http://ansinet.com/itj

ITJ

ISSN 1812-5638

# INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (12): 1999-2004, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.1999.2004

# Secret Link Through Simulink: A Stego on OFDM Channel

Padmapriya Praveenkumar, G.S. Hemalatha, Bharathsimha Reddy, K. Thenmozhi,
J.B.B. Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering,
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

**Abstract:** The prerequisite of internet and multimedia communication in the present wireless age is impregnability and higher data rata. In this study, a pragmatic approach was accomplished by the Simulink model of Orthogonal Frequency Division Multiplexing (OFDM) using image steganography incorporating BPSK and QPSK modulation schemes. To contemplate the distortion in the image, the discerning distortion metrics called as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) were computed. The BER of OFDM system was also analysed.

**Key words:** OFDM, steganography, BPSK, QPSK, QAM, simulink

## INTRODUCTION

The World Wide Web, cognized as the inspiration for technological evolution in the epoch of wireless communication has revolutionised the digital world by revivifying the data rates a manifold. Coalesced with the evolution of internet, the number of users across globe reached a huge number but simultaneously several methods of hacking also increased. This in turn calls for higher data rate along with sound security. OFDM is a spectrally efficacious multichannel modulation scheme whose orthogonality has made it attractive over all modulation schemes. The orthogonality was first introduced by Chang (1996). Chang and Gibby (1968) typify that multiplexing can be done in OFDM. The parallel transmission in OFDM was described by Saltzberg (1967).

Higher data rates with effective spectral utilization was presented by Zimmerman and Kirsch (1967). Weinstein and Ebert (1971) suggested data transmission through Discrete Fourier Transmission (DFT). Peled and Ruiz (1980) introduced cyclic prefix to improve data transmission through frequency domain. A stego system requires cover image which holds the secret data (Kumar *et al*., 2011). The hidden data can be an image, bit, ciphertext or a plain-text (Katzenbeisser and Petitcolas, 2000; Xiang *et al*., 2011; Yang *et al*., 2011). The secret data embedded within the cover image forms the stego image (Praveenkumar *et al*., 2012a, b).

Robustness, security and capacity are the key features of any digital image steganography (Cheddad *et al*., 2010; Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012; Zhao and Luo, 2012; Zhu *et al*., 2011). The number of bits that can be embedded decided the capacity of the cover image (Amirtharajan *et al*., 2012). Robustness refers to the resistivity of the image after data embedding (Marvel *et al*., 1999; Padmaa *et al*., 2011; Praveenkumar *et al*., 2012c). Security deals with the unintended user figuring out the secret data in the cover image (Amirtharajan and Rayappan, 2012a-d).

To prevent unauthorised access and copyright of the data in digital form, confidentiality and data integrity are essential as most of the data access are done through the internet, while to eradicate it, some secret data has been embedded (Thanikaiselvan *et al*., 2011a, b; Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2012) in the digital data which cannot be extracted easily without the intended algorithm. Cryptic effect can be introduced to the input image by applying any of the cryptographic algorithm and then data embedding was carried out to ensure two levels of security (Thenmozhi *et al*., 2012).

Aforementioned literature shows that, there are excellent works carried out in information hiding in image as cover both in time and frequency domain. Most of the implementation has been carried in matlab, Visual C++ and Java or in some programming languages and not even a few in simulink. Hence this study takes an optimistic effort to implement image steganography through OFDM in simulink. The succeeding section explains the proposed simulink model followed by results, discussion and conclusion.

**Corresponding Author:** Padmapriya Praveenkumar, Department of Electronics and Communication Engineering,
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

## PROPOSED SIMULINK MODEL DESCRIPTION

Read the cover image using Image from file block. To workspace block is used to display the pixels of the image in the workspace. Reshape is used to convert 2D array into 1D. Then integer into binary conversion is done using Integer to Bit converter and the number of bits per integer is 8. Reshape1 will convert single dimension binary bits into 8 rows and 65536 column matrix. By giving the starting and ending value of the required row and column to the Sub matrix extracting the required values from the matrix can be done.

Transposing rows to columns and vice versa is done using transpose block. To read the data from workspace constant block is used. Reshape 2 will convert the given data in to K rows and 65536 columns, where K denotes the number of bits to be embedded. The data Output is converted into 1D array and is further converted into integer values by Bit to integer block. Then the data to be embedded is displayed in the workspace using to workspace data_embedding block.

Matrix concatenate block is used to concatenate the outputs of the blocks. The output of this is given to the Transpose 2 block. Then the matrix obtained is reshaped into 1D array using Reshape block and the binary bits are converted into integers using Bit to integer block. Then the integer matrix is converted into [256 256] matrix using reshape 5 block and this matrix is displayed in the workspace. This is the pixel matrix in which the data has to be embedded.

The integer matrix is converted into binary matrix and is displayed in the workspace using to workspace 9 that will perform integer to bit conversion. Then the embedded image is transmitted through the OFDM sub system. The input to the OFDM system is the binary matrix. The subsystem contains BPSK/QPSK/QAM modulator, IFFT block, AWGN channel, FFT block and BPSK/QPSK/QAM demodulator. Reshape 4 is used for converting the 1D array of the OFDM subsystem output into a matrix of 8 rows and 65536 columns and is displayed in the workspace.

Submatrix1 is used to extract the required data matrix from Reshape 4 block. Then it is converted into 1D array and the bits are converted into integers and the received data has been displayed in the workspace using To workspace 8 block (received_data). Then the BER graph will be plotted using BPSK and QAM modulation techniques. Finally, the MSE and PSNR of the image will be computed for K = 1 and 2 bit embedding and the results will be tabulated. Flowchart of the proposed methodology is given in Fig. 1, subsystem of OFDM system and the overall simulink model of OFDM transmission and reception are given in Fig. 2 and 3, respectively.

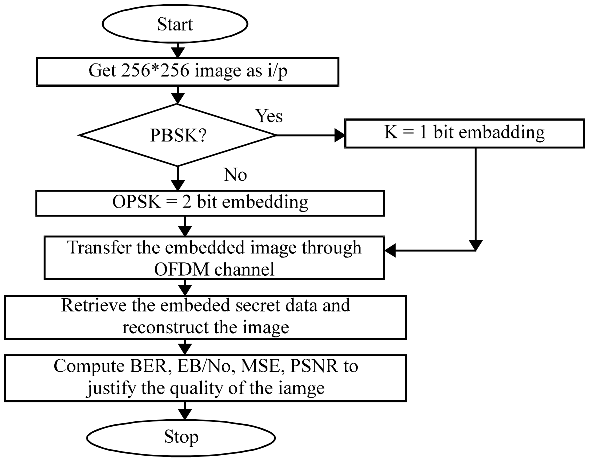
Start
Get 256*256 image as i/p
PBSK?
Yes
K = 1 bit embadding
No
OPSK = 2 bit embedding
Transfer the embedded image through OFDM channel
Retrieve the embeded secret data and reconstruct the image
Compute BER, EB/No, MSE, PSNR to justify the quality of the iamge
Stop

Fig. 1: Flowchart of the proposed methodology

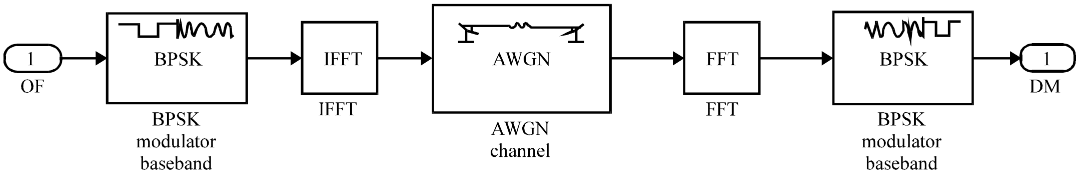

Fig. 2: Subsystem in OFDM Simulink model

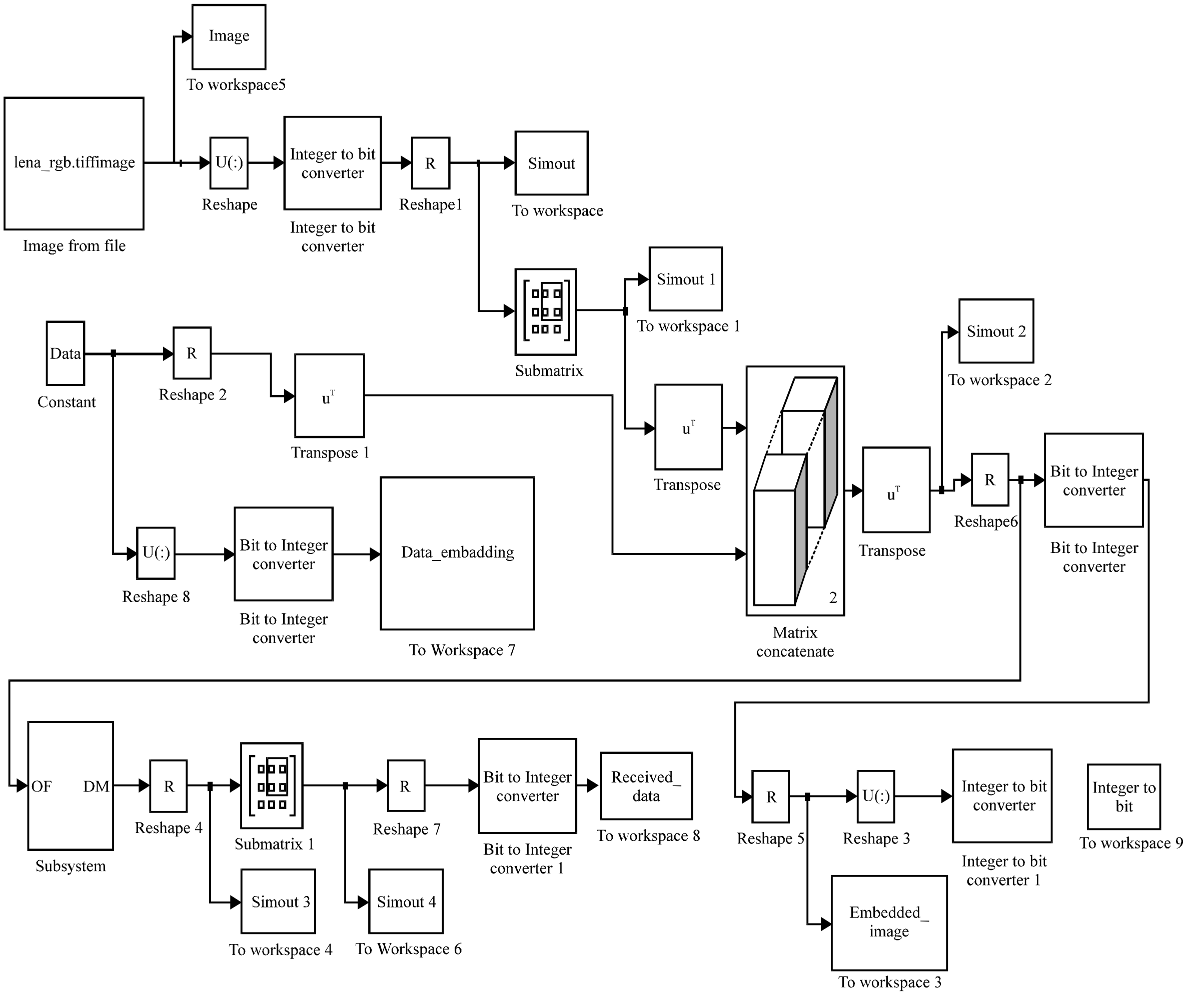

Fig. 3: Simulink Model of OFDM with data embedding, transmission and reception

**Algorithm for data embedding and extraction:**

**Step 1:** Get the input cover image of 256×256

**Step 2:** Modulation acts as the key

**Step 3:** If BPSK modulation is selected, then one bit of secret data has been embedded in the cover image

**Step 4:** Else QPSK modulation was carried out and the data embedded will be of two bits

**Step 5:** Transmission was done through OFDM channel

**Step 6:** At the receiver, demodulate the data using the key

**Step 7:** Retrieve the embedded data and original cover image

**Step 8:** Compute MSE and PSNR to analyse the image quality

## RESULTS AND DISCUSSION

To validate, the implemented Simulink Model of OFDM with data embedding, transmission and reception, Lena cover image of size 256×256 pixels of gray image has been considered. An experiment is conducted for full embedding capacity (k = 1 and 2) by considering 256×256 random bits and 256×256×2 bits respectively and the results are shown in Fig. 4a-c where Fig. 4a input cover image, Fig. 4b and c are the stego images with 1 and 2 bit embedding, respectively.

To compare the performance of the implemented Simulink model, MSE and PSNR were computed using Eq. 1 and 2 and the results are given in Table 1:

$$\text{MSE} = \frac{1}{XY}\sum_{M=1}^{X}\sum_{N=1}^{Y}(\text{Stego}_{M,N} - \text{Cover}_{M,N})^2 \quad (1)$$

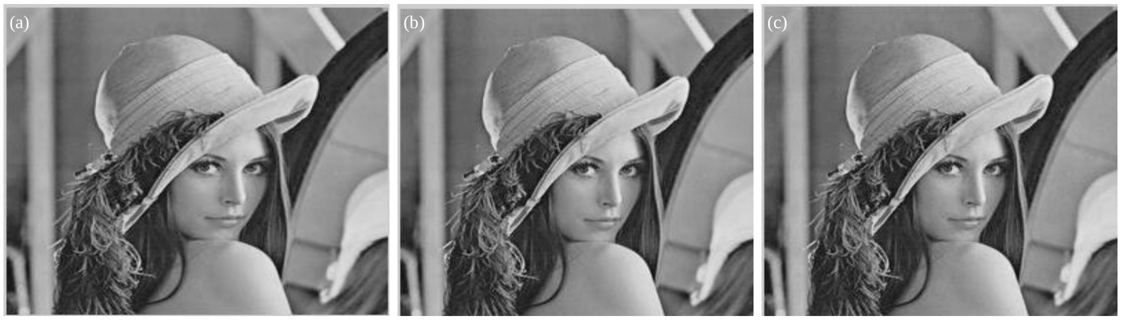

Fig. 4(a-c): (a) Cover image, (b) Stego image for K=1 bit embedding and (c) Stego image for K = 2

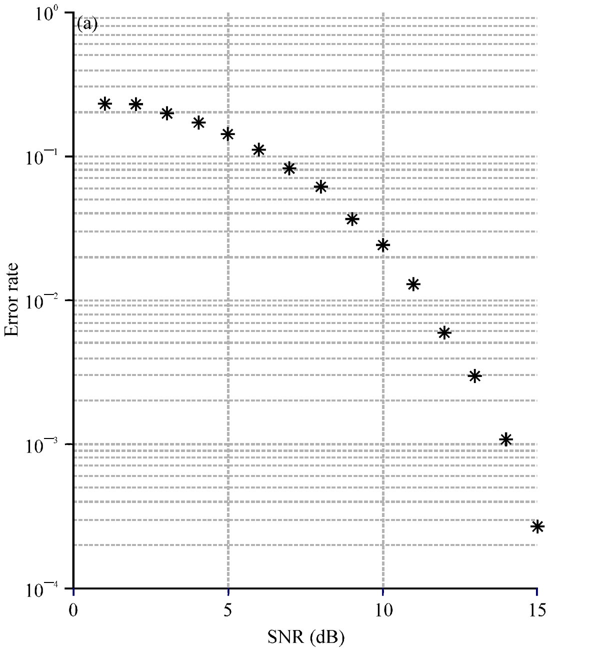

Fig. 5: BER graph of BPSK in OFDM after data embedding

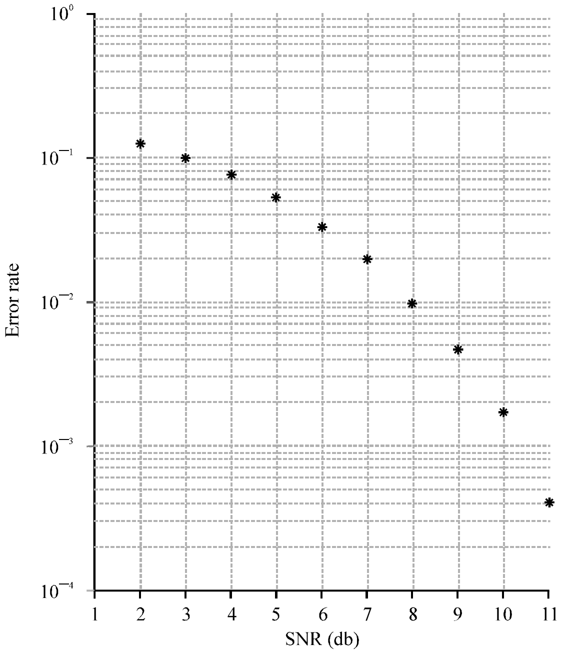

Fig. 6: BER graph of QPSK in OFDM after data embedding

Table 1: MSE and PSNR values for K = 1 and 2 bit embedding

| No. of bits embedded | MSE | PSNR |
|---|---|---|
| K = 1 | 0.4972 | 51.1655 |
| K = 2 | 2.4996 | 44.1521 |

where, X, Y represents the coordinates of the image, M, N represents the image dimensions, $\mathrm{Cover}_{M,N}$, $\mathrm{Stego}_{M,N}$ represents the Cover and the stego images, respectively:

$$\mathrm{PSNR} = 10\ \log_{10}\left(\frac{\mathrm{MI}^{2}}{\mathrm{MSE}}\right) \qquad (2)$$

where, MI represents the maximum intensity value of the pixel in the image.

From Table 1, MSE and PSNR for K = 1 and two bit embedding is done and is comparable as in Amirtharajan and Rayappan (2012a-d). Figure 5 and 6 shows the BER graph after data embedding using BPSK and QPSK modulations in OFDM. From the figure, QPSK modulation outperforms BPSK as mentioned in Praveenkumar *et al.* (2012a) and Thenmozhi *et al.* (2012). For QPSK at SNR = 11 dB, BER reaches zero whereas in BPSK, at SNR = 15 dB, BER reaches zero.

## CONCLUSION

Information hiding is an excellent option to preserve the privacy of the individual's confidential information. Like cryptography, image steganography will also used for secret communication with additional security. In this study, hiding information in the redundant bits of the cover image without losing its integrity was carried out through the Simulink model of OFDM. The stego image quality is also good and it would never raise doubt to hackers. Image steganography expects better imperceptibility and capacity, this method offers both. BER of QPSK modulation is appreciable compared to BPSK even after data embedding. There is a good possibility to improve the implemented method for covert communication with higher data rate and BER.

## REFERENCES

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012c. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R. and J.B.B. Rayappan, 2012d. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Chang, R.W. and R.A. Gibby, 1968. A theoretical study of performance of an orthogonal multiplexing data transmission scheme. IEEE Trans. Commun. Technol., 16: 529-540.

Chang, R.W., 1996. Orthogonal frequency division multiplexing. U.S. Patent 3,488.445, January 6, 1970.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Katzenbeisser, S. and F.A.P. Petitcolas, 2000. Information hiding techniques for steganography and digital watermarking. EDP Audit Control Security Newslett., 28: 1-2.

Kumar, P.P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2011. Steg-OFDM blend for highly secure multi-user communication. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, IEEE, Chennai, India, pp: 1-5.

Marvel, L.M., C.G. Jr. Boncelet and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.

Padmaa, M., Y. Venkataramani and R. Amirtharajan, 2011. Stego on $2^n$: 1 Platform for users and embedding. Inform. Technol. J., 10: 1896-1907.

Peled, A. and A. Ruiz, 1980. Frequency domain data transmission using reduced computational complexity algorithms. Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, April 1980, IEEE Computer Security, USA., pp: 964-967.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving: A multicarrier stego. Procedia Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., R. Amirtharajan, Y. Ravishankar, K. Thenmozhi and J.B.B. Rayappan, 2012c. Random and AWGN road for MC-CDMA and CDMA bus to phase hide: A MUX in MUX stego. Proceedings of the International Conference on Computer Communication and Informatics, January 10-12, 2012, Coimbatore, India, pp: 1-6.

Saltzberg, B., 1967. Performance of an efficient parallel data transmission system. IEEE Trans. Commun. Technol., 15: 805-811.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2011a. Wave (let) decide choosy pixel embedding for stego. Proceedings of the International Conference on Computer, Communication and Electrical Technology, March 18-19, 2011, India, pp: 157-162.

Thanikaiselvan, V., S. Kumar, N. Neelima and R. Amirtharajan, 2011b. Data battle on the digital field between horse cavalry and interlopers. J. Theor. Applied Inform. Technol., 29: 85-91.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego = Secure Communication: A Review. Res. J. Inform. Technol., 4: 31-46.

Weinstein, S.B. and P.M. Ebert, 1971. Data transmission by frequency-division multiplexing using discrete fourier transforms. IEEE. Trans. Commun., 19: 628-634.

Xiang, L., X. Sun, Y. Liu and H. Yang, 2011. A secure steganographic method via multiple choice questions. Inform. Technol. J., 10: 992-1000.

Yang, B., X. Sun, L. Xiang, Z. Ruan and R. Wu, 2011. Steganography in Ms Excel document using text-rotation technique. Inform. Technol. J., 10: 889-893.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.

Zhu, J., R.D. Wang, J. Li and D.Q. Yan, 2011. A huffman coding section-based steganography for AAC audio. Inform. Technol. J., 10: 1983-1988.

Zimmerman, M.S. and A.L. Kirsch, 1967. The AN/GSC-10 (KATHRYN) variable rate data modem for HF radio. IEEE Trans. Commun. Technol., 15: 197-204.