Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 14 (16): 1786-1797, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.1786.1797

Coded Crypted Converted Hiding (C^3H)-A Stego Channel

Padmapriya Praveenkumar, Rengarajan Amirtharajan, K. Thenmozhi and J.B.B. Rayappan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract: Wireless communication with its enhanced efficiency, greater flexibility, mobility and reduced cost has encompassed human needs and sophistications to a greater extent. Several techniques adopted in the wireless standards solely contribute to its heightened demand. Orthogonal Frequency Division Multiplexing (OFDM) is one such technique adopted to provide robust and high speed networks by countenancing signal overlap. The data transmission over wireless, in general, is unsecure and open to the hands of the hackers. A method has to be devised to uniquely identify the copyright owner of the data and prevent the misuse of it. However, on the negative side, the hackers are on par with the experts in this field to combat against piracy. This necessitates the introduction of a method to impart security to the data being transmitted. This study embeds secret data bits in punctured convolutional encoder's output which are then encrypted using Chaotic means to uphold discretion and then traversed through OFDM system. Integrity is made certain by four-level encryption of secret bits and is stored as key in Cyclic Prefix's (CP) output. Comparison graphs for the performance of Bit Error Rate (BER) are plotted for different modulation schemes with different rates of punctured convolutional codes. These plots are for puncture patterns with convolutional encoder before and after infixing the secret data. Widespread metrics for performance measurement like BER and correlation values are computed. This estimation reveals the security and arbitrariness of data encryption both with and without embedding the secret.

Key words: OFDM, BER, punctured convolutional codes, steganography, encryption

INTRODUCTION

The telecommunication technology needed a transition from 3rd generation to 4th generation to cater higher data rates in multimedia applications. OFDM is a unique form of multi carrier scheme (Bahai *et al*., 2004), though projected in 1960s, was dormant for few years. Implementing it in real time was a hard row to hoe until the semiconductor and computer technologies advanced in the recent years. Frequency Division Multiplexing (FDM) has evolved to gain omnipotence and yielded OFDM (Chang, 1966; Chang and Gibby, 1968; Chang, 1970).

OFDM is a digital modulation technique that converts the serial data stream into smaller sub-streams and modulated on low speed sub-carriers. The entire spectrum is divided into smaller sub bands which makes the channel effects flat over a sub band of concern. This makes the symbol period much longer than the delay spread produced by the time dispersive channel (Saltzberg, 1967). Longer symbols are less susceptible to multipath interference and the synchronization is made easier by the lower data rate of sub streams. The sub-streams are modulated through any of the popular modulation techniques like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) and M-ary Quadrature Amplitude Modulation (QAM). This study proposes a unique steganographic tactic using contemporary multiplexing know-how. OFDM is a widely accepted beneficial means for steganography as it possesses competent interference dismissal and admirable bandwidth efficacy. Moreover, unlike any other stego methods, OFDM smoothes progress of implementation. It also minimizes system cost. It lends a helping hand for steganography by resisting fading; this makes OFDM an important come reliable steganographic mode.

Transmission is achieved through any of the media like wireless, coaxial cable, fiber-optic cable, twisted pair cable. Cyclic prefix, also known as guard intervals are inserted to combat inter channel interference and inter symbol interference. All these features coupled together make OFDM superior to all other transmission techniques. Also, OFDM allows the sub carriers to overlap without causing inter-channel interference (Weinstein and Ebert, 1971; Thenmozhi *et al*., 2011, 2012). This is achieved by orthogonal nature of the subcarriers. Orthogonal in the sense, the peak of the carrier will occur at the null of the other.

Corresponding Author: Padmapriya Praveenkumar, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

The orthogonality is incorporated to the symbols by performing Inverse Fast Fourier Transform (IFFT) operation. IFFT and Fast Fourier Transform (FFT) serves the purpose of modulation at the transmitter and demodulation at the receiver. The basis functions of IFFT are orthogonal sinusoidal. IFFT assigns each sinusoid with a phase and amplitude depending on the values of the corresponding symbol (Van Nee and Prasad, 2000). The number of IFFT inputs determines the number of sub-carriers in OFDM. The output will be a complex sum of all the sinusoids with varying phase and amplitude. All these output samples corresponds to one OFDM symbol. In the same way, demodulation is performed by FFT operation (Hwang *et al*., 2009). This makes the OFDM system, especially for steganography, substantially computation efficient.

In wireless communication, error detection and error control are the methods which facilitate steadfast electronic data delivery through erratic communication medium which introduce unwanted signals, introducing errors all through transmission from one end to other. While the former permits identifying errors, the latter makes possible the restoration of original signal or message. Error control codes are of great help when it comes to secret sharing. They add one more level of security. The aim of this study is to maintain privileged secrecy level through manifold persona of a cohesive system. In Forward Error Correction (FEC), the data is encoded by Error Control Code (ECC) before transmission. It is recovered at the receiving end through redundant information added during transmission (Peterson and Weldon, 1972).

FEC finds applications where there is impossible or expensive retransmission, for instance, one-way communication linkage and transmission to more than one receiver at a time etc. FEC has two main classifications viz., block codes, convolutional codes (Forney, 1971). The former operates on fixed-size packets (blocks of bits) or symbols and the latter functions on bit streams or symbols of random length. Noteworthy here is the fact that these classifications are very obliging in constructing different steganographic algorithms. Also, they manage the computational parts of secret data bits on the word of the implementation. Convolutional encoder is described in two forms, polynomial description and trellis description (Forney, 1970). The first one has two constituents namely Constraint lengths and Generator polynomials. Constraint lengths generate a vector of length as per (number of) inputs in the encoder which indicates the total bits accumulated in shift register, together with that of the present input (Forney, 1973).

For illustration, say, it possesses k, n inputs and outputs respectively, then, k-by-n is called code generator matrix. The effect of possible encoder input on its output and state transitions is better explained by a trellis description. If some parity bits are removed after they get encoded by ECC, then it is called puncturing. This seems similar to that when done via ECC having lower redundancy or higher rate. On the other hand, with this puncturing, unchanged decoder can be utilized irrespective of the number of bits punctured, thus leading to increased flexibility devoid of appreciably escalating intricacy. On the whole OFDM remains immune against frequency-selective fading straits thereby making steganographic algorithms well-built (Praveenkumar *et al*., 2012a-c, 2013a-j).

The nascent field of Information Hiding has got over post-natal hiccups to evolve into a robust field of technology to combat piracy (Al-Azawi and Fadhil, 2010). Its growth has increased manifold in the past few years and a spate of effective techniques have been developed (Amirtharajan and Balaguru, 2011; Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al*., 2011, 2012a, b; Ramalingam *et al*., 2014; Thanikaiselvan *et al*., 2012a, b, 2013; Thenmozhi *et al*., 2012).

Among them, steganography and Water-marking have evoked maximum interest from scientists (Amirtharajan *et al*., 2013a-e; Stefan and Fabin, 2000; Janakiraman *et al*., 2012a, b; Padmaa *et al*., 2011; Rajagopalan *et al*., 2012). Steganography in Latin means covered writing. It involves hiding the desired message inside another message called cover (Al-Frajat *et al*., 2010; Alanizi *et al*., 2010). The prime aim in steganography is to maintain the secrecy (Anderson and Petitcolas, 1998). The hidden message can be known only to the sender and receiver. Putting it in other words we can say that this technique serves its purpose only if the presence of secret message is undetectable, failing which renders this technique useless (Tseng *et al*., 2002). An image is most often the preferred choice of cover. The redundancy in an image is used to camouflage the message. Spatial domain steganography, transform domain steganography and spread spectrum image steganography are some of the subcategories of Steganography. Spatial domain steganography embeds the secret information directly into the pixels of the cover object. For instance, the cover object can be an image, video or audio file. LSB (Least Significant Bit) steganography is a classic example of Spatial domain steganography (Amirtharajan and Rayappan, 2013; Petitcolas *et al*., 1999).

In this technique, the bits of the least significant plane are used to embed data. These bits are replaced with the secret message and the overall quality of the cover

object remains unaffected. It is the simplest technique of all and has a very high payload. On the contrary, this simplest technique would lend itself to attack by the hackers and is more likely to be deciphered than other techniques. Several detection methods are already available. Transform domain steganography transforms the cover image using one of the transforms like fourier transform, Hartley transform and wavelet transform. Embedding is performed on the transformed coefficients of the cover image.

In Watermarking a piece of data is embedded into the message to be transmitted. This piece of data is called watermark and it served to uniquely identify the copyright owner for that piece of data. This technique, unlike steganography, gives much importance to robustness. Its essence lies in the inability of a hacker to remove the watermark alone without significantly damaging the data. Cryptography is a data security technique that introduces security by making the message undecipherable rather than hiding it. We prefer steganography to cryptography as it is better to make the message undetectable than to leave it in undecipherable form in the hands of the hacker, since there is a possibility for a hacker to break the encryption method by some means (Schneier, 2007). The power of steganography increases by several folds when it is incorporated with cryptography.

Spread Spectrum Image Steganography (SSIS) uses spread spectrum concept used in digital communication (Marvel *et al*., 1998). It is a technique that broadens the bandwidth of a message signal which usually takes the narrowband form by combining over a wide band of spectrum that ensures the energy of the narrow band message waveform is lower at any frequency. This aspect is exploited to incorporate security in an image through spread spectrum. SSIS camouflages the message inside the noise typical to the natural image (Marvel *et al*., 1999). This noise is combined with the cover image to yield the stego image. Thus the message is well-incorporated without changing the statistical properties of the image.

The security provided by the steganography has to be broken when used by the wrong-doers for passing messages between them. The art of detecting the presence of secret message is known as steganalysis (Amirtharajan *et al*., 2012c). It is the reverse procedure of steganography methodology. The residual effects left by the steganography algorithms on the image have aided the development of steganalysis methods. Most of methods use the statistical properties of the image to compare the cover image and the stego image. However these methods can only detect the presence of hidden message, but cannot be used to retrieve it. Various information hiding techniques in OFDM has been suggested by Thenmozhi *et al*. (2012), Lin *et al*. (2006) and Lin and Pan (2008). Secret sharing skill can be much more made resourceful by taking up encryption algorithms. Thus this blend guarantees security and immunity to a routine both at the steganographic and cryptographic levels.

Image cryptosystem promises enhanced security when it is combined with chaotic (block cipher) algorithm. Authentication is assured with the use of hash based encryption means. Besides these, pixel based image encryption methods are also found to be valuable. Fast encryption routines, literally minimizes the computation time. Image encryption, on the whole, sees to the fact that the secret message is austerely enciphered. Since they do not give even a hint of what is hidden, this demesne has astonished many. The fundamental motto of Chaos is to scramble image pixel positions; which is highly reliable as far as image encryption is concerned (Alvarez *et al*., 1999, 2000; Zhu, 2012). This kind of encryption practices two basic ideas: Mystification and dissemination. It executes image encryption via pixel scuffling and grey scale spaying. At this moment in time, chaotic means proves to be an amazing tool for image encryption due to its sharp compassion to minute changes too. Therefore, this means to be a rapid, unharmed encryption means.

After reviewing the available literature on steganography, OFDM and FEC, this study proposes a data embedding scheme after convolutional encoder utilizing puncture patterns, then four levels of encryption is done on the secret data bits and is stored as a key value at the output of CP to maintain integrity and confidentiality of the data transmitted over wireless transmission system. Comparison graphs among various modulation schemes before and after embedding the secret data bits are plotted, then encrypting the secret data bits and embedding it after CP output is also plotted. Chaotic based encryption is done on the punctured outputs and the metrics are computed to validate the performance.

METHODOLOGY

Sample input data bits of 256 are passed over scrambler. It is a popular technique in digital data transmission to protect the data from burst errors. There may be cases when a lot of errors occur subsequently in a row during data transmission. Such errors correspond to burst errors and they exceed the correctable number of bits in an error correction scheme. This scenario can be overcome by interleaving the data before transmission. This scrambling ensures that many errors do not occur in the same code word and will be distributed over many

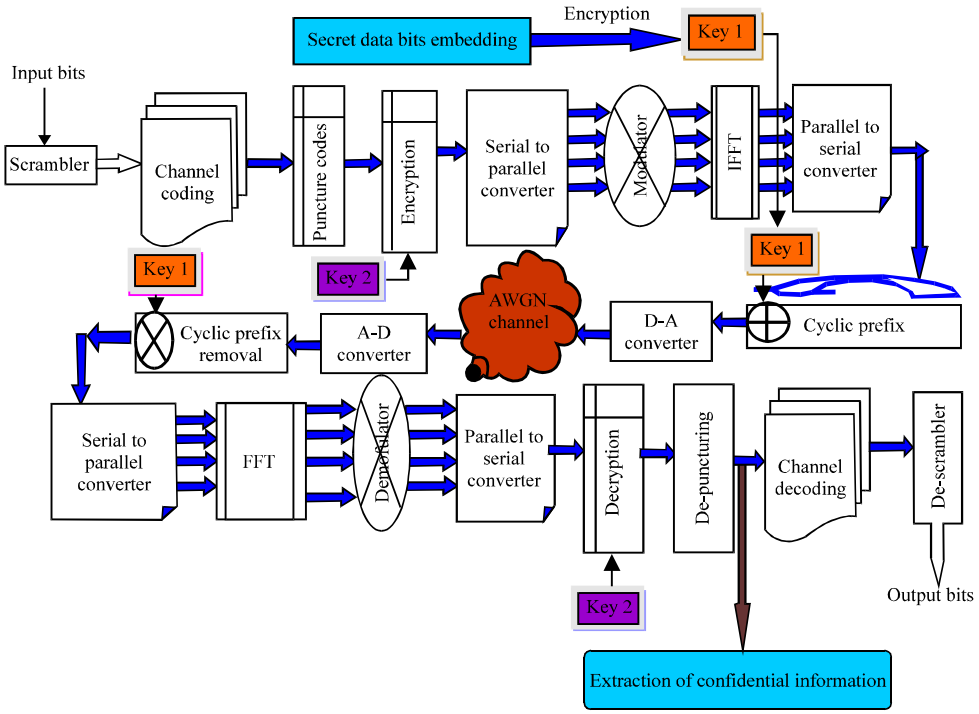

Fig. 1: Proposed block diagram

code words. It needs a specific key or algorithm to stipulate the scrambling of the data bits as shown in Fig. 1.

Then the scrambled data's are passed over channel coder. The most popular among them is convolutional coding and Viterbi decoding. It's a prodigious type error-control coding, the message bits come in serially rather than in blocks and hence it should have memory. Despite the fact that the convolutional coder acknowledges fixed message symbols producing fixed code symbols, the reckoning counts on certain prior input values apart from that in progression. It consists of finite number of shift registers in the company of given connections provided to modulo-2 adders and multiplexer which serializes the former's outputs. It accepts k input bit streams from 2k possible input symbols and produces n output bit streams out of 2n possible output symbols. The rate of the encoder is given as n/k where n represents the number of input bits and k represents the number of output bits. Then coded output bits are outputted to puncturing matrix/vector. It is the one, where the bits are deleted according to a pre-defined pattern.

Then, the inverse operation, known as de-puncturing, is implemented by the decoder. Output vector is generated by the puncture blocks which is done through eliminating certain elements in input vector but by maintaining others. Input may either be real or complex of length K. Operation of puncture block depends on its parameter (Puncture Vector) which is given below. Let the parameter be k:

Table 1: Simulation parameters

Input	Convolutional encoder rate	Coded output	Constraint length	Punctured pattern	IFFT	Cyclic prefix	Channel
256	1/2	512	5	[1 0]	64	1/4	AWGN
256	1/3	768	5	[1 1 0]	64	1/4	AWGN
256	2/3	384	[5 4]	[1 1 0]	64	1/4	AWGN
258	3/4	344	[5 4 5]	[1 1 0 0]	64	1/4	AWGN

- If k = 0, then the input vector's kth element is eliminated
- If k = 1, then the input vector's kth element gets potted in output vector

Puncture vector parameter's length should divide K. If needed, this process is repeated for the entire input elements. The simulation parameters used in the proposed system is given in Table 1. Then the confidential data bits are embedded at the output of the punctured convolutional encoder. Four level of encryption is done on the secret data bits and then they are stored as a key in the cyclic prefix part to maintain integrity.

Embedding algorithm to store the confidential data bits:

- Calculate the length of the punctured data output bits

- Divide the entire length in to different shares of equal length, decide the range of embedding
- Get the number of bits to be embedded
- Convert the secret bits into bipolar form
- The pattern is repetitive and starts from the LSB to MSB in a reverse manner

Consider m_2 to be the secret data, l be the length of m_2 and share be Q. Let N be the length of the actual data output, Q_1 decides the data bits to be embedded. $Q_1 = Q*1$ The length of the data after embedding $Q_2 = N-1$, $Q^* = Q_2 - Q_1$.

Encryption to store the secret key value at CP:

- Get the secret data input bits, flip it horizontally and use it as the key for the process
- Take XOR of actual input bits with the flipped one and the output is represented as a_k Eq. 1:

$$\text{Let } b_k \text{ be the bit representation } a_k = b_k \oplus b_n\text{-}(k\text{-}1) \quad (1)$$

- Then for the output obtained, perform bitwise XOR keeping the LSB bit unchanged, it is represented as C_k Eq. 2:

$$c_k = \begin{cases} a_k \oplus a_{k+1} & k \neq n \\ a_n & k = n \\ k \text{ ranges from } 1 \text{ to } n \end{cases} \quad (2)$$

- Then keeping MSB unchanged, perform bitwise XOR to the encrypted data which is represented as d_k Eq. 3:

$$d_k = \begin{cases} c_k \oplus c_{k-1} & k \neq 1 \\ c_k & k = 1 \end{cases} \quad (3)$$

Then this encrypted value as a key is embedded after CP to maintain integrity between transmitter and receiver.

Decryption to retrieve the key:

- At the receiver end, the region of embedding should be known, to carry out decryption process
- Get the encrypted data
- Retaining the MSB of the acquired data, perform XOR operation from left to right Eq. 4:

$$dec1_k = \begin{cases} d_k & k = 1 \\ dec_{k-1} \oplus d_k & k \neq 1 \; k = 1 \text{ to } n \end{cases} \quad (4)$$

- Retaining LSB of $dec1_k$, perform XOR operation from left to right Eq. 5:

$$dec2_{(n+1)-k} = \begin{cases} dec1_{n-(k-1)} & k = 1 \\ dec2_{(n+1)-(k-1)} \oplus dec1_{(n-(k-1))} & k \neq 1 \; k = 1 \text{ to } n \end{cases} \quad (5)$$

- To get the original data, $dec2_{(n+1)-k}$ is XORed with the key

Extraction of the confidential information: After identifying the range where embedding has happened, extraction of the secret data can be performed using Eq. 6:

$$S_k = Z_k \text{ (new)}/Z_k \text{ (old)} \qquad k = Q^*+1 \text{ to } Q_2 \quad (6)$$

S_k Can either be 1 or -1 and Z_k Can be any processed function. Then chaos based encryption is done on the punctured data bits.

Chaotic process: Chaos can be defined as a dynamic system which relies largely on preliminary specifications that are subjective and impulsive. The input values get encrypted using shambling bit values and modifying it to produce ciphered output values. This is done by the formulae:

$$A(c+1) = \text{mod}(b(c) + 1 - 1.4 * A(c) * A(c), 256) + 1$$

$$b(c+1) = \text{mod}(0.3 * A(c) + 0.7 * b(c) * A(c), 256) + 1$$

where, (A, b) is bit location, A is row; b is column. (A, b) is mapped to a different location by means of transformation function.

Chaotic algorithm:

- Generate random values from 0 to 255
- XOR the above values with bit values in the input by:

$$A(c+1) = \text{mod}(b(c) + 1 - 1.4 * A(c) * A(c), 256) + 1$$

$$b(c+1) = \text{mod}(0.3 * A(c) + 0.7 * b(c) * A(c), 256) + 1$$

Now the values are modified. The above given equations produce recursive random numbers; also, user

is allowed to provide the key to set initial values. Then the encrypted data bits are sent to the modulators like BPSK, QPSK, 8, 16, 32 and 64 QAM, respectively to produce complex constellation points.

With the sub carriers very closely placed, mutual influence is hard to avoid but higher efficiency can still be obtained by the proper selection of the orthogonal frequencies using IFFT. By Cyclic prefix, ¼ th of total OFDM symbol is added as prefix to combat ISI (Inter symbol Interference) and ICI (Inter Carrier Interference).

Then scaling is done to transmit the data over Additive White Gaussian Noise (AWGN) channel. At the receiver end, two types of decryption algorithm should be known at the receiver end. One to extract the secret data bits, other to extract the data output bits. Two keys are required at the receiver end .If K2 is known decryption of the original data bits over OFDM system will be extracted. If both the keys K1 and K2 are known, then secret data bits along with the original data are recovered contributing to the security multi-fold.

RESULTS AND DISCUSSION

Sample input data bits of 256 are passed over OFDM system considering AWGN channel, graphical results are for BER comparison of Punctured convolutional encoder with dissimilar rates of according 1/2, 1/3, 2/3 and 3/4. It is vivid that performance is intensified as secret bits are embedded after deflated convolutional encoder after which chaotic encryption is performed.

Pixel correlation is one of the important parameters for consideration of image encryption. Every image encryption algorithm aims at reducing this correlation to literally null value to vindicate the performance. Correlation value of 1 show that high correlation exists among pixels and 0 indicates the other way round. If the result is 0, then the algorithm offers nothing but abstruseness and randomness. This work is justified in this regard where encrypted data show 0 correlation among their pixels. The correlation coefficient is given by:

$$c = \frac{\mathrm{cov}(i, j)}{\sigma_i \sigma_j}$$

Here, σ_i, σ_j is i and j's standard deviations accordingly, cov (i, j) is covariance of i and j.

Covariance is expressed as:

$$\mathrm{cov}(i, j) = \frac{1}{N}\sum_{a=1}^{N}(i_a - \mu_i)(j_a - \mu_j)$$

Here, μ_i and μ_j are i and j's mean, respectively.

From Fig. 2-9, for a BER of 10^-2, BPSK is 2.5 dB which is 1 dB improvement over QPSK which in turn

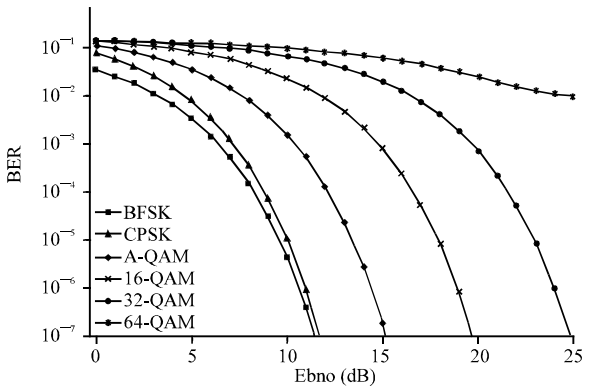

Fig. 2: Encrypting the data without embedding using convolutional encoder of rate 1/2

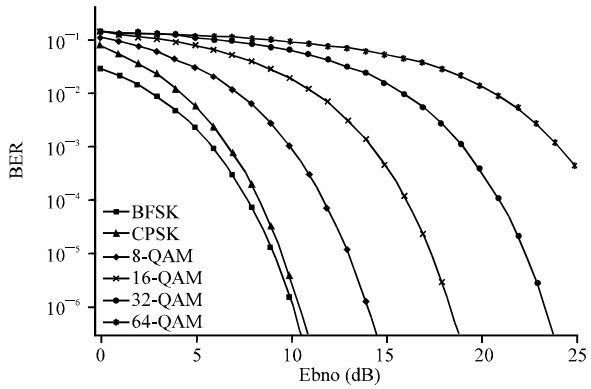

Fig. 3: Encrypting the data without embedding using convolutional encoder of rate 1/3

provides an improvement of 3 dB with respect to 8 QAM, which provides an improvement of 3 dB with respect to 16 QAM, which overruns 32 QAM by 5 dB which is heightened by 5 dB with respect to 64 QAM. The maximum improvement in SNR by 17.5 dB is guaranteed with respect to BPSK.

From Fig. 2-4, for an Eb/No of 10 dB, 64 and 32 QAM is around 10^-1, 16 QAM is around 10^-2, 10^-3 for 8 QAM, QPSK is around 10^-5 and BPSK is about 10^-6. Thus QPSK and BPSK schemes are ideal among all the modulation schemes when encryption is considered.

Figure 6-9, respectively provides BER curve before and after embedding the secret data bits adopting convolutional encoder of rates 1/2, 1/3, 2/3 and 3/4. Before and after embedding the secret data bits in 1/2 and 1/3, there is no appreciable change in BER curve before and after embedding the confidential information till 16 QAM, then after 0.1 TO 1 dB difference exists before and after embedding the secret data bits in 32 and 64 QAM.

Before and after embedding the secret data bits in 2/3 and 3/2, there is no appreciable change in BER curve

Table 2: Encrypted data metrics with embedding

Encoding rate	1/2	1/3	2/3	3/4
Correlation value	0.0339	0.0227	0.0157	0.0327

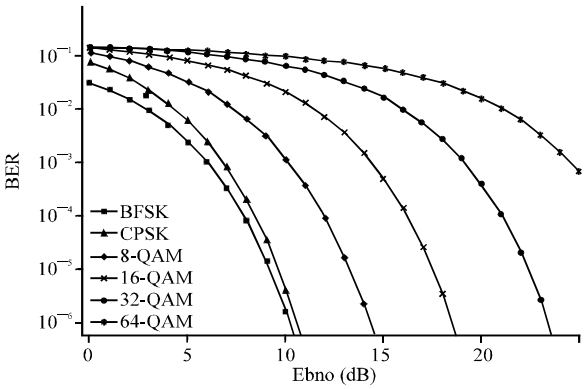

Fig. 4: Encrypting the data without embedding using convolutional encoder of rate 2/3

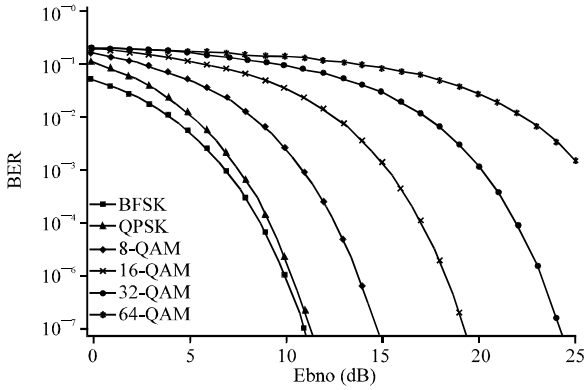

Fig. 5: Encrypting the data without embedding using convolutional encoder of rate 3/4

before and after embedding the confidential information till 8 QAM, then after 0.1 to 1.2 dB difference exists before and after embedding the secret data bits from 16 QAM onwards in 2/3 coding. In 3/2, till 15db all the modulation schemes work fine and 64 QAM alone deteriorates from 0.1 to 2 dB. Thus other than 64 QAM, all other modulation schemes are ideal when embedding is concentrated.

Table 2 provides the data metrics for encryption with embedding. It is obvious that BER of the convolutional encoder of rate 2/3 is higher which denotes that it produces more random and obscure output. Those with other rates are also competently high error giving justifying this encryption. Besides this, correlation values are also brought to minimum level. This means the bonding between data bits i.e., data bits relationship is very much affected due to the encryption. So, the output shows no sign of having surreptitious information in it. The 2/3 encoder gives the best results of all encoders when encryption is considered.

Table 3 provides the encrypted data metrics for different coding rates. This study has resulted in anticipated bit error rates of approximately 0.06. Of all, one with the rate of 2/3 offers high BER which signifies that the error produced is comparatively greater. This shows how random the encrypted data is. Without qualm, this study has brought the pixel correlation to a zilch which is what most needed in an encryption routine. This is so because, the minimum the correlation, the maximum is the obscurity and in turn security. Convolutional encoder with rate 2/3 is good at this regard.

Figure 10 and 11 gives the cyclic prefix output before and after embedding the key value, from

Table 3: Encrypted data metrics without embedding

Encoding rate	1/2	1/3	2/3	3/4
Correlation value	0.0419	0.0323	0.0313	0.0381

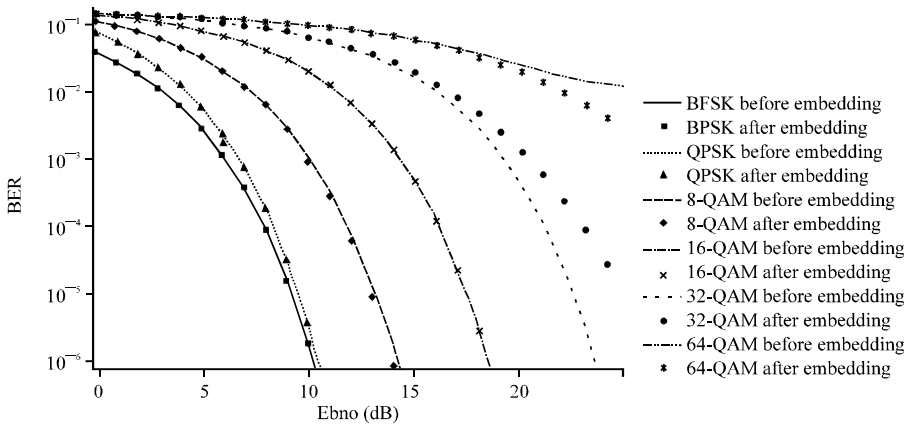

Fig. 6: Comparison among various modulation schemes using convolutional encoder of rate 1/2 with embedding before encryption

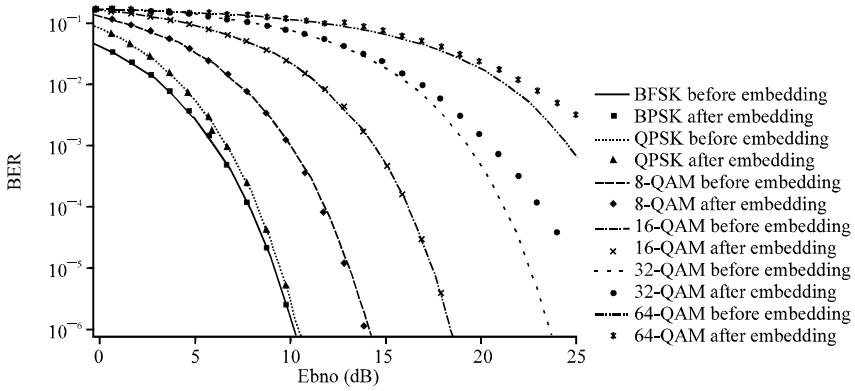

Fig. 7: Comparison among various modulation schemes using convolutional encoder of rate 1/3 with embedding before encryption

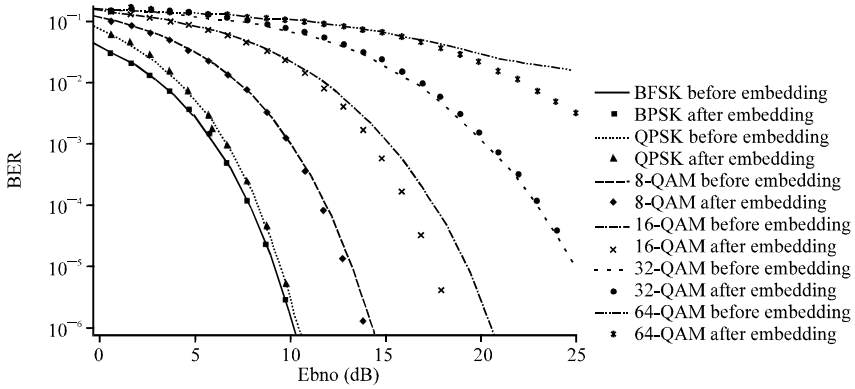

Fig. 8: Comparison among various modulation schemes using convolutional encoder of rate 2/3 with embedding before encryption

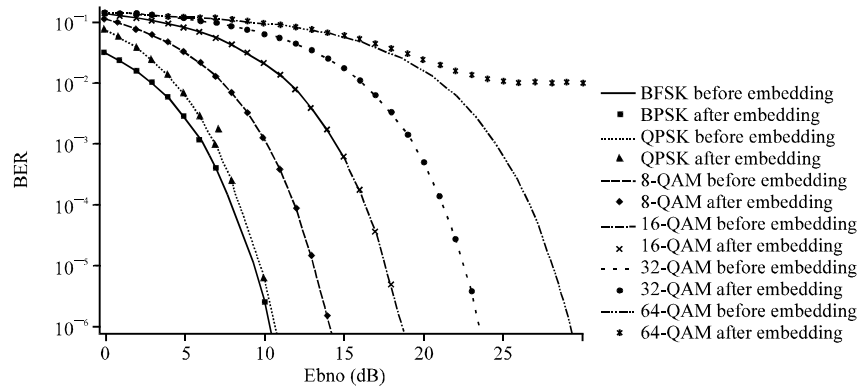

Fig. 9: Comparison among various modulation schemes using convolutional encoder of rate 3/4 with embedding before encryption

the figure there is no appreciable change in the cyclic prefix output before and after embedding.

When the two methods i.e., with and without embedding are concerned, method one outperforms the second as the high correlation existed among pixels in original image is brought to a zilch after encryption. The encoders with rates 1/3 and 2/3 are able to produce correlation values of 0.0227 and 0.0157, respectively which is slightly greater than the second method.

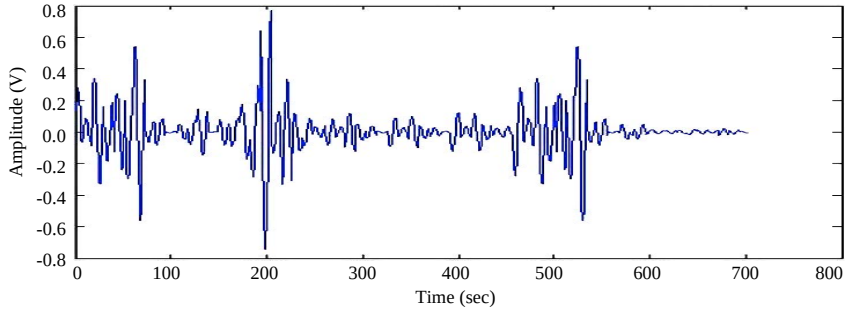

Fig. 10: Cyclic prefix output before embedding

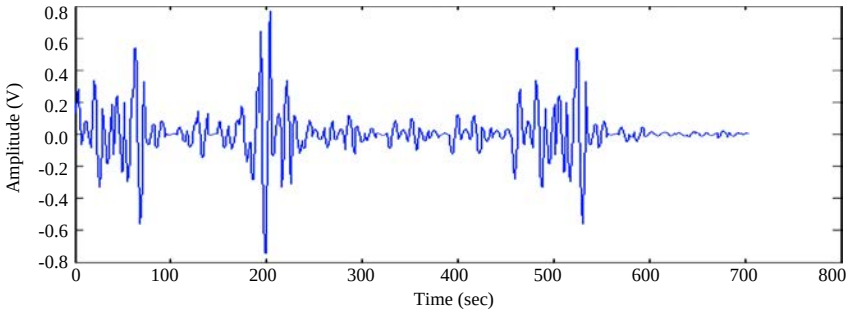

Fig. 11: Cyclic prefix output after embedding

CONCLUSION

OFDM makes the most of orthogonality that exist between carriers which is the most substantive requisite for broadband applications as they oblige privileged bandwidth. In this study, incorporated assorted rates, puncture patterns, modulation schemes and finally at the output of the convolutional encoder, secluded bits are engrafted to ensure confidentiality. Subsequently, four-level encryption is performed on the secret data bits which are then hired away as the key at cyclic prefix's output. This serves as an integrity appraisal between the two parties indulged in communication. Hence, QPSK and BPSK are the preferred modulations as they prove to be an effectual means to share the secret encrypted data. Thus, soaring level of privacy and security is maintained all through the process and any line of attack would go in vain. Thus robustness is ensured as well. As far as the two methods are concerned, method 1 is found to be beneficial as it emerges with incredible results. Of convolutional encoders with different rates, the one with rate 2/3 is found to be superior. Graphical testimonies are illustrated for BER amongst versatile modulation schemes engaging convolutional encoders of diverse puncture patterns and rates. Wireless technology blended with information security emerged as a solution to all types of communication threats and problems. This expertise with technical advancements will definitely be one worth to explore. When the gap is bridged between some technical problems and practical implementation possibilities, future scope is very promising for the forth coming wireless generations.

REFERENCES

Al-Azawi, A.F. and M.A. Fadhil, 2010. Arabic text steganography using kashida extensions with huffman code. J. Applied Sci., 10: 436-439.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

Alanizi, H.O., M.L.M. Kiah, A.A. Zaidan, B.B. Zaidan and G.M. Alam, 2010. Secure topology for electronic medical record transmissions. Int. J. Pharmacol., 6: 954-958.

Alvarez, E., A. Fernandez, P. Garcia, J. Jimenez and A. Marcano, 1999. New approach to chaotic encryption. Phys. Lett. A, 263: 373-375.

Alvarez, G., F. Montoya, M. Romera and G. Pastor, 2000. Cryptanalysis of a chaotic encryption system. Phys. Lett. A, 276: 191-196.

Amirtharajan, R. and R.J.B. Balaguru, 2011. Covered CDMA multi-user writing on spatially divided image. Proceedings of the 2nd International Conference on Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, February 28-March 3, 2011, Chennai, India, pp: 1-5.

Amirtharajan, R., R.R. Subrahmanyam, P.J.S. Prabhakar, R. Kavitha and J.B.B. Rayappan, 2011. MSB over hides LSB: A dark communication with integrity. Proceedings of the IEEE 5th International Conference on Internet Multimedia Systems Architecture and Application, December 12-14, 2011, Bangalore, Karnataka, India, pp: 1-6.

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. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

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

Amirtharajan, R., K. Ramkrishnan, M.V. Krishna, J. Nandhini and J.B.B. Rayappan, 2012b. Who decides hiding capacity? I, the pixel intensity. Proceedings of the International Conference on Recent Advances in Computing and Software Systems, April 25-27, 2012, Chennai, India, pp: 71-76.

Amirtharajan, R., V. Mahalakshmi, N. Sridharan, M. Chandrasekar and J.B.B. Rayappan, 2012c. Modulation of hiding intensity by channel intensity-Stego by pixel commando. Proceedings of the International Conference on Computing, Electronics and Electrical Technologies, March 21-22, 2012, Kumaracoil, pp: 1067-1072.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

Amirtharajan, R., S. Sulthana, P.S. Priya, G. Revathi, A.K. Infant and J.B.B. Rayappan, 2013a. Seeable visual but not sure of it-A visual cryptographic perspective for TAMIL characters. Int. J. Eng. Technol., 5: 2000-2007.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013b. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013c. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013d. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013e. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Anderson, R.J. and F.A.P. Petitcolas, 1998. On the limits of steganography. IEEE J. Sel. Areas Commun., 16: 474-481.

Bahai, A.R.S., B.R. Saltzberg and M. Ergen, 2004. Multi-Carrier Digital Communications: Theory and Applications of OFDM. 2nd Edn., Springer, USA., ISBN-13: 978-1441935502.

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

Chang, R.W., 1966. Synthesis of band-limited orthogonal signals for multi-channel data transmission. Bell Syst. Tech. J., 45: 1775-1796.

Chang, R.W., 1970. Orthogonal frequency division multiplexing. U.S. Patent No. 3488445.

Forney, Jr. G.D., 1970. Convolutional codes I: Algebraic structure. IEEE Trans. Inform. Theory, 16: 720-738.

Forney, Jr. G.D., 1971. Burst-correcting codes for the classic bursty channel. IEEE Trans. Commun. Technol., 19: 772-781.

Forney, Jr. G.D., 1973. The viterbi algorithm. IEEE Proc., 61: 268-278.

Hwang, T., C.Y. Yang, G. Wu, S.Q. Li and G.Y. Li, 2009. OFDM and its wireless applications: A survey. IEEE Trans. Veh. Technol., 58: 1673-1694.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Firmware for data security: A review. Res. J. Inform. Technol., 4: 61-72.

Janakiraman, S., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Pixel forefinger for gray in color: A layer by layer stego. Inform. Technol. J., 11: 9-19.

Lin, C. and J.S. Pan, 2008. An information hiding scheme for the MDC-OFDM wireless networks. Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, August 15-17, 2008, Harbin, China, pp: 1013-1016.

Lin, C., J.S. Pan, C.S. Shieh and P. Shi, 2006. An information hiding scheme for OFDM wireless networks. Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, December 18-20, 2006, Pasadena, CA., USA., pp: 51-54.

Marvel, L.M., C.T. Retter and C.G. Jr. Boncelet, 1998. A methodology for data hiding using images. Proceedings of the IEEE on Military Communications Conference, October 18-21, 1998, Boston, MA., USA., pp: 1044-1047.

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.

Peterson, W.W. and E.J. Weldon, 1972. Error-Correcting Codes. The MIT Press, Cambridge, UK..

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving-a multicarrier stego. Proc. 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, J. Bosco and 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.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013a. Secret link through Simulink: A stego on OFDM channel. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013c. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013d. Purposeful error on OFDM: A secret channel. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013e. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013f. Spread and hide: A stego transceiver. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013g. Stego in multicarrier: A phase hidden communication. Inform. Technol. J.

Praveenkumar, P., K. Thenmozhi, M.N. Dinesh and R. Amirtharajan, 2013h. Fixing, padding and embedding: A modulated stego. Int. J. Eng. Technol., 5: 2257-2261.

Praveenkumar, P., K. Thenmozhi, S. Vivekhanandan, J.B.B. Rayappan and R. Amirtharajan, 2013i. Intersect embedding on OFDM channel-a stego perspective. Proceedings of the IEEE Conference on Information and Communication Technologies, April 11-12, 2013, JeJu Island, pp: 1211-1214.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013j. Convolution and viterbi EN(DE)coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Rajagopalan, S., R. Amirtharajan, H.N. Upadhyay and J.B.B. Rayappan, 2012. Survey and analysis of hardware cryptographic and steganographic systems on FPGA. J. Applied Sci., 12: 201-210.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014. Stego on FPGA: An IWT approach. Sci. World J. 10.1155/2014/192512

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

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., John Wiley and Sons, New Delhi, India.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013. A graph theory practice on transformed image: A random image steganography. Sci. World J. 10.1155/2013/464107

Thenmozhi, K., V.K. Konakalla, S.P.P. Vabbilisetty and R. Amirtharajan, 2011. Space Time Frequency coded (STF) OFDM for broadband wireless communication systems. J. Theor. Applied Inform. Technol., 3: 53-59.

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.

Tseng, Y.C., Y.Y. Chen and H.K. Pan, 2002. A secure data hiding scheme for binary images. IEEE Trans. Commun., 50: 1227-1231.

Van Nee, R. and R. Prasad, 2000. OFDM for Wireless Multimedia Communications. Artech House, Norwell, MA., USA., ISBN-13: 9780890065303, Pages: 260.

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

Zhu, C., 2012. A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun., 285: 29-37.