J Med Syst (2010) 34:1129–1139
DOI 10.1007/s10916-009-9332-3

ORIGINAL PAPER

Reliable and Robust Transmission and Storage Techniques for Medical Images with Patient Information

Myagmarbayar Nergui · U. Sripati Acharya · Rajendra Acharya U · Wenwei Yu

Received: 2 April 2009 / Accepted: 10 June 2009 / Published online: 2 July 2009

Abstract There is an increased emphasis on the use of digital techniques in all aspects of human life today. Broadcast radio and television, cellular phone services, consumer and entertainment electronics etc are increasingly using digital signal processing techniques to improve the quality of service. Transmission and storage of documentation and images pertaining to patient records cannot remain an exception to this global trend. Hence, patient records (text and image information) are increasingly stored and processed in digital form. Currently, text and image information, which constitute two separate pieces of data are handled as different files. Thus, there is a possibility of the text and message information, pertaining to different patients, being interchanged and thus mishandled. This can be avoided by merging text and image information in such a manner that the two can be separated without perceptible damage to information contained in either file. Digital watermarking techniques can be used to interleave patient information with medical images. In this work, we have employed digital watermarking along with strong cryptographic protocols and powerful error correcting codes. This reduces the probability of sensitive patient information falling into the wrong hands and ensures information integrity when it is conveyed over noisy channels.

Keywords Digital watermarking · Reed–Solomon codes · Turbo codes · Advanced Encryption Standard (AES) · Additive White Gaussian Noise (AWGN)

M. Nergui · U. S. Acharya
Department of Electronics & Communication,
National Institute of Technology Karnataka,
Surathkal, India

R. Acharya U (✉)
Department of ECE, Ngee Ann Polytechnic,
Singapore, Singapore
e-mail: aru@np.edu.sg

W. Yu
Graduate School of Medical System Engineering,
Chiba University,
Chiba 263-8522, Japan

Introduction

Patient information and medical images constitute a large chunk of the data generated in hospitals and health care centers. Increasing use of electronic diagnostic instruments contributes to the increase in the volume of data that has to be processed and stored. It is of utmost importance to organize patient information and medical images securely, so that they do not fall into wrong hands or are distorted due to imperfections of the storage or transmission media. The current practice is to enter patient details in a separate text file during admission, which is updated during every subsequent examination. The patient (text) information and all medical images are saved under the patient name or hospital number as an identity. The medical images are stored separately in a standard file format. If the identity of the file is lost, then it becomes difficult to map this image to the correct patient. Further, these data are not protected against unauthorized access. Hence, secure and reliable handling of patient information has to be given highest priority. Digital Imaging and Communication in Medicine (DICOM) [1, 2] is a standard file format for transmission and storage of medical images in health care centers, the DICOM image format utilizes its header to store relevant patient information. This ensures that the image is never mistakenly separated from patient information. Most of the data management systems currently in place in hospitals are

based on DICOM standard [1, 2]. This system suffers from two weaknesses. Firstly, no attempt is made to protect sensitive patient information from being accessed by unauthorized personnel. Secondly, no attempt has been made to protect the integrity of information during transmission over imperfect channels or during storage in imperfect media. In this paper, we wish to propose a solution to these two lacunae in the DICOM standard. We propose the use of cryptographic protocols to preserve information security (prevent it from falling into the wrong hands) and the use of Error Control Codes (ECC) to protect information integrity.

Digital Watermarking Technologies [3–10] can be used to hide demographic information into image data. Digital watermarking is used in various applications such as copyright protection and authentication of intellectual property. Using this approach, text information, such as patient history and diagnosis can be hidden into the respective medical image [11–13]. The information, to be camouflaged, is embedded into another piece of data, which is referred to as cover data. Cover data is usually selected, so as to be innocuous. The cover data can be audio, image, or video. Care is taken to ensure that neither piece of information is perceptually distorted as a result of this watermarking. Thus, digital watermarking technique can be used to embed patient information into image data. This gives rise to a composite block of data containing both image and hidden text information. This composite block of data is processed by cryptographic algorithms and error control codes to ensure information security and integrity.

Watermarking can be done in two major domains namely, spatial domain and frequency domain. The spatial domain method employs least significant bit (LSB) insertion [4, 5, 7, 8]. The LSB of each pixel value of the image is replaced by one bit of the ASCII character set representing the information to be watermarked. In this way, all the information that needs to be watermarked is inserted into the LSB of successive pixels in the image. Text information with 192 kb of data can be watermarked into a 256×256 digital color image. The mean square error between the original image and the watermarked image is so small that the human eye is not able to detect the distortion. The second category is frequency domain watermarking [5, 7, 9], where the watermarking is done in the transform domain. The redundant frequency content, which is associated with the image, is replaced with characters from the text file. In this approach, watermarking can be accomplished using Discrete Fourier Transform (DFT), Discrete cosine Transform (DCT), or the Discrete Wavelet Transform (DWT). As diagnosis records often contain sensitive and private information, a cryptographic algorithm namely, Advanced Encryption standard (AES) [14, 15] is employed to secure patient information from falling into wrong hands. This algorithm is very robust and is considered to be safe against attacks by hackers.

It is well known that information flowing across a communication channel can be disturbed by several impairments. This is because of non-idealities in the channel and receiving equipment. The physical channel attenuates the transmitted signal and introduces noise. Attenuation is caused by energy absorption and scattering in the propagation medium. This effect is called “free space loss” in satellite communication terminology and can exceed 200 dB on a 14/12 GHz geosynchronous satellite channel [16]. In mobile radio applications, the attenuation is not fixed but tends to fluctuate with speed of the vehicle, geometry of the surrounding buildings and terrain. Buildings, mountains and vegetation can cause a signal moving from one point to another to take several different paths. As these paths may have different lengths and may offer differing degrees of attenuation, various copies of the signal may interfere with each other constructively or destructively, depending upon the location of the receiver. If the receiver is moving, it will see a series of energy crests and troughs, whose frequency of occurrence depends on vehicle speed. Such communication channels are called “multi-path fading channels”. Hence, we conclude that communication channels are not perfect and can often deliver data that has been corrupted during the process of transmission.

In 1948, Shannon [17] demonstrated that by proper precoding of information, errors induced by a noisy channel could be reduced to any desired level without sacrificing the rate of information as long as information rate is less than the “capacity” of the channel. The discipline of Error Control Coding (ECC) emerged as a result of attempts to find practical techniques to realize the promise of this theorem. In the last sixty years, ECC has emerged as a powerful tool to protect information integrity as it flows over communication channels or is stored in storage media. It can often provide the difference between an operating communication or storage system and a dysfunctional one. It has been a significant enabler in the telecommunications revolution, the internet, Digital recording, and space exploration [18]. Every Compact disk, CD-Rom and DVD employ codes to protect data embedded in them. In fact, the working of these systems and devices would be severely compromised without the use of ECC. ECC algorithms are applied in the data link layer and their primary goal is to improve the reliability of the physical communication channel.

The patient information is encrypted (using the AES algorithm) before being embedded into the medical image. The composite block of data comprising of text information

and image is encoded using ECC algorithms. This is done to enhance data security and integrity. We have used Reed–Solomon (RS), and Turbo Codes in our study. To quantify the improvement provided by this scheme of coded data transmission over uncoded data transmission, we determine the Bit Error Rate (BER) at the receiver, for coded and uncoded transmission over an AWGN channel by using Monte-Carlo techniques. The same image (with embedded text information) is communicated over a simulated AWGN channel by using Monte-Carlo techniques with and without the ECC. The BER values at various values of SNR are obtained and plotted. The Coding gain is determined from this plot. The Coding Gain offered by a code is a measure of the reduction in the SNR required to achieve a given BER as compared to uncoded transmission. Thus, the Coding Gain serves to quantify the improved information integrity provided by use of the ECC.

The paper is organized in the following manner. In the following section, we discuss the encryption algorithm and the digital watermarking technique used for providing security and data hiding features. In 'Error control coding', we discuss salient features of the ECC techniques and interleavers used in this work. In 'Results', we present the simulation results that quantify the effectiveness of these schemes in combating the effect of imperfections in channels. 'Discussion' discusses. Finally, the paper concludes in 'Conclusion'.

Figure 1a and b show the block diagrams of the proposed transmission and receiver arrangement, respectively.

Encryption and watermarking of text information

The information, to be stored, is encrypted before watermarking to enhance the security. A highly secure algorithm called Advanced Encryption Standard (AES) [14], has been used for encrypting the text. This algorithm is also called as Rijndael algorithm, has been designed by John Daemen and Vincent Rijmen [14, 15].

The process of encryption converts data (Plain text) to an unintelligible form called Cipher text. Encrypted information is embedded in the image using watermarking techniques. This composite piece of information is coded with an appropriate ECC algorithm and conveyed across the channel. At the receiver, ECC algorithms are used to correct the effects of channel impairments on the composite data. Then the text (patient diagnosis) information is extracted and decrypted to convert it back to its original form (Plain text). AES is a capable of using cryptographic keys of 128, 192, and 256-bit length to encrypt and decrypt data in blocks of 128 bits.

The Rijndael algorithm for AES offers a combination of security, performance, efficiency, ease of implementation, and flexibility. Specifically, the Rijndael algorithm appears to be consistently a very good performer in both hardware and software across a wide range of computing environments regardless of its use in feedback or non-feedback modes. Its key setup time is excellent, and its key agility is good. The very low memory requirements of the Rijndael algorithm make it very well suited for restricted-space environments, in which it also demonstrates excellent performance. The amount of security that it offers is quantified by the time and computational power required to break the cipher by brute-force techniques. AES is one of the most popular algorithms used in symmetric key cryptography. AES is the first publicly accessible and open cipher approved by the National Security Agency for top-secret information transmission. In this paper, we have employed AES algorithm. Cryptographic key of 256 bits was used to encrypt and decrypt data in blocks of 128 bits of data.

Figure 2a and b show the original patient data and encrypted data, respectively.

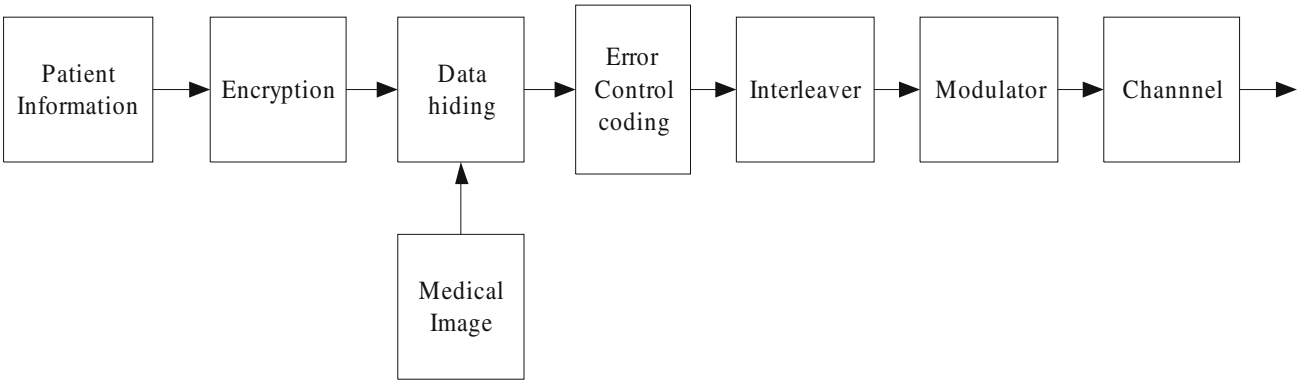
Digital watermarking technique

Digital watermarking is the process of embedding information into a digital signal (called cover data). For example, the signal may be audio, pictures or video. If the signal is copied, then the information is also carried in the copy.

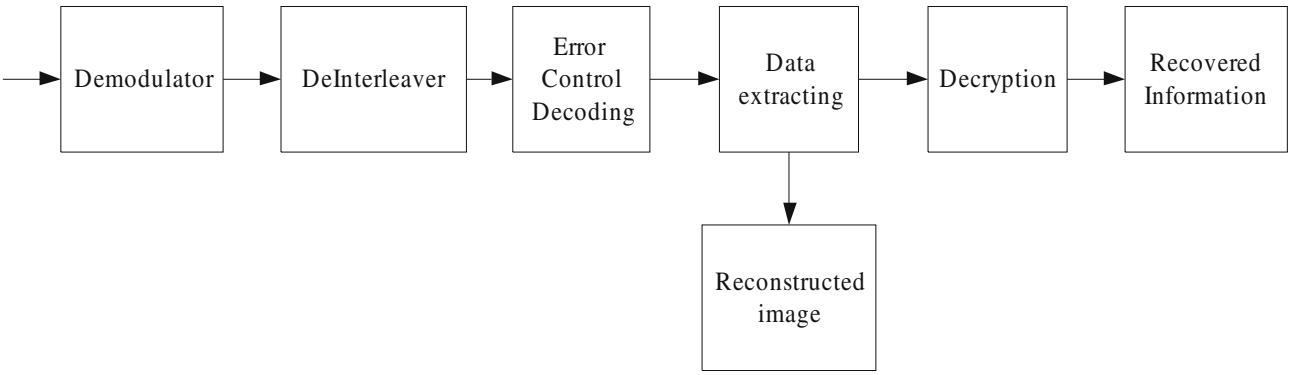
Digital watermarking can be classified into two categories, namely visible and invisible watermarking. In visible watermarking, the information is visible in the picture or video. Typically, the information is a text or a logo, which identifies the owner of the media. In invisible watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such. Important applications of invisible watermarking are copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media.

Steganography is an application of digital watermarking, where two parties communicate a secret message embedded in the digital signal [3]. Digital watermarking provides means of embedding a message as into cover data without distorting its identity. So, this technique can be used for compact storage or transmission of text information and still images.

We show an original medical image in Fig. 3a and a watermarked or an embedded image, which contains patient information, using a LSB insertion watermarking technique in Fig. 3b. No distortion in image of Fig. 3b is discernible to the eye. Each pixel in a medical image containing color information is represented using 24 bits.



a. Block diagram of the proposed transmission arrangement.



b. Block diagram of the proposed receiver arrangement.

Fig. 1 **a** Block diagram of the proposed transmission arrangement. **b** Block diagram of the proposed receiver arrangement

Error control coding

It is a common observation that communication channels and storage media are not perfect and introduce errors in the data processed by them. Error detecting and correcting codes (ECC) are widely used to mitigate the errors introduced by imperfect channels and storage media. This is accomplished by adding controlled amount of redundancy into the messages produced by information. This redundant information can be used to detect and correct errors introduced into the information content. Thus, with the protection provided by ECC schemes, original information can be recovered from data corrupted by channel noise or imperfect storage media. ECC techniques have become ubiquitous today and are employed in securing deep space communications as

Fig. 2 **a** An original patient information. **b** An encrypted patient information

KMC HOSPITAL, MANIPAL, MANGALORE
Patient Name: Ashok
Hospital No 8970987
Name of the Doctor. Dr Rao
Age: 40 years
Address: Manipal
Case history:
Date of Admission: 20.08.2008
Results: T wave Inversion
Diagnosis: Suspected MI
Treatment: Sublingual Nitroglycerin

a. An original patient information

²ÕÉ¾"=ÚG¬Þ4»JD¬xÑ¡×7ÓÕÃ÷
Ëü→−äÂ→s↕ðÁ³½Úê¦¼ÅLô?xÎK┤↕ᴛ=k→ß¦Ù,
Y→&ô◀¾
ë→åùC=ëM←9→ÄUú−ÌüBaØ:S→Ë→Ìõj+ºû©§1la
Ð!é
→gæ^¬¤→L¿¬vSh]→Ð¦4J"@)|Mã→→¢Åÿèc¯á→Çx
¡ãí→6j→t|→ÙÔÓU`@ÇX¥Â→ÿçÄ&1→ËÙFò×D
PWþ"→→┐!V¥ÃÚ→µÊ ÷ð¾h'¡.ÿ,ƒ·tÁ2→ò¾→→áòí¢
q→üƒdj↑→ùÜ'õ←ðÃA
Ì`e¾x/¶áé→┤Ù¹ *¹G┴y.┤²¨^→DÙ"/FÉæ→Añ<½
ç→Z$~ºÈ┤↕EøcÕ┌(ë
J→=º»ù(◀·ZÜ→~→xBBÃ [→┌WÊ{oÑytõÚûÅ0

b. An encrypted patient information

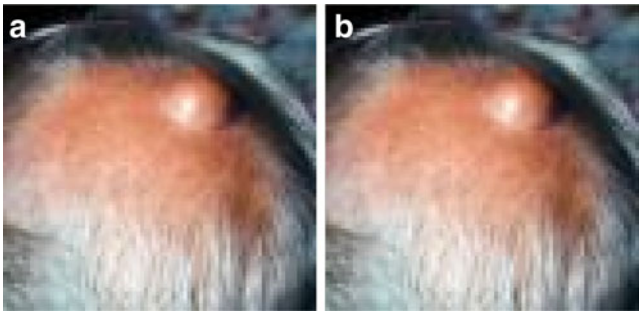


Fig. 3 **a** An original medical image. **b** A watermarked/embedded medical image

well as optical and recording media. It would not be an exaggeration to say that many of the communication gadgets that we take for granted in modern life would not exist in their current forms if the discipline of ECC did not exist. The encoding/decoding operations are performed in the data-link layer. These techniques are primarily used to improve the reliability of the physical channel.

Communication channels and storage media can introduce many different types of errors. Hence, many classes of ECC have been designed to tackle different types of impairments [16, 18–22].

Error control codes are classified into two broad types, namely Block codes and Trellis codes, depending upon their structure. Reed–Solomon (RS) codes and Turbo codes are examples of Block codes and Trellis codes, respectively, which have found widespread application. In our study, we have employed RS codes and Turbo codes to enhance the reliability of transmission and storage of watermarked medical images. A comparative study of their abilities is quantified by computing the Bit Error rate (BER) as a function of the Signal to noise ratio (SNR) after using the code to correct errors. The BER is defined as the ratio of the number of bits received in error to the total number of bits conveyed in a given time slot. Thus, it is an objective measure of the capability of the code to protect information against channel/storage media induced disturbances. We have chosen the AWGN channel model in our simulations for reasons of simplicity. We have also considered the possibility of signal strength variation at the receiver by considering channels where the SNR varies randomly with time. Such variation in signal strength is characteristic of fading channels. The performance of RS codes over such channels is illustrated in Fig. 6.

Reed–Solomon (RS) codes are block-based error correcting codes with a wide range of applications in digital communications and storage. The RS encoder takes a block of information bearing symbols and adds additional redundant symbols. These redundant symbols depend on the information content of the message. The encoder outputs a codeword containing information and redundant symbols. The codeword is modulated so that it can be efficiently propagated across the channel or stored efficiently in the storage medium. At the receiver, the attenuated and corrupted version of the transmitted codeword is received and is processed by the RS decoder. The decoder attempts to detect and correct errors introduced by the channel/storage media in order to provide the user with reliable information. RS codes have a number of properties, which have resulted in their widespread deployment. In particular, RS codes are Maximum Distance separable (MDS) codes [16, 18–23].

A Reed–Solomon code is specified as a (n, k) RS code over $GF(q^m)$. This means that the encoder takes k data symbols of m bits each and adds $n–k$ parity symbols to make an n symbol codeword. There are $n–k$ parity symbols of m bits each. The MDS property implies that for a given value of n and k, RS codes possess largest possible minimum distance $d_{\min}$. RS codes constitute a subclass of linear systematic block codes. The basic building block of RS codes is a symbol consisting of m bits where m is a natural number and $m \geq 2$. For a given value of m, the natural length of a RS code composed of m bit symbols is 2^m-1. For example, if $m=8$, each symbol is 8 bits wide, each codeword has $2^8-1=255$ symbols and the arithmetic has to be performed over $GF(2^8)$. Some salient properties of RS codes are [16, 18–23],

- Code length: $n = q^m - 1$
- k data symbols, with each symbol being represented by m bits.
- Minimum distance: $d_{\min} = n - k + 1$
- Code rate$=k/n$
- Error correcting capability: $t = \left[\frac{n-k}{2}\right]$

Turbo codes

Shannon's noisy channel coding theorem [17] has established that it is possible to communicate information over a noisy channel with arbitrarily small probability of error as long as the rate of information transfer is less than the channel capacity C. The channel capacity is a function of the SNR and bandwidth of the channel. Further, he has calculated a lower bound on the minimum value of SNR required for sustaining a given rate of information transfer with arbitrarily small probability of error. This is known as the Shannon limit. An error control code is deemed powerful if it approaches the Shannon limit in performance.

The development of Turbo codes in 1993 [24] represented a very important breakthrough in the development of channel codes. Until their advent, most code designs fell far

short of achieving the performance promised by Shannon's channel coding theorem. Turbo codes are capable of achieving near Shannon capacity performance. However, iterative approaches for decoding Turbo codes increase the decoder complexity and introduce large decoding delays. Traditional code designs, like BCH and Reed Muller or algebraic code designs, have a great deal of algebraic or topological structure, which is used to guarantee good distance properties and decoding algorithms for the code. Turbo codes possess random like properties as originally envisaged by Shannon with just enough structure to allow for an efficient iterative decoding method. For any code rate and information length greater than bits, turbo codes with iterative decoding can achieve BER as low as at SNRs within 1 dB of the Shannon limit. Turbo codes are composed of two or more simple constituent codes along with a pseudo random interleaver. At the decoder, soft in–soft out (SISO) decoders for each constituent code are employed in an iterative manner in which the soft output values of one decoder are passed to the other and vice versa until the final decoding estimate is obtained [25]. We have employed a simple Turbo code to ensure information integrity as it is conveyed over imperfect channels. The results obtained by using Turbo codes in this application are shown in Fig. 8.

Results

Patient information is encrypted and then embedded into the image by digital watermarking. After that, the image with embedded information is converted into a bit stream and coded using a suitable error control code. We assume that the channel modulation scheme is Binary Phase Shift Keying (BPSK). These symbols are then transmitted through a simulated channel corrupted by AWGN noise. The objective is to measure the quality of the extracted text data and reconstructed image, bit error rate (BER) and symbol error rate (SER) are evaluated as a function of SNR after decoding the received noisy image from the channel output. Figure 4a–g allow us to visually judge the difference between the image and patient data as recovered over an AWGN channel with 10 dB SNR and the same information after being processed by the (15, 11) RS code. It is seen that there is a dramatic improvement in the quality of the image as well as text data. The robustness and reliability of the transmission system is demonstrated for two types of ECC schemes namely, Reed Solomon and Turbo codes.

In Fig. 4a, we show the original medical image. In Fig. 4b the original patient information (text), information that has to be embedded is shown. In Fig. 4c we show the

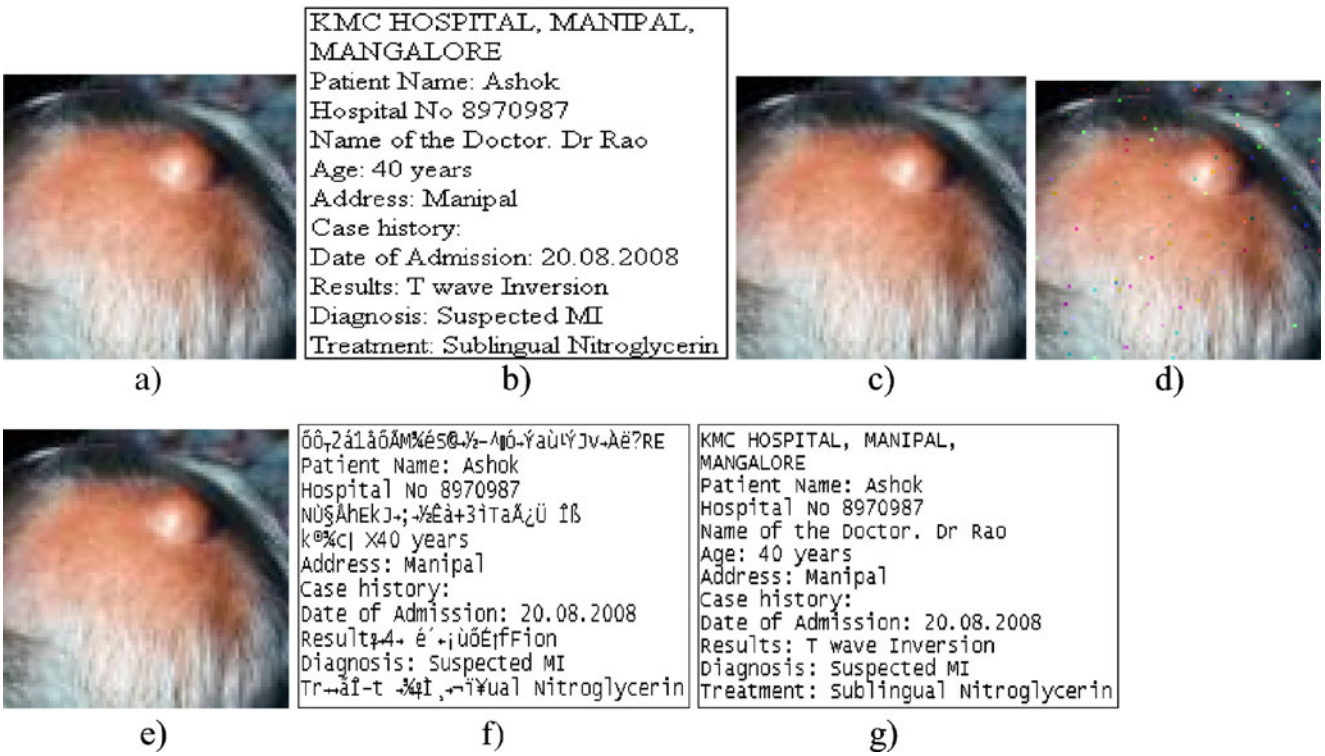


Fig. 4 **a** An original medical image. **b** Original patient information (text). **c** The image after embedding data. **d** Noise corrupted embedded image (image+text) for 10 dB SNR. **e** The image after recovery with ECC for 10 dB SNR. **f** Noise corrupted patient information for 10 dB SNR. **g** Patient information after recovery with ECC for 10 dB SNR

image after embedding text data. Noise corrupted embedded image (image+text) with 10 dB SNR as obtained at the receiver before decoding is shown in Fig. 4d. The image after recovery with ECC (10 dB SNR) is shown in Fig. 4e. Noise corrupted patient information (10 dB SNR) is shown in Fig. 4f. Patient information after recovery with ECC (10 dB SNR) is illustrated in Fig. 4g. In this paper, we used (15, 11) RS code over $GF(2^4)$. This means that the encoder takes *11* data symbols of *4* bits each and adds parity symbols to make a *15* symbol codeword. There are four parity symbols of 4 bits each.

Minimum distance of $(15, 11)$RS code is $d_{\min} = n - k + 1 = 15 - 11 + 1 = 5$
Code rate $= 11/15 = 0.7333$

The Primitive polynomial corresponding to the Galois Field $GF(2^4)$ is x^4+x+1. The generator polynomial of (15, 11) RS code has been computed by employing design rules for RS codes and is equal to $x^4 + \alpha^{13}x^3 + \alpha^6x^2 + \alpha^3x + \alpha^{10}$ where α is a primitive element of the field $GF(2^4)$. This ECC can correct up to a maximum of two symbols in error within a length 15-symbol codeword. In a fading channel affected by burst errors, errors tend to occur in bursts rather than in random patterns. Interleaving is a simple but effective technique to increase the burst error correcting capability of an error control code. An *interleaver* is a device that rearranges the order of the symbol sequence in a deterministic manner. Associated with the interleaver is a *deinterleaver* that applies the inverse permutation to restore the original sequence. Block interleaver is the simplest and the most commonly used interleaver in communication systems. The data stream is written into the interleaver row wise and the interleaver contents are then read out by columns. In this paper, we used a block interleaver to improve the burst error correction capability of the (15, 11) RS code.

The plots in Fig. 5a and b show the performance of (15, 11) Reed Solomon code during medical image transmission in the form of BER (bit error rate) plot and SER (symbol error rate) plot respectively. It can be observed from the first plot that the (15, 11) RS code gives a coding gain in excess of 2.5 dB at a BER of 2×10^{-6}. A similar observation can be made from the second (SER) plot as well. The significance of this plot is that with the use of the RS code, we can ensure that on average only two bits in every 10^6 transmitted bits are likely to be in error. Studying the plot, we conclude that for uncoded transmission, the BER would rise to approximately 10^{-4}. This means that on an average there would be one bit in error for every 10^4 bits conveyed. Thus, the use of RS code has resulted in an increase of information integrity. These results are comparable to those found in literature. In the chapter on Block code performance analysis in [22], Wicker has given a plot of the probability of decoder error (essentially symbol error rate) as a function of SNR for a (31, 27) two error correcting error control code. It is observed that the symbol error rate is approximately 10^{-5} at a SNR of 8 dB. Our simulation with the (15, 11) RS code indicates a symbol error rate of 10^{-5} at 10 dB SNR.

RS codes are well suited for correction of burst errors. Hence, we decided to check the performance of these codes over time variant channels. Propagation conditions in these channels vary unpredictably with time. This means that there are time intervals during which propagation conditions are good and the channel introduces very few errors. The channel can make a sudden transition from this good state to a bad state where a very large number of errors are

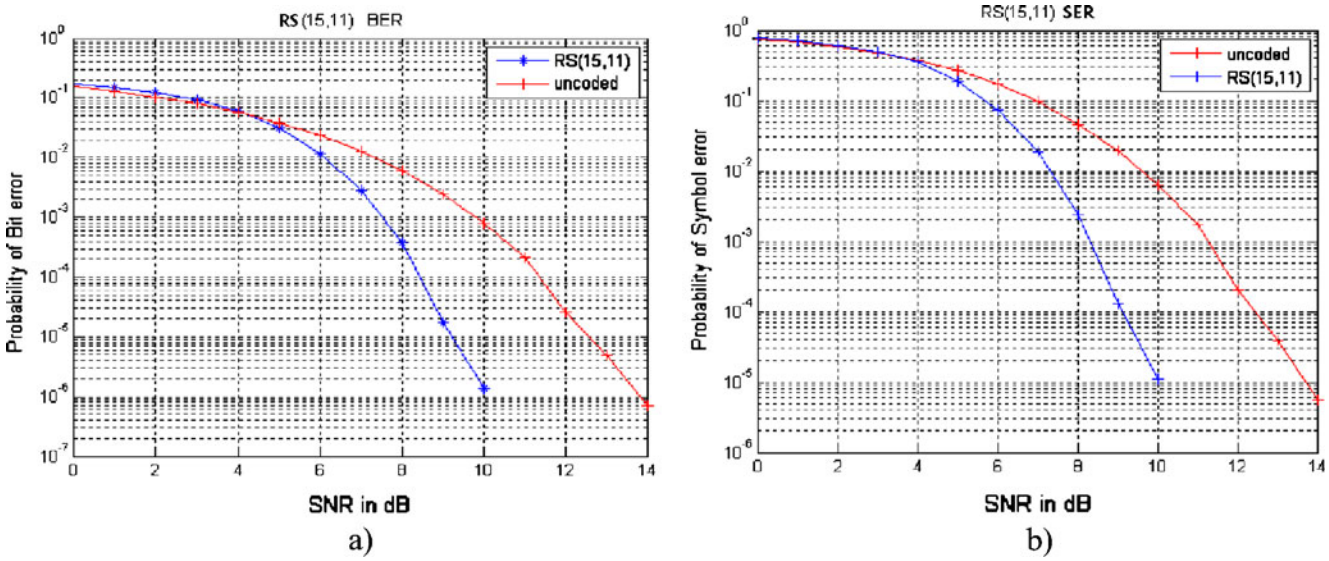


Fig. 5 Performance of (15, 11) Reed Solomon code with block Interleaver during transmission of medical images over channels corrupted by AWGN noise

introduced and hence almost all transmitted symbols are received in error. Such errors are referred to as burst errors in fading channels. To check the performance of RS codes over such channels, we carried out simulations by varying the SNR on the channel in a random manner. The channel SNR was varied over ten values ranging between 10 dB (representing high SNR) to 0 dB (representing poor SNR). The performance of the RS code is documented in the form of the bit-error rate plot and the symbol–error rate plot in Fig. 6. We observe an improvement of the order of about 4 dB at a BER of 10^{-5}.

Use of Turbo codes for medical information transmission

After studying the performance of the (15, 11) RS code, we have considered the use of a Turbo code. We have used the Turbo code encoder shown in Fig. 7a. Turbo code encoder employs two identical systematic recursive convolutional (RSC) encoders connected in parallel with an interleaver preceding the second recursive convolutional encoder. The information bits are encoded by both RSC encoders. The first encoder operates on the input bits in their original order, while the second encoder operates on the input bits as permuted by de interleaver. The rate of a Turbo code can be altered by the use of puncturing [21]. We have demonstrated results for the original rate 1/3 Turbo code and the punctured rate 1/2 Turbo code in this paper.

Figure 7b shows an RSC encoder, which is used in the Turbo encoder. u_k is an input information bit, c_k is the coded output symbol.

A systematic convolution code is generated by passing the information sequences, to be transmitted, through a linear finite-state shift register. The Interleaver used in the Turbo codes plays a major role in the performance of the Turbo codes. In this paper, we used the pseudo random interleaver. This is because the pseudo random interleaver has been proved to be optimum [26].

Puncturing and Multiplexing is the process of deleting some bits from the codeword according to a puncturing matrix. It is usually used to increase a given code rate. The same decoder architecture can be used with normal and punctured Turbo codes with some modifications. A block diagram of the decoding algorithm is shown in Fig. 7c. The process of Turbo code decoding starts with the formation of *a posteriori probabilities* (APPs) for each data bit, which is followed by choosing the data-bit value that corresponds to the *maximum a posteriori* (MAP) probability for that data bit [25]. Upon reception of a corrupted code-bit sequence, the process of decision making with APPs allows the MAP algorithm to determine the most likely information bit to have been transmitted at each bit time.

A logarithmic ratio of the a posteriori probability of u_k, conditioned on the received signal y, is defined as

$$L(u_k) \triangleq \log\left[\frac{P(u_k = 1/y_1^N)}{P(u_k = 0/y_1^N)}\right] \tag{1}$$

The decoding decision of $\widetilde{u}_k$ is made based on the sign of $L(u_k)$, i.e.

$$\widetilde{u}_k = \text{sign}[L(u_k)]. \tag{2}$$

$L(u_k)$ is computed by three terms, which are *L_apriori, L_channel*, and $L^e(u_k)$. *L_apriori* is a priori information

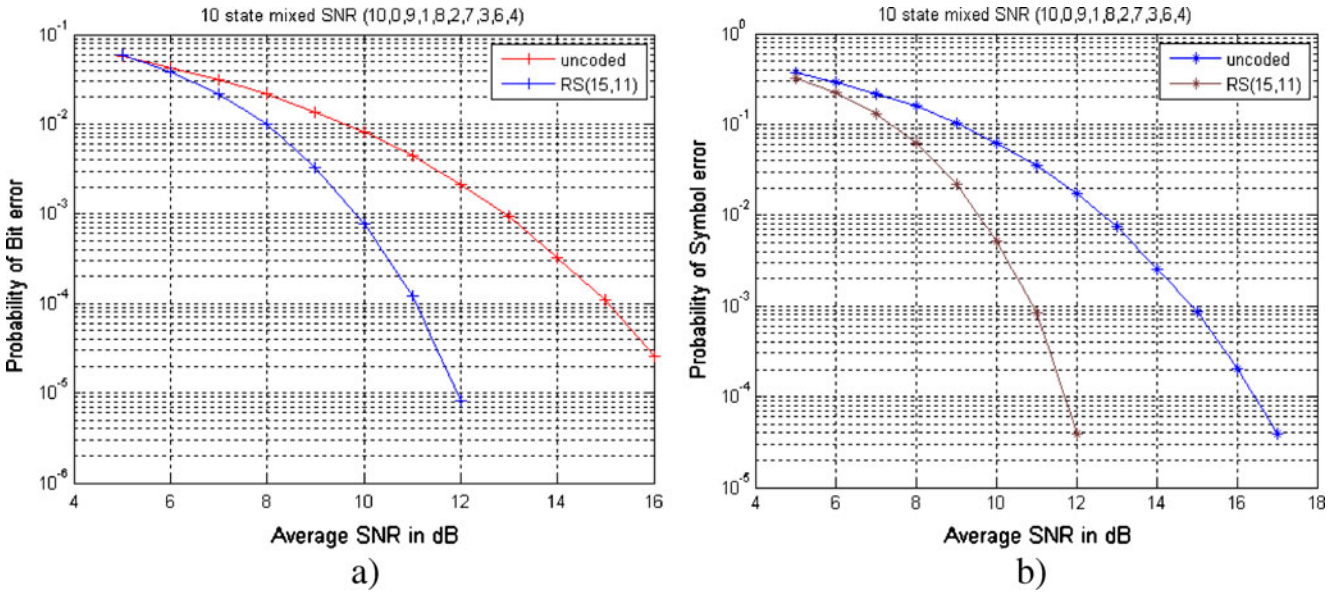
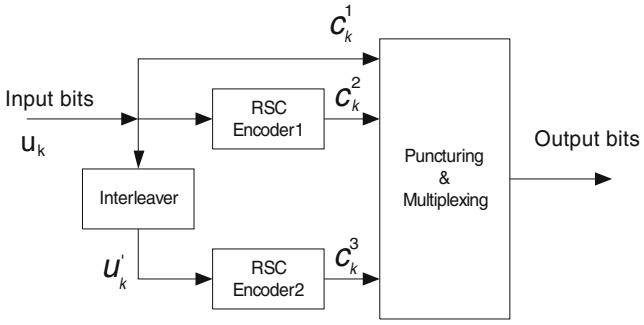
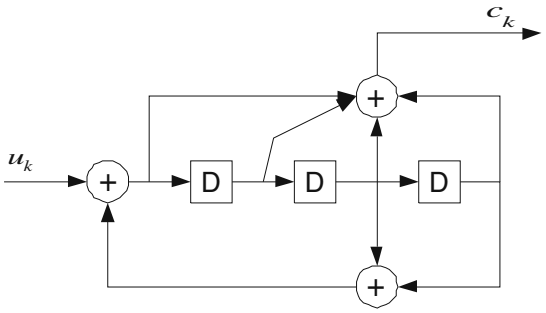


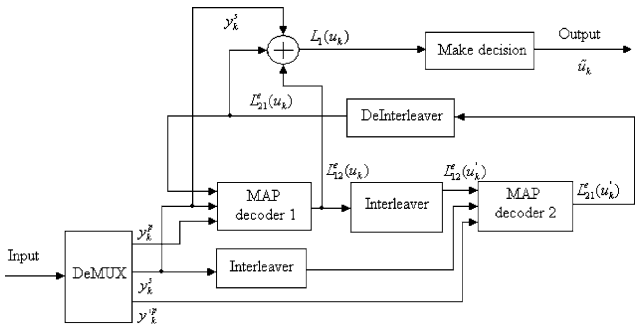
Fig. 6 Performance of (15, 11) Reed Solomon code during transmission of medical images over channels corrupted by (various SNR levels) burst noise



a. Turbo code encoder.



b. Recursive Systematic Convolutional encoder



c. Block diagram of a Turbo decoder [25]

Fig. 7 **a** Turbo code encoder. **b** Recursive Systematic Convolutional encoder. **c** Block diagram of a Turbo decoder [25]

based on the input bit u_k at time k. It is provided by the previous decoder.

$$L(u_k) = \left[L_a^e(u_k) + Lc \cdot y_k^{1,s}\right] + \log \frac{\sum_{u^+} \tilde{\alpha}_{k-1}(s') \cdot \tilde{\beta}_k(s) \cdot \gamma_k^e(s',s)}{\sum_{u^-} \tilde{\alpha}_{k-1}(s') \cdot \tilde{\beta}_k(s) \cdot \gamma_k^e(s',s)} = L\_apriori + L\_channel + L^e(u_k), \quad (3)$$

where *L_apriori* and *L_channel* denote $L_a^e(u_k)$ and $Lc \cdot y_k^{1,s}$ respectively. $\sum_{u^+}()$ is the summation over all the possible transition branch pair (s_{k-1}, s_k) at time k given input u_k=1 and $\sum_{u^-}()$ is the summation over all the possible transition branch pair (s_{k-1}, s_k) at time k given input u_k=0. Lc is the channel reliable factor; its computation is given as the following,

$$Lc = \frac{4 \cdot A \cdot SNR\_b}{p}, \quad (4)$$

where A is a fading amplitude, equal to 1 for an AWGN channel, SNR_b is the bit signal-to-noise-ratio $\left(\frac{E_b}{N_0}\right)$, p denotes $1/r_c$, r_c is code rate of the Turbo encoder.

$L_a^e(u_k)$ is extrinsic information based on all parity and systematic information except the systematic value at time k. $L_a^e(u_k)$ is extrinsic information for decoder 1, derived from decoder 2, and $L^e(u_k)$ is the third term in equation (3) which is used as the extrinsic information for decoder 2 derived from decoder 1. It can be passed on to a subsequent decoder. It is computed using the following equations:

$$L_a^e(u_k) \triangleq \log \frac{\sum_{u^+} \tilde{\alpha}_{k-1}(s') \cdot \gamma_k^e(s',s) \cdot \tilde{\beta}_k(s)}{\sum_{u^-} \tilde{\alpha}_{k-1}(s') \cdot \gamma_k^e(s',s) \cdot \tilde{\beta}_k(s)}, \quad (5)$$

where

$$\gamma^e(s',s) = \exp\left[\sum_{i=2}^{q}\left(Lc \cdot \frac{1}{2} \cdot y_k^{i,p} \cdot c_k^i\right)\right]. \quad (6)$$

$\tilde{\alpha}_k(s)$, $\tilde{\beta}_{k-1}(s')$ can be computed recursively, with initial conditions, as described below:

$$\tilde{\alpha}_k(s) = \frac{\sum_{s'} \tilde{\alpha}_{k-1}(s') \cdot \gamma_k(s',s)}{\sum_{s}\sum_{s'} \tilde{\alpha}_{k-1}(s') \cdot \gamma_k(s',s)}, \quad \tilde{\alpha}_0(s) = \begin{cases} 1 & \text{if s = 1} \\ 0 & \text{otherwise} \end{cases}. \quad (7)$$

$$\tilde{\beta}_{k-1}(s') = \frac{\sum_{s} \tilde{\beta}_k(s) \cdot \gamma_k(s',s)}{\sum_{s}\sum_{s'} \tilde{\alpha}_{k-2}(s') \cdot \gamma_{k-1}(s',s)}, \quad \tilde{\beta}_N = \begin{cases} 1 & \text{if s = 1} \\ 0 & \text{otherwise} \end{cases} \quad (8)$$

$$\gamma_k(s',s) \propto \exp\left[\frac{1}{2} \cdot L^e(u_k) \cdot u_k + Lc \cdot \frac{1}{2} \cdot y_k^{1,s} \cdot c_k^1\right] \exp\left[\sum_{i=2}^{q}\left(Lc \cdot \frac{1}{2} \cdot y_k^{i,p} \cdot c_k^i\right)\right] \quad (9)$$

For example, at any given iteration, decoder 1 $L_1(u_k)$ is computed as

$$L_1(u_k) = Lc \cdot y_k^{1,s} + L_{21}^e(u_k) + L_{12}^e(u_k), \quad \tilde{u}_k = \text{sign}[L_1(u_k)], \quad (10)$$

where $L_1(u_k)$ is given in Eq. (3). $L_{21}^e(u_k)$ is extrinsic information for decoder 1, derived from decoder 2, and $L_{12}^e(u_k)$ is the third term in Eq. (3), which is used as the extrinsic information for decoder 2 derived from decoder 1. The decoders share the information with each other. The value of $L_1(u_k)$ decides the degree of the reliability of $\widetilde{u}_k$.

In this paper, we have used the Turbo code with code rate 1/2 and 1/3 for error correction codes. The rate 1/2 code is derived by puncturing both the parity bits and the data bits. In the decoding algorithm, we also reinserted parity bits are in the parity streams to replace those that were deleted by puncturing.

The plots in Fig. 8a and b show the performance of Turbo codes during transmission of medical images over a channel corrupted by AWGN for two Turbo codes with rate 1/2 and 1/3 respectively. It is observed that these codes give a superior performance as compared to RS codes. However, this advantage is obtained at the cost of greater decoder complexity and a larger decoding delay.

Discussion

With the present trend of using the wired and wireless media to transmit images and patient data, utmost importance should be given to ensuring privacy and authenticity of patient information. The technique of "watermarking" embedding text data with images for copyright authentication is adapted here to embed patient data with medical images. Twenty-four bits are usually employed to indicate the color level of image pixel, and the LSB is replaced by the "text" information for identification. Thus, the LSB is "sacrificed" for the purpose of embedding patient data and the consequent loss of detail is usually acceptable. The use of the AES encryption algorithm enhances the security and privacy of patient information. Transmission over physical transmission media and/or storage in imperfect storage media can result in corruption of data. Therefore, different error-correcting codes/techniques are employed to make the data handling more robust with respect to channel and storage media imperfections.

The effect of Gaussian noise on embedded patient information was studied using simulation techniques [13]. They have studied the performance of repetition and (7, 4) Hamming code to correct the error bits. Their results demonstrated that (7, 4) Hamming code was superior to the repetition code in a channel corrupted by AWGN noise. Our simulation results show that encoding data using suitable error-correction techniques can reduce the impact of channel-induced errors significantly. The results have demonstrated that Turbo code with code rate 1/3 performs the best amongst the three codes for which performance studies have been carried out. However, the complexity of decoding algorithm results in large decoding delays. If the protection given by the RS code is adequate, then it may represent a more practical choice in many applications.

It is expected that data-hiding techniques combined with error control will be deployed for a wide range of applications in areas such as secure medical image data transmission and storage and image authentication in medical and law enforcement in the future.

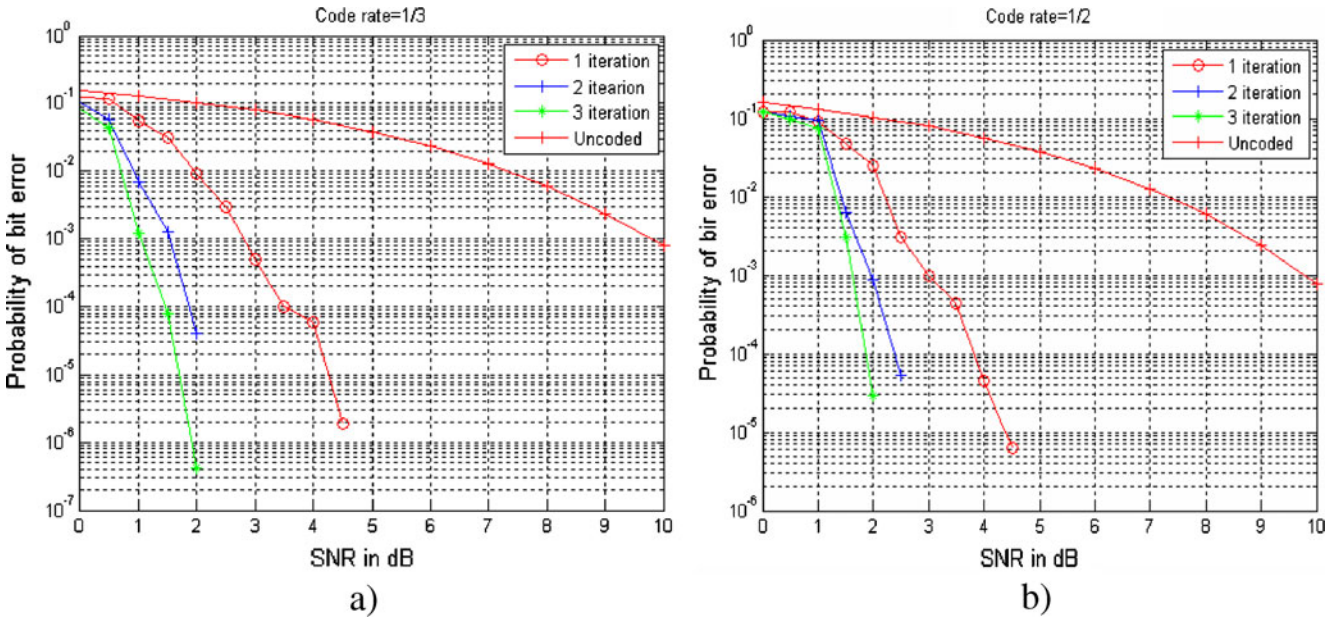


Fig. 8 The performance of Turbo Code with code rate **a** 0.333 and **b** 0.5

Conclusion

A technique of embedding patient information such as text documents and physiological signals with medical images is presented for facilitating efficient storage and transmission. Patient data is encrypted before hiding it in the medical image. The technique is tested for different channel conditions (various SNR levels) and with RS and Turbo error-correcting codes. These techniques can also provide protection against errors induced by imperfect storage media. We conclude that while Turbo codes give the best performance, the large decoding delays associated with their use can result in large waiting periods. Thus, real time recovery of data may not be possible in all applications. The (15, 11) RS code gives reasonably good performance with negligible decoding delay and may represent a practical choice in many applications. If the protection offered by this code is deemed insufficient, longer and more powerful RS codes with suitable interleavers can de designed for this application.

References

1. Digital Imaging and Communications in Medicine (DICOM), National Electrical Manufacturers Association. Rosslyn, Virginia, USA, DICOM Committee, 2001.
2. Sergio, S. F., Marina, S. R., Ramon, A. M., Marcelo, S., Nivaldo, B., Gustavo, H. M. B. M., et al., "Managing medical images and clinical information" InCor's experience. *IEEE Trans. Inf. Technol. Biomed.* 11 (1)17–24, 2007. 451.
3. Stefan, K., and Fabien, A. P. P., *Information hiding techniques for steganography and digital watermarking*. Artek House, Boston, 2000. ISBN: 1-58053-035-4.
4. Chris Shoemaker—Independent Study, Hidden bits: a survey of techniques for digital watermarking, EER-290 Prof Rudko Spring 2002.
5. Chung, Y. Y., and Wong, M. T., Implementation of digital watermarking system. *Dig. Tech. Pap. IEEE Int. Conf. Consum. Electron.*, 214–215, 2003.
6. Giakoumaki, A., Pavlopoulos, S., and Koutsouris, D., Secure and efficient health data management through multiple watermarking on medical images. *Med. Biol. Eng. Comput.* 44 (8)619–631, 2006.
7. Gonzales, R. C., Woods, R. E., and Eddins, S. L., *Digital image processing using MATLAB*. Prentice Hall, Upper Saddle River, 2004.
8. Gonzales, R. C., and Woods, R. E., *Digital image processing,* 2nd ed. Prentice Hall, Upper Saddle River, 2001.
9. Elliott, M., and Schuette, B., *"Digital image watermarking" ECE 533 image processing*. University of Wisconsin-Madison, 21 Dec 2006.
10. Miyazaki, A., Digital watermarking protection technique for multimedia. *Tech. Rep. IEICE*. 102 (41)61–66, 2002.
11. Acharya, U. R., Deepthi, A., Bhat, P. S., and Niranjan, U. C., Compact storage of medical images with patient information. *IEEE Trans. Inf. Technol. Biomed.* 5 (4)320–323, 2001.
12. Acharya, U. R., Bhat, P. S., Kumar, S., and Min, L. C., Transmission and storage of medical images with patient information. *Comput. Biol. Med.* 33:303–310, 2003.
13. Nayak, J., Bhat, P. S., Acharya, U. R., and Kumar, M. S., *Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes*. Springer, New York, 2008.
14. Announcing the Advanced Encryption Standard, Federal Information Processing Standards Publication 197, Nov 26, 2001 http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
15. Daemen, J., and Rijmen, V., AES Proposal Rijndael, Version 2, 1999.
16. Wicker, S. B., and Bhargava, V. K., *Reed–Solomon codes and their applications*. IEEE Press, New York, 1994.
17. Shannon, C. E., A mathematical theory of communications, Bell System Technical Journal, pp. 379–423 (Part I), pp. 623–656 (Part 2), July 1948.
18. Moon, T. K., *Error correction coding: mathematical methods and algorithms*. Wiley, Hoboken, 2005.
19. Blahut, R. E., *Algebraic codes for data transmission*. Cambridge University Press, Cambridge, 2002.
20. Pretzel, O., *Error correcting codes and finite fields*. Clarendon, Oxford, 1992.
21. Lin, S., and Costello, D. J. Jr., *Error control coding fundamentals and applications*. Prentice Hall, Upper Saddle River, 2004.
22. Wicker, S. B., *Error control coding for digital communication systems*. Prentice Hall, Upper Saddle River, 1995.
23. McEliece, R. J., *The theory of information and coding*, II ed. Cambridge University Press, Cambridge, 2002.
24. Berrou, G., Glavieuc, A., and Thitmajshima, P., Near Shannon limit error-correcting coding: Turbo codes, in Proc. 1993, Int. Conf. Com., Geneva, Switzerland, May 1993, pp. 1064–1070.
25. Benedetto, S., Divsalar, D., Montorsi, G., and Pollara, F., A soft-input soft-output Maximum A Posteriori (MAP) module to decode parallel and serial concatenated codes, TDA progress report 42-127, November 15, 1996.
26. Rekh, S., Subharani, S., and Shanmugam, A., Optimal choice of interleaver for turbo codes. *Acad. Open Internet J.* 15, 2005.