Robust Steganography Model for Highembedding Capacity with Minimal Distortion by using Integer Wavelet Transform

Harendra Kumar
Assistant Professor, Department of Computer science and engineering
Shekhawati Group of Institutions Sikar, Rajasthan

Abstract: Steganography is the art and science of concealing information in unremarkable cover media so as not to arouse an eavesdropper's suspicion. It is an application under information security field. Being classified under information security, steganography will be characterized by having set of measures that rely on strengths and counter measures (attacks) that are driven by weaknesses and vulnerabilities. Today, computer and network technologies provide easy-to-use communication channels for steganography. The aim of this present paper, the use of optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the cover image in order to maximize the hiding capacity as much as possible. We also used a pseudorandom generator function to select the embedding locations of the integer wavelet coefficients to increase the system security.

Keywords: security, Steganography, wavelets, information hiding and cryptography.

I. INTRODUCTION

Steganography is a type of hidden communication that literally means "covered writing" (from the Greek words *stegano* or "covered" and graphos or "to write"). The goal of steganography is to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message [6, 7, and 8]. Oftentimes throughout history, encrypted messages have been intercepted but have not been decoded. While this protects the information hidden in the cipher, the interception of the message can be just as damaging because it tells an opponent or enemy that someone is communicating with someone else. Steganography takes the opposite approach and attempts to hide all evidence that communication is taking place. Essentially, the information-hiding process in a Stenographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography's goal is to keep its mere presence undetectable, but stenographic systems, because of their invasive nature, leave behind detectable traces in the cover medium through modifying its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called StatisticalStego analysis.

II. INFORMATION HIDING SYSTEM FEATURES

An information-hiding system is characterized be having three different aspects that contend with each other as shown in Figure 1: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information, and robustness to the amount of modification the stego medium can withstand before an adversary can destroy hidden information [6]. Generally speaking, information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness-that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, strives for high security and capacity, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

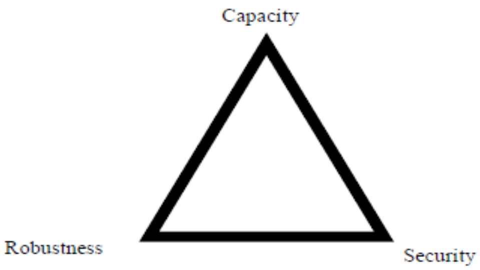


Figure 1. Information-hiding system features.

III. STEGANOGRAPHY SYSTEM

A classical stenographic system's security relies on the encoding system's secrecy. Although such a system might work for a time, once it is known, it is simple enough to expose the entire received media (e.g., images) passing by to check for hidden messages ultimately, such a steganographic system fails.

Modern steganographic system, as shown in Figure 2 attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes [4, 6].

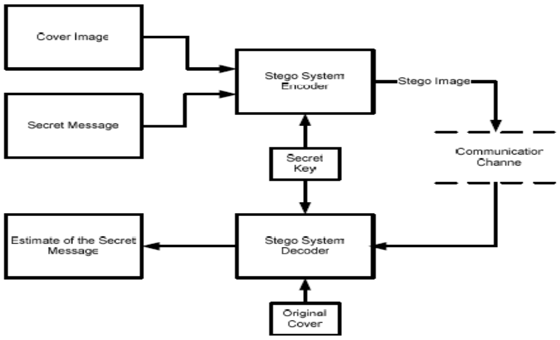


Figure 2 Modern Steganography system

Three basic types of stego systems are available:

- . Pure stego systems - no key is used.
- . Secret-key stego systems - secret key is used.
- Public-key stego systems - public key is used.

The technique that is followed in this paper will use secret key to encrypt the hidden message that will be encapsulated inside a cover media.

IV. USE OF WAVELET TRANSFORM IN STEGANOGRAPHY

The Wavelet domain is growing up very quickly. A lot of mathematical papers and practical trials are published every month. Wavelets have been effectively utilized as a powerful tool in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing [1, 9].

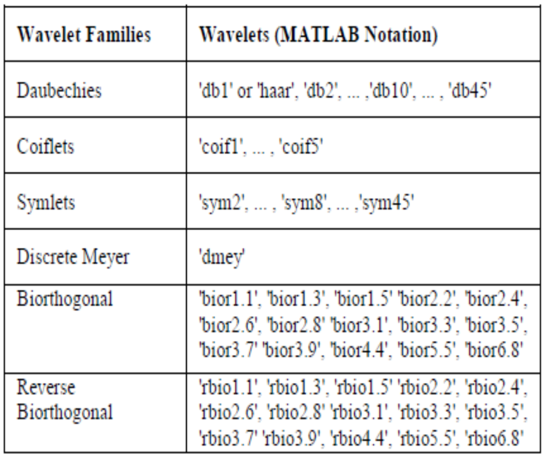
Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the Information- Hiding system features. The work described in this paper implements steganography in the Wavelet domain. The hierarchical nature of the Wavelet representation allows multi-resolution detection of the hidden message, which is a Gaussian distributed random vector added to all the high pass bands in the Wavelet domain. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain [1, 8, and 9].

A Wavelet is simply, a small wave which has itsenergy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two-parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal. In Wavelet transform, the original signal (1-D, 2-D, 3-D) is transformed using predefined wavelets. The wavelets are orthogonal, orthonormal, or bi-orthogonal, scalar or multiwavelets [2, 10].

The DWT used in this paper is implemented using the functions available with MATLAB to simplify the analysis and minimize development time. The following discussion illustrates the idea of Wavelet transformation as applied to the area of image processing [10].

4.1 Wavelet Filters:

In order to use the Wavelet transform, Wavelet filters should be selected and used in the transformation and inverse-transformation. For that purpose, a lot of theoretical work is available to illustrate different Wavelet filters with different features. For the purpose of fast analysis and development, the Wavelet filters available with MATLAB Wavelet toolbox were selected and tested [10, 8, and 9]. Available orthogonal or bi-orthogonal Wavelets are listed in the Table 1 [10].



Wavelet Families	Wavelets (MATLAB Notation)
Daubechies	'db1' or 'haar', 'db2', ... ,'db10', ... , 'db45'
Coiflets	'coif1', ... , 'coif5'
Symlets	'sym2', ... , 'sym8', ... ,'sym45'
Discrete Meyer	'dmey'
Biorthogonal	'bior1.1', 'bior1.3', 'bior1.5' 'bior2.2', 'bior2.4', 'bior2.6', 'bior2.8' 'bior3.1', 'bior3.3', 'bior3.5', 'bior3.7' 'bior3.9', 'bior4.4', 'bior5.5', 'bior6.8'
Reverse Biorthogonal	'rbio1.1', 'rbio1.3', 'rbio1.5' 'rbio2.2', 'rbio2.4', 'rbio2.6', 'rbio2.8' 'rbio3.1', 'rbio3.3', 'rbio3.5', 'rbio3.7' 'rbio3.9', 'rbio4.4', 'rbio5.5', 'rbio6.8'

Table 1. Wavelet Families

In this paper, different Wavelet families were tried in the transformation. However, sym4 was chosen as a case study.

V. Cryptography and Steganography

The use of cryptography as a way to secure the hidden message mainly addresses the security requirement in the Information-Hiding system. For the purpose of steganography, symmetric encryption is followed. The symmetric encryption is a method of encryption that uses the same key to encrypt and decrypt a message. If one person encrypts and decrypts data, that person must keep the key secret. If the data is transmitted between parties, each party must agree on a shared secret key and find a secure method to exchange the key [9].

The security of encrypted data depends on the Secrecy of the key. If someone gains knowledge of the secret key, he or she can use the key to decrypt all the data that was encrypted with the key [9, 11]. Table 2 shows common algorithms for symmetric key encryption.

No encryption method is completely secure. Given knowledge of the algorithm and enough time, attackers can reconstruct most encrypted data. A strong algorithm (the one that is built on sound mathematical methods, creates no predictable patterns in encrypted data, and has a sufficiently long key) can deter most attacks [3, 9, 11].

When a strong algorithm is used, the only way tobreak the encryption is to obtain the key. An attacker can obtain a key by stealing it, by tricking someone into revealing the key (a form of social engineering), or by trying all possible key combinations. This last method is commonly known as a brute force attack. Increasing the key length exponentially increases the time that it takes an attacker to perform a brute force attack.

VI. The Proposed Method:

Although steganography is applicable to all dataobjects that contain redundancy, in this paper, JPEG images are considered only. People often transmit digital pictures over email and other Internet communication, and JPEG is one of the most common formats for images. Moreover, steganographic systems for the JPEG format seem more interesting because the systems operate in a transform space and are not affected by visual attacks. (Visual attacks mean that steganographic messages can be seen on the low bit planes of an image because they overwrite visual

structures; this usually happens in BMP images). The proposed method contains the following modules and some steps that were implemented using MATLAB 7.6.
6.1 Embedding module: The main work of this type of module is to insert a secret message within the cover grayscale image using a key that one known as encryption key. Before any processing, the entire cover image is partitioned into 8x8 blocks. The frequency domain representation of the respective created blocks is estimated by 2D IWT in order to accomplish 4 sub bands LL1, HL1, LH1, and HH1. Randomly 1 to 64 genes are generated containing the pixels numbers of each 8x8 blocks as after the mapping function. The message bits in 4-LSBs co-efficient of IWT in each pixel according to mapping function are embedded. Fitness evaluation based, Optimal Pixel Adjustment Process on the Image is applied. At last, inverse 2D IWT is computed in this module in order to generate the stego image.The proposed method contains the following steps that were implemented using MATLAB.

6.1.1 Embedding Algorithm:

The following steps explain the embedding process:

Step1. Divide the cover image into 8×8 blocks.

Step2. Find the frequency domain representation of blocks by 2D Haar DWT and get four sub bands LL1, HL1, LH1, and HH1.

Step3. Generate 16 genes containing the pixels numbers of each 8×8 blocks as the mapping function.

Step4. Embed the message bits in k-LSBs IWT coefficients each pixel according to mapping function. For selecting value of k, images are evaluated from k = 3 to 6. k equal to 1 or 2, provide low hiding capacity with high visual quality of the stego image and k equal to 7 or 8, provide low visual quality versus high hiding capacity.

Step5. Fitness evaluation is performed to select the best mapping function.

Step6. Apply OPAP on the image.

Step7. Calculate inverse 2D-HDWT on each 8×8 block.

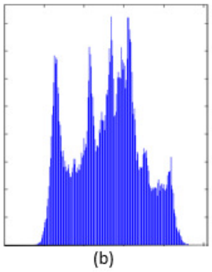
6.2 Extraction module: The main task of this module is the extraction of the actual user text information from the stego image to understand the effectiveness of process of message embedding. It takes the stego image as input with key for decrypting the hidden message from the stego image. Once the data has been transmitted over the communication channel and when the receiver receives the embedded image file, then it becomes necessary to again segment the image data and then take out the text data available at the space covered by the text data at the time of message embedding. The extraction can be summarized in a simple sentence as to take out the data that has been embedded.The proposed method contains the following steps for feature extraction that were implemented using MATLAB.

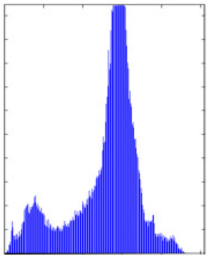
6.2.1 Extraction Algorithm:

The extraction algorithm consists of four steps as follows:
Step1. Divide the cover image into 8×8 blocks.
Step2. Extract the transform domain coefficient by 2D IIWT of each 8×8 block.
Step3. Employ the obtained function in the embedding phase and find the pixel sequences for extracting.
Step4. Extract k-LSBs in each pixel.

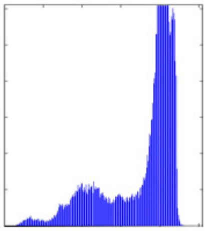
VII. EXPERIMENTAL RESULT

The proposed implementation of RS-analysis using genetic algorithm for the robust security in Steganography application is done on standard 32-bit windows OS with 1.84 GHz processor and 2 GB RAM. The proposed method is applied on 512x512 8-bit grayscale images “Jet”, “Boat”, “Baboon” and “Lena”. The messages are generated randomly with the same length as the maximum hiding capacity.

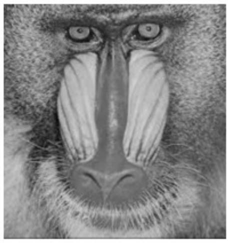


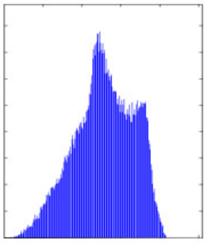


(c) (d)



(e) (f)





(g) (h)

Above figure shows the original cover images along with their histogram analyze which will be used later to compare it with the ones of the resulting stego image to test for imperceptibility.

After some comparison we provide result in table no.2of the obtained PSNR between our proposed method and methods in [11], [12], [13] and [14]. Hence, it can be seen that the proposed system has better performance in compared to majority of the Steganographic techniques using integer wavelet transform and genetic algorithm with RS analysis.

Table 4.5 Comparison of hiding capacity achieved and the obtained PSNR between our proposed method and methods in [11,12, 13 and 14]

Cover Image	Method	Hiding capacity (Bits)	PSNR (DB)
Lena	Proposed	2,13,7696	54.83
	High Capacity [11]	1,048,576	39.94
	Adaptive [12]	986,408	31.8
	HDWT [13]	801,842	33.58
	DWT [14]	573,550	44.90
Baboon	Proposed	2,13,7696	57.83
	High Capacity [11]	1,048,576	40.34
	Adaptive [12]	1,008,593	30.89
	HDWT [14]	883,220	32.69
	DWT [15]	573,392	44.96
Jet	Proposed	2,13,7696	33.51
	High Capacity [11]	1,048,576	45.20
	DWT [15]	573,206	44.76
Boat	Proposed	2,13,7696	54.83
	High Capacity [11]	1,048,576	40.44
	DWT [15]	573,318	44.92

This Table shows the results as compared to previous methods.We can easily analyzefrom the table and results that when k equal to 4, we obtain the higher hiding capacity and reasonable visual quality. So, we take k equal to 4 as the number of bits per pixel.

VIII. CONCLUSION

This work introduced a novel steganography technique to increase the capacityand the imperceptibility of the image after embedding. Geneticalgorithm employed to obtainan optimal mapping function to lessen the error difference between the coverand the stego image and use the block mapping method to preserve the localimage properties. Also we applied the OPAP to increase the hiding capacity of thealgorithm in comparison to other systems.

The presented work proposed a data hiding scheme that hides data into the integer wavelet coefficients of an image. The system combines an integer wavelet transform and the optimum pixel adjustment algorithm to maximize the hiding capacity of the system compared to other systems. The proposed system embeds secret information in a random order using a secret key only known to both sender and receiver. It is an adaptive system which embeds different number of bits in each wavelet coefficient according to a hiding capacity function in order to increase the hiding capacity without sacrificing the visual quality of resulting stego image. The proposed system also reduces the difference between original coefficients values and modified values by using the optimum pixel adjustment algorithm.

REFERENCES

[1] Bilgin A., Sementilli J., Sheng F., and Marcellin W., "Scalable Image Coding Using Reversible Integer Wavelet Transforms," *Computer Journalof Image Processing IEEE Transactions*, vol. 9, no. 4, pp. 1972 - 1977, 2000.

[2] Calderbank R., Daubechies I., Sweldens W., and Yeo L., "Lossless Image Compression Using Integer to Integer Wavelet Transforms," *inProceedings of International Conference onImage Processing*, USA, pp. 596-599, 1997.

[3] Fridrich J., Goljan M., Soukal D., and Holotyak T., "Forensic Steganalysis: Determining the Stego Key in Spatial Domain Steganography," *inProceeding of Electronic Imaging SPIE*, Spain, pp. 631-642, 2005.

[4] Johnson N. and Jajodia S., "Steganography: Seeing the Unseen," *IEEE Computer Magazine*, vol. 25, no. 4, pp. 26-34, 1998.

[5] Lee K. and Chen H., "A High Capacity Image Steganographic Model," *in IEEE Proceedings onVision Image and Signal Processing*, China, pp. 288-294, 2000.

[6] Lu S., *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*, Idea Group Publishing,2005.

[7] Popa R., "An Analysis of Steganographic Techniques," *Working Report on Steganography,* Faculty of Automatics and Computers, 1998.

[8] Provos N. and Honeyman P., "Hide and Seek: An Introduction to Steganography," *ComputerJournal of IEEE Security and Privacy Magazine*, vol. 2, no. 3, pp. 32-40, 2003.

[9] Walker S., *A Premier of Wavelets and Their Scientific Applications*, CRC Press, 1999.

[10] Misiti M., Misiti Y., Oppenheim G., and Poggi J., *Wavelet Toolbox for Use with MATLAB*, User Guide MathWorks Inc., 2000.

[11] Ghasemi E, Shanbehzadeh J, Fassihi N "*High capacity image steganography using wavelet transform and genetic algorithm. In: Lecture notes in engineering and computerscience: proceedings of the international multiconference of engineers and computer scientists 2011"*, IMECS 2011, Hong Kong, 16–18 March 2011, pp 495–498

[12] C. C. Chang, T. S. Chen, and L. Z. Chung, "*A steganographic method based upon JPEG and quantization table modification," Information Sciences",* vol. 141, pp. 123{138, Mar. 2002.

[13] Lai B, Chang L (2006) "*Adaptive data hiding for images based on haar discrete wavelet transform. In: Lecture Notes in Computer Science, Springer-verlag Berlin Heidelberg"*, vol 4319, pp 1085–1093.

[14] A. D. Ker*, "Steganalysis of lsb matching in grayscale images,"* IEEE Signal Processing Letters, vol. 12, pp. 441{444, Jun. 2005.