Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions

S. Manimurugan, Department of Computer Science and Engineering, MBC College of Engineering and Technology, Kerala, India
C. Narmatha, Department of Electronics and Communication Engineering, Karpagam University, Coimbatore, India

ABSTRACT

Exchanging a medical image via network from one place to another place or storing a medical image in a particular place in a secure manner has become a challenge. To overwhelm this, secure medical image Lossless Compression (LC) schemes have been proposed. The original input grayscale medical images are encrypted by Tailored Visual Cryptography Encryption Process (TVCE) which is a proposed encryption system. To generate these encrypted images, four types of processes are adopted which play a vital role. These processes are Splitting Process, Converting Process, Pixel Process and Merging process. The encrypted medical image is compressed by proposed compression algorithms, i.e Pixel Block Short algorithm (PBSA) and one conventional Lossless Compression (LC) algorithm has been adopted (JPEG 2000LS). The above two compression methods are used to separate compression for encrypted medical images. And also, decompressions have been done in a separate manner. The encrypted output image which is generated from decompression of the proposed compression algorithm, JPEG 2000LS are decrypted by the Tailored Visual Cryptography Decryption Process (TVCD). To decrypt the encrypted grayscale medical images, four types of processes are involved. These processes are Segregation Process, Inverse Pixel Process, 8-Bit into Decimal Conversion Process and Amalgamate Process. However, this paper is focused on the proposed visual cryptography only. From these processes, two original images have been reconstructed which are given by two compression algorithms. Ultimately, two combinations are compared with each other based on the various parameters. These techniques can be implemented in the field for storing and transmitting medical images in a secure manner. The Confidentiality, Integrity and Availability (CIA property) of a medical image have also been proved by the experimental results. This paper focuses on only proposed visual cryptography scheme.

Keywords: JPEG 2000LS, Medical images, Pixel Block Short algorithm, Tailored Visual Cryptography Encryption Process

DOI: 10.4018/IJDCF.2015010102
INTRODUCTION
Chung-Ping (2005), Shortt .A.E (2006) and Cheng .H (2000) discussed a secret sharing scheme suitable for encrypting colour images and the required colour shares were obtained during encryption by operating at the bit-levels. Perfect reconstruction was achieved by the decryption module using only logical operations. The author paper has invented two approaches for integrating encryption with multimedia compression systems which included selective encryption and modified entropy coders with multiple statistical models. This can be examined for the limitations of selective encryption using cryptanalysis, and provide examples that use selective encryption successully. Martin .K., (2009), Qiu-Hua Lin (2002) and Zuo-Dian Chen (1999) have been presented a biometric encryption system that addressed the privacy concern in the deployment of the face recognition technology in real-world systems. In particular, they focused on a self-exclusion scenario (a special application of watch-list) of face recognition and proposed a novel design of a biometric encryption system deployed with a face recognition system under constrained conditions. Shujun Li (2008) and Sudharsanan, (2005) have proposed a system which uncovers a new image scrambling (i.e., encryption) scheme without bandwidth expansion which is based on two-dimensional discrete prolate spheroidal sequences. A comprehensive crypt-analysis was given on that image scrambling scheme, showing that it is not sufficiently secure against various crypto graphical attacks including cipher text-only attack, known/chosen-plaintext attack, and chosen-cipher text attack. Detailed cryptanalytic results suggested that the image scrambling scheme could be used to realize perceptual encryption but not to provide content protection for digital images.

InKoo Kang., et. al., (2011) has designed an indigenous approach for Visual Information Pixel (VIP) synchronization and error diffusion enhancing the attainment of a color visual cryptography encryption method that produced meaningful color shares with high visual quality. VIP synchronization retained the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares pleasant to human eyes. Comparisons with previous approaches showed superior performance of the new method. Rajendra Acharya (2001), Servetti .A (2002) and Monga .V (2007) had used the methods of Digital Watermarking for interleaving patient information with medical images to reduce storage and transmission overheads. The text data were encrypted before interleaving with images to ensure greater security. The graphical signals were compressed and subsequently interleaved with the image. Differential pulse-code-modulation and adaptive-delta-modulation techniques were employed for data compression, and encryption and results were tabulated for a specific example. Bourbakis .N and Dollas .A (2003) had invented a SCAN-based method for image and video compression-encryption-hiding with application to digital video on demand. The software SCAN implementation running on a Pentium IV took about 1 second for 25 video frames. As an alternative solution, however, they developed a FPGA-based architecture, which operated in real time. Schonberg .D., et. al., (2008) have discussed a property of sparse representations in relation to their capacity for information storage. It was then shown that that feature could be used for an application that was termed Encrypted Image Folding. The proposed procedure was realizable through any suitable transformation. In particular, this paper has illustrated the approach by recourse to the Discrete Cosine Transform and a combination of redundant Cosine and Dirac dictionaries. The following sections are discuss about proposed visual cryptography in detailed manner.

OVERVIEW OF THE PROPOSED SYSTEM
Taking into account of the limitations, taken from the above section, the proposed system has
Related Content

The Simulation of the Journey to Residential Burglary
[www.igi-global.com/chapter/simulation-journey-residential-burglary/5268?camid=4v1a](www.igi-global.com/chapter/simulation-journey-residential-burglary/5268?camid=4v1a)

An Enhanced Fuzzy ARM Approach for Intrusion Detection
[www.igi-global.com/article/enhanced-fuzzy-arm-approach-intrusion/55502?camid=4v1a](www.igi-global.com/article/enhanced-fuzzy-arm-approach-intrusion/55502?camid=4v1a)
Designing Light Weight Intrusion Detection Systems: Non-Negative Matrix Factorization Approach
Václav Snášel, Jan Platoš, Pavel Krömer and Ajith Abraham (2009). Socioeconomic and Legal Implications of Electronic Intrusion (pp. 216-229).
www.igi-global.com/chapter/designing-light-weight-intrusion-detection/29366?camid=4v1a

Biometrical Processing of Faces in Security and Forensics
www.igi-global.com/chapter/biometrical-processing-faces-security-forensics/39214?camid=4v1a