# Analysis of Message Authentication in Turbo Coded Halftoned Images using Exit Charts

Andhe Dharani, P. S. Satyanarayana, and Andhe Pallavi

***Abstract***—Considering *payload, reliability, security and operational lifetime* as major constraints in transmission of images we put forward in this paper a steganographic technique implemented at the physical layer. We suggest transmission of Halftoned images (*payload constraint*) in wireless sensor networks to reduce the amount of transmitted data. For low power and interference limited applications Turbo codes provide suitable reliability. Ensuring security is one of the highest priorities in many sensor networks. The Turbo Code structure apart from providing forward error correction can be utilized to provide for encryption. We first consider the Halftoned image and then the method of embedding a block of data (called secret) in this Halftoned image during the turbo encoding process is presented. The small modifications required at the turbo decoder end to extract the embedded data are presented next. The implementation complexity and the degradation of the BER (bit error rate) in the Turbo based stego system are analyzed. Using some of the entropy based crypt analytic techniques we show that the strength of our Turbo based stego system approaches that found in the OTPs (one time pad).

***Keywords***—Halftoning, Turbo codes, security, operational lifetime, Turbo based stego system.
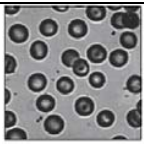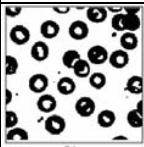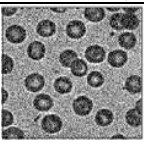
## I. INTRODUCTION

### A. Halftoning

HALFTONE imagery is bilevel imagery, which appears to have multiple grey-levels due to the microstructure [1]. Applications of Halftone imagery include active and passive color liquid-crystal displays (LCD's) (already used in notebook personal computers, and also proposed in wall-mounted displays for HDTV), & other display devices such as light-emitting diodes (LED's), electro-luminescent displays, and plasma displays, which are additive color systems using a mosaic of red, green, and blue "dots" to produce color. The data rate of an uncompressed Halftoned image is 1 bit per pixel, which is very much reduced relative to the rate of the original grayscale image (8 bits per pixel) as shown in Table I. However, large Halftoned images still require several megabytes of data to be transmitted. Data compression can be used to reduce this further.

TABLE I
COMPARISON OF INTENSITY, BINARY & HALFTONED IMAGES

| Parameter | Intensity Image | Binary Image | Halftoned Image (using random modulation) |
|---|---|---|---|
| Eg. Images |  |  |  |
| size in pixels | 265 X 272 | 265 X 272 | 265 X 272 |
| Bits per pixel | 8 | 1 | 1 |
| size in Bits | 576640 | 72080 | 72080 |
| Visual quality | Highest | Low | medium |
| Example pixels (1:3,1:5) in Fig. 2.2 | 46 46 48 56 73<br>46 46 48 56 68<br>46 46 46 55 68 | 0 0 0 0 0<br>0 0 0 0 0<br>0 0 0 0 0 | 0 0 0 0 0<br>0 0 0 1 0<br>0 1 0 0 0 |

### B. Wireless Sensor Networks

Due to its unique features of fault tolerance, rapid deployment, flexibility and low maintenance cost, the wireless video sensor network (WVSN) has been envisioned for a wide range of important applications, including battlefield intelligence, environment tracking and health monitoring. In WVSN each sensor is equipped with image/ video capture and processing capabilities and is tasked to capture digital information about the target event or situation and deliver the data to a remote control unit for further information analysis and decision making. Existing research work on sensor network mainly focus on conventional 1-D data sensors such as temperature, moisture, biochemical sensors, etc. [2] wherein the data rate is often low, data processing is simple and the energy consumption in data processing is assumed to be negligible. This is not true for image processing applications. Large data rate, high power consumption (aggravated by complex data processing tasks) and overall image quality issues are the major performance metrics. For a simulated configuration of system resources, such as ensuring a low data rate, reduced power supply consumption (at the

Andhe Dharani is with RVCE, Visveswaraya Technological University, Asst.Prof, Dept of MCA, Bangalore, India (corresponding author to provide phone: +919945309844; e-mail: dharani_ap@yahoo.com).

Dr. P. S. Satyanarayana is with BMS College of Engineering, Prof & Head Department of E & C, Bangalore India (e-mail: pss_vittala@yahoo.com).

Andhe Pallavi is head of IT department of RNSIT, Bangalore, India (e-mail: pallavi_ap@yahoo.com).

transmitter end) and lower computational capability, we propose to use Halftoned images for WVSN.

### C. Turbo Codes

In these wireless networks the transmitted data is Turbo coded as Turbo codes have been found to be well suited for low power applications and interference limited applications [3]. The nodes in a sensor network are typically battery powered and hence their limited lifetime should be optimized, which is achieved by transmitting at low powers. The Turbo coding employed enables *reliable* transmission at low SNRs (Signal to Noise Ratio).

### D. Steganography

Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file. Ensuring security is a common requirement in many sensor networks, which may range from a simple authentication to user identification. Usually message authentication is a higher layer function [4]. However due to the highly dynamic nature of wireless networks such a layered architecture is generally not followed. In this paper we demonstrate that message authentication (a form of steganography, also referred to as Digital Signature Algorithm (DSA)) [5] when performed at the physical layer using Turbo coded data (especially image data such as Halftoned images are being transmitted) consume no extra transmission bandwidth, has little performance degradation in terms of bit error rate and is very easy to implement.

In this paper we refer to this scheme as a Turbo based stego system. Specifically we intend to use halftoned images as the cover image, with the message authentication code as the secret data to be embedded. Here the authentication is used for enabling the legitimate user to confirm the source of the message and also to infer that it has not been tampered with. Where as the other receivers (unintended users) should not be aware of the authentication code also being transmitted.

The below sections provide a description of the modification required at the turbo encoder and decoder end followed by the strength analysis of the turbo based stego system.

## II. IMPLEMENTATION

### A. Turbo Encoder Revisited

A parallel-concatenated Turbo encoder employing two convolutional codes is depicted in Fig. 1(a). Each recursive systematic convolutional (RSC) code produces a systematic bit and a parity bit. The input to the Turbo code is divided into blocks, where the block size is determined by the interleaver size. The input to the second RSC is the interleaved version of the input fed to the first RSC. The output of the Turbo encoder consists of the systematic bits of the first RSC and the parity bits of both the RSCs. The systematic bits of the second encoder are not transmitted. During decoding, decoder of the

first RSC uses the systematic u and parity bit p, whereas the interleaved systematic bits and parity bit q are used by the second RSC as shown in Fig. 1(b) (extrinsic and a priori information not shown).
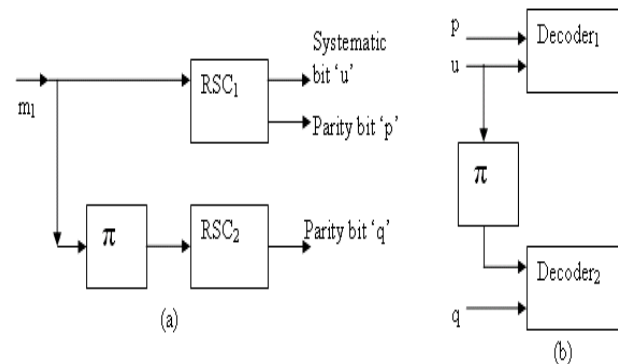


Fig. 1 a) Turbo Encoder b) Channel inputs to constituent decoders

The above described Turbo encoder and decoder are slightly modified to provide for steganography as elucidated below.

**1. Secret embedding at the encoder:** Steganography involves - the secret and the cover. The secret message (user identification data block) is to be embedded inside a cover image (Halftoned image produced direct from the sensor/mobile camera) to produce the stego image. In our technique the Halftoned image data (before being fed to the Turbo encoder) can be further compressed and forms the bits m1 (shown in Fig. 2.).

The first step in the Turbo based stego system is to pass both the secret data bits m2 and the cover image bits m1 into the Turbo encoder. The m1 bits are sent to RSC1 as shown in Fig. 2. RSC2 has a multiplexer at the input of its interleaver $\pi$ as shown in Fig. 3. The m1 and m2 bits are fed into RSC2 at a predetermined rate (say one m2 bit per every ten m1 bits represented by the m2/m1 ratio = 1/10) by the multiplexer. The EXIT charts [6] in section II.C analyze the number of m2 bits that can be embedded in m1 and its effect on the turbo encoded halftoned image.

The next few examples illustrate the embedding of m2 in m1.

Let m1(in hexadecimal) =BEB89810A5B90D7FF4D47C8D and
m2 (in binary) = 0 0 1 1 0 0 0 1 1 0 1 0 then m1 with every 8th bit replaced by m2 bits is BEB89911A4B80C7FF5D47D8C

In this example the ratio m2/m1 = 1/8. We can observe that almost every byte has its 8th bit (i.e., the LSB) changed. In general since most of the steganographic methods are based on the LSB insertion principle, in our paper we avoid having the ratio m2/m1 equal to 1/8. Instead we use other ratios such as 1/9, 1/10, etc, which give a better performance of Turbo code (in terms of BER) as compared to the 1/8 ratio and also spread the changes in the bit positions (when the bits are

viewed as bytes)(instead of the change being always at the 8$^{th}$ position). This is illustrated in the below example.

Let m1 (in hexadecimal) = 614EFAB1B41581A028DC08E0 and

m2 (in binary) = 0  1  0  0  0  1  0  0  1  0 then

m1 with every 10$^{th}$ bit replaced by the above m2 bits is 610EFAB1B41581B028DC08E0
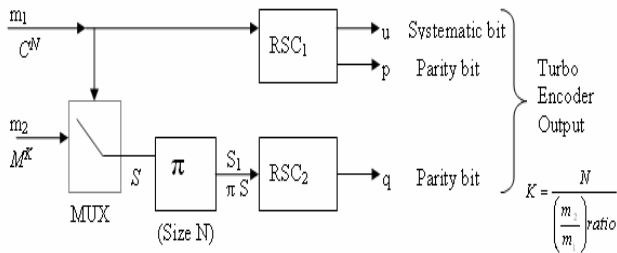


Fig. 2 Embedding of secret bits m2 in cover bits m1 with additional steganographic notations

We will use the standard terminology for steganography as discussed in [8]. Here in this paper the cover image bits m1 is represented by a random variable C, the embedded message m2 is represented by a random variable M, and the stego image bits (m1 with embedded m2 at the input of the Turbo interleaver) is represented by a random variable S. In [9] it is stated that most of the stegosystems are modeled with Eve getting her hands only on the stegoimage and is shown that there must be an uncertainty in the cover image else Eve could always tell if she had a stegoimage or a cover image. In other words, if Eve had knowledge of both the coverimage & stegoimage, it is impossible to have any sort of steganographic security (as Eve can compare both & see that something is amiss). In our Turbo based stegosystem, Eve can get both the cover image and the interleaved stegoimage (i.e., C & πS), which we will discuss later.

The m1 bits are encoded by RSC1 to produce the systematic bits u & the parity bits p. The embedded message bits (m1 with m2) is passed through an interleaver π, thereby distributing the changes in m1 due to m2 i.e., the regular pattern of change in m1 (due to m2 presence) is broken. Hence interleaving after the insertion of m2 in m1 provides an additional layer of security.

The permutation of the interleaver is kept secret between the sender and the receiver. Also the permutation of the interleaver is varied for every block according to the random variable generated by the seed (which is shared between the sender and receiver). This procedure of generating the pseudo random interleaver at the Turbo encoder and decoder ensures OTP like security for our Stego system even with Eve getting both the cover image and the interleaved stegoimage The output of the interleaver is encoded by RSC2 whose parity bits 'q' are transmitted.

The output of the Turbo encoder consists of bits u, p and q transmitted over the channel considered to be AWGN in our paper. The channel is simulated by adding randomly generated noise to the signal according to the required $E_b/N_0$. The received bits are sent to the modified Turbo decoder to extract both the cover bits and secret bits. The modified Turbo decoder is presented next.

**2. Secret extraction at Turbo decoder:** The block diagram of the Turbo decoder slightly modified to provide for secret extraction is shown in Fig. 3.

The standard Turbo decoder is modified to accept the received noise corrupted bits u, p & q from the channel and perform iterations to decode m1 & m2 bits. The operation of decoder1 during the first iteration is same as that presented in [7]. For the second decoder zeros are inserted at bit positions where m1 is replaced by m2 bits in the interleaved systematic input sequence and also at the apriori input LLR values (derived by interleaving the extrinsic LLRs of the decoder1).
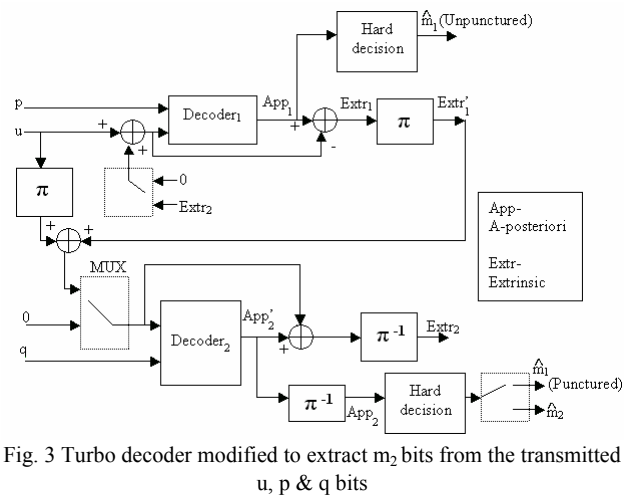


Fig. 3 Turbo decoder modified to extract $m_2$ bits from the transmitted u, p & q bits

Similar care is taken at the beginning of the second iteration (and all further iterations) of decoder1 for its apriori input values. At the output of the second decoder after the required number of iterations are over, hard decision is performed on the soft values and hence $\hat{m}_1$ and $\hat{m}_2$ bits are decoded to obtain the cover and secret bits. The $\hat{m}_1$ obtained at the output of the second decoder is punctured, i.e., zeros replace the $\hat{m}_1$ bits at $\hat{m}_2$ bit positions. Hence in the Turbo decoder modified for steganography, after the required number of iterations is over, hard decision is also performed on the a-posteriori information of Decoder₁ (App₁) to obtain the un-punctured $\hat{m}_1$ i.e., the cover bits.

*B. Simulation Results*

Simulations were carried out to determine the error performance of the Turbo based stego system. The Turbo encoder had the following parameters: RSC1 & RSC2 are

identical with the generator matrix [1, 5 / 7] and the RSC1 code is terminated. The Turbo code interleaver's permutation was randomly generated for each block of input data. The parity bits were not punctured, hence leading to a rate 1/3 code. The Turbo encoded output was BPSK modulated and added with the required AWGN noise to simulate the specified $E_b/N_0$. At the Turbo decoder end Log MAP decoding algorithm was used and the decoding was performed for eight iterations. The resulting BER was averaged over a large number of blocks (approximately 10,000 blocks). The simulations were carried out for Turbo codes with and without the secret bits and the plots of BER (for m2/m1 ratio = 1/10) versus $E_b/N_0$ for various interleaver sizes (2000 bit & 1000 bit) were obtained, shown in Fig. 4. Both m1 and m2 bits were randomly generated for the simulations. As observed from Fig. 4 the intuitive result of larger interleaver sizes resulting in a better error performance is verified. Also obtained was the performance degradation of the Turbo code with embedded m2. The degradation of around 0.5 dB at a BER of $10^{-4}$ is obtained for both 1000 & 2000 bit size interleavers.

Also the ratio of m2 to m1 bits was increased (from 1/10, 1/5 to ½) and for each value the plot of BER versus $E_b/N_0$ was simulated for eight iterations (for an interleaver size of 1000), shown in Fig. 5. These simulation results are compared with that obtained from EXIT analysis below and hence the performance of the Turbo based stego system is verified.

*C. Analysis of Turbo Based Stego System Using Exit Charts*

Now we use the EXIT analysis to verify the performance of the Turbo based stego system as obtained from simulations. EXIT charts based on evolution of mutual information [6] is used. The exchange of extrinsic information is visualized as a decoding trajectory in the EXIT chart.

Fig. 6 shows the EXIT curves of a Turbo code for the cases of without secret embedding (i.e., without m2) and with m2 (1/2 and 1/5 ratioes considered). From these generated EXIT charts for different m2/m1 ratios the BER performance and the convergence behavior of the turbo decoder is analyzed and hence the robustness of our Turbo based stego system is analyzed.

From Fig. 6 we observe that increasing the embedding rate in the Turbo based stego system leads to a decrease in the Tunnel between the decoder1 and decoder2 EXIT curves. The narrowing of the tunnel is credited due to the loss of m2 number of systematic and extrinsic bits during every iteration of Turbo decoder implementing secret (m2) extraction. It is known that systematic bits help in providing a good initial extrinsic information estimate when little a-priori information is available and if some of these systematic bits are replaced by zeros, the convergence behavior will be degraded as verified by the EXIT chart. As the ratio of m2/m1 increases, i.e., as the number of m2 bits inserted for a given m1 bit block length increases, the tunnel narrows down further. Once the tunnel completely closes, i.e., the EXIT curves touch each other or cross each other, the Turbo code fails to converge.
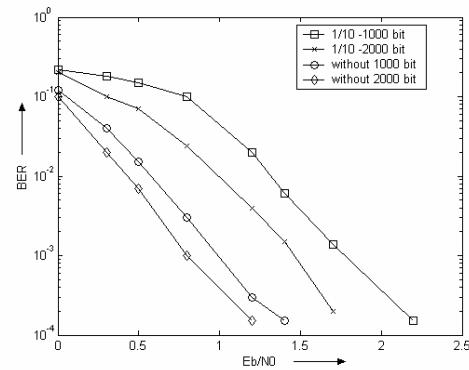


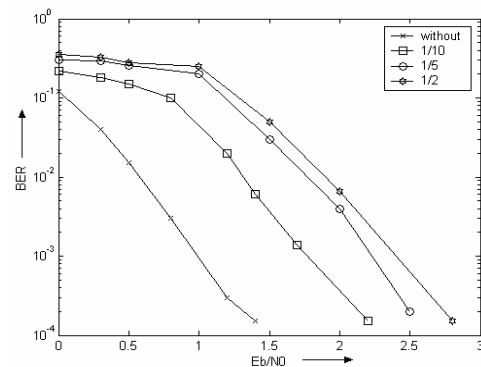Fig. 4 BER Versus $E_b/N_0$ [in dB] for various simulation conditions



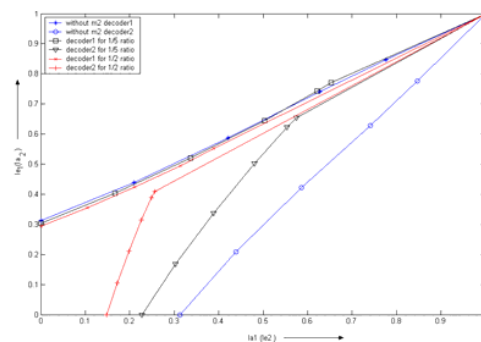Fig. 5 BER Versus $E_b/N_0$ [in dB] for various m2/m1 ratios



Fig. 6 EXIT charts for the different cases of the Turbo based stego system without m2(i.e., without secret transmission) and with m2/m1 ratioes of ½ and 1/5
(PCCC, rate = 1/3, $E_b/N_0$ = 1 dB, generator matrix at turbo encoder = [1, 5/7]interleaver size = 10,000 bits, AWGN channel with coded BER scaling)
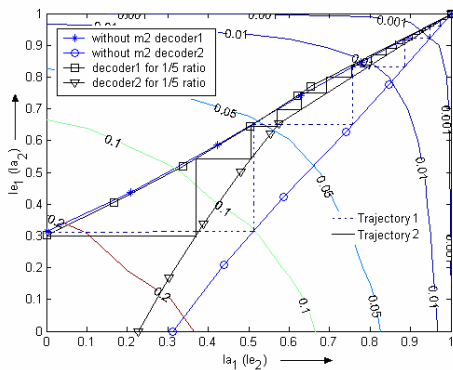
Fig. 7 EXIT chart showing the two cases of with (m2/m1 = 1/5) and without m2 with coded BER contours and decoding trajectories

Trajectory1 (dashed line) in Fig. 7 shows the decoding trajectory of the Turbo code without secret embedding. It is observed that the Turbo code reaches convergence for around three iterations for an $Eb/N0 = 1$ dB. Trajectory2 (solid line) shows the decoding trajectory of the Turbo code with secret embedding. For the same BER of 0.001 (indicated by the BER contour plot overlaid on the EXIT chart), it is observed that Turbo decoder implementing steganography requires considerably more number of iterations (around eight) as compared to the three iterations required by the standard Turbo decoder. This is due to the narrowing of the Tunnel in the EXIT chart.

### D. Strength of the Turbo Based Stego Model against Malicious Attacks

The attack considered here is one wherein the attacker may influence the coded message but has otherwise no access to the encoding and decoding functions. The attacker may change some of the transmitted bits before it reaches the receiver. Some of the bits may be flipped (i.e., a 1 may be made a 0 or vice versa) or may be totally erased. Usually this attack will not tamper with a large amount of data, as it is easily detected at the decoder end. The small amount of tampering can be modeled as channel noise (performance in terms of BER presented in section II.B) and our stego system based on Turbo codes at the decoder end is capable of rectifying this tampering. Hence our stego system based on Turbo codes is resistant to the malicious attacks.

### E. Advantages of Our Turbo Based Stego System over Conventional Steganographic Methods

The main disadvantage of conventional steganographic methods such as LSB insertion methods is that it requires a lot of overhead to hide a relatively few bits of information. Also once the system is discovered it becomes virtually worthless. The sender and receiver must share a common cover carrier beforehand. If the steganalyst (also called Eve) ever gets two stego images created with the same cover image, he can easily detect the message.

These problems have been overcome in the Turbo based Stego system which has the following features:

The insertion method depends on a key (i.e., the permutation of the interleaver). This key can not only be changed during every use / session, but its length can also be varied, making the detection tougher for the steganalyst.

The secret is embedded in a cover carrier, which is also a part of the data being communicated between the sender and receiver. As mentioned earlier, the cover carrier is our halftoned image. The sender and receiver need not share the cover carriers earlier; rather the cover carrier being transmitted through bits u & p (Fig. 1) and the stego image through the bits q solves this problem. This method increases the amount of usable communicated data and also the robustness of the stego system.

The Turbo code basically an error control code decodes the insertion/deletion errors introduced during transmission, whereas with say for example the plain LSB insertion steganography, this is not available.

### III. IMPLEMENTATION ISSUES

The strength of the Turbo based stego system approaches that found in OTP as detailed above. This is similar to the disadvantages found in OTPs wherein to communicate P bits of data, the sender and receiver should share K (>P) bits of secret key before hand and also a new key needs to be generated and communicated over a secure channel for every Halftoned image that is going to be sent. This creates a severe key management problem that has limited the use of the OTPs in commercial applications. However the OTPs has been employed in military and diplomatic contexts where unconditional security may be of great importance.

Our Turbo based Stego system can be easily implemented in many of the nodes that implement the 3GPP/4GPP standard. The 3GPP standard specifies the Turbo code to be used completely in all respects. Some of these specifications include the length of the interleaver which can be varied from block to block of data being transmitted, which can change from as low as 40 bits to 5114 bits. This has already being implemented in many of the Turbo cores brought out by Xilinx, Altera, etc. Hence in our Turbo based Stego system the sender node and receiver node have to securely communicate only an initial seed. This seed generates random numbers which will select an entry from the Table of permutations already inbuilt in the 3G devices. Hence our Turbo based stego system with a security approaching that of the OTPs are easily implemented commercially.

### IV. CONCLUSION

In retrospect, the Turbo code interleaver permuting the stego data before convolutional coding provides an additional layer of security. Varying the size and permutation of the interleaver enhances the appeal of the Turbo codes for implementing steganography. This scheme of joint channel coding and security using the basic architecture of parallel-

concatenated Turbo Codes though provides data secrecy, has a slight degradation in the BER performance of the Turbo encoded cover carrier. This degradation increases as the secret embedding rate is increased. But if the cover carrier is a general image or voice, this slight degradation in the performance can be tolerated when compared to the OTP like security available for the secret transmission. Our Turbo based stego system can easily be implemented on the latest adaptive devices [10] and are light weight (i.e., do not require extensive algorithms, proprietary software (may contain backdoors [11]).

REFERENCES

[1]  Jonas Gomes, Luiz velho, "Image processing for computer graphics", Springer Verlag, NewYork, 1997.
[2]  Zhihai He and Sanjit K. Mitra, "From rate-distortion analysis to resource distortion analysis", IEEE Circuits and systems magazine, vol.5, Number 3, Third quarter 2005, pp 6-18.
[3]  Claude Berrou, Bretagne, "The Ten-Year-Old Turbo Codes are Entering into Service", IEEE Communications Magazine, August 2003, pp110-116.
[4]  William Stallings: "Cryptography and network Security- principles and applications", Second Edition, Pearson education Inc.
[5]  Bruce Schneier: "Applied Cryptography", Second Edition, John Wiley & Sons, Inc.
[6]  S. ten Brink: "Convergence behavior of iteratively decoded parallel concatenated codes", IEEE Trans. Inform. Theory, vol. 49, Oct. 2001, pp. 1727-1737.
[7]  Jason P Woodard and Lajos Hanzo: "Comparative study of turbo decoding techniques: an overview", IEEE Trans. on vehicular technology, vol. 49, No. 6, Nov 2000, pp 2208-2233.
[8]  B. Ptzmann, "Information Hiding Terminology", First International Workshop on Information Hiding, Springer-Verlag, vol. 1174 of LNCS, 1996, pp. 347-350.
[9]  J. Zollner, H. Federrath, H. Klimant, A. Ptzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the Security of Steganographic Systems", Second International Workshop on Information Hiding, Springer-Verlag, vol. 1525 of LNCS, 1998, pp. 344-354.
[10] Thomas Wollinger, Jorge Guajardo and Christof paar, "Security on FPGAs: State-of-the-art implementations and attacks", ACM Transactions on Embedded Computing Systems, Vol. 3, No. 3, August 2004, pp. 534-574.
[11] Bruce Schneier, "Applied Cryptography", John Wiley & Sons, Inc., Second Edition, 2001.