ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

Effect of convolutional coding on hidden data

V. Mithya, S. Deepa

Assistant Professor, Department of ECE, Karpagam College of Engineering, Coimbatore, India

ABSTRACT -This project simulates an effective data hiding technique i.e. steganography based on LSB insertion and RSA encryption in order to provide seven million times better security than the previous work. The Main idea of proposed scheme is to encrypt secret data by RSA 1024 algorithm, convert it in to binary sequence bit and then embedded into each cover pixels by modifying the least significant bits (LSBs) of cover pixels. The result image is also known as steganography image. This steganography image is transmitted through AWGN channel, and performance of channel coding (convolutional coding) is simulated. The images and hidden data are reconstructed with the SNR level ≥9 dB without channel coding, whereas with channel coding it is reconstructed at SNR ≥6 dB. The convolutional coding with viterbi decoding improves the reconstruction performance up to 3 dB.

KEYWORDS: Steganography, LSB, RSAalgorithm, convolutional coding

I . INTRODUCTION

In companies with rapid growth of computer and communication networks, internet has been established worldwide that brings numerous convenient applications. Internet is an open system to transmit secret data securely is an issue of great concern. Security could be introduced by hiding this secret information. To hide secret information steganography and cryptography are cousins in the information hiding family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen.

Networks must be able to transfer data from one device to another with complete accuracy. A system that cannot guarantee that the data received by one device are identical to the data transmitted by another device is essentially useless. Reliable systems must have a mechanism for detecting and correcting the errors and are done by using error detection and correction methods. In this implementation, we combine one of the error correction techniques (that is convolutional code) with this data hiding mechanism in the process of sending a data between two computers over a network. The popularity of the Internet offers a great convenience to the transmission of a large amount of data over networks. The internet is not a single network, but a

worldwide collection of loosely connected networks which are accessible by individual computer hosts, in a variety of ways, to anyone with a computer and a network connection. Thus, individuals and organizations can reach any point on the internet without regard to national or geographic boundaries or time of day.

However, along with the convenience and easy access to information come risks. Information may be about employees, customers, research, products or financial operations .Among them are the risks that valuable information may be lost, stolen, changed, or misused. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home they may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can also create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

So Security viewed by information systems has become vital. The term information security means protecting information and information systems from unauthorized access, use, disruption, or destruction. From here the concept of information security is introduced. [1]

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

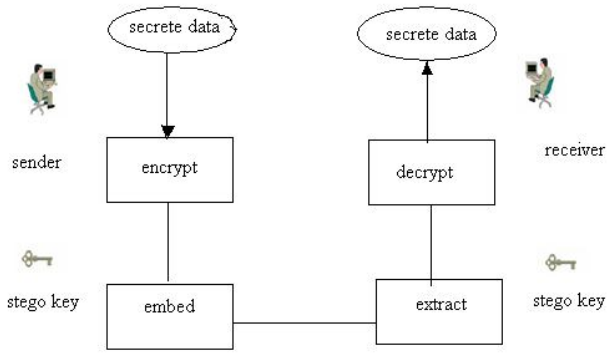


Fig 1 Steganography Mechanism

II LEAST SIGNIFICANT BIT INSERTION METHOD

Least significant bit insertion is a common, simple approach to embed information in a cover file [2]. Usually, three bits from each pixel can be stored to hide an image in the LSBs of each byte of a 24-bit image. The resulting stego-image will be displayed indistinguishable to the cover image in human visual system [3].

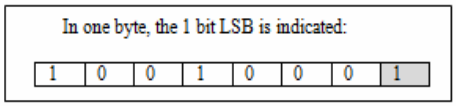


Fig. 2: Least Significant Bit

The last bit of the byte is selected as least significant bit in one bit LSB as illustrated in Figure 2 because of the impact of the bit to the minimum degradation of images [4]. The last bit or also known as right-most bit is selected as least significant bit, due to the convention in positional notation of writing less significant digit further to the right [5]. In bit addition, the least significant bit has the useful property of changing rapidly if the number changes slightly. For example, if 1 (binary 00000001) is added to 3 (binary00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100).

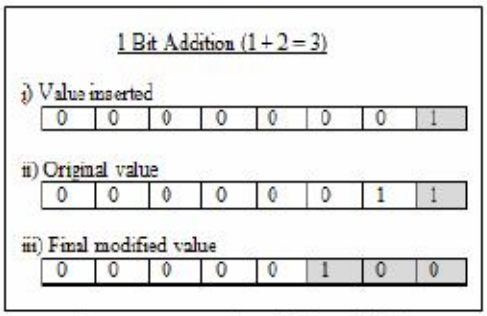


Fig. 3: Example of bit addition

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

There are numbers of steganograpic tools which employ LSB insertion methods available on the web. For example, S-Tools take a different approach by closely approximating the cover image which may mean radical palette changes. Instead, S-Tools reduce the number of colors while maintaining the image quality, so that the LSB changes do not drastically change color values. Another tool which is using LSB manipulation is EzStego. It arranges the palette to reduce the occurrence of adjacent index colors that contrast too much before it inserts the message. This approach works quite well in gray-scale images and may work well in images with related colors [3]. On the other hand, StegCure keeps the advantage of S-Tools and EzStego that is maintaining the image quality, but it can prevent the attack from hackers by restricting user to have only one attempt to perform destego method. If the user has used the wrong destego method for the first time, there is no second attempt to recover the hidden data in the image even though the user has chosen the correct destego method.

III.CONVOLUTIONAL CODES

Convolutional codes are commonly specified by three parameters; (n,k,m), where: n is the number of output bits, k is the number of input bits, and m is the number of shift register stages of the coder. The constraint length L of the code represents the number of bits in the encoder memory that affect the generation of the n output bits and is defined as L = mk. The code rate r of the code is a measure of the code efficiency and is defined by r = k/n [6].

A. Code parameters and the structure of the convolutional code:

Figure4 shows the convolutional encoder structure CC (2, 1, 3)) used in this paper and is built from its parameters. It consists of 3 (m=3) shift register stages and two modulo-2 adders (n= 2) giving the outputs of the encoder. The rate of the code is r = 1/2. The minimum distance of the code is dmin =3. The outputs of the adders are sampled sequentially yielding the code symbols. The total number p of bit symbols is given by p = n (nb + m) where nb is the total number of bits of information. The outputs v_1 and v_2 of the adders are governed by the following generator polynomial. The generator polynomial for the output v_1 is given by

$$g_1(x) = 1 + x + x^2$$

The generator polynomial for the output v_2 is given by

$$g_2(x) = 1 + x^2$$

g_1(x) And g_2(x) select the shift register stages bits to be added to give the outputs of the encoder which are, for the case of CC (2, 1, 3) encoder as follow

$$v_1 = u_0 \oplus u_1 \oplus u_2 \qquad (1)$$

$$v_2 = u_0 \oplus u_2 \qquad (2)$$

The polynomials give the code its unique error protection quality [6].

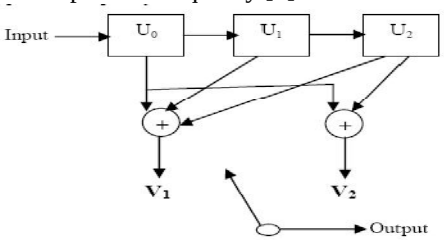


Figure 4- Convolutional code CC (2, 1, 3)

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

B. Coding a message sequence:
In this section a 4 bit sequence of 1001is coded to show how the encoder works. The bits are passed through the encoder sequentially and the outputs of the encoder are calculated using equations (1) and (2) for each time step.

Table1- Coding process of CC(1,2,3) code

Time instant	Input	U_0	U_1	U_2	V_0	V_1
t= 0		0	0	0	0	0
t= 1	1	1	0	0	1	1
t= 2	0	0	1	0	1	0
t= 3	0	0	0	1	1	0
t= 4	1	1	0	0	1	1
Reset process	0	0	1	0	1	0
	0	0	0	1	1	1
	0	0	0	0	0	0

The data in bold are the input bits which are shifted in the memory register for every time clock. The code output sequence is: 11 10 11 11 10 11 00 where the last 6 bits (= nm) are the reset bits and they do not contain any information. Table 2 shows the code words of different 4-bit messages calculated by using the procedure described above [6].

Table-2 Code words of different 4-bit messages

Message number	Message	Codeword
1	0000	00 00 00 00 00 00 00
2	0001	00 00 00 11 10 11 00
3	0010	00 00 11 10 11 00 00
4	0011	11 01 01 1100 00 00
5	0100	00 11 10 11 00 00 00
6	0101	11 01 00 01 11 00 00
7	0110	00 11 01 01 10 00 00
8	0111	11 01 10 01 01 00 00
9	1000	00 00 00 11 10 11 00
10	1001	11 10 11 11 10 11 00
11	1010	00 11 10 00 10 11 00
12	1011	11 01 01 00 10 11 00
13	1100	11 01 01 00 10 11 00
14	1101	11 01 01 00 10 11 00
15	1110	11 01 10 01 11 00 00
16	1111	11 01 10 10 01 11 00

IV DECODING USING VITERBI ALGORITHM

There are several different approaches for decoding of convolutional codes. These are grouped in two basic categories: sequential decoding (Fano algorithm), Maximum likelihood decoding (Viterbi algorithm) [7].

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

Both these methods represent two different approaches to the same basic idea behind decoding. Assume that 4 bits were sent via rate 1/2 code. One receives 8 bits. (And 6 reset bits that are not considered here for simplicity). These 8 bits may or may not have errors. One knows from encoding process that these map uniquely. So a 4 bit sequence will have a unique 8 bit output. But due to errors one can receive any and all possible combinations of the 8 bits, (28 combinations). The permutation of 4 input bits results in 16 possible input sequences. Each of these has a unique mapping to an 8 bit output sequence by the code as shown in table2. These form the set of permissible sequences and the encoder's task is to determine which one was sent. Let us say one received 11111100. It is not one of the 16 possible sequences shown in table2. How does one decode it? One can do two things.

1. Compare this received sequence to all permissible sequences and pick the one with the smallest Hamming distance (or bit disagreement)
2. Perform a correlation and pick a sequence with the best correlation.

The first procedure is basically what is behind hard decision decoding and the second the soft-decision decoding [7]. In the following sections these two techniques are described.

A .Maximum Likelihood and Viterbi decoding

Viterbi decoding is the best known implementation of the maximum likelihood decoding [7]. The assumptions made in this technique are as follow:

1. The errors occur infrequently, the probabilities of errors are small.
2. The errors are distributed randomly.

The Viterbi algorithm examines an entire received sequence of a given length. The decoder computes a metric for each path and makes a decision based on this metric. All paths are followed until two paths converge on one node. Then the path with the higher metric is kept and the one with the lower metric is discarded. The selected paths are called the survivors. For an N bit sequence, the total number of possible received sequences is 2N; only 2k(L-1) of these are valid. The Viterbi algorithm applies the maximum likelihood principles to limit the comparison to 2k(L-1) surviving paths instead of checking all paths. The most common metric used is the hamming distance metric. This is just the dot product between the received code word and the allowable codeword. These metrics are cumulative so that the path with the largest total metric is the final winner.

The metric branch mj
(J) at jth instant is given by:

$$m_j^{(\propto)} = Ln \prod_{i=1}^{n} p\ \left(r_{ij} / c_{ji}^{(\propto)}\right) = \sum_{i=1}^{n} Ln\ \left(p(r_{ij}\ / c_{ji}^{(\propto)}\right.$$

Where rij is the ith bit received at jth instant. And cji is the ith bit transmitted at jth instant.

The metric path M(J) of the path J at the jth instant is the sum of the metric branches of the path J from the first instant to the jth instant and is given by:

$$M^{(\propto)} = \sum_{j}^{J} m_j^{(\propto)}$$

The winner is the path with the highest metric path i.e.
Max ($M_1^{(\propto)}$, $M_2^{(\propto)}$ ... ... $M_k^{(\propto)}$

V.SIMULATED RESULTS

Tool used: MATLAB Simulink version 7.0 .The name of images are baboon,lena,boat, size of image is 256x256, and format of image is BMP which we have taken for simulation .Here 256x256 meaning that number of rows and column of pixels, and BMP meaning that the format of image i.e. bit map format. These three images are gray scale images i.e. 8 bits per pixel. The proposed method hides secret data bits in LSB of each pixel so we can hide 65536 secret data bits in an

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

image by using row ×column × n relationship. Where n is no of LSBs used.The results are tabulated in Table 3. In Table 3, the column labeled 'Capacity' is the number of bits can be embedded into the host-image and the column labeled 'PSNR' is the peak-signal-to-noise-ratio of the stego-image. The results are the average value of embedding 65536 random bit-streams into the host images.

A simulation results when secret data bits are hide in cover image

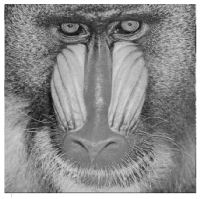
TABLE 3 SIMULATION RESULS WHEN SECRET DATA BITS ARE HIDE IN COVER IMAGE

Name of the images	Embedding secret data capacity in bits	PSNR in db
Baboon	65536	54.00
Lena	65536	53.32
Boat	65536	52.55

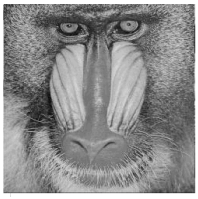
- Here PSNR is calculated by following relation

$$MSE=\frac{1}{H\times W}\sum_{I=1}^{H}\cdot\sum_{J=1}^{W}\left(PVOFCOVER\ IMAGE\ (I,J)-PV\ OF\ STEGO\ IMAGE(I,J)\right))^2 \quad (3)$$

$$PSNR = 10\log\frac{255^2}{MSE} \quad (4)$$



Cover image of Baboon



Stego image of baboon PSNR =54.00

Cover image of Lena

Stego image of Lena PSNR =53.32

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013


Cover image of Boat


Stego image of Boat PSNR =52.55

Fig 5 Images Used In This Simulation

When these images are transmitted through AWGN channel, noises are introduced in it, thereby this stego images may be corrupted by noise and also hidden secret data bits are affected by that noise. The experimental results shown in table 4, 5, and 6 that how much stego bits and data bits are corrupted by noise.The solution of this problem is that detects these errors and corrects these errors .In proposed method use channel coding to correct corrupted secret hidden data bits by noise. For this purpose use convolutional coding and viterbi algorithm to detect and correct errors .The experimental results shown in table 4, 5, and 6 that how much secret data bits and stego bits are corrected by channel coding. The size of image is 256x256 i.e.65536 total no of pixels or 524288 data streams are transmitted through noisy channel. Additive white Gaussian noises are used in this experiment. The characteristic of this communication system with bit error rate (*BER*) versus signal noise ratio (*SNR*, E_b/N_0, *dB*), where E_0 is energy per bit and N_0 is noise spectral density. Such a controlled noise was added in every channel and that stego image is transmitted over the channel bit by bit. The number of error bits was measured at every controlled noise level to obtain BERs for test image during the stego image transmission. The received stego bits are used to reconstruct the stego image, and extract secret data bits by using decryption algorithm. The error correction results of the proposed method are given in the table 4, 5, 6.

B. simulation results when data stream is transmitted through AWGN channel with and without channel coding for the Baboon image

Table 4 simulation results when stego image is transmit through AWGN channel

	Without channel coding		With channel coding	
SNR IN db	No of bits corrupted through AWGN/ 524288	No of hidden data bits corrupted through AWGN /65536	No of bits corrupted through AWGN /524288	No of hidden data bits corrupted through AWGN /65536
0	41086	5080	25479	3199
1	29086	3688	12880	1624
2	11958	1466	1879	250
3	6491	815	488	66
4	3231	411	101	5
6	1217	146	10	4
8	86	14	8	3
9	24	4	6	2
10	2	1	4	1

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

C. simulation results when data stream is transmitted through AWGN channel with and without channel coding for the Lena image

Table 4 simulation results when stego image is transmit through AWGN channel				
	Without channel coding		With channel coding	
SNRIN db	No of bits corrupted through AWGN /524288	No of hidden data bits corrupted through AWGN /65536	No of bits corrupted through AWGN /524288	No of hidden data bits corrupted through AWGN /65536
0	40086	5180	24479	3099
1	20086	3088	13880	1524
2	10958	1566	1779	251
3	6291	715	408	66
4	3331	401	100	6
6	1227	136	11	5
8	76	13	7	3
9	34	3	6	2
10	3	1	3	1

D.simulation results when data stream is transmitted through awgn channel with and without channel coding for the Boat image

Table 4 simulation results when stego image is transmit through AWGN channel				
	Without channel coding		With channel coding	
SNRIN db	No of bits corrupted through AWGN/ 524288	No of hidden data bits corrupted through AWGN /65536	No of bits corrupted through AWGN /524288	No of hidden data bits corrupted through AWGN /65536
0	42086	5180	24479	3099
1	23086	3788	11880	1524
2	10958	1366	1579	252
3	6391	715	408	69
4	3031	421	100	4
6	1117	136	11	3
8	96	13	9	2
9	20	3	5	1
10	2	1	4	1

VI.CONCLUSION

The conclusion of these experimental results is that- The proposed data hiding scheme is an efficient data hiding scheme based on the LSB insertion and RSA encryption method by its PSNR value of image like baboon is 54.00 dB, 53.32dB, 52.55dB which is not noticeable by human eyes. Enhance security of hidden data by $7x10^6$ times than the RSA-512 in terms of its time complexity, and 2650 times in space complexity. The steganography images are transmitted through AWGN channel, and performance of channel coding (convolutional coding) is simulated. The image and hidden data are reconstructed with the SNR level ≥9 dB without channel coding, whereas with channel coding it is reconstructed at SNR ≥6

ISSN (Print): 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2013

dB with channel coding. The convolution coding with viterbi decoding improves the reconstruction performance up to 3 dB.

REFERENCES

1. Implementing Cisco IOS Network Security (IINS) Catherine Piquet Copyright © 2009 Cisco Systems, Inc. Published by: Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA
2. Chandramouli R and Memon N, "Analysis of LSB based image steganography techniques", *Proceedings 2001 International Conference on Image*, Vol. 3, pp. 1019-1022
3. StegCure: An Amalgamation of Different Steganographic Methods inGIF Image L.Y. Por1, W.K. Lai2, Z. Alireza3, B. Delina4 Faculty of Computer Science and Information Technology University of Malaya 50603, Kuala Lumpur MALAYSIA .
4. S. Katzenbeisser, Fabien A.P. Petitcolas, *Information Techniques for Steganography and Digital Watermarking*, Artech House, Boston, London, 2000.
5. John Kadvany, "Positional Value and Linguistic Recursion", *Springer Netherlands*,Vol. 35, December 2007, pp. 487-520.
6. comparison between viterbi algorithm soft and hard decision decoding Dr H. MelianiAl-Ahsa College of Technology,KSAA.Guellal University of Blida, Algeria
7. Charon Langton, Coding and decoding with conventional codes1999.
8. N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen," *IEEEComputer*, February 1998, pp.26-34.*Image*, Vol. 3, pp. 1019-1022. L.Y. Por1, W.K. Lai2, Z. Alireza3, B. Delina4,2008.
9. Mohammed Al-Mualla and Hussain Al- Ahmad, "Information Hiding: steganography and Watermarking". [Online]. Available:*http://www.emirates.org/ieee/information_hiding.pdf*,[Accessed: March 12, 2008].
10. Andrew D. Ker,"Steganalysis of Embedding inTwo Least-Significant Bits",*IEEETransactions On Information Forensics And Security*,Vol. 2, No 1, March 2007, pp. 46-54.
11. NeetaDeshpande,SnehalKamalapurandJacobsDaisy,"Implementation of LSBsteganography and Its Evaluation for VariousBits",*1st International Conference on DigitalInformation Management*, 6 Dec. 2006 pp.173-178.
12. Muthiyalu Jothir,Navaneetha Krishnan,"Statistical models for Secure steganographySystems", *Digital Rights Management Seminar*, 15th May, 2006.
13. S. Reinsberg, et. al., Phys. Med. Biol. 50, 2651-2661, (2005) T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", *Proceedings of the Fifth Annual InformationSecurity South Africa Conference (ISSA2005)*.
14. Mahomet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp and Eli Saber."LosslessGeneralized-LSBDataEmbedding", *IEEETransaction on Image Processing*, Vol. 14, No.2, Feb 2005, pp. 253-266.Sandton, South Africa, 2005.
15. Alain Brainos, "A Study of steganography and the Art of Hiding Information", *SecurityWriter*,July 27, 2004.
16. Chip Fleming, 'A tutorial on convolutional coding with Viterbi algorithm',2003.
17. Der-Chyuan Lou and Jiang-Lung Liu,"Steganographic Method for Secure Communications", *Elsevier Science Ltd*, Vol21, No 5, 2002, pp 449-460.
18. Simon Haykin, 'Communication Systems', 4th edition, John Wiley & sons, Inc. 2001.
19. John G. Proakis, 'Digital Communications', Mc.Graw Hill, 4th edition, 2001.
20. Petitcolas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking.", 2000
21. Krinn, J., "Introduction to Steganography", 2000
22. S. Katzenbeisser, Fabien A.P. Petitcolas,*Information Techniques for Steganography and Digital Watermarking*, Artech House, Boston,London, 2000.
23. Charon Langton, Coding and decoding with conventional codes', July 1999.
24. Westfield Andreas and Andreas Pfitzmann, Attacks on Steganographic Systems, *Third International Workshop, IH'99 Dresden Germany*, October Proceedings, Computer Science 1768, 1999, pp. 61-76.
25. N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen," *IEEE Computer*, February 1998, pp.26-34.
26. Memon, N. and Rodila, R. ,"Transcoding GIFimages to JPEG-LS", Consumer Electronics,IEEE Transactions on Consumer Electronics,Vol. 43, Issue 3, Aug 1997.
27. Raymond Steel, ' Mobile radio communication',Raymond Steel Publishers, London edition,995.
28. Jacques Dupraz, 'Théorie du signal et transmission de l'information', Eyrolles édition,1989.
29. J.C. Bic/ D. Duponteil., J.C. Imbeaux,'Eléments de communications numériques.Transmission sur fréquence porteuse'. Dunod edition, 1986.
30. J.C. Fantou, 'Théorie de la transmission numérique', édition, 1977.
31. J. Clavier, M. Niquil, G. Coffinet, F.Behr 'Théorie et technique de la transmission de des données', Tome1, Masson, Paris édition, 1972.
32. Manjeet Singh,Ian J. Wassel 'Comparison between Soft and Hard decision decoding using quaternary convolutional encoders and thedecomposed CPM model', Laboratory for communications Engineering, Department of Engineering, University of Cambridge.