Vector Quantization In Image Steganography

[1]Veerdeep Kaur Maan, [2]Harmanjot Singh Dhaliwal
[1]*Student, M.Tech ECE, Punjabi University Patiala*
[2]*Assistant Professor, UCOE, ECE, Punjabi University Patiala*

Abstract

With the growth of data communication security has become a major concern. Image Steganography is the greek origin word which means "hidden writing". The redundant bits in cover media are removed and secret data is inserted into the space. The stegano-image should be almost identical to the original image thus the information content should not be lost. The value of performance parameters i.e Capacity, PSNR should be large and at the same time has minimum MSE and reduced computation time.

1. Introduction

Steganography is embedding a secreat message in a cove message. Watermarking aims to protect the copyrights of digital media (i.e. images, music, video and software) owners. Therefore, the goal of steganography is the secret messages while the goal of watermarking is the cover object itself [1].

The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a significantly larger object so that the change is undetectable by the human eye [2].

All digital file formats can be used for steganography, but the formats those are with a highdegree of redundancy are more suitable [3]. The redundant bits of an object are those bits that canbe altered without the alteration being detected easily. The most popular cover objects used for steganography are digital images. Digital images often have a large amount of redundant data, and this is what steganography uses to hide the message [4].

Steganography and Cryptography are parallel data security techniques and the techniques can be implemented side by side, in fact steganographic system can implement cryptographic data security. With cryptography we can protect the message but not hide its existence [5]. Steganography pay attention to the degree of invisibility while cryptography pays attention to the security of the message [6]. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [7]. Cryptography merely obscures the integrity of the information so that it does not make sense to anyone except the creator and the recipient. Steganography could be considered as the dark cousin of cryptography. Cryptography assures privacy whereas Steganography assures secrecy. Steganography and cryptography are both used to ensure data confidentiality. However, steganography differs from cryptography in the sense that the cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Thus, with cryptography anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message in such a way that nobody can see that both parties are communicating in secret [8, 9].

The strength of steganography can thus be increased by combining it with cryptography. There is a great interest in this subject over the last two decades, and there are two main reasons. Firstly, the publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in, audio recordings, books and multimedia products; an appreciation of new market opportunities created by digital distribution is coupled with a fear that digital works could be too easy to copy. Secondly, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages. The ease with which this can be done may be an argument against imposing restrictions [10].

Other applications for steganography include the automatic monitoring of radio advertisements, where it would be convenient to have an automated system to verify that adverts are played as contracted; indexing of videomail, where we may want to embed comments in the content; and medical safety, where current image formats such as DICOM separate image data from the text (such as the patient's name, date and physician), with the result that the link between image and patient occasionally gets mangled by protocol converters. Thus embedding the patient's name in the image could be a useful safety measure. Where the application involves the protection of intellectual property, we may distinguish between watermarking and _ngerprinting. In the former, all the instances of an object are marked in the same way, and the object of the exercise is either to signal that an object should not be copied, or to prove ownership in a later dispute. One may think of a watermark as one or more copyright marks that are hidden in the content. With _ngerprinting, on the other hand, separate marks are embedded in the copies of the object that are supplied to different customers. The effect is somewhat like a hidden serial number: it enables the intellectual property owner to identify customers who break their license agreement by supplying the property to third parties. In one system we developed, a specially designed cipher enables an intellectual property owner to encrypt a _lm soundtrack or audio recording for broadcast, and issue each of his subscribers with a slightly different key; these slight variations cause imperceptible errors in the audio decrypted using that key, and the errors identify the customer. The system also has the property that more than four customers have to collude in order to completely remove all the evidence identifying them from either the keys in their possession or the audio that they decrypt [11,12].

Data hiding methods for images can be divided into two parts, spatial-domain methods and frequency-domain methods. In the spatial domain the secret messages are directly embedded into the image pixels. In the frequency-domain firstly, the secret image is transformed to the frequency-domain, and then the messages are embedded in the transformed coefficients. [13]. Any stego algorithm removes the redundant bits in the cover media and inserts the secret data into the space. Many carrier messages can be used in the recent technologies, such as Image, text video and many others. The image file is the most popular used for this purpose because it easy to send during the communication between the sender and receiver. The images are divided into three types: binary (Black- White), Gray scale and Red-Green-Blue (RGB) images. The binary image has one bit value per pixel represent by 0 for black and 1 for white pixels. While the gray scale image has 8 bits value per pixel represent from 00000000 for black and 11111111 for white pixels. The RGB image has 24 bits values per pixel represent by (00000000, 00000000 and 00000000) for black and (11111111, 1111111 and 11111111) for white pixels. The RGB image is the most suitable because it contains a lot of information that help in hiding the secret information with a bit change in the image resolution which does not affect the image quality and make the message more secure[14].

Vector Quantization (VQ) is one of the techniques based on the principle of block coding that have long been used to compress media in order to make efficient use of network bandwidth and data storage space. The codewords of the codebook are used to substitute the closest pixel block of the image during the compressing. The resultant compressed image is a table of indexes of the codewords. Some steganographic methods for VQ compressed images have been reported in the recent years .A common feature of the methods is that they all partition the codebook into a number of groups or clusters and then embed the secret message by replacing the codeword indexes of the compressed image with those of the same group / cluster selected according to the corresponding secret bits For example with a cluster of 8 (= 23) codewords, each codeword can embed 3 bits of the secret message. If the sequence of the secret bits is 102, (or 112), the second (or third) codeword is used to replace the original codeword. The receiving end of the stego-image needs to have the same clustering of the same codebook. The secret message is extracted by concatenating the position (in binary form) of the received codewords in their groups / clusters. Therefore, we can see that the greater the cluster, the greater the embedding capacity. However, the greater a cluster is, the greater the variance among the codewords in the group becomes. It means the average embedding distortion can be greater because the possibility that a codeword get replaced with a more distant codeword is higher. So striking a balance between embedding capacity and distortion is important but, unfortunately, not trivial. The feasibility resides in the optimality of the codebook clustering algorithm [15].

A. Evaluation Parameters

Most researchers use Peak Signal to noise ratio (PSNR), Mean Square Error (MSE) and Hiding Capacity as performance parameters to measure the quality of image.

(a) **Mse:** It is defined as square of error between cover & stego image. The error indicates the distortion in an image.

MSE can be calculated by using 2-D mathematically equation described as follows:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where Xij = The value of pixel in cover image *X* ij = The value of pixel in stego image N=Size of image

(b) **Psnr**: It is measure of quality of image.

PSNR can be calculated by using mathematically equation given below:

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

(c) **Capacity:** Steganographic capacity is the maximum no of bits that can be embedded in a cover image with a negligible probability of detection by an adversary [13]. It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp) and the Maximum Hiding Capacity (MHC) in terms of percentage.

2. Related Work

Tseng and Chang proposed a novel steganographic method based on JPEG. The DCT for each block of 8x8 pixels was applied in order to improve the capacity and control the compression ratio [16]. The widely known JPEG-based steganographic tool Jpeg-Jsteg divides the cover image into nonoverlapping blocks of 8x8 pixels. It embeds the secret data in the LSB of the quantized DCT coefficients of each block. Since it embeds only one bit in each quantized coefficient whose value is not 1, 0, or -1, the capacity of this method is very limited [17]. Since the energy of images is concentrated in the lower frequency coefficients, modifying such coefficients may cause a quality degradation of output image. However, high frequency coefficients will be discarded due to the quantization process. Chang et al. developed a steganographic method based upon JPEG and modified 8x8 quantization table in order to improve the hiding capacity of Jpeg-Jsteg method. They utilized the middle frequency for embedding in order to achieve better hiding capacity and acceptable stego-image quality [18].

After that, Almohammad et al. proposed a steganographic method based upon blocks of size 16x16 pixels and modified 16x16-pixel quantization table with the same technique used by Chang et al. They found that their method can embed more secret messages than the method based on 8x8-pixel blocks. Additionally, the computational time of their method is a bit less than Chang et al.'s method as well [19].

After that, Natee Vongurai and Suphakant Phimoltares proposed a the frequency based steganography using block size of 32x32 pixels. The interpolated 32x32-pixel quantization table was created by using the cubic spline interpolation technique. The cover image is first transformed into frequency domain by using DCT and the secret messages are then embedded after the quantization process. The results showed that large secret messages can be embedded than the others and compression ratiowas also better. Also, computation time taken was less than that of the other methods [20].

3. Conclusion

Steganography is a technique to hide data in a image. In this paper various block sizes are discussed in which the secret data can be hided. From the above discussion it is concluded that by increasing the block size of cove image performance can be improved. In future, work can be done by increasing the size of the blocks.

4. References

[1]- R. Chu, X. You, X. Kong and X. Ba, "A DCT-based image steganographic method resisting statistical attacks", *In Proceedings of (ICASSP '04), IEEE International Conference on Acoustics, Speech, and Signal Processing*, 17-21 May. vol.5,2004,ppV-953-6.

[2]- Huang, Y. S., Huang, Y. P., Huang, K.N. and Young, M. S. (2005), "The Assessment System of Human Visual Spectral Sensitivity Curve by Frequency Modulated Light", *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, pp. 263-265.

[3]- Laskar, S.A. and Hemachandran, K. (2012), "An Analysis of Steganography and Steganalysis Techniques", *Assam University Journal of Sscience and Technology*, Vol.9, No.II, pp.83-103, ISSN: 0975-2773.

[4]- Curran, K. and Bailey, K. (2003), "An Evaluation of Image Based Steganography Methods", *International Journal of Digital Evidence Fall* 2003, Volume 2, Issue 2.

[5]- Younes, M.A.B. and Jantan, A. (2008), "Image Encryption Using Block-Based Transformation Algorithm," *International Journal of Computer Science*, Vol. 35, Issue.1, pp.15-23.

[6]- Friedman, W.F. (1967), "Cryptology", *Encyclopedia Britannica*, Vol. 6, pp. 844-851, 1967.

[7]- Dickman, S.D. (2007), "An Overview of Steganography", *JMU-INFOSEC-TR*-2007-002,

[8]- Raphael, A. J. and Sundaram, V. "Cryptography and Steganography – A Survey", *Int. J. Comp. Tech. Appl.*, Vol 2 (3), pp. 626-630 , ISSN:2229-6093.

[9]-Shamim Ahmed Laskar1 and Kattamanchi Hemachandran," High Capacity data hiding using LSB Steganography and Encryption", *International Journal of Database Management Systems (IJDMS)* Vol.4, No.6, December 2012.

[10]- E Franz, A Jerichow, S M¨oller, A P_tzmann, I Stierand "Computer Based Steganography in Information Hiding", *Springer Lecture Notes in Computer Science* v 1174 (1996) pp 7-21.

[11]- R Anderson, C Manifavas, "Chameleon A New Kind of Stream Cipher", *to appear in Proceedings of the 4th Workshop on Fast Software Encryption* (1997)

[12]- Ross J. Anderson, Fabien A.P. Petitcolas," On The Limits of Steganography'', *IEEE Journal of Selected Areas in Communications*, 16(4):474-481, May1998.

[13]- Neha Batra, Pooja Kaushik, "Implementation of Modified 16×16 Quantization Table Steganography on Colour Images", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue10,October2012.

[14]- Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality",*Applied Mathematical Sciences*, Vol. 6, 2012,no.79,p.3907–3915.

[15]- Yue Li and Chang-Tsun Li," Steganographic Scheme for VQ Compressed Images Using Progressive Exponential Clustering", *Proceedings of the IEEE International Conference on Video and Signal Based Surveillance* (AVSS'06) 0-7695-2688-8/06.

[16]-H.-W.Tseng and C.-C. Chang, "Steganography using JPEG-compressed images", *The Fourth International Conference on Computer and Information Technology, CIT* '04, 14-16 Sept 2004,pp.12-17.

[17]- Y.-H. Yu, C.-C. Chang and Y.-C. Hu, "Hiding secret data in images via predictive coding*", Pattern Recognition*, vol. 38, 2005, pp. 691-705.

[18]- C.-C. Chang, T.-S. Chen and L.-Z. Chung, "Asteganographic method based upon JPEG and quantization table modification", *Information Sciences*, vol. 141, 2002, pp. 123-138.

[19]- A. Almohammad, R. M. Hierons, G. Ghinea, "High capacity steganographic method based upon JPEG*," IEEE 3rd Int. Conf. On Availability, Reliability and Security*, 2008, pp. 544-549.

[20]- Natee Vongurai and Suphakant Phimoltares, "Frequency-Based Steganography Using 32x32 Interpolated Quantization Table and Discrete Cosine Transform*", 2012 Fourth International Conference on Computational Intelligence, Modelling and Simulation.*