*International Journal of Information Technology and Knowledge Management*
*December 2012, Volume 6, No. 1, pp. 19-21*

# A STEGANOGRAPHIC METHOD BASED UPON JPEG AND QUANTIZATION TABLE MODIFICATION

**Ramandeep Kaur Toor[1] and Ramanjot Kaur[2]**

***Abstract***: Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. The combination of cryptography and steganography provide high level security to the secrete information. Cover image is known as carrier image and is the original image in which the secret data ie., the payload is embedded. The unified image obtained after embedding the payload into the cover image is called the stego image. The recent boom in IT industry facilitates embedding data and security issues effectively. This paper presents an efficient authentication method for JPEG images based on Genetic Algorithms (GA). The current authentication methods for JPEG images require the receivers to know the quantization table beforehand in order to authenticate the images. Moreover, the quantization tables used in the JPEG compression are different for different quality factors, thus increasing the burden on the receivers to maintain several quantization tables. We propose a novel GA-based method which possesses three advantages. First, the computation at the receiver end is simplified.

***Keywords***: Genetic Algorithms, steganography, JPEG- JSteg.

## 1. INTRODUCTION

Digital images are the most common cover files used for steganography. In this paper, a new steganography method called JMQT based on modified quantization table is proposed. This steganography method is compared with steganography method JPEG-JSteg. Two performance parameters namely capacity and stego size has been compared. As a result capacity increases and stego size increases. So JMQT provides better capacity and JPEG-JSteg provides better stego-size. Joint photographic expert-group (JPEG) is a famous file for images. It applies the discrete cosine transformer (DCT) to image content transformation. DCT is a widely used tool for frequency transformation. If we apply JPEG images to data hiding, the stego-image will not easily draw attention of suspect. There is a JPEG hiding-tool Jpeg-Jsteg. In the Jpeg-Jsteg embedding method, secret messages are embedded in the least signification bits (LSB) of the quantized DCT coeficients whose values are not 0, 1, or) 1. The main drawback of Jpeg-Jsteg is less message capacity. This is because, after the DCT transformation and quantization of JPEG, the coeficients are almost all zero and cannot hide messages according to the definition of Jpeg- Jsteg. To improve the message capacity of Jpeg-Jsteg, a new data hiding method based on JPEG and quantization table modification is proposed.

[1,2] Department of CSE, Adesh Institute of Engg. and Tech. Faridkot, India
[1] *E-mail: kirandeep2226@gmail.com*

## 2. PRESENT WORK

Digital Image processing has been a field which has a wide area of expansion and work terminology. After having a deep study of the stegnograpy and the watermarking algorithms and research that is there any modification possible in the terms of Peak Signal to noise ratio and Maximum Hiding Capacity. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. **Watermarking techniques** are particular embodiments of steganography. The use of watermarks is almost as old as paper manufacturing. Our ancients poured their half-stuff slurry of fiber and water on to mesh molds to collect the fiber, then dispersed the slurry within deckle frames to add shape and uniformity, and finally applied great pressure to expel the water and cohere the fiber. This process hasn't changed too much in 2000 years. One by-product of this process is the **watermark** - the technique of impressing into the paper a form of image, or text derived from the negative in the mold, as the paper fibers are squeezed and dried. Paper Watermarks have been in wide use since the late Middle Ages. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. In this thesis, work has been carried out on Digital Watermarking. Throughout the rest of the report, watermarking refers to digital watermarking. To avoid the unauthorized distribution of images or other multimedia property, various solutions have been proposed. Most of them make unobservable modifications to images that can be detected afterwards.

Such image changes are called watermarks. Watermarking is defined as adding a payload signal to the host signal. The payload can be **detected** or **extracted** later to make an assertion about the object *i.e.* the original data that may be an **image** or **audio** or **video**.

In general, any watermarking scheme (algorithm) consists of three parts.

- **The watermark** (payload)
- **The encoder** (marking insertion algorithm)
- **The decoder and comparator** (verification or extraction or detection algorithm)

Watermarking techniques complement encryption by embedding a secret imperceptible signal, a watermark, directly into the original data in such a way that it always remains present. Such a watermark is used for the following purposes :

1. Copyright protection: A watermark is used to carry copyright information as a proof in case of a copyright or ownership dispute.
2. Fingerprinting: Unique information, directly coupled to user identification, is embedded in the data as a watermark. In case of copyright violation, this watermark can be used to trace the source of illegal copies.
3. Copy protection: A watermark is used to carry information prohibiting copying of protected data on compliant hardware.
4. Broadcast monitoring: A watermark is embedded into data, for example, commercials or copyrighted materials, to allow automatic monitoring of the data in the broadcasting channels. The results of this monitoring can be used for royalty or copyright protection purposes.

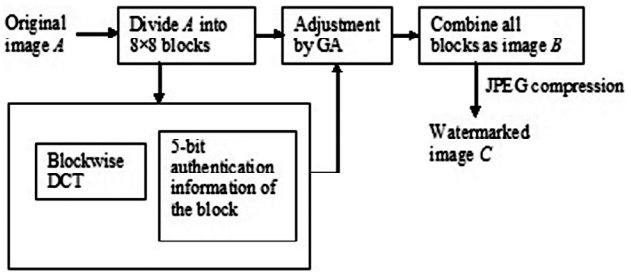


**Figure 1: The Overall Watermark Embedding Procedure**

## 3. RESULT AND DISCUSSION

For the performance analysis of Cover Image (CI) and Payload (PL) of any size and formats are considered. The payload Barbara image is that the embedded into the cover Lena image to derive the stego image and the payload is retrieved from stego image using reverse embedding process. The cover Baboon image is considered into which the payload Cameraman (CM) image is hidden to generate stego image. The Maximum Hiding Capacity (MHC) in terms of bits and percentage as well as the PSNR between the cover image and stegoimage is tabulated for existing algorithm. Adaptive Steganography Based on Integer Wavelet Transform (ASIWT). It is observed that the PSNR is improved around 25% in the proposed algorithm compared to the existing algorithm for the same MHC.

**Figure 2: (*a*) CI: Lena (*b*) PL: Barbara (*c*) Stego Image (*d*) Retrieved PL**

**Figure 3: (*a*) CI: Baboon (*b*) PL: Cameraman (*c*) Stego Image (*d*) Retrieved PL**

## 4. CONCLUSION

The conclusion of the data hiding is to avoid peeper from discovering the secret messages embedded in the cover-images. To improve the capacity of hidden message, we propose a new steganographic method to increase the message load in every block of the stego-image while keeping the stego-image quality acceptable. In our method, the secret message is embedded in the middle-frequency part of the quantized DCT coefficients. Our experimental results show the proposed method provides acceptable image quality and a large message capacity. Moreover, based on our security analysis, we observe that the proposed method has the same camouflage and thus has the same security level as Jpeg- Jsteg. Overall, the proposed method matches the requirement of steganography with a larger message capacity than that of Jpeg-Jsteg.

## REFERENCES

[1] Raja K.B., C.R. Chowdary, Venugopal K.R., L.M. Patnaik. (2005). "A Secure Steganography using LSB, DCT and Compression Techniques on Raw Images", *IEEE International Conference on Intelligence Sensing and Information Processing*, pp. 171-176.

[2] Kumar V. and Kumar D. (2010). "Performance Evaluation of DWT Based Image Steganography", *IEEE International Conference on Advance Computing*, pp. 223-228.

[3] Weiqi Luo, Fangjun Huang, and Jiwu Huang (2010). "Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE Transactions on Information Forensics and Security*, **5(2)**, pp. 201-214.

[4] R.O. El Safy, H.H. Zayed and A. El Dessouki (2009). "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", *International Conference on Networking and Media Convergence*, pp. 111-117.

[5] Mathkour H., Al-Sadoon B. and Touir A. (2008). "A New Image Steganography Technique", *International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4.

[6] V. Vijaylakshmi, G Zayaraz and V Nagaraj, (2009). "A Modulo Based LSB Steganography Method", *International Conference on Control, Automation, Communication and Energy Conservation*, pp. 1-4.

[7] Wien Hong, Tung-Shou Chen and Chih-Wei. (2008). "Lossless Steganography for AMBTC-Compressed Images", *Congress on Image and Signal Processing*, pp. 13-17.

[8] A.W. Naji, Teddy S. Gunawan, Shihab A. Hameed, B.B. Zaidan and A.A. Zaidan. (2009). "Stego-Analysis Chain, Session One", *International Spring Conference on Computer Science and Information Technology*, pp. 405-409.

[9] M. Hassan Shirali-Shahreza and Mohammad Shirali-Shahreza. (2008). "A New Synonym Text Steganography", *International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1524-1526.

[10] Vladimir Banoci, Gabriel Bugar and Dusan Levicky (2009). "Steganography Systems by using CDMA Techniques", *International Conference on Radio Electronika*, pp. 183-186.