Robustness of Parity Checker Method against Various Watermarking Attacks

Rajkumar Yadav
Assistant Professor
U.I.E.T, M.D.U, Rohtak

Abstract
In the 21th century, information security has become a geart issue. Steganography and watermarking provide solution to these issues. Watermarking is mainly used for copyright protection. There are many techniques which have been developed for watermarking in the past decade both in the spatial and frequency domain. In this paper, robustness of Parity Checker Method [1] which is a spatial domain technique is checked has been checked against the two watermarking attacks blurring and cropping .By analysis of the result we found that this method provides favorable results.

Keywords: Steganography , Watermarking, Robustness, Parity Checker Method

1. Introduction

In the recent years, with the growth of multimedia system in distributed environment, the problem associated with multimedia security and multimedia copy right protection have become important issues. Also the technology designed to make electronic publishing feasible has also increased the threat of intellectual property threat. Illegal copying and redistribution of digital images, audio or video without any information loss is also a threat to the society. These issues can be solved by using water marking techniques available [2, 3, 4, 5, 6]. The process of digital watermarking involves the modification of original multimedia data to embed a watermark containing the key information as a authentication or copy right codes. The embedding method must leave the original data perceptually unchanged, yet should imposed modification which can be detected by using an appropriative extraction algorithm. A water mark is an imperceptible, robust and secure message embedded directly in digital elements such as image, audio, and sound which uniquely identifies its owner. It should be noted that digital water mark could not itself prevent copying, modification and redistribution of documents [7]. However if encryption and copy protection fails, water marking allows the documents to be traced back to its right owner and prevents unauthorized use. The water mark must be difficult to remove and immune to multimedia data operations. A water mark containing the information regarding owner should be small in size so that it can be easily embedded into images. The water mark can also be embedded as a noise component in image. In general, the watermark can be visible or invisible. A visible watermark typically contains a evidently visible message or a company logo indicating the ownership of the image. The invisible watermark contents appear perceptually identical to the original.

In this paper, the robustness of parity checker method has been checked against the two watermarking attacks. In parity checker method, parity of the the pixel value is checked to insert the watermark bit. The watermark bit inserted at a pixel position according to the parity of the pixel value. The analysis of this technique against the blurring and cropping attack show the favorable results.

The rest of the paper is organized as follows: Section 2 describes the various attacks on the watermarking. Parity Checker Method has been given in the section 3. At last , section 4 gives the result and analysis.

2. Attacks on Watermarking

There may be many attacks on watermarked image namely, blurring, cropping, compression, scaling etc. Here in this paper blurring and cropping have been discussed in section four.

3. Parity Checker Method [1]

In this method, the concept of even and odd parity has been used by using the parity checker. As we already know that even parity means that the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's. In this method '0' bit is inserted at a pixel value where pixel value has odd parity and if the parity is even then odd parity is made by adding or subtracting '1' to the pixel value. Similarly, '1' is inserted at a pixel value if it had even parity. In case, if even parity is not present at that location then even parity is made over that location by adding or subtracting '1'. In this way '0' or '1' is inserted at any location. The insertion process is shown in figure 1 and 2.

For retrieval of message, again parity chacker is used. If odd parity is present at the selected location then '0' is message bit, else message bit is '1'. Retrieval process is repeated for all locations. In this way, the message bits are retrieved bits from all the locations where these have been inserted. The retrieval process is shown in Figure 3.

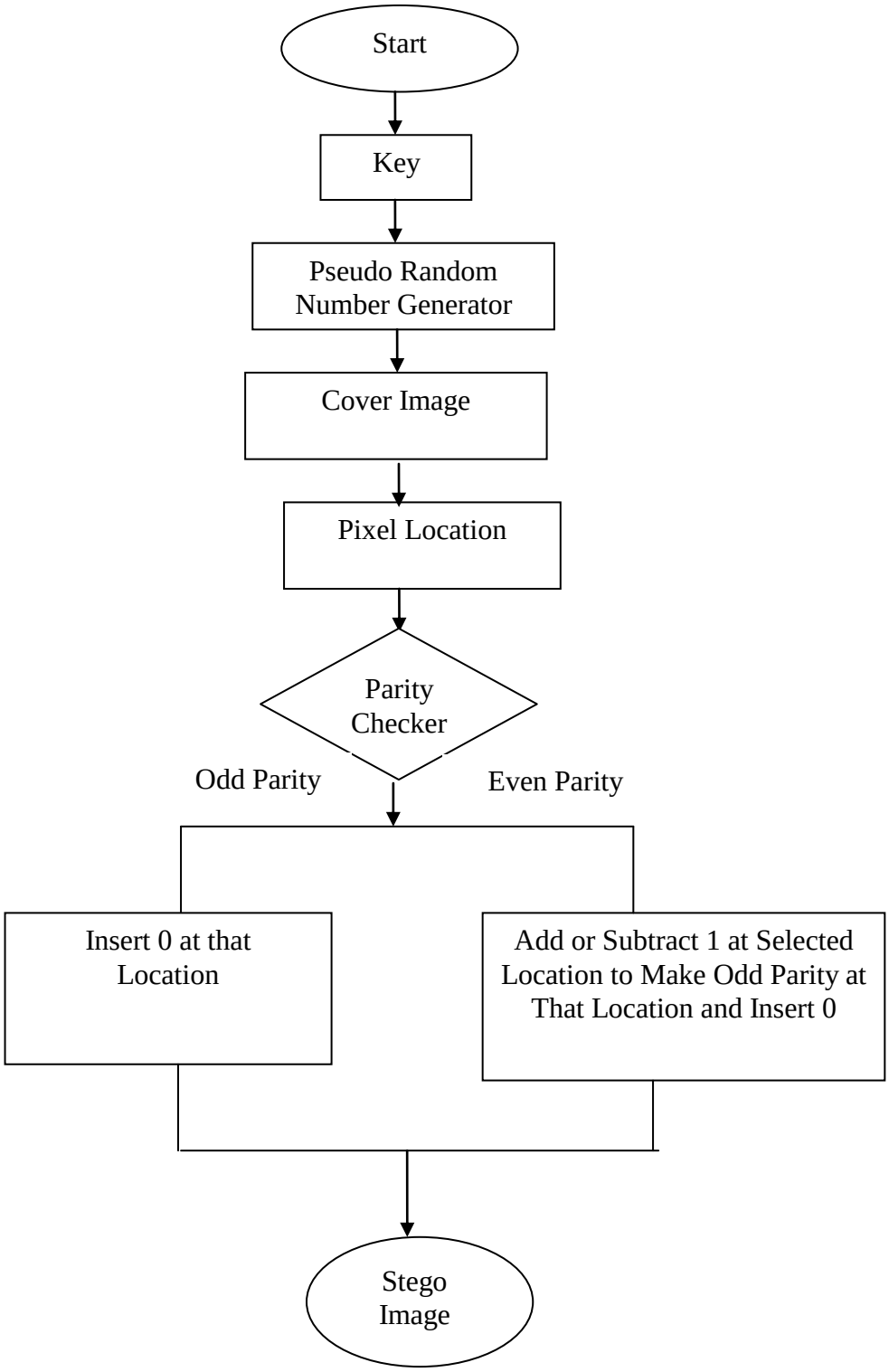

Fig. 1 (Insertion of 0)

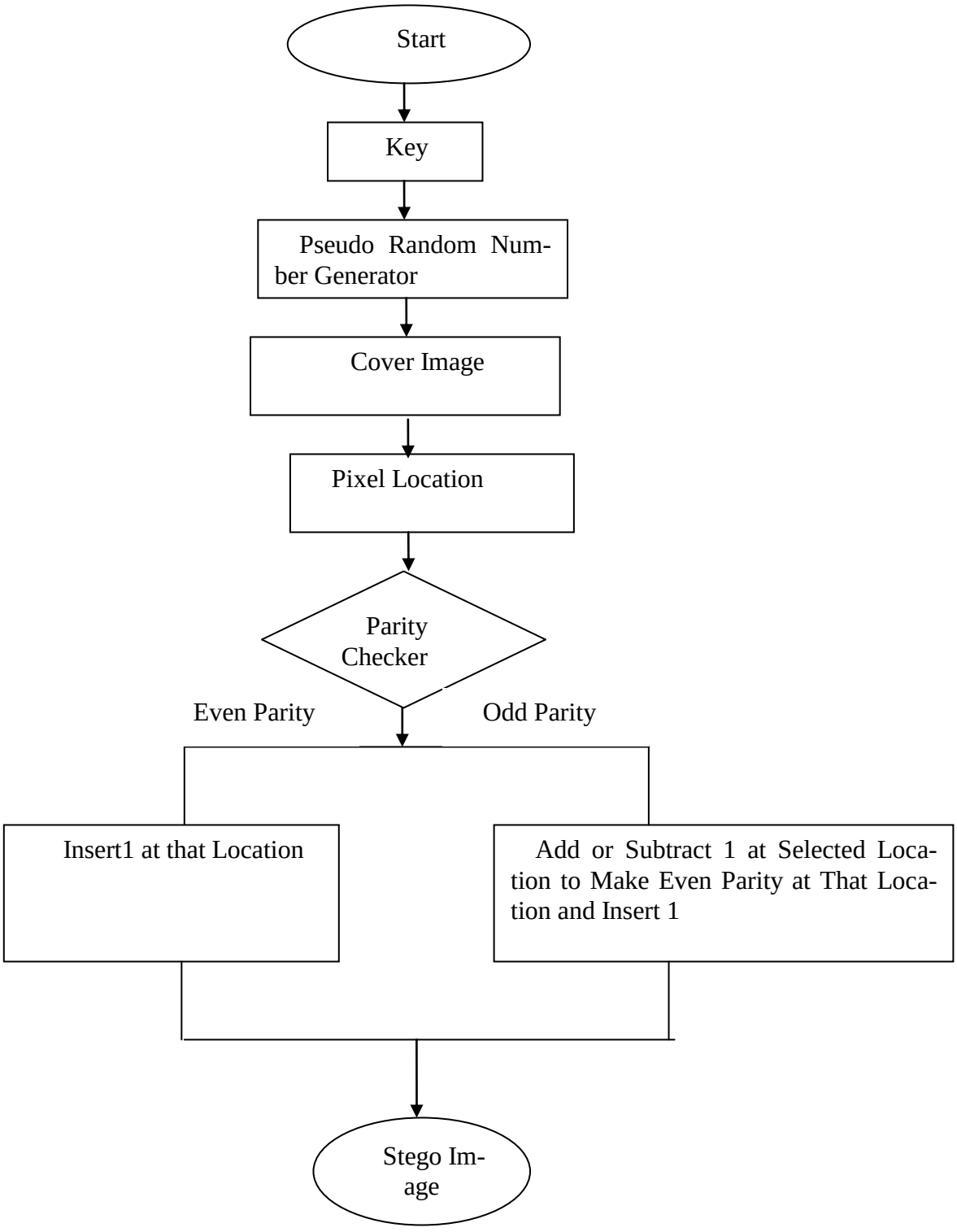

Fig.2 (Insertion of 1)

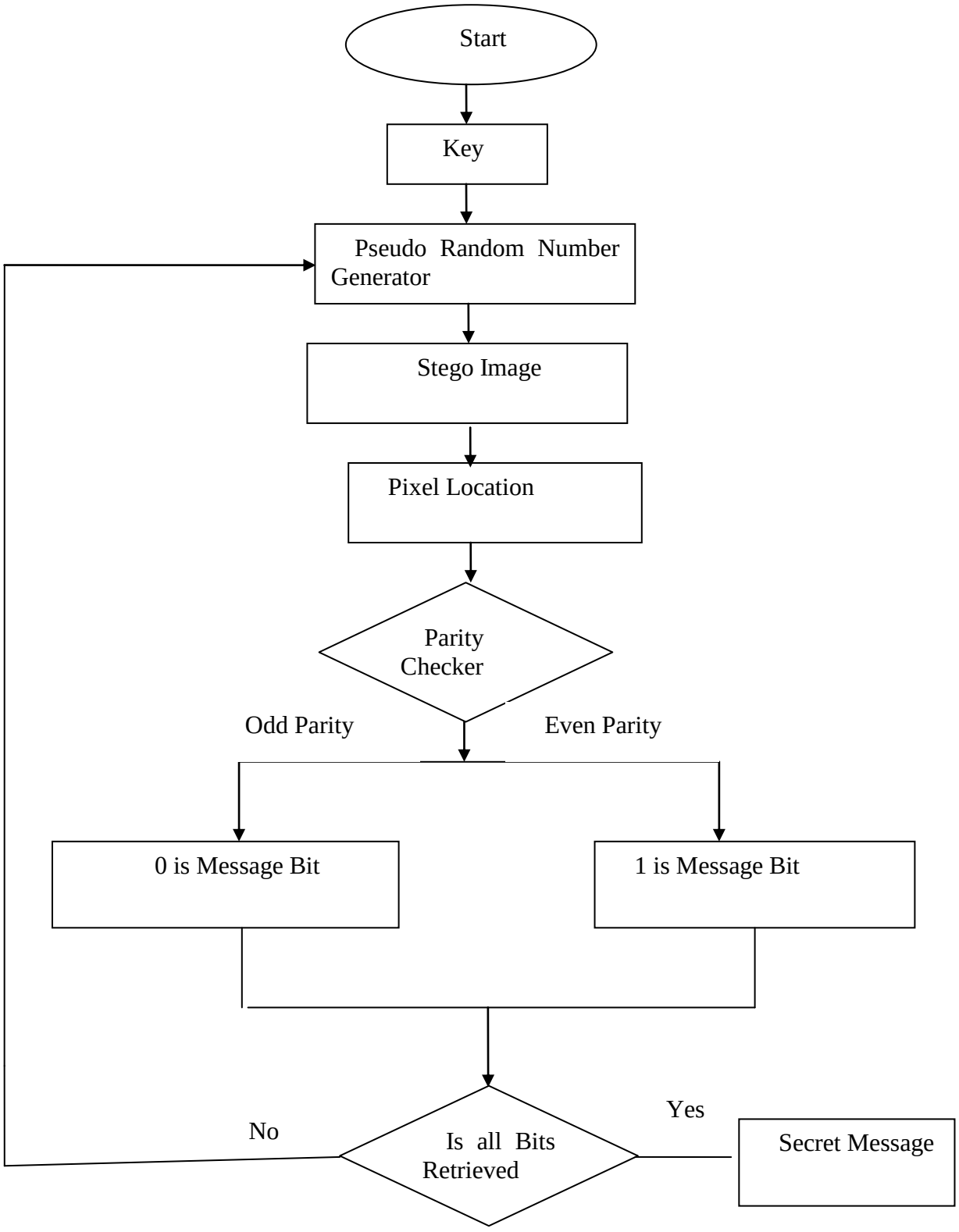

Fig. 3 (Retrieval)

3.4.2 Algorithm [1]

3.4.2.1 Assumption

(i) Sender and recipient agree on the cover object in which message is supposed to be hidden.

(ii) Both sender and recipient agree on the same pseudo–random key to decide the random locations where message is to be inserted.

3.4.2.2 Insertion Algorithm

(i) Find pseudo-random location (L) in cover image from secret key to insert the message bit. (For detail see [Franz et al (1996)] and [Lee and Chen (2000)]).

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

(iii) (a) Check whether at location (L) pixel value is having odd parity. If yes, insert 0 at location 'L' and go to END If no, go to step (b)

(b) Make the parity of pixel value odd by adding or subtracting 1 and then insert 0. Go to END

(v) (a) Check wheather at location 'L' the pixel value is of even parity. If yes, insert 1 at location (L) and go to END. If no, go to step (b).

(b) Make the parity of pixel value by adding or subtracting 1 and then insert 1 and go to END.

(vi) END

3.4.2.3 Retrieval Algorithm

(i) Trace out the location (L) from the same secret key as used for insertion of message.

(iii) Check whether at location (L).

(a) If the parity of pixel value is odd then '0' is the message bit.

(b) If the parity of pixel value is even then '1' is the message bit

(iv) END

4. Results and Analysis

Here in this section robustness of watermarking scheme against two attacks i.e. cropping and blurring of imagehas been analyzede. Figure 4 shows the original image and figure 5 shows the watermarked image with watermark 'Rajkumar' inserted four times in the original image. Figure 6 shows the blurred image and figure 7 shows the cropped image.

Fig.4 Original Image

Fig.5 Watermarked Image

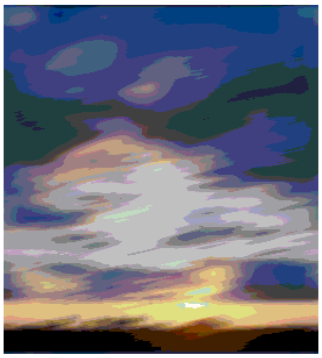

Fig.6 Blurred Image

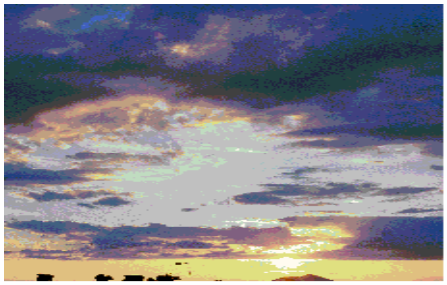

Fig.7 Cropped Image

From this we can easily analyze the above images based on PSNR (Peak signal to noise ratio) in dB by using the software HAYDWT Video watermark. The PSNR values of original image and stego image are given in table 1 Table 2 shows the PSNR values under the various attacks

Table 1

Component	PSNR (Original Image and Stego Image)
Red	**9.59**
Green	**10.03**
Blue	**11.28**

Table 2

Attack	PSNR of Red component (Original Image and Attacked Image)	PSNR of Green component (Original Image and Attacked Image)	PSNR of Blue component (Original Image and Attacked Image)
Blurring	**7.84**	**8.53**	**9.50**
Cropping	**9.67**	**9.62**	**9.51**

After analyzing the results from table 4.3 and 4.4 it is found that PSNR values decrease after applying the various attacks. Under the blurring attack the PSNR value of red, green, and blue component decreases by 1.35dB, 1.54dB, and 1.78dB respectively. Similarly, in cropping the PSNR values of green and blue components decreases by 0.41dB and 1.77 dB respectively. There is slightly in the PSNR values in the red component i.e. 0.08dB. So on the basis of above facts it is concluded that there is very less change in PSNR values under the various attacks which shows the robustness of watermarking technique.

5. References

1. Rajkumar Yadav, Rahul Rishi & Sudhir Batra, "A New Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010.
2. Su, P.C., Kuo, C.C.J. and Wang, H.J.M. (1999), "Blind digital watermarking for cartoon and map images", In: Security and Watermarking of Multimedia Contents. Wong PW, Delp EJ. (eds.); 3657: 296–306.
3. Andres, F. (2001), "Multimedia and Security", IEEE Multimedia, pp 20-21.
4. Mintzer, F. and Braudaway, G.W. (1999), "If one watermark is good, are more better?", In: International Conference on Acoustics, Speech and Signal Processing. IEEE Signal Processing Society.: 2067–2070. ISBN 1-876346-19-1.
5. Mintzer, F., Braudway, G.W. and Yeung, M.M. (1997), "Effective and Ineffective Digital Watermarks", IEE ICIP vol III, pp 9-12, Santa-Barba, Cal.

6. Peticolas, F.A.P., Anderson, R.J. and Kuhn, M.G. (1999), "Information Hiding: A Survey", Proceedings of IEEE, 87, no. 7, pp 1062-1078.

7. Eager, J.J. and Girod, B. (2001), "Quantization Effect on Digital Watermark", Signal Processing, vol 81, no 2, pp 239-263, EURASIP.

8. I.Cox,J Kilan, " Secure Spread Spectrum Watermarking for Images,Audio and Video" , in Proc. IEEE International Conference on Image Processing ,1996,vol 3,pp. 243-246.

9. 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.

10. Chun-Yu-Chang,"The Application of a Full Counterpropagation Neural Network to Image Watermarking", 2005, IEEE

11. H. Y. Gao, The theory and application of audio information hiding, PH.D. dissertation, Beijing university of Posts and Telecommunications, Beijing, China, 2006.

12. J. F. Delaigle, C. Devleeschouwer, B. Macq et al., "Human visual system features enabling Watermarking J," in Proceedings of IEEE International Conference on Multimedia and Expo, pp. 489–492, Lusanne, Switzerland, 2002.

13. S. Katzenbeisser and F. A. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, ArtechHouse Press, Norwood, Mass, USA, 2000.

14. 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.