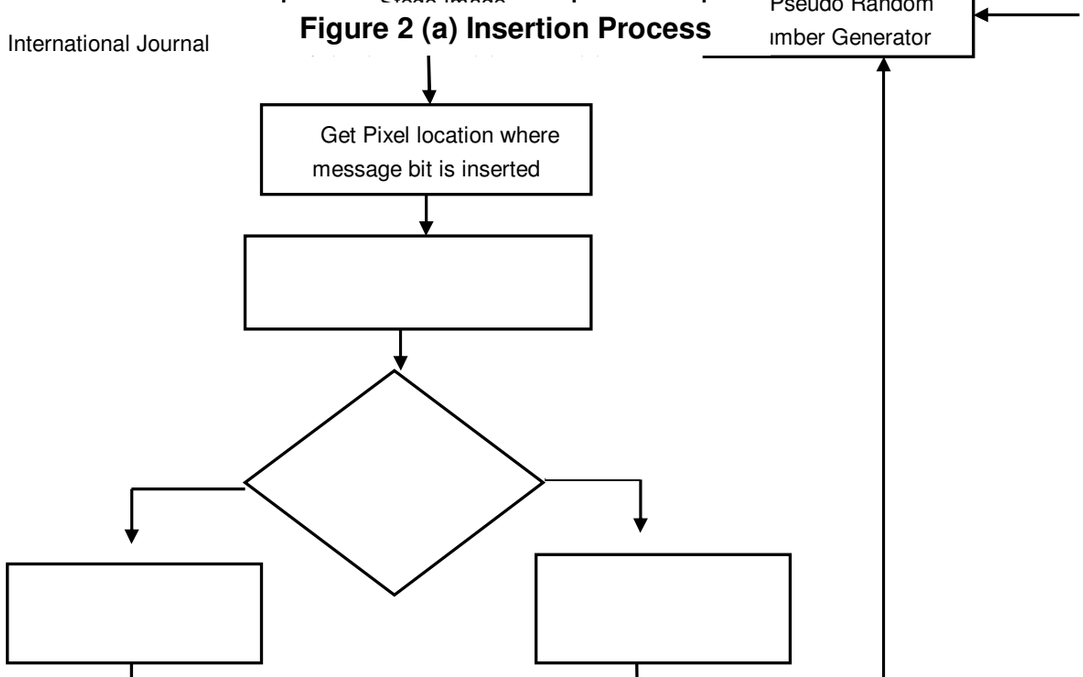


Figure 2 (a) Insertion Process



3. LGORITHMS

3.1. Assumptions

I. Sender and Receiver agree on the cover image in which message is to be hidden.

II. Both sender and receiver agree on the same pseudo-random key to decide the pseudo random locations where message is to be inserted.

III. Both sender and receiver either agree on the length of message "OR" the length of the message is hidden with the message itself at some prespecified locations which are known to both sender and receiver.

3.2. Insertion Algorithm

I. Find the pseudo-random location (L) in cover image from secret key to insert the message bit (For detail see [13] and [14]).

II. Extract the last two bits of the selected pixel location (L).

III. If we want to insert 0 then go to step (iv) else go to step (v).

IV. (a) If the last two bits of the selected pixel location (L) is 00 or 10 then insert 0 at location (L) and go to END.
(b) If the last two bits of the selected pixel location (L) is equal to 01 or 11 then make them 00 or 10 by adding or subtracting 1 at pixel location (L). Insert 0 to that location and go to END.

V. (a) If the last two bits of the selected pixel location (L) is 11 or 01 then insert 1 at location (L) and go to END.
(b) If the last two bits of the selected pixel location (L) are equal to 00 or 10 then make them 11 or 01 by adding or subtracting 1 at pixel location (L). Insert 1 to that location and go to END.

VI. END.

3.3. Retrieval Algorithm

I. Generate the pixel location (L) from the same secret key as used for insertion of message.

II. Extract the last two bits of the selected pixel location (L).

III. If last two bits of the selected pixel location (L) is 00 or 10 then 0 is the message bit else 1 is the message bit.

IV. END.

4. CHANGES IN PIXEL VALUE AFTER THE INSERTION OF MESSAGE

Now, we see how various pixel values changes during insertion of message. Table I shows how pixel values changes during insertion of 0 and Table II shows how pixel values changes during insertion of 1.

5. CHANGE IN PIXEL VALUE WHEN INTRUDER CHANGES LSB'S OF ALL PIXEL VALUES

Here, we have considered the case in which intruder changes the least significant bits of pixel values of the cover image with message. Table III shows changes the LSB's of pixel value and 0 is inserted at the pixel value. Table IV shows change in pixel value when intruder changes the LSB's of pixel value and 1 is inserted at the pixel value.

TABLE 1 (Change in Pixel Value after Insertion of 0)

TABLE II (Change in Pixel Value after Insertion of 1)

Decimal Value	Pixel value before insertion of '0'	Pixel value after insertion of '0'	Change in Pixel value comment for insertion of
0	00000000	00000001	+1, Insert
0	00000000	00000000	NC, Insert
1	00000001	00000001	NC, Insert
1	00000001	00000010	+1, Insert
2	00000010	00000011	+1, Insert
2	00000010	00000010	NC, Insert
3	00000011	00000011	NC, Insert
3	00000011	00000100	+1, Insert
4	00000100	00000011	-1, Insert
4	00000100	00000100	NC, Insert
5	00000101	00000101	NC, Insert
5	00000101	00000100	-1, Insert
6	00000110	00000111	+1, Insert
6	00000110	00000110	NC, Insert
7	00000111	00000111	NC, Insert
7	00000111	00000110	-1, Insert
8	00001000	00001001	+1, Insert
8	00001000	00001000	NC, Insert
9	00001001	00001001	NC, Insert
9	00001001	00001000	-1, Insert
10	00001010	00001001	-1, Insert
10	00001010	00001010	NC, Insert
11	00001011	00001011	NC, Insert
11	00001011	00001100	+1, Insert
12	00001100	00001011	-1, Insert
12	00001100	00001100	NC, Insert
13	00001101	00001101	NC, Insert
13	00001101	00001110	+1, Insert
14	00001110	00001111	+1, Insert
14	00001110	00001110	NC, Insert
15	00001111	00001111	NC, Insert
15	00001111	00001110	-1, Insert
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
127	01111111	01111111	NC, Insert
127	01111111	10000000	+1, Insert
128	10000000	01111111	-1, Insert
128	10000000	10000000	NC, Insert
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
.	.	.	.
254	11111110	11111111	+1, Insert
254	11111110	11111110	NC, Insert
255	11111111	11111111	NC, Insert
255	11111111	11111110	-1, Insert

TABLE III (Change in Pixel Value after Insertion of 0 with Changed LSB)

Decimal Value	Pixel value befor insertion of '0' (C1)	Pixel value after i sertion of '0'	Pixel value after i sertion of '0' with changed LSB's by in truder (C2)	Net change i.e C2 - C1
0	00000000	000000000	000000000	NIL
1	00000001	000000010	000000010	+2
2	00000010	000000100	000000100	+2
3	00000011	000000110	000000110	+2
4	00000100	000001000	000001000	+2
5	00000101	000001010	000001010	NIL
6	00000110	000001100	000001100	+2
7	00000111	000001110	000001110	+2
8	00001000	000010000	000010000	+2
9	00001001	000010010	000010010	NIL
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
254	11111110	111111100	111111100	NIL
255	11111111	111111110	11111110	-1

TABLE IV (Change in Pixel Value after Insertion of 1 with Changed LSB)

6. RESULTS AND CONCLUSIONS

6.1 The Following Results Obtained From Table I And Table Ii Tells Us How Our Method Is Better Than The Previous Methods.

(i) The message bit will be inserted at the pseudorandom location at first chance = 512/512*100 = 100%.
(ii) Chance when message is inserted, no change in pixel value is required = 256/512*100 = 50%.

6.2 The Comparison Table Of Our Method With 6th & 7th Bit Method And 6th, 7th & 8th Bit Method Is Shown Below:

Method	Message bit Insertion at pseudorandom location at firs chance	No change in Pixel value when message bit is inserte
6th, 7th Bit	50%	50%
6th, 7th & 8th Bit	85.93%	43.18%
7th, 8th Bit	100%	50%

TABLE V (Comparison Table)

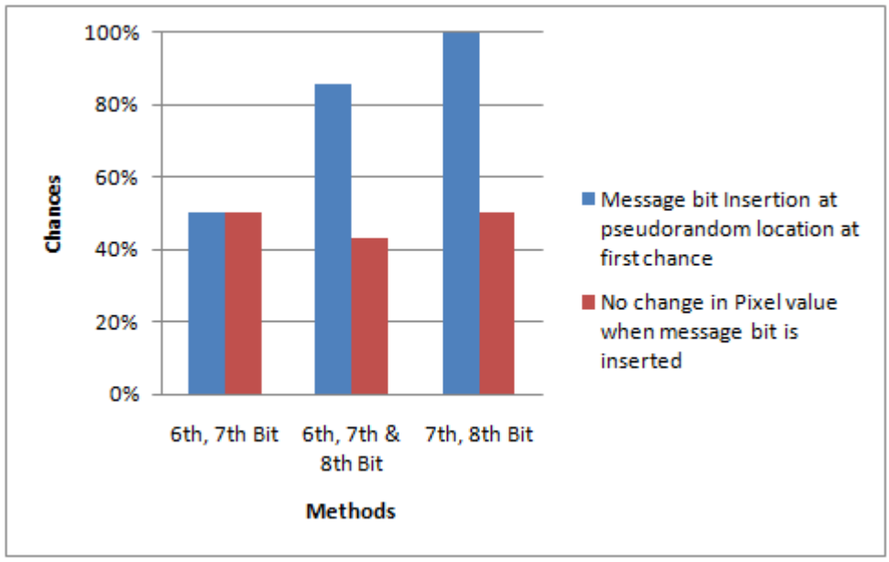


FIGURE 6 (a) Comparison Chart

From Table V and Figure 6 (a), we conclude that our method provides maximum chances of message insertion at a pixel location i.e. 100% which is an improvement over earlier existing methods like 6th, 7th bit method and 6th, 7th & 8th bit method. 6th , 7th bit method provides only

50% chances of message insertion at a pixel value due to which approximately half of the pixel locations cannot be used for insertion of the message. 6^{th} , 7^{th} & 8^{th} bit method increases the chances of message insertion at a pixel value from 49% to 85.93% which is also not a optimal solution. Our method provides optimal solution in case of chances of message insertion which is an improvement over earlier existing methods.

6.3. Table III and Table IV shows that when intruder tries to change the LSB's of all pixel values when message is inserted in the image then the change at some pixel values becomes +2 or -2 which will be visible to human eye. So, in case of our algorithm if intruder tries to distort our message by changing LSB's of all pixel values then it reflects at the receiver end that something has gone wrong in the middle. In this situation, receiver asks to sender to send the message again for retrieval of correct message.

REFERENCES

[1] A. Gutub, M. Fattani, "A Novel Arabic Text Steganography Method using letter Points and Extension", WASET International Conference on Computer Information and System Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[2] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer*, pp. 26-34, February 1998.

[3] D. Kahn, *The Codebreakers,* Macmillian, New York, 1967.

[4] B. Norman, *Secret Warfare*, Acropolis Books, Washington D.C., 1973.

[5] Parvinder Singh, Sudhir Batra and HR Sharma, "Evaluating the Performance of Message Hidden in First and Second Bit Plane," WSEAS Transaction on Information Science and Technology, Vol. 2, No 89, pp 1220-1222, Aug 2005.

[6] Sudhir Batra, Rahul Rishi and Raj Kumar, "Insertion of Message in 6^{th}, 7^{th} and 8^{th} bit of pixel values and its retrievals in case intruder changes the least significant bits of image pixels", International Journal of Security and its application, Vol. 4, No. 3, July 2010.

[7] Simmons G. J, "The Prisoners Problem and the Subliminal Channel", Proceedings of crypto '83, Plenum Press, pp 51-67, 1983.

[8] Anderson R. J, "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48, 1996.

[9] Anderson R. J, Peticolas FAP, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

[10] N.F. Johnson and Zoran Duric, S. G. J. *Information Hiding : Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1)*. Kluwer Academic Publishers, February 15, 2001.

[11] Eugene, T.L., Delp Edward J., "A Review of Data Hiding in Digital Images".

[12] Amirtharajan Rengarajan, Ganesan Vivek, Jithamanyu R, Rayappan John Bosco Balaguru, "An Invisible Communication for Secret Sharing against Transmission Error", Universal Journal of Computer Science & Engineering Technology, 1 (2), 117-121, Nov-2010.

[13] 13. E Franz, A Jerichav, S Moller, A Pfitznaun, I Steierand, “Computer Based Stegnography”, Information Hiding, Springer Lecturer Notes in Computer Science, Vol. 1174, pp. 7-21, 1996.

[14] Yeuan-Luen Lee, Ling-Hwei Chen, “A Secure Robust Image Stegnography Nodel,”10th National Conference on Information Security, Hualien, Taiwan, pp 275-284, May 2000.

[15] Stallings.W. Cryptography and network security: Principles and practice. In *Prentice Hall*, 2003.

[16] Chandramouli, R., Memon, N.D., ‘Steganography capacity: A steganalysis perspective’, Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis, 2003

[17] S.Craver ,N. Memon , “Resolving Rightful Ownership with Invisible Watermarking Techniques: Limitations, Attacks and Implications”, IEEE Trans.,Vol 16,No. 4,pp. 573-586,1998.

[18] W. Bender,D. Gruhl, N.Morimoto, and A. Lu, “Techniques for data hiding,” IBM Systems Journal, vol. 35, no. 3-4, pp. 313–335, 1996.

[19] N. Nikolaidis and I. Pitas, “Robust image watermarking in the spatial domain,” Signal Processing, vol. 66, no. 3, pp. 385–403, 1998.

[20] Jing Dong and Tieniu Tan, “Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations”, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, P.O. Box 2728, 10190, Beijing, China.

[21] Jessica Fridrich, Miroslav Goljan , Rui Du, “Detecting LSB Steganography in Color and Gray-Scale Images”, IEEE Multimedia, issue 4, vol 8, 2001

[22] Johnson, Neil F., Zoran Duric, S. G. J., Information Hiding: Steganography and Watermarking – Attacks and Countermeasures (Advances in Information Security, Volume I). Kluwer Academic Publishers, February 15, 2001.

[23] RJ Anderson, FAP Petitcolas, “On the Limits of Stegnography”, IEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481, May 1998.

[24] Ko-Chin Chang., Chien-Ping Chang., Ping S. Huang., and Te-Ming Tu,: A Novel Image Steganographic Method Using Tri-way Pixel-Value Differencing, Journal of Multimedia , VOL. 3, NO. 2, JUNE 2008.

[25] Parvez M. T. and Gutub A., “RGB Intensity Based Variable-Bits Image Steganography”, APSCC 2008-Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12 December 2008.

[26] Pal, S.K., Saxena, P.K., Muttoo, S.K., ‘Image steganography for wire less networks using the handmaid transform’, International Conference on Signal Processing & Communications (SPCOM), 2004