Fixing, padding and Embedding – A Modulated Stego

Padmapriya Praveenkumar[#1], K.Thenmozhi[#2], M. Naga Dinesh[#3] and
Rengarajan Amirtharajan[#4]
[#]School of Electrical & Electronics Engineering, SASTRA University,
Tamil Nadu, India – 613401
[1]padmapriya@ece.sastra.edu, [2]thenmozhik@ece.sastra.edu, [3]mnaga.dinesh@gmail.com,
[4]amir@ece.sastra.edu

***Abstract*— Broadband application of wireless communication calls for good signal to noise ratio (SNR) and variable high data rates. In the midst of a spate of available techniques, Orthogonal Frequency Division Multiplexing (OFDM) has proven to be effective. OFDM systems have high tolerance towards multipath effects in fading channels. Wireless communication will become tortuous in the presence of Inter Symbol Interference (ISI). This complex situation is un-raveled by introducing Cyclic Prefix (CP) prior to transmission over fading channels. In this paper, an idea has been proposed for incorporating Cyclic Prefix (CP), Cyclic Post Fix (CPOF), Zero Padding (ZP) schemes in OFDM system while embedding the secret data for secure data transmission. BER graphs are simulated and compared for various modulation techniques like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) and Quadrature Amplitude Modulation (QAM) prior to embedding and after embedding the secret data.**

Keyword - Cyclic prefix (CP), Cyclic Post Fix (CPOF), Zero Padding (ZP) schemes, OFDM, Steganography.

I. INTRODUCTION

The requirements for higher data rates and better techniques to combat inter carrier interference (ICI) and Inter Symbol Interference (ISI) propelled mankind to develop new techniques of combining various data streams into a single channel using a technique called multiplexing. This method of combining the signals is of various types namely Time Division Multiplexing (TDM), Frequency Division Multiplexing (FDM), Space Division Multiplexing (SDM) and Code Division Multiplexing (CDM).

FDM uses a multi carrier technique where the data are modulated onto subcarriers of various frequencies each with a guard band in between them. The ever increasing demand for increasing the channel drove FDM towards Orthogonal Frequency Division Multiplexing (OFDM) which aims at maximizing the spectral efficiency. It facilitates the overlapping of sub carriers. All the sub channels are orthogonal and hence the need for guard bands is eliminated [1]; thus using the overall spectrum of the channel more efficiently. The overall data rate of the channel is distributed over several low data rate signals each modulated over a sub carrier frequency.

The guard bands used in FDM is eliminated in OFDM since the principle of orthogonality is involved. Under ideal conditions the subcarriers used are perfectly orthogonal and hence they can be overlapped without any concern about Inter Carrier Interference (ICI) [2, 3]. Since the data rates of individual channels are also relatively low, there are lesser possibilities for Inter Symbol Interference (ISI) [4]. Under non ideal conditions the use of Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform (FFT) at the transceiver of OFDM converts an ISI inducing channel with AWGN into parallel channels ridden of ISI. The use of cyclic prefixes for each block with a specified length eliminates Inter Block Interference (IBI).

Each channel can be individually equalized or filtered at the receiver to extract the desired signal. Though proposed for wireless systems initially OFDM is widely used for Digital Audio Broad (DAB) and Digital Video Broad casting (DVB) systems besides Wireless Local Area Network (WLAN). The advent of OFDM has simply revolutionized the communication world by providing a whole new dimension to the way with which man communicates. In spite of so many advantages, OFDM suffers from a serious drawback called the peak to average power ratio, necessitating the use of high power amplifiers with a very high dynamic range. To reduce this, various techniques have been proposed. Using those, the disadvantages can be overcome paving way for the use of the positive aspects of OFDM.

The methods of encoding and decoding are used to in digital communication systems to achieve privacy in data is said to have failed when an intruder suspects the possibility of a hidden message in a file. Various technologies were developed to embed a message or a cipher text inside an image or a multimedia file to embed secret data. Embedding secret data after encoding the data by OFDM modulation has been carried out to ensure

secure wireless communication [5- 9]. Invisible communication has evolved over the years and is termed as steganography [10].broadly subdivided in to steganography, Cryptography and watermarking.

By the implementing these techniques the intruder is denied about the existence of the secret message. Ensconced the weakness of the human senses is exploited as a minute change due to the embedded message can't be detected. The simplest LSB steganography technique [11], changes the LSB of any of the layers of the RGB color pattern of an image. The palette based technique hides the message in one of the color palettes of the image. Alternatively, the transform based techniques employ an alteration in the coefficients of the frequency domain representation of the image [12]. The LSB, though primitive, is the easiest to implement [13] . The Spread spectrum image steganography [14-16] is method where the image is transformed and spreaded, then the data bits are embedded which obeys orthogonal property of the Sequences used in Communication systems. A detailed literature survey about steganography and its branches with various embedding techniques associated with its merits and demerits are illustrated [17-19]

The steg analysis is a technique used to retrieve the secret information from the stego file. Cryptography and watermarking are the two techniques that are very closely related to steganography. While watermarking is another type of technology, cryptography uses keys for protecting the messages. Watermarking is used to protect the ownership of a file or a message or simply to copyright a file. The creator's name is embedded in the file that is undetectable which prevents any other else claim the ownership of that file.

Cryptography generates keys that are known only to the sender and the receiver during each transmission to secure the message [20]. Without the knowledge of these keys one cannot open the message. As the techniques of hiding a message have increased, the ways to detect and extract it have also been developed. Several algorithms are used to extract the message or delete the watermark without altering the multimedia file [21-24]. The efficiency depends on the capacity of the system to embed the data in the file with the least possible alteration [25-29]. The system is said to have failed when an intruder suspects the possibility of a hidden message in a file.

After reviewing the literature on OFDM and steganography, this paper proposes CP, ZP, CPOF in OFDM system using BPSK, QPSK and QAM systems. Confidential data bits are embedded in the redundant bits to ensure wireless security. BER graphs are plotted before and after embedding secret data bits in CP, ZP and CPOF, Proposed system and its description were carried out in section II. Section III analyses the results and discussion. Conclusions are analysed in Section IV.

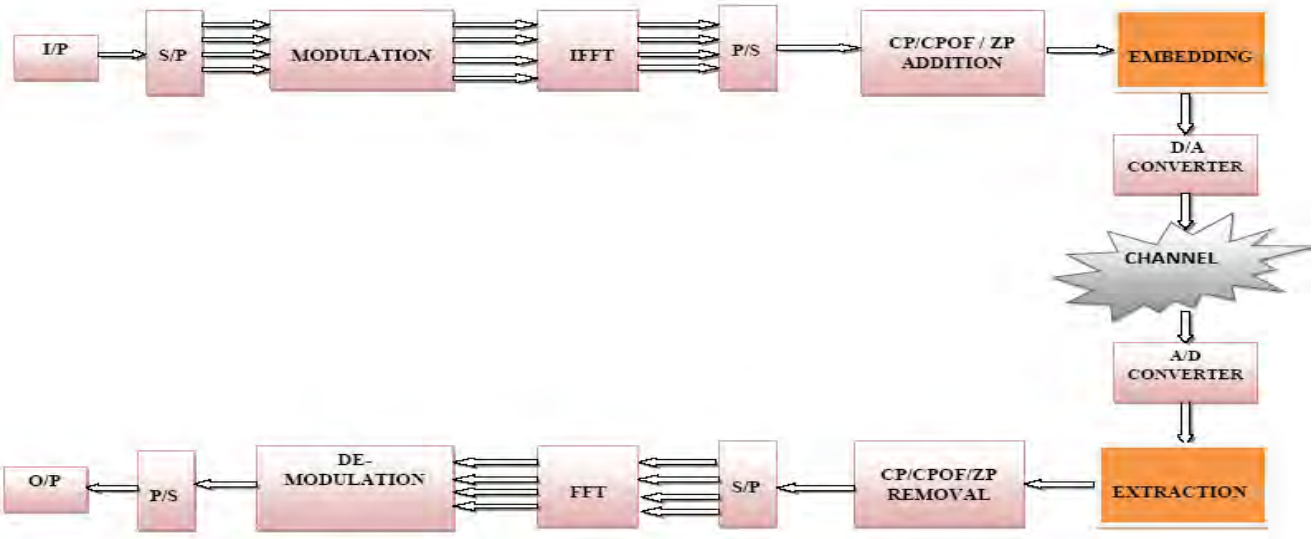

Fig. 1.Block diagram of the proposed methodology

II. PROPOSED METHODOLOGY

The system is fed with a binary bit stream as input. Then the serial data stream is converted to parallel before being sent to the modulator block as in Fig 1. The modulation block is used to modulate the given data using various schemes such as BPSK, QPSK and 8-QAM. Then Inverse Fast Fourier Transform (IFFT) is taken is for the modulated data in order to provide the composite signal out of all the sub-carriers inserted to obtain OFDM symbols

After this, the data is again made linear by parallel-to-serial conversion. The next block of the system performs one of the operations from ZP, CP and CPOF. These are mainly done to avoid interference in the signals transmitted. Cyclic prefix refers to the prefixing of a symbol with a repetition at the front end of the

symbol which as a buffer region where delayed information from the previous symbols can get stored. If the additional bits are added at the end of a symbol, it is called cyclic postfix. If, instead of making a repetition, zeroes are added either as prefix or postfix, it is said to be zero padding. Then data bits are embedded from the data obtained from the Cp/CPOF/ZP outputs. The number of bits to be embedded in the redundant bits and the positions are known only to the transmitter and receiver end.

The digital data is converted into analog form for transmission through channel. The channel considered for transmission is Additive White Gaussian Channel (AWGN). The received information at the other end is again converted back to digital form for further processing. Now the data embedded during the transmission phase is extracted by knowing the key value. According to whether zero padding or cyclic prefix or postfix was done earlier, the corresponding inverse operation is done to remove the excess redundant bits.

Then the serial data transmission is made to parallel and then FFT operation is performed on it, to separate the carriers of the OFDM signals individually. Now the demodulation is performed and the original message output bits are decoded. Then, BER graphs are plotted for various modulation schemes like BPSK, QPSK and QAM.

III. Results and Discussion

The comparison graphs between CP, CPOF and ZP before and after embedding using BPSK, QPSK and QAM has been plotted in Figs 2,3and 4 respectively. The BER Vs EB/No values before and after embedding secret data's are tabulated in table 1 and 2.

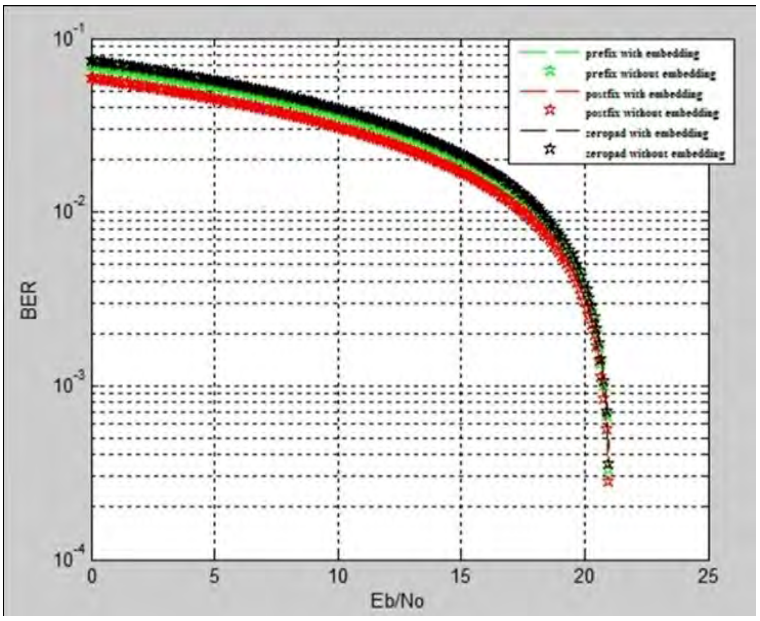

Fig. 2. Comparison between CP, CPOF, ZP with embedding in OFDM - BPSK

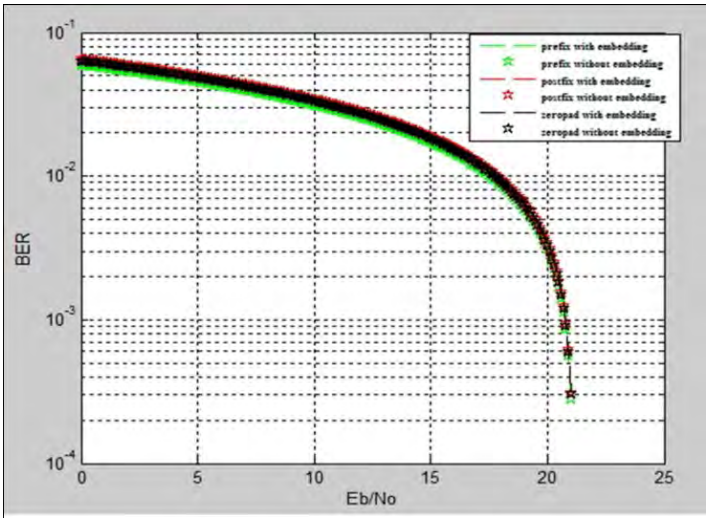

Fig. 3. Comparison between CP, CPOF, ZP with embedding in OFDM using QPSK

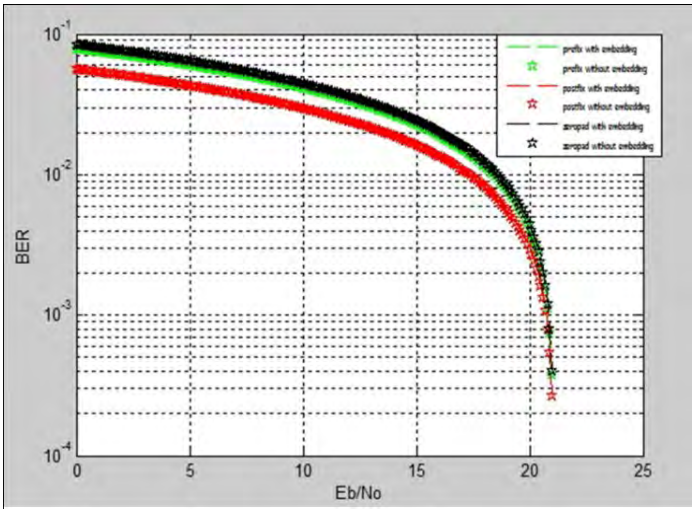

Fig. 4. Comparison between CP, CPOF, ZP with embedding in OFDM – QAM

TABLE I
BER Vs EB/N0(dB) using CP, CPOF and ZP using BPSK, QPSK and QAM before embedding

BER	Cyclic Prefix (CP)			Cyclic Postfix (CPOF)			Zero Padding (ZP)		
	Eb / N0 (dB)			Eb / N0 (dB)			Eb / N0 (dB)		
	BPSK	QPSK	QAM	BPSK	QPSK	QAM	BPSK	QPSK	QAM
10^-2	8.7	8.9	9	8.9	8.7	9	8.8	8.9	8.8
10^-2.1	9	9	9	9	9.1	9.2	9	9	9.1
10^-2.2	9.1	9.31	9.2	9.2	9.3	9.3	9.2	9.3	9.3
10^-2.3	9.3	9.50	9.5	9.4	9.54	9.3	9.4	9.5	9.5
10^-2.4	9.6	9.7	9.7	9.7	9.7	9.7	9.6	9.7	9.7
10^-2.5	9.7	9.9	10	9.9	10	10	9.8	9.9	9.9
10^-2.6	10.1	10.1	10.1	10	10.1	10.1	10	10.2	10.1
10^-2.7	10.3	10.1	10.2	10.2	10.3	10.3	10.2	10.3	10.3
10^-2.8	10.5	10.2	10.5	10.5	10.5	10.6	10.4	10.4	10.5

TABLE II
BER Vs EB/N0(dB) using CP, CPOF and ZP using BPSK, QPSK and QAM after embedding

BER	Cyclic Prefix (CP)			Cyclic Postfix (CPOF)			Zero Padding (ZP)		
	Eb / N0 (dB)			Eb / N0 (dB)			Eb / N0 (dB)		
	BPSK	QPSK	QAM	BPSK	QPSK	QAM	BPSK	QPSK	QAM
10^-2	8.8	8.95	9	8.9	8.9	9	8.85	8.95	8.9
10^-2.1	9.1	9.1	9.2	9.1	9.2	9.2	9	9.15	9.15
10^-2.2	9.3	9.35	9.4	9.3	9.4	9.4	9.25	9.35	9.35
10^-2.3	9.5	9.55	9.6	9.5	9.55	9.6	9.5	9.55	9.55
10^-2.4	9.7	9.75	9.8	9.75	9.75	9.8	9.7	9.75	9.75
10^-2.5	9.9	9.95	10	9.95	10	10	9.9	9.95	9.95
10^-2.6	10.2	10.2	10.2	10.15	10.2	10.2	10.2	10.2	10.2
10^-2.7	10.4	10.4	10.4	10.4	10.4	10.4	10.4	10.4	10.4
10^-2.8	10.6	10.6	10.6	10.6	10.6	10.6	10.6	10.6	10.6

From the BER graphs, BPSK is better in CP and QPSK is better in CPOF and QAM provides better performance in ZP. Even after embedding secret data bits in ZP, CP and CPOF the BER values are comparatively good.

IV. CONCLUSION

OFDM system is more prone to ICI and ISI and has better spectral efficiency due to the usage of the orthogonal subcarriers. In this paper, OFDM system incorporating CP, ZP and CPOF are used to eliminate ISI for various modulation schemes like BPSK, QPSK and QAM. Secret data bits are embedded in the redundant bits to maintain security and confidentiality of the transmitted data over OFDM. From the BER graphs, it is noted that BPSK outperforms with CP and QPSK is well organized with CPOF and ZP coordinates with QAM even after embedding confidential data bits.

REFERENCES

[1] Van nee, Richard, and Ramjee prasad. *OFDM for Wireless Multimedia Communications*, Boston: Artech House 2000.

[2] A. Peled and A. Ruiz, "Frequency domain data transmission using reduced computational complexity algorithms," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP'80)*, vol. 5, pp. 964-967,1980.

[3] B. Saltzberg, "Performance of an Efficient Parallel Data Transmission System," *IEEE Trans. on Commun. Technol.*, vol. 15, no. 6, pp. 805 - 811.

[4] Taewon Hwang, Chenyang Yang, Gang Wu, Shaoqian Li, and G.Ye Li, "OFDM and Its Wireless Applications: A Survey," *IEEE Trans. on Vehicular Technol.* , vol. 58, no. 4, pp. 1673 – 1694.

[5] P.P. Kumar, R. Amirtharajan, K. Thenmozhi, and J.B.B. Rayappan, "Stego-OFDM blend for highly secure multi-user communication," *2nd International Conference on Wireless Commun., Vehicular Technol., Inform. Theory and Aerospace and Electron. Systems Technol., Wireless VITAE*, pp. 1-5, 2011.

[6] K. Thenmozhi, P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan, and J.B.B. Rayappan, "OFDM+CDMA+Stego = secure communication: A review," Res. J. of Inform. Technol., vol. 4, no. 2, pp. 31-46, 2012.

[7] S. katzenbeisser and F.A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Norwood: Artech House, 2000.

[8] P. Praveenkumar, R. Amirtharajan, Y. Ravishankar, K. Thenmozhi, and J.B.B. Rayappan, "Random & AWGN road for MC-CDMA & CDMA bus to phase hide - A MUX in MUX stego," *International Conference on Computer Commun. and Informatics (ICCCI)*, pp.1-6, 2012.

[9] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J.B.B. Rayappan, "Phase for face saving - A multicarrier stego," *Procedia Engineering*, pp.790-797, 2012.

[10] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J.B.B. Rayappan, "Regulated OFDM-role of ECC and ANN: A review," J. of Applied Sciences, vol. 12, no. 4, pp. 301-31, 2012.

[11] M. Padmaa, Y. Venkataramani, and R. Amirtharajan, "Stego on 2n:1 platform for users and embedding," *J. Inform. Technol.*, vol. 10, no. 10, pp. 1896-1907, 2011.

[12] V. Thanikaiselvan, P. Arulmozhivarman, R. Amirtharajan, and J.B.B. Rayappan, "Wave (let) decide choosy pixel embedding for stego," *International Conference on Computer Commun. and Electrical Technol. (ICCCET 2011)*, pp. 157, 2011.

[13] R. Amirtharajan and J.B.B. Rayappan, "An intelligent chaotic embedding approach to enhance stego-image quality," *Inform. Sciences*, vol. 193, pp. 115-124, 2012.

[14] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing*, pp. 1673-1687, 1997.

[15] M. Marvel, Jr. Boncelet, and C.T. Retter, "Spread spectrum image steganography," *IEEE Trans. on Image Processing*, Vol. 8, no.8, pp. 1075-1083, 1999.

[16] R. Amirtharajan and J.B.B. Rayappan, "Covered CDMA multiuser writing on spatially divided image," *2nd International Conference on Wireless Commun., Vehicular Technol., Inform. Theory and Aerospace and Electron. Systems Technol., Wireless VITAE*, pp. 1-5, 2011.

[17] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul Mc Kevitt, *Digital image steganography: Survey and analysis of current methods*, 2010, pp. 727-752.

[18] R. Amirtharajan, J. Qin, and J.B.B. Rayappan, "Random image steganography and steganalysis: Present status and future directions," *J. Inform. Technol.*, vol. 11, no. 5, pp. 566-576, 2012.

[19] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn,"Inforamtion hiding – a survey," In *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062-1078, 1999.

[20] B. Schneier, *Applied Cryptography Protocols, Algorithm and Source Code in C*. 2nd ed. Wiley India edition, 2007

[21] R. Amirtharajan and J.B.B. Rayappan, "Inverted Pattern in Inverted Time Domain for Icon Steganography," *J. Inform. Technol.*,vol. 11, pp. 587-595, 2012.

[22] S. Rajagopalan, R. Amirtharajan, Har Narayan Upadhyay, and J.B.B. Rayappan, "Survey and Analysis of Hardware Cryptographic and Steganographic Systems on FPGA," *J. of Applied Sciences*,vol. 12, pp. 201-210, 2012.

[23] S. Janakiraman, R. Amirtharajan, K. Thenmozhi, and J.B.B. Rayappan, "Pixel Forefinger for Gray in Color: A Layer by Layer Stego," *J. Inform. Technol.*,vol. 11, pp. 9-19, 2012.

[24] S. Janakiraman, R. Amirtharajan, K. Thenmozhi, and J.B.B. Rayappan, "Firmware for Data Security: A Review," Res. J. of Inform. Technol., vol. 4, pp. 61-72, 2012.

[25] R. Amirtharajan, R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha, and J.B.B. Rayappan, "MSB over hides LSB — A dark communication with integrity," *IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application (IMSAA)*, pp.1-6, 12-13 Dec, 2011.

[26] R. Amirtharajan, V. Mahalakshmi, N. Sridharan, M. Chandrasekar, and J.B.B. Rayappan, "Modulation of hiding intensity by channel intensity - Stego by pixel commando," *International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pp. 1067-1072, 21-22 March 2012.

[27] R. Amirtharajan, R, Anushiadevi, V. Meena, V. Kalpana, and J.B.B. Rayappan, "Seeable visual but not sure of it," *International Conference on Advances in Engineering, Science and Management (ICAESM)*, pp. 388-393, 30-31 March 2012.

[28] R. Amirtharajan, K. Ramkrishnan, M. Vivek Krishna, J. Nandhini, and J.B.B. Rayappan, "Who decides hiding capacity? I, the pixel intensity," *International Conference on Recent Advances in Computing and Software Systems (RACSS)*, pp.71-76, 25-27 April 2012.

[29] V. Thanikaiselvan, P. Arulmozhivarman, R. Amirtharajan, J.B.B. Rayappan, "Horse Riding & Hiding in Image for Data Guarding," *Procedia Engineering*, Vol. 30, pp. 36-44, 2012.