RELIABLE INFORMATION TRANSMISSION FOR BIOMEDICAL APPLICATIONS

1. Dr. U. SARAVANAKUMAR, 2. GANGA RAMESH JAKKAMSETTI
1. Associate professor, Dept. of ECE, VEL Tech University, Chennai, Tamil Nadu.
2. Research Scholar, Dept. of ECE, VEL Tech University, Chennai, Tamil Nadu.

ABSTRACT:
The main objective of this concept is to design an efficient and enhanced data hiding techniques in digital images for secured communication, authentication and integrity verification. Digital data hiding/watermarking technique, through embedding of an auxiliary message within the original data, has proven its credibility as a potential & widely used solution for the stated problems over the last few years. Watermarking is the process that embeds data called a watermark, tag or label into a multimedia object, such as images, video or text for their copyright protection. This concept proposing Secure Image Transmission scheme with modified hybrid data encoding with Low power dissipation and LDPC based Data Encoding system for Error Identification and correction. The modified Encoder operates under low power using distributed switching activity. The LDPC based Encoder used generate Parity added Test Data for Transmitter Under test.

KEYWORDS: Low Density Parity Check (LDPC), Error correction, Parity, Digital Watermarking, Data Encoding, Switching activity

INTRODUCTION:
Electronic watermarking was invented in 1954 by Emil Hembrooke of the Muzac Corporation (1). A vast research community involving experts from computer science, cryptography, signal processing, and communications has come together in the last decade to develop watermarks suitable for various applications. Digital watermarking is intended by its developers as the solution to the requirement of providing value-added protection on top of data encryption and scrambling for content protection. Like any other technology under development, digital watermarking raises a number of essential questions (The success of the Internet allows for the prevalent distribution of multimedia data in an effortless manner. Due to the open environment of Internet downloading, copyright protection introduces a new set of challenging problems regarding security and illegal distribution of privately owned images. One potential solution for declaring the ownership of the images is to use watermarks. Watermarking is a technique for labelling digital pictures by hiding secret information in the images. Thestudying key point is that the embed information can neither be removed nor decoded without the required secret keys. Indeed, there are a number of desirable characteristics that a watermarking technique should exhibit. Owing to the usage of Internet, concerns about protecting and enforcing intellectual property (IP) rights of the digital content are mounting. Unauthorized replication and manipulation of digital content is relatively easy and can be achieved with inexpensive tools. Digital rights management (DRM) systems [1], [2] address issues related to ownership rights of digital content. Various aspects of content management – namely, content identification, storage, representation, and distribution – and IP rights management are highlighted in DRM. Although unauthorized access of digital content is being prevented by implementing encryption technologies, these approaches do not prevent an authorized user from illegally replicating the decrypted content. Digital watermarking is one of the key technologies that can be used in DRM systems for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication, and facilitating content authentication. Therefore, a two-layer protection mechanism utilizing both watermarking and encryption is needed to build effective DRM systems that can address IP rights and copyright issues [3]. We recently designed a high-performance, high-throughput, and area-efficient very-large-scale (VLSI) architecture for the Rijndeal Advanced Encryption Standard (AES) algorithm [4].

CONTRIBUTIONS OF THIS PAPER:
The contributions of this paper are multifold. First, it introduces an invisible robust image watermarking algorithm and an invisible fragile image watermarking algorithm, both of which are spatial domain watermarking algorithms. The algorithms were first validated by using MATLAB simulation to evaluate their performance. The algorithms were developed such that their software implementation is simple yet provides high performance XILINX also.

RELATED RESEARCH

The current literature is rich in watermarking algorithms developed for various types of media, such as image, video, audio, and text data, and their software implementations. The algorithms work in various domains like spatial, DCT, and wavelet and insert-extract different types of watermarks including invisible robust, invisible fragile, and visible. These watermarking algorithms primarily work off-line; i.e., the images are first acquired and then the watermarks are inserted before the watermarked images are made available to the user. Thus, in this approach, there is a gap between image capture and image transmission. The objective of this research work was to develop a hardware-based watermarking system to bridge this gap. The watermark chip will be fitted in any electronic component that acquires the images, which are then watermarked in real time while capturing. In this section, we

briefly discuss the few hardware-based watermarking systems mentioned in the current literature. These hardwarebased watermarking systems were designed and implemented on an FPGA board, Trimedia processor board, or custom IC using different CMOS technologies. Strycker et al. [24] have proposed a real-time watermarking algorithm in the spatial domain for television broadcast monitoring. They address the implementation of a real-time watermark embedder and detector on the Trimedia TM1000 very long instruction width (VLIW) processor developed by Philips Semiconductor. In the insertion procedure, pseudorandom numbers are added to the incoming video stream based on the luminance value of each frame, and watermark detection is based on the calculation of the correlation values. Mathai et al. [23] describe a VLSI chip designed with 0.18µm CMOS technology implementing the above video watermarking algorithm. A DCT domain invisible watermarking chip is presented by Tsai and Lu [25]. The watermarking system embeds a pseudorandom sequence of real numbers with a selected set of DCT coefficients and is extracted without using the original image. The chip is implemented with TSMC 0.35µm technology and has a die size of 3.064 × 3.064mm2 and 46,374 gates. The chip is estimated to consume 62.78mW of power when operated at 50MHz frequency with a 3.3V supply. Garimella et al. [26] have proposed a watermarking VLSI architecture for invisible fragile watermarking in the June19,2009 DRAFT spatial domain. In this scheme, the differential error is encrypted and interleaved along with the first sample. The watermark can be extracted by accumulating the consecutive least significant bits (LSBs) of the pixels and then decrypting them. The extracted watermark is then compared with the original watermark for image authentication. The application specific integrated circuit (ASIC) is implemented using 0.13µm technology. The area of the chip is 3453 × 3453µm2 , and the chip consumes 37.6µW of power when operated at 1.2V . The critical path delay of the circuit is 5.89ns. Mohanty et al. [2] have proposed another watermarking hardware architecture that can insert two visible watermarks in images in the spatial domain. This architecture can insert either of the two watermarks depending on the requirements of the user. The chip is implemented with 0.35µm technology and occupies an area of 3.34 × 2.89mm2 and consumes 6.9286mW when operated at 3.3V and 292.27MHz. Fan et al. [7] have proposed a visible watermarking design based on an adaptive discrete wavelet transform (DWT).They propose efficiently reduced operational and resource-sharing techniques using an existing algorithm. Host image and watermark are transformed into three-level multi-resolution structures. The host image signal is divided into two sequences with the same pattern length. Processing time is reduced by using a two-path parallel processing architecture. The signal is sent to different processing elements by the demultiplexers. The watermark image is embedded by modifying the coefficients of the image.

PROPOSED METHODOLOGY:

MRI Image Acquisition:

The MR image formation process subdivides a section of the patient's body into a set of slices and then each slice is cut into rows and columns to form a matrix of individual tissue voxels. This is achieved by encoding or addressing the signals during the acquisition phase and then, in effect, delivering the signal intensities to the appropriate pixels which have addresses within the image during the reconstruction phase. Because there are two dimensions, or directions, in an image, two different methods of encoding must be used. This is analogous to mail that must have both a street name and a house number in the address. We are about to see that the two methods of addressing the signals are called *frequency-encoding* and *phase-encoding*. One method is applied to one direction in the image and the other method is used to address in the other direction.

Signal Acquisition

During the acquisition phase the RF signals are emitted by the tissue and received by the RF coils of the equipment. During this process the signals from the different slices and voxels are given distinctive frequency and phase characteristics so that they can be separated from the other signals during image reconstruction. The acquisition phase consists of an imaging cycle that is repeated many times. The time required for image acquisition is determined by the time TR, which is the duration of one cycle or its repetition time, and the number of cycle repetitions. The number of cycles is determined by the image quality requirements. In general, the quality of an image can be improved by increasing the number of acquisition cycles.

Image Reconstruction

Image reconstruction is a mathematical process performed by the computer. It transforms the data collected during the acquisition phase into an image. We can think of reconstruction as the process of sorting the signals collected during the acquisition and then delivering them to the appropriate image pixels. The mathematical process used is known as *advanced transformation*. Image reconstruction is typically much faster than image acquisition and requires very little, if any, control by the user.

WATERMARKING USING DCT:

Digital watermarking is a technology for embedding various types of information in digital content. In general, information for protecting copyrights and proving the validity of data is embedded as a watermark. A digital watermark is a digital signal or pattern inserted into digital content. The digital content could be a still image, an audio clip, a video clip, a text document, or some form of digital data that the creator or owner would like to protect. The main purpose of the watermark is to identify who the owner of the digital data is, but it can also identify the intended recipient. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarkinginformation into the middle frequency bands of an

image. It has become easy to connect to the Internet from home computers and obtain or provide various information using the World Wide Web (WWW). All the information handled on the Internet is provided as digital content. Such digital content can be easily copied in a way that makes the new file indistinguishable from the original. Then the content can be reproduced in large quantities. For example, if paper bank notes or stock certificates could be easily copied and used, trust in their authenticity would greatly be reduced, resulting in a big loss. To prevent this, currencies and stock certificates contain watermarks. These watermarks are one of the methods for preventing counterfeit and illegal use. Digital watermarks apply a similar method to digital content. Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies.

ERROR CORRECTION CODES:

HYBRID METHODOLOGY:

LDPC (31,8) and Turbo (3,1) :

Since the mid 2000s, LDPC codes have found a wide variety of commercial applications. Much about these codes is well understood, but rather frequently little attention is paid to the minimum (Hamming) distance between codewords. The minimum distance of a code can limit the error performance at high SNR and is important in understanding the likelihood of undetected errors. The error-correcting performance of low-density parity check (LDPC) codes, when decoded using practical iterative decoding algorithms, is known to be close to Shannon limits for codes with suitably large blocklengths. A substantial limitation to the use of finite-length LDPC codes is the presence of an error floor in the low frame error rate (FER) region. This paper develops a deterministic method of predicting error floors, based on high signal-to-noise ratio (SNR) asymptotics, applied to absorbing sets within structured LDPC codes. The approach is illustrated using a class of array-based LDPC codes, taken as exemplars of high-performance structured LDPC codes.

Low complexity turbo-like codes based on simple two-state trellis or simple graph structure results in encoding with low complexity. Out of this Convolution encoder and turbo codes are widely used due to the excellent error control performance. The most popular communications encoding algorithm, the iterative decoding requires an exponential increase in hardware complexity to achieve greater encode accuracy. This project focuses on the realization of turbo encoder and decoder using Log-Map based Iterative decoding technique. The turbo codes are designed with the help of Recursive Systematic Convolutional and are separated by interleaver, which (component used to rearrange the bit sequence) plays a vital role in the encoding process.

TURBO ENCODER:

As conventional code, the encoder for a Turbo code accepts k-bit blocks of the information sequence u and produces an encoded sequence (code word) p of n-symbol blocks. Moreover, each encoded block depends not only on the corresponding k-bit message block at the same time unit, but also on m previous message blocks.

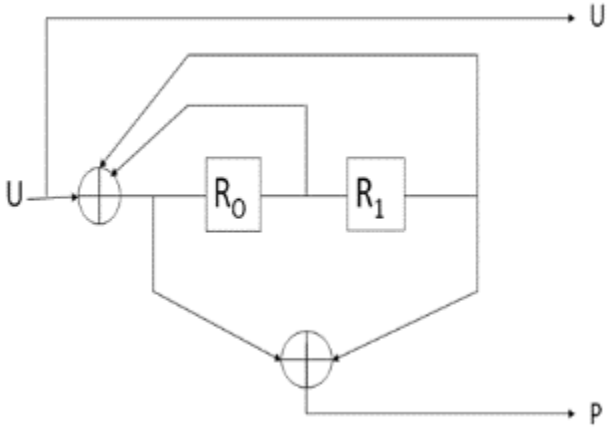


Fig.1: Encoder Block Diagram for an RSC Code

The encoder is a memory-two encoder. The two memory elements can take on four possible states. A hardware realization for encoder is shown in Figure 1. The value of the two memory elements in the encoder, R0 and R1; define the "state" of the encoder. A state diagram is created from the possible state changes of R0 and R1 (as all possible input sequences are generated) and is used to create a trellis diagram utilized in the decoder operation. The state diagram for the encoder is shown in below.

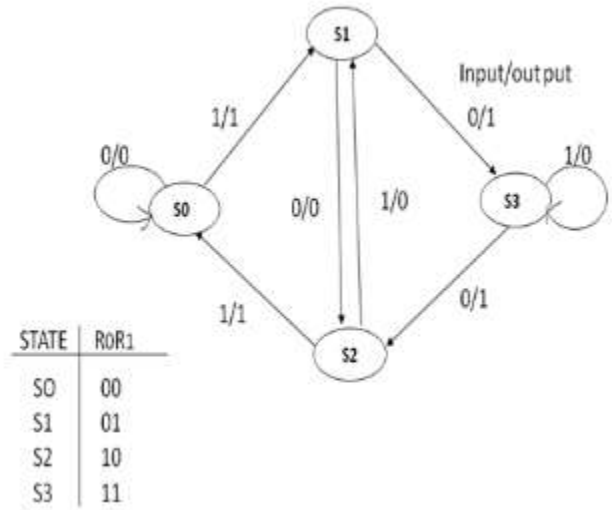


Fig. 2: State diagram for the encoder.

Turbo encoders and decoders are key elements in today's communication systems to achieve possible data reception with the fewest possible errors the best Turbo System where Encoder generates a multiplexed code of two coders fed with direct and interleaved data.

Forward Error Correction (FEC) is a technique for error control during data transmission, whereby redundant information is added to the original data, which allows the receiver to detect and correct errors without the need to resend the data. RSC encoders and an interleaver as shown in figure 3 Here the purpose of interleaver is to scramble input information so that there is no correlation between the data applied to the encoders.

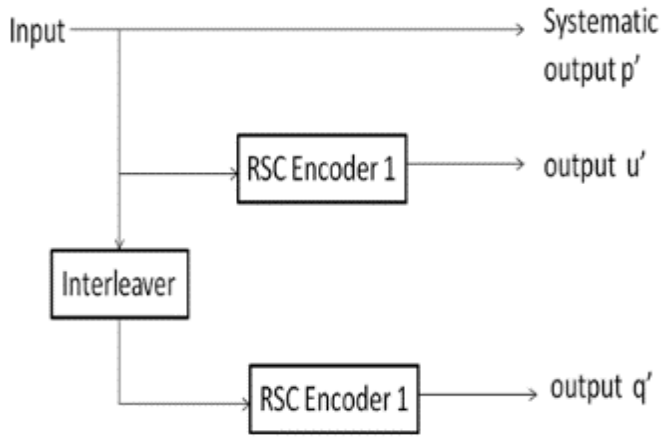


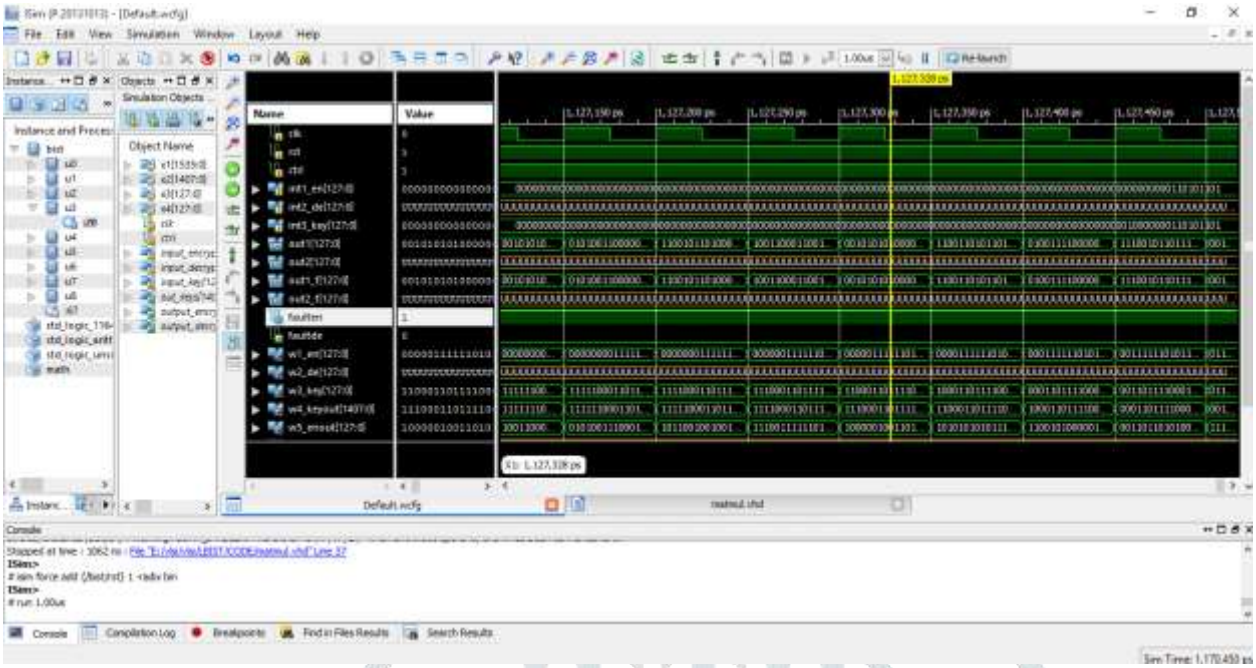
Fig. 3: Encoder of Turbo Code

The Turbo encoder comprises two RSC encoders and an interleaver as shown in figure 3. Here the purpose of interleaver is to scramble input information so that there is no correlation between the data applied to the encoders.

ADVANTAGES: • Watermarking should provide high robustness and hiding capacity • It should prevent unauthorized copying, illegal users hacking, and redistributing multimedia data. • Additional information should be ready in the event of any error correction • It must be able to prove the ownership by tracing the malicious user

APPLICATIONS: • Annotation • Authentication and Integrity Verification • Broadcast monitoring • Content description/recovery • Covert communication • Protection of Copy-rights or Access control • Defense application • Transaction tracing Digital fingerprinting or Content labeling

RESULT:



CONLUSION: Finally, an efficient and enhanced secured VLSI architecture is implemented with hybrid algorithms. Digital water marking for security is implemented and tested in rigidity environment; reliability issue like error detection, correction also designed and successfully verified in public environment.

REFERENCES:

[1] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding Digital Watermarks using Multiresolution Wavelet Transform," IEEE Trans. Industrial Electronics, vol. 48,no. 5, Oct. 2001, pp. 875–82 [2] Security Protection between Users and the Mobile Media Cloud. Honggang Wang, University of Massachusetts Shaoen Wu,Ball State University Min Chen, Huazhong University of Science and Technolog Wei Wang, South Dakota State University. [3] Evaluation of Lossless Watermarking Techniques Dr.Smitha Rao M.S Reva Institute of Technology and Management Bangalore, India. [4] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark,"Proc. IEEE Int. Conf. Image Processing, vol. 2, pp. 86– 90, 1994. [5] W. R. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," Proc. SPIE: Storage and Retrieval of Image and Video Database, vol. 2420, pp. 164–173, Feb. 1995. [6] N. Nikolaidis and I. Putas, "Copyright protection of images using robust digital signatures," in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, vol. 4, May 1996, pp. 2168–2171.