Securable Watermarking Of Compressed And Encrypted Medical Image In Medical Information System

R. Kokila
Student

V. Padmavathi
Student

P. Kasthuri
Student

Abstract

The aim of the project is to provide a security in medical image using compression and watermarking technique. The compression process would have packed the information of raw media into a low number of bits. For compression the spread spectrum and Quantization Index Modulation schemes are used. After compression the encryption technique is used it would have randomized the compressed bit stream. The image is encrypt by using RC4 encryption algorithm and also the decryption is done in the same way. The watermark scheme provide security, embedding capacity, and robustness.

Keywords—watermarking, compression and encryption process .JPEG Image, Decryption.

1. INTRODUCTION

IMAGE PROCESSING

Image processing is a method to convert an image into digital form and perform some operations on it, in order to get an improved image or to extract some useful information from it. The two types of methods used for image processing are analog and digital image processing. Analog techniques used in hard copies like printouts and photographs. Digital processing techniques help in manipulation of the digital images by using computers. Image processing is any form of signal processing for which the input is an image, such as a photograph or video. The output of image processing may be either an image or a set of characteristics or parameters related to the image.

2. RELATED WORK

There are several related image watermarking techniques proposed to date .Deng *et al.* proposed an efficient buyer-seller watermarking protocol based on composite signal representation given in the existing system. The encryption is performed on most significant bit planes while watermarking the rest of lower significant bit planes. In case lesser number of sub-bands/bit planes are used for encryption ,an attacker can manipulate the unencrypted sub bands/bit planes and further extract some useful information from the image, although the image may not be of good quality. On the other hand, if more sub bands/bit planes are encrypted and only rest few sub bands/bit planes are watermarked, it might be possible for an attacker to remove the watermarked sub bands/bit planes while maintaining the image quality.

3. PROPOSED WORK

In proposed work take a medical image it is in the form of JPEG type image. create the text watermark on the image. Take the watermarked image and compressed the watermarked image. Now check the size of watermarked image with compressed image. The compressed image size is less than the watermarked image size. The compression process only reduce the image size it not reduce the quality of the image. The compressed image is encrypted by using RC4 encryption method.RC4 is also known as ARC4 or ARCFOUR. It is a stream chipper type.RC4 generates a random stream of bits. The random key is generate by user at the run time. At receiver side the encryption image is decrypt by using the same key, which one is created by user in the runtime at the sender side.

The proposed system architecture describes the process of the Security provided to the image in an image processing domain.

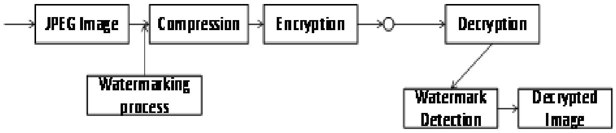

Figure 3

This architecture show the security process clearly. The watermarking compression and encryption provide security to a image from unauthorized access. The JPEG Image is watermark and compressed. The compressed image is encrypted in the sender side. The watermark detection and the decryption is done in the receiver side.

3.1 Watermarking Process

This is the first module in the proposed system. In this module take a medical image it is in the formate of JPEG .Embed the watermark text on the image through choose the clarity level. we can apply font style to the watermark text. choose save option for save the watermark text for further operations .Now the watermark text is embedded on the medical image.

3.2 Compression Process

The compression process follow the watermarking process, the watermarked image is compressed by using compression techniques such as Spread Spectrum and Quantization Index Modulation. The Spread Spectrum is used to calculate the image pixel range .The Quantization Index Modulation technique separate the image in some smaller blocks and merge the pixels without change. Through this techniques the watermark image is compressed. The compressed image also saved for further operations.

3.3 Image Encryption

The watermarked and compressed image is encrypted by using RC4 crypto method. The encryption is done by the sender. RC4 is also known as ARC4 or ARCFOUR. It is a stream chipper type.RC4 generates a random stream of bits. The random key is generate by user at the run time. Through this RC4 method the image is encrypted.

3.4 Image Decryption

The image decryption is done at the receiver side. The image is decrypt by using random key which one is developed by the sender at the run time. The encrypted image is only decrypted by valid user.

After decryption the image is view by the user. All modules provide security.

4. SIMULATION TESTBED

The proposed system is implemented in .NET frame work. The compression ,encryption and decryption process are implemented using C# . The C# language is a simple, modern, general-purpose, object-oriented programming language. For maintain information sql database is used. The Microsoft .NET Framework is a platform for building, deploying, and running Web Services and applications. The sample screen shots are given below:

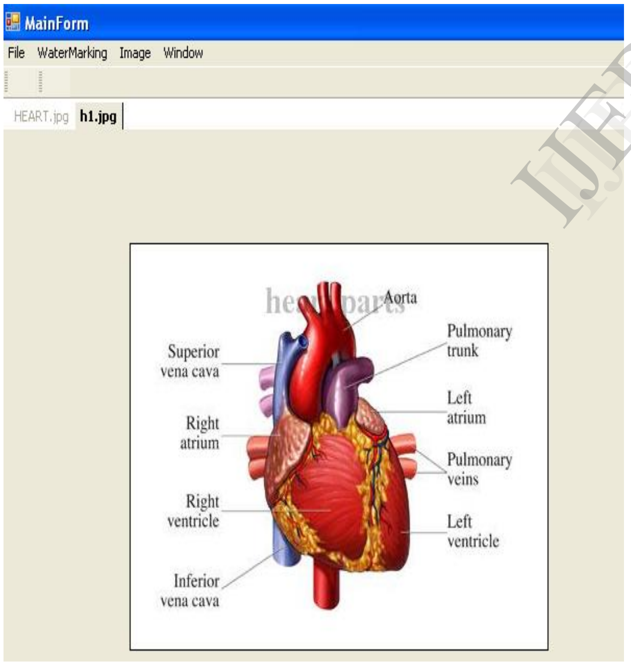

Figure 4.1: Watermark text.

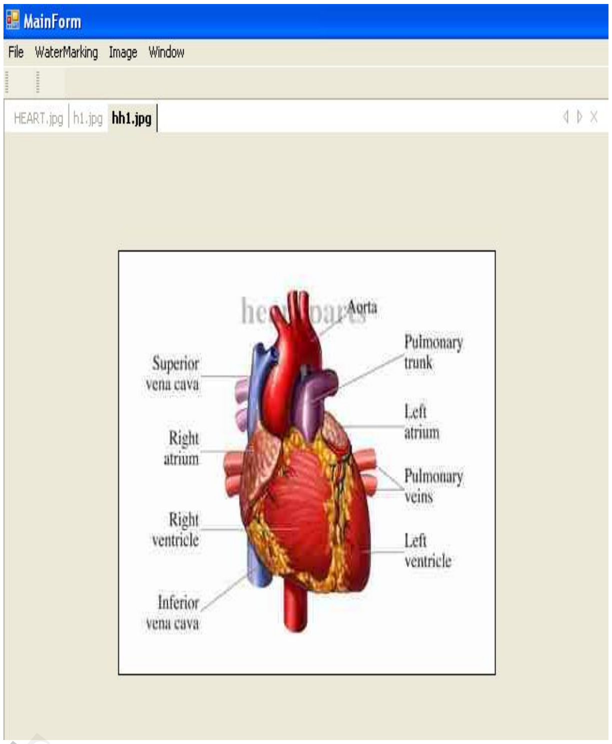

Figure 4.2:Compressed image.

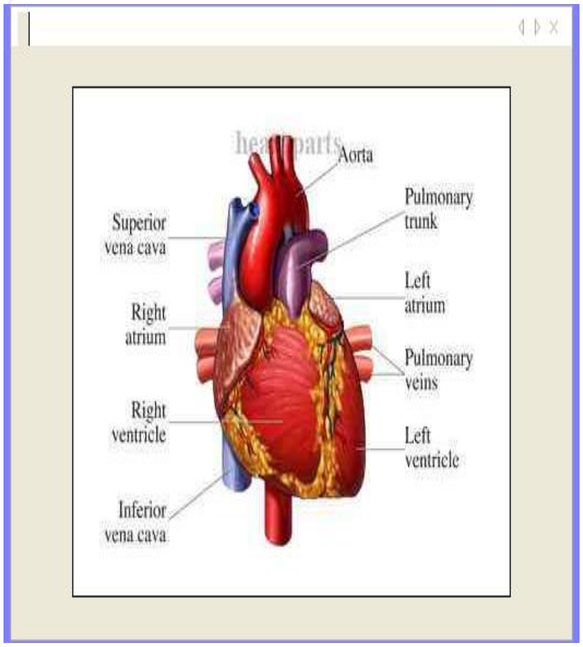

Figure 4.3:Decrypted image.

5. CONCLUSION

The proposed system provide security through watermarking and compression. The watermarking provide security, such as owner ship and copy right. The major concept of this work is compression the image size or reduce the image size .The compression process reduce the image size only it does not reduce the image quality. Further security is provided through encryption. The project concluded the image size is reduce successfully without reduce the quality of the image.

6.REFERENCE

[1] S. Hwang, K. Yoon,K. Jun, andK. Lee, "Modeling and implementation of digital rights," *J. Syst. Softw.*, vol. 73, no. 3, pp. 533–549, 2004.
[2] A. Sachan, S. Emmanuel, A. Das, and M. S. Kankanhalli, "Privacy preservingmultiparty multilevel DRM architecture," in *Proc. 6th IEEE Consumer Communications and Networking Conf., Workshop Digital Rights Management*, 2009, pp. 1–5.
[3] T. Thomas, S. Emmanuel, A. Subramanyam, and M. Kankanhalli, "Joint watermarking scheme for multiparty multilevel DRM architecture," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 758–767, Dec. 2009.
[4] A. Subramanyam, S. Emmanuel, and M. Kankanhalli, "Compressedencrypted domain JPEG2000 image watermarking," in *Proc. IEEE Int. Conf. Multimedia and Expo*, 2010, pp. 1315–1320.
[5] H. Wu and D.Ma, "Efficient and secure encryption schemes for JPEG 2000," in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, 2004, vol. 5, pp. 869–872.
[6] M. Deng, T. Bianchi,A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.
[7] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 180–187, Mar. 2010.
[8] S. Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative watermarking and encryption for media data," *Opt. Eng.*, vol. 45, pp. 1–3, 2006.
[9] F. Battisti, M. Cancellaro, G. Boato, M. Carli, and A. Neri, "Joint watermarking and encryption of color images in the Fibonacci-Haar domain," *EURASIP J. Adv. Signal Process.*, vol. 2009.