Steganography Performance over AWGN Channel

Fahd Alharbi
Faculty of Engineering
King Abdulaziz University, Rabigh, Saudi Arabia

***Abstract*—Steganography can be performed using frequency domain or spatial domain. In spatial domain method, the least significant bits (LSB) is the mostly used method where the least significant bits of the image's pixels binary representation are used to carry the confidential data bits. On the other hand, secret data bits in the frequency domain technique are hidden using coefficients of the image frequency representation such as discrete cosine transform (DCT). Robustness against image attacks or channel's noise is a key requirement in steganography. In this paper, we study the performance of the steganography methods over a channel with Added White Gaussian Noise (AWGN). We use the bit error rate to evaluate the performance of each method over a channel with different noise levels. Simulation results show that the frequency domain technique is more robust and achieves better bit error rate in a noisy channel than the spatial domain method. Moreover, we enhanced the steganography system robustness by using convolution encoder and Viterbi decoder. The effect of the encoder's parameters, such as rate and constraint length is evaluated.**

Keywords—Steganography; robustness; noise; AWGN; viterbi

I. Introduction

Steganography is the process of concealing critical and important information undetectably in a cover medium such as image, voice and video [1, 2]. The steganography model is illustrated in Fig. 1, where the important message hidden in the cover image using the embedding process. The watermarked image which is the cover image with concealed data is transmitted through a communication channel. The receiver recovers the secret message using the extracting process. The embedding and extracting processes are implemented using spatial domain [3-5] or frequency domain techniques [6, 7].

A. *Spatial Domain Steganography*

The mostly used method for spatial domain steganography is the least significant bit (LSB). LSB first decomposes the image's pixels value using the binary system, then insert the secret bits into the least significant bits. For example, the process of hiding the letter A (ASCII Code: 1000001) into seven pixels of a gray-scale image is illustrated at Table I. The effect of the LSB on the cover image is hardly noticed by the human eye since the bit used for data hiding has a small value.

B. *LSB Performance*

Now, we study the performance of the LSB embedding method in a communication system with Added White Gaussian Noise channel (Fig. 2). The watermark image W is hidden into the cover image C using the LSB embedding process module. The watermarked image I is transmitted through an AWGN communication channel. The received watermarked image I' is fed to the LSB extracting process module to extract the recovered watermark image W'.

We change the variance of Added White Gaussian Noise for different channel noise levels. The effect on the watermarked image I is evaluated by computing PSNR (Peak Signal to Noise Ratio). The PSNR between the 8-bit gray-scale watermarked image I and the received watermarked image I' is computed as following:

$$PSNR = \frac{10\log_{10}(255)^2}{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I(i,j) - I'(i,j)\right]^2} \tag{1}$$

where *M* and *N* represent the size the watermarked image.

The performance of the LSB steganography over the AWGN channel is measured by computing the bit error rate (BER). The BER is calculated using Eq. (2), where the watermark image W is a black-and-white image with a size of K by L pixels. The calculation performs Exclusive-OR ($\oplus$) between the watermark bits $W(i, j)$ and the recovered watermark bits $W'(i, j)$.

$$BER = \frac{\sum_{i=0}^{K-1}\sum_{j=0}^{L-1}\left[W(i,j) \oplus W'(i,j)\right]}{KL} \tag{2}$$

The watermarked image I (Fig. 3) is generated by hiding the watermark image W into the cover image C using the LSB embedding technique. The watermarked image is transmitted through the AWGN channel. We vary the AWGN level and for each case, we compute the PSNR and the BER. The performance of the LSB steganography is illustrated at Table II and Fig. 4, where LSB is very weak against the channel noise.

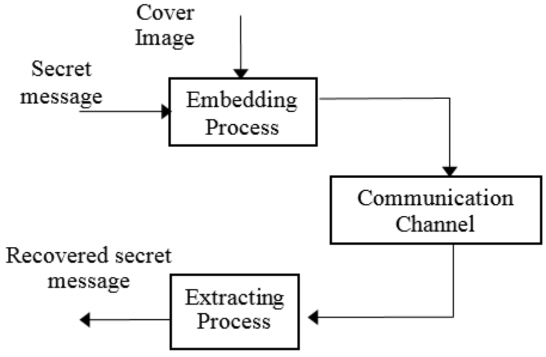


Fig. 1. Steganography Model.

TABLE. I. LSB EMBEDDING

Pixel number	Pixels before embedding	letter A	Pixels after embedding	Effects on pixel value
1st	01001111	1	0100111**1**	0
2nd	01001101	0	0100110**0**	-1
3rd	01001110	0	0100111**0**	0
4th	01001111	0	0100111**0**	-1
5th	01010000	0	0101000**0**	0
6th	01001011	0	0100101**0**	-1
7th	01010000	1	0101000**1**	+1

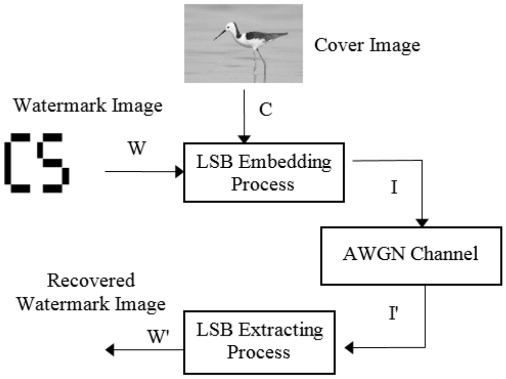


Fig. 2. LSB Steganography Model.

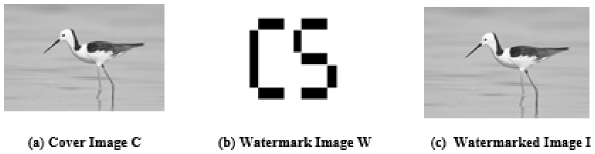

(a) Cover Image C (b) Watermark Image W (c) Watermarked Image I

Fig. 3. Embedding Process.

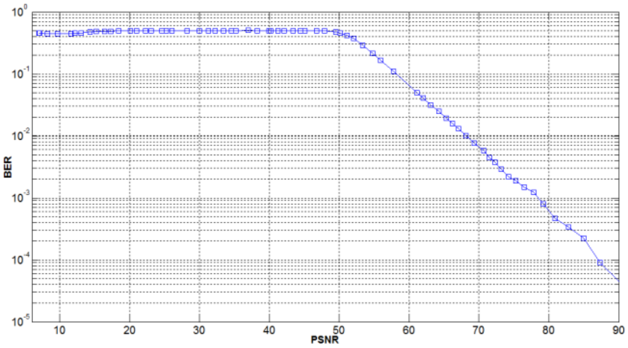


Fig. 4. LSB Steganography Performance.

C. Frequency Domain Steganography

In the frequency domain methods, the cover image is first transformed from spatial to frequency domain using the discrete cosine transform (DCT) and then the secret message bits are embedded using the transformation coefficients. The cover image C is divided into 8 x 8 blocks *f(x,y)* where each block is converted using the 2D DCT (Eq. 3) to its Discrete Cosine Transform *F(x,y)* coefficient blocks.

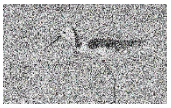
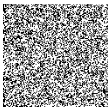
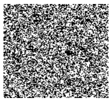
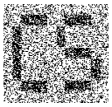
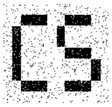
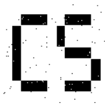
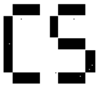
$$F(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (3)$$

where

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for k} = 0 \\ \sqrt{\frac{2}{N}} & \text{for k} = 1, 2, \ldots. N-1 \end{cases}$$

The 2D DCT transformation result in 8 x 8 matrix of DCT2 coefficients is shown at Fig. 5, where the frequency components are the lowest frequency components FL, the middle frequency components FM and the higher frequency components FH [8]. Embedding in the FL components will affect the cover image quality while embedding in the FH components will make the secret message vulnerable against the lossy compression. Accordingly, the FM components are selected to embed the watermark to maintain the cover image quality and provide resistance to the compression. The secret message bit then embedded into the 2D DCT coefficients and the inverse 2D DCT is performed. This process is repeated for the other secret bits where each bit embedded in an 8 x 8 block.

TABLE. II. LSB STEGANOGRAPHY PERFORMANCE

PSNR	Received Watermarked Image I'	Recovered watermark W'	BER
10 dB			0.45
50 dB			0.45
53 dB			0.3
60 dB			0.06
70 dB			0.006
80 dB			00006

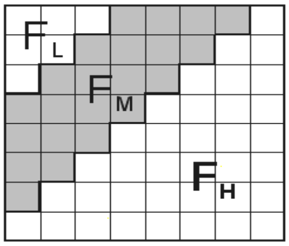


Fig. 5. The 2D DCT Frequency Components.

D. DCT Performance

The process of the DCT embedding method in a communication system with Added White Gaussian Noise channel is shown at Fig. 6. The watermark image W is hidden into the cover image C using the DCT embedding process module. The watermarked image I is transmitted through an AWGN communication channel. The received watermarked image I' is fed to the DCT extracting process module to extract the recovered watermark image W'.

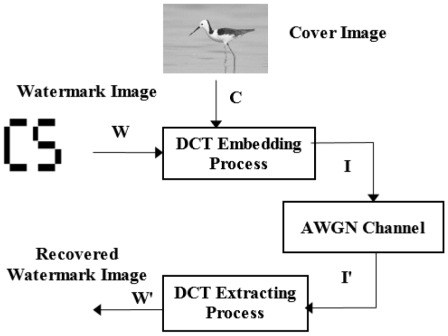


Fig. 6. DCT Steganography Model.

The watermarked image I (Fig. 7) is generated by hiding the watermark image W into the cover image C using the DCT embedding technique. The performance of the DCT steganography is illustrated at Table III and Fig. 8, where the DCT steganography technique is more robust against the channel noise than the LSB steganography technique.

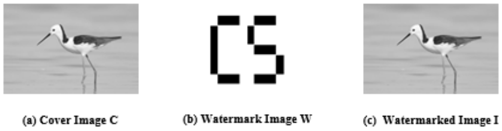


Fig. 7. DCT Embedding Process.

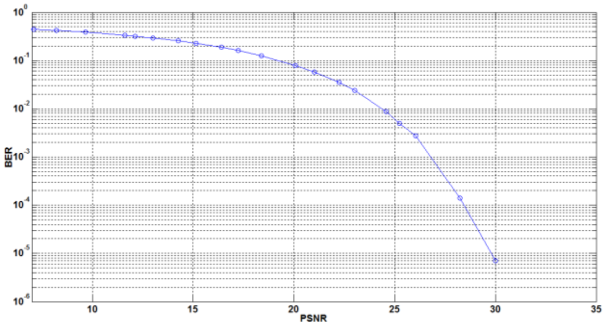
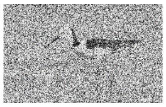
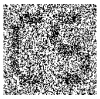
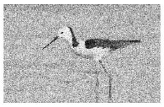
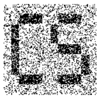
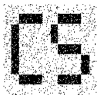
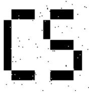
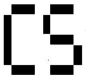
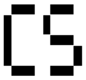


Fig. 8. DCT Steganography Performance.

TABLE. III. DCT STEGANOGRAPHY PERFORMANCE

PSNR	Received Watermarked Image I'	Recovered watermark W'	BER
10 dB			0.37
15 dB			0.23
20 dB			0.08
25 dB			0.0053
28 dB			0.00013
30 dB			0.000007

II. ROBUST STEGANOGRAPHY SYSTEM

In this section, the robustness of the steganography system is enhanced by introducing the errors detection and correction capability (Fig. 9) [9-12]. The watermark bits are encoded using convolutional encoder (Fig. 10), where each m-bit at the encoder input are encoded into n-bit symbol. The convolutional encoder is categorized by the code rate $R = m / n$ and the constraint length CL that represent the number of memory elements. The encoded watermark bits are fed to the embedding process at the transmitter. At the receiver side, the received bits ate coded using a Viterbi decoder to obtain the watermark W'.

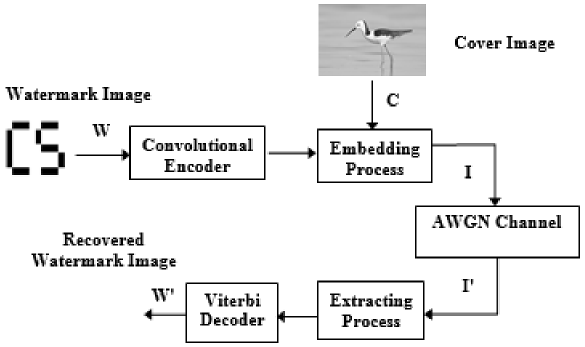


Fig. 9. Robust Steganography Model.

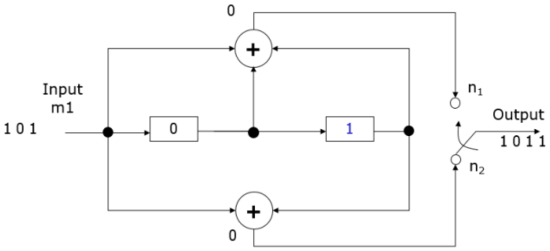


Fig. 10. Convolutional Encoder *R* =1/2 and *CL* =3.

A. Robust Steganography Performance

The performance of the robust steganography system is evaluated for the LSB embedding method and the DCT embedding method. The experiments evaluate the impact of convolutional encoder parameters such as the code rate *R* and the constraint length *CL*. The performance of the LSB steganography using convolutional encoder and Viterbi decoder is illustrated at Fig. 11-14. The encoder rate *R* is set to 1/2 and we vary the constraint length *CL* (Fig. 11). Moreover, the constraint length *CL* is set and we vary the encoder rate *R* (Fig. 12-14) where it is clear that the encoded LSB technique is still weak against the AWGN channel. On the other hand, the performance of the DCT steganography using convolutional encoder and Viterbi decoder is illustrated at Fig. 15-18 where the robustness is significantly enhanced. The results show that with higher *R* and *CL*, the system will achieve better robustness against the AWGN channel.

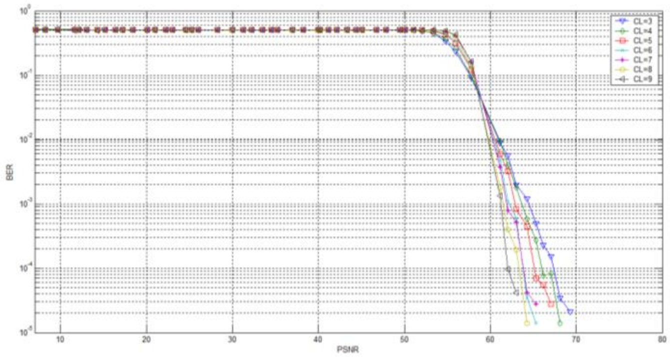


Fig. 11. LSB Steganography Performance with R=1/2.

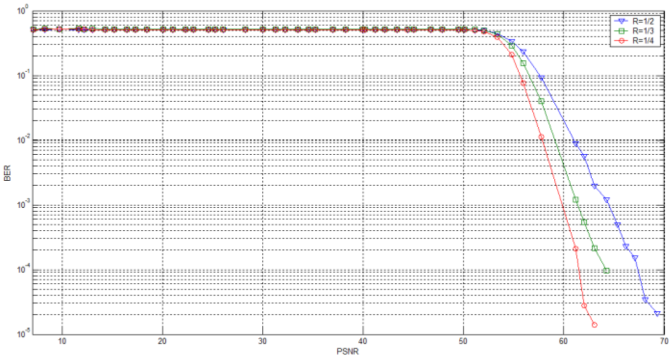


Fig. 12. LSB Steganography Performance with CL=3.

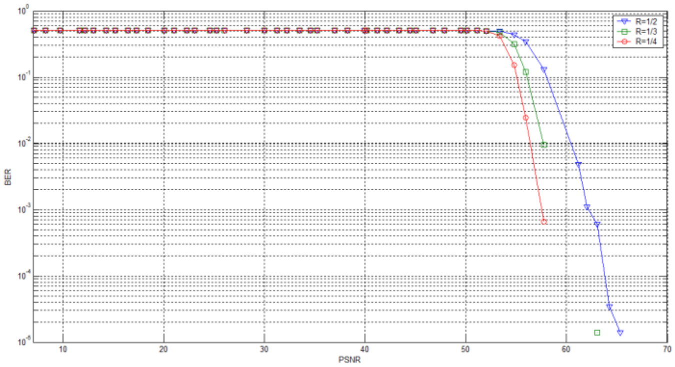


Fig. 13. LSB Steganography Performance with CL=6.

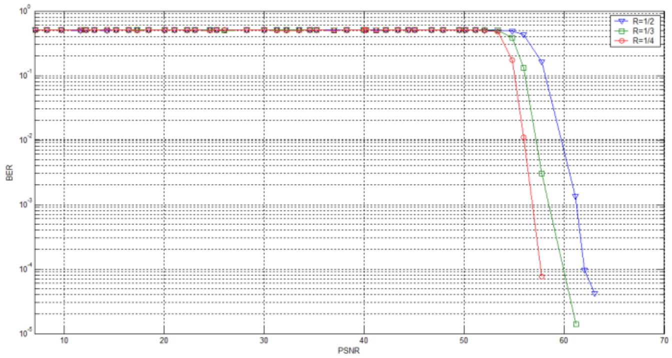


Fig. 14. LSB Steganography Performance with CL=9.

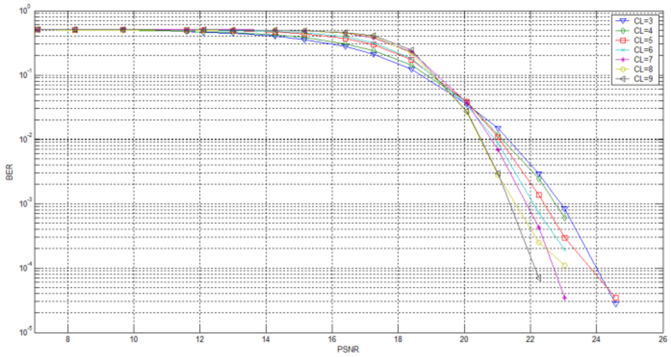


Fig. 15. DCT Steganography Performance with R=1/2.

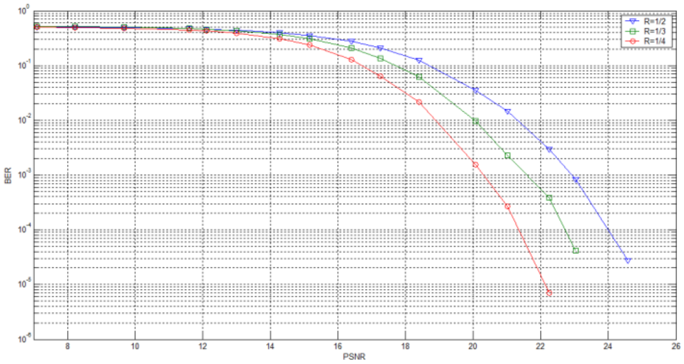


Fig. 16. DCT Steganography Performance with CL=3.

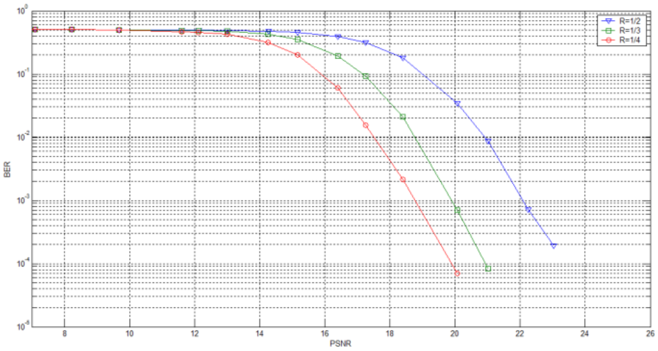


Fig. 17. DCT Steganography Performance with CL=6.

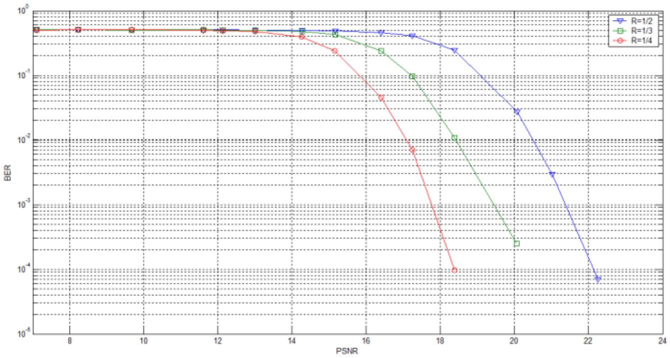


Fig. 18. DCT Steganography Performance with CL=9.

III. Conclusion

In this paper, steganography performance over a channel with Added White Gaussian Noise a noisy is evaluated. The secret message concealed using frequency domain or spatial domain then transmitted over the noisy channel. The performance of the steganography technique is measured by computing the bit error rate for each method over a channel with different noise levels. The results show that the DCT technique outperform the LSB technique in achieving better BER. Also, the steganography robustness is enhanced by using convolution encoder and Viterbi decoder. Moreover, the impact of the encoder's parameters such as rate and constraint length are evaluated. Simulation results illustrate that the steganography system robustness against the AWGN channel is improved with higher *R* and *CL*.

References

[1] Fridrich, J., [Steganography in Digital Media: Principles, Algorithms, and Applications], Cambridge University Press (2009).

[2] Mansi S. Subhedar a, Vijay H. Mankar b," Current status and key issues in image steganography: A survey," Computer Science Review Volumes 13–14, November 2014, Pages 95-113.

[3] M. Gaaed and M. Tahar, "Digital Image Watermarking based on LSB Techniques: A Comparative Study", International Journal of Computer Applications, vol. 181, no. 26, pp. 30-36, 2018.

[4] H. Zangana, "Watermarking System Using LSB", IOSR Journal of Computer Engineering, vol. 19, no. 3, pp. 75-79, 2017.

[5] Fahd Alharbi," Novel Steganography System using Lucas Sequence," International Journal of Advanced Computer Science and Applications(IJACSA), Volume 4 Issue 4, 2013.

[6] H. Fang and Z. Hua, "A Study on the Performance of Watermarking Algorithm Based on DCT", Advanced Materials Research, vol. 846-847, pp. 1040-1043, 2013.

[7] D. Singh and S. Singh, "DCT based efficient fragile watermarking scheme for image authentication and restoration", Multimedia Tools and Applications, vol. 76, no. 1, pp. 953-977, 2015.

[8] Amin P.K., Ning Liu, Subbalakshmi K. P. "Statistical Secure Digital Image Data Hiding", IEEE 7th workshop on Multimedia Signal Processing .pp.1-4, 2005.

[9] S. V. Viraktamath1 , Preeya H. Patil, G. V. Attimarad "Impact of code rate on the performance of Viterbi decoder in AWGN channel", 2014 IEEE International Conference on Computational Intelligence and Computing Research, 2014.

[10] P. Elias, Predictive coding--II, IRE Transactions on Information Theory, 1955. vol. 1, no. 1, p. 24 - 33.

[11] SKLAR, B. Digital Communications: Fundamentals and Applications. 2nd ed. System View, 2001.

[12] BATSON, B. H., MOOREHEAD, R. W. Simulation Results for the Viterbi Decoding Algorithm. NASA-TR-R-396, Technical report, 1972.