Visual quality of stego-image using Haar Wavelet

Subrahmanyam.Ch[1], P.Kiranmayi[2], Dr.V.Sailaja[3], K.Jyothi[4]

[1]*Department of Technical Education Andhra Pradesh, Hyderabad*
[2,3,4]*Godavari Institute of Engineering & Technology*

Abstract: *In this paper, we present the quality images using Haar wavelet. In order to provide large capacity of the secret data while maintaining good visual quality of stego-image, the embedding process is performed in transform domain of Discrete Wavelet transform (DWT) by modifying of transform coefficients in an appropriate manner. In addition, the proposed method do not require original image for successful extraction of the secret information. The experimental results show that the proposed method provides good capacity and excellent image quality. This fact is more critical in stego analysis research of area, where its methods could easily find the patterns of artificial changes by comparing the original and stego object.*

I.   Introduction

Digital watermarking is mainly used in copyright protection, while steganography is a method of embedding the secret message into a camouflage media to ensure that unintended recipients will not be aware of the existence of the embedded secret data in cover media. Thus, whole system can be considered as secret communication. However, steganography is different from cryptography as it is a part of secret communication where its techniques may fail since a cipher text has meaningless form and thus easily arouses the curiosity of malicious attackers who are willing to consume the substantial amount of time and energy to recover or destroy data. Unlike cryptography, steganography conceals the fact that there is secret communication going on and still image may be represented as well suited camouflage media for embedding of secrete data. Even more, the advantage of cryptography techniques are executed on secret data before embedding into still image; to strengthen security level and also to suppress the energy compaction of secret data.

Firstly, *visual attacks* try to reveal the presence of hidden information through inspection with naked eye or with the assistance of a computer, which can separate the image into bit planes for further analysis. Secondly, *statistical attacks* are more powerful and successful, because they reveal the smallest alterations in an image´s statistical behaviour. These attacks can be further classified as (i) Passive attack and (ii) Active attack. Passive attacks deal with identifying the presence or absence of a covert message or the embedding algorithm used etc. whereas the goal of active attacks is to estimate the embedded message length or the locations of the hidden message or the secret key used in embedding. Thirdly, *structural attacks* are based on fact that format of the data files often changes as the data to be hidden are embedded; on identifying these characteristic structure changes can detect the existence of image.

II.   Stego-image

The basic principle of embedding secret object is defined in sense of similarities stego and cover object and its measure can be expressed by function of conformity. However, this function of perceptibility does not have wide practical use. Hence, the objective measures, which stem from statistical approach, are used in general. Subjective measures are based on human examination (cluster of observers), which results are categorized to multi-level hierarchy. The measurement of subjective measures is hard to conduct and replicate with identical values even though its results converging to ideal state in case of examination of stego image by human observer. Contrariwise, the objective measures are based on the mathematical apparatus and therefore are independent to The Contrast Sensitivity Function (CSF) denotes sensitivity of the different frequency of HVS model to the different spatial frequencies.

The algorithm calculates the peak signal to noise ration weighted by CSF function. The aim of this objective measure was to approximate to ideal subjective measures.

III.   Experiment

The proposed method processes grey scale images as cover object for creating subliminal channel and it utilizes transform coefficients of 2-Dimensional Discrete Transform (2-DWT) for embedding process. The secret object could consist of any kind of binary data file. The elected cover image is decomposed by DWT transform. This transform provides an approximation and three detail coefficients (horizontal, vertical and

diagonal) on each decomposition level. The main objective is fulfill the condition of stealth communication as well as imperceptibility of embedded secret message in cover object and that is in the case of image steganography scrutinized by human observer or any statistical methods. Therefore, the detail coefficients are the most convenient area for secret message embedding.

IV. Results
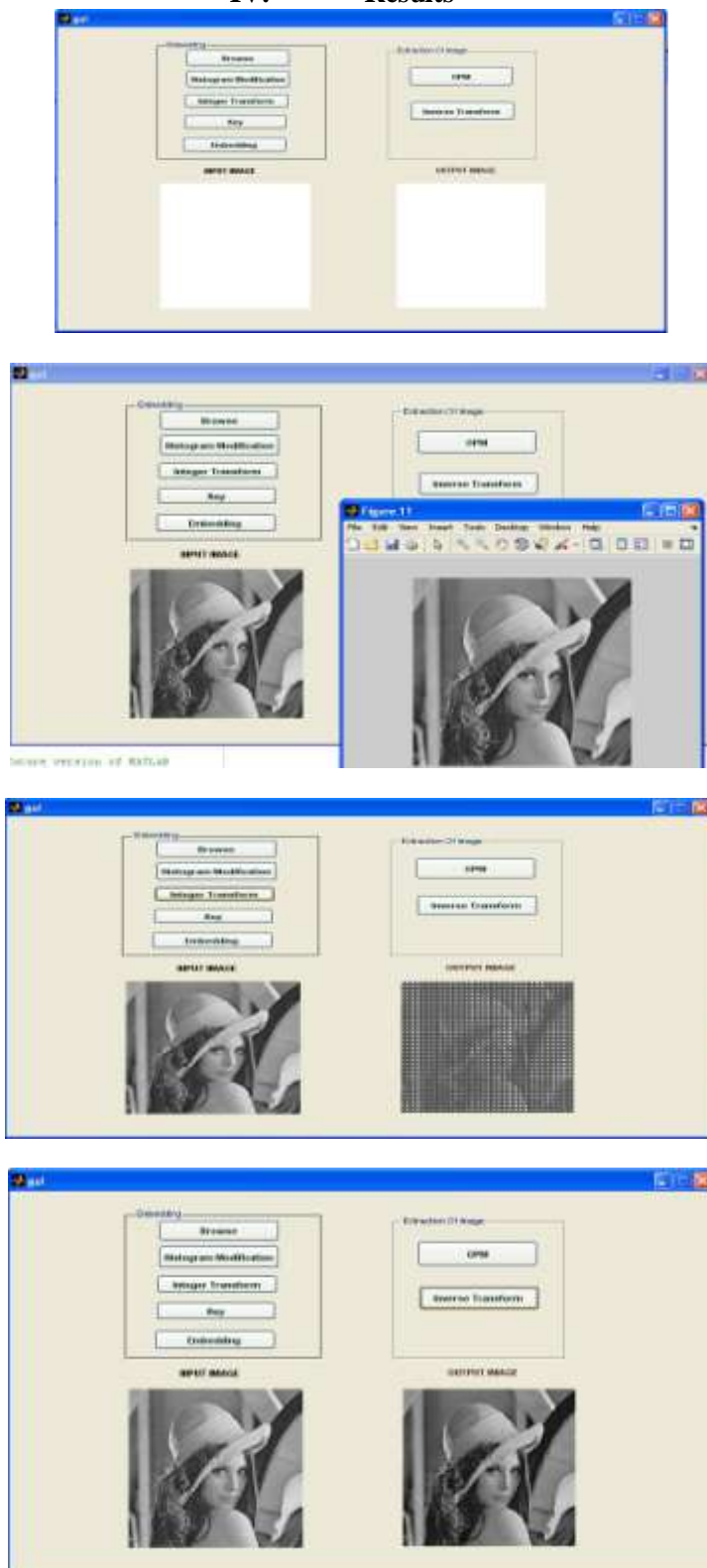
The capacity of the method remains the same and it is represented by 1/4 of cover image size for 1-level decomposition of the cover image. The payload is 0.25 bit/pixel in case of using the maximum capacity and it also varies depending on numbers of detail coefficient are used during the embedding phase. The proposed algorithm employs 1-Level *L* decomposition of the image hence the total capacity (in bits) is represented by 1/4 of image size number of DWT detail coefficient, which are altered.

V.   Conclusion

The model is implemented, based on the local image characteristics around quality, to expose only the perceptually prominent regions in an image. The proposed method is validated with stego-image regions resulting from experiment, and shows to be highly consistent with subjective data. The performance of our approach is compared to existing alternatives in literature, and has been proved to be promising in terms of both reliability and computational efficiency. The proposed method is meanwhile extended with a DWT annoyance metric that can quantify perceived annoyance of compressed images.

References

[1]   I.-R. R., *BT.500-11, Methodology for the Subjective Assessment of the Quality of Television Pictures*. Geneva, Switzerland: Int. Telecommun. Union, 2002.

[2]   C. Liu, R. Szeliski, S. B. Kang, C. L. Zitnick, and W. T. Freeman, "Automatic estimation and removal of noise from a single image," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 30, no. 2, pp. 299–314, Feb. 2008.

[3]   S. Paris and F. Durand, "A fast approximation of the bilateral filter using a signal processing approach," *Int. J. Comput. Vis.*, vol. 81, pp. 24–52, 2009.

[4]   S. H. Oguz, "Morphological post-filtering of ringing and lost data concealment in generalized lapped orthogonal transform based image and video coding," Ph.D. dissertation, Univ.Wisconsin, Madison, WI, 1999.

[5]   M. Shen and C. J. Kuo, "Review of postprocessing techniques for compression artifact removal," *J. Vis. Commun. Image Rep.*, vol. 9, no. 1, pp. 2–14, 1998.

[6]   J. Luo, C. Chen, K. Parker, and T. S. Huang, "Artifact reduction in low bit rate dct-based image compression," *IEEE Trans. Image Processing*, vol. 5, pp. 1363–1368, 1996.

[7]   K. Zon and W. Ali, "Automated video chain optimization," *IEEE Trans. Consum. Electron.*, vol. 47, pp. 593–603, 2001.

[8]   Z. Wang, A. C. Bovik, and B. L. Evans, "Blind measurement of blocking artifacts in images," in *Proc. IEEE Int. Conf. Image Processing*, 2000, vol. 3, pp. 981–984.

[9]   H. Liu and I. Heynderickx, "A perceptually relevant no-reference blockiness metric based on local image characteristics," *EURASIP J. Adv. Signal Process.*, vol. 2009.

[10]   S. Rusinkiewicz and M. Levoy, "Efficient variants of the ICP algorithm," in *Proc . 3rd Int. Conf. 3D Digital Imaging and Modeling (3DIM)*, Jun. 2001, pp. 145–152.

[11]   G. C. Sharp, S. W. Lee, and D. K. Wehe, "Icp registration using invariant features," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 1, pp. 90–102, Jan. 2002.

[12]   D. Arthur and S. Vassilvitskii, "Worst-case and smoothed analysis of the icp algorithm, with an application to the k-means method," in *Proc. 47th Annu. IEEE Symp. Foundations of Computer Science (FOCS)*, 2006, pp. 153–164.