Steganography Enhancement by combining text and image through Wavelet Technique

Najran N. H. Al_Dawla
Department of CS & IT,
Dr. B. A. M. University,
Aurangabad, India

M. M. Kazi
Department of CS & IT,
Dr. B. A. M. University,
Aurangabad, India

K. V. Kale,
Professor and Head,
Department of CS & IT,
Dr. B. A. M. University,
Aurangabad, India

ABSTRACT

The rapidly proliferated information and evolution of digital technologies by Information hiding in multimedia data has improved the ease of access to digital information enabling reliable, faster and efficient storage, transfer and processing of digital data and leads to the consequence of making the illegal production and redistribution of digital media easy and undetectable. Hence, it poses a novel challenges for researchers. In this paper we present a novel integration of an incorporating text and image steganography to find a solution for enhancing security and protecting data. We proposed an enhancement of steganography algorithm which involves the scheme of discrete wavelet transformation combining text and image by secretly embed encrypted secrete message text data (cipher text) ortext image in the content of a digital image. The system based on levels of encryption and decryption methods performed to enhance the security of the system. Here first generate secrete message text (cipher text) or text image, and then processing deals with embedding and extracting Steganography algorithms. Finally the process deals with extraction of the hiddensecrete message. The experimental result shows a high level of efficiency and robustness of the proposed system.

Keywords

Steganography, Cryptography, Text, Image, Secret Key, Security, DWT.

1. INTRODUCTION

In this era, the incorporate of Digital Steganography and cryptography are the fascinating scientific area which falls under the umbrella of security system.

Due to the escalation use of multimedia across the Internet, multimedia distribution became an imperative way to deliver services around the world. It is commonly applied in Internet marketing campaigns and electronic commerce web sites. In particular, has explored means of new business, scientific, entertainment, and social opportunities. One of the great advantages of digital data is that it can be reproduced without losing the quality. Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. The ease by which digital information can be duplicated and distributed has led to the need for effective copyright protection tools. [1] For instance, identity and verify document attacks are on the rise because easy-to-use digital image tools that available at decreasing prices [2] security has become an important issue during the storing and transmission of digital data. The security of images is an application layer technology to guard the transmitted information against unwanted disclosure as well as to protect the data from modification while in transit. There are many real life applications of Steganography being used [2, 4].

Digital Steganography describe techniques that are used to imperceptibly convey information by hide secrets into the cover-data such as an image, document, audio, video file, so that no other people can detect or extract the existence of the secrets. [1, 3] A steganography method consists of an embedding algorithm and an extraction algorithm. The embedding algorithm describes how to hide a message into the cover object and the extraction algorithm illustrates how to extract the message from the steganography object.

On the other hand, Cryptography [6, 7] is the art or science of secret writing [4], studies the mathematical techniques of secrecy or information security such as confidentiality, data integrity, entity authentication and data origin authentication. Secrecy is at the heart of cryptography [5] Encryption and Decryption are a practical way of achieving information secrecy.

This paper is organized as follows. In section 2, we discuss an introduction of generating an encryption and decryption of a secrete message. Embedding and extracting strategies is proposed and describes in section 3, Experimental result and conclusion are given in section 4 and 5 respectively.

2. GENERATE ENCRYPTION AND DECRYPTION OF SECRETE MESSAGE

This section describe the generation of an encryption and decryption of a secrete message such as text or text image. Cryptography is formally the art and science of encoding data in a way that only the intended recipient can decrypt it, and know that the message is authentic and unchanged. Fig .1 Shows the process of how to Encrypt and decrypt the secrete message as text by using a complex mathematical algorithms [6] which take messages as numbers or algebraic elements on a space and then transform them into two regions, a region of meaningful messages as input called clear text; when an encryption algorithm is applied it will result in an unintelligible message as output i.e.cipher text (unreadable cipher) in a second region [4].

These algorithms transfer the data into streams or blocks of seemingly random characters. By applying the reverse process of encryption, that is, decryption, the encryption information will be restored to its original content. An encryption key might encrypt, decrypt, or perform both functions, depending on the type of encryption algorithm being used. The system of encryption and decryption algorithms together with the keys and description of the format of messages constitute a cryptosystem. The term key refers to a numerical value used by an algorithm to alter information, making that informationsecure and visible only to individuals who have the corresponding key to recover the information,where the security of the system is based on the difficulty of encrypt and decrypt computation without special side information known as keys. A cipher is a mathematical function that both encrypts and decrypts a message with the known (secret) key. The result of using the decryption method and the decryption key to decrypt cipher text produced by using the encryption method and the encryption key should always be the same as the original secrete message.

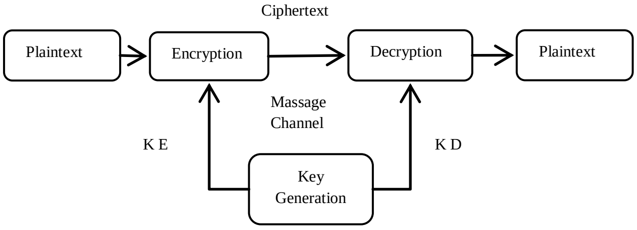


Fig 1: Cryptographic System scheme.

3. HIDING DATA SCHEME

In this section, we will discuss in detail the overall view of combining text (cipher text) as secret information and image of the introduced hiding Secrete Data Scheme. It is composed to the following processes: (1) process of cryptographic system: (2) Discrete wavelet transformation (DWT). (3) Embedded secrete message process. (4) Detected and extract secrete message process. Fig.2. illustrates the overall view of the system.

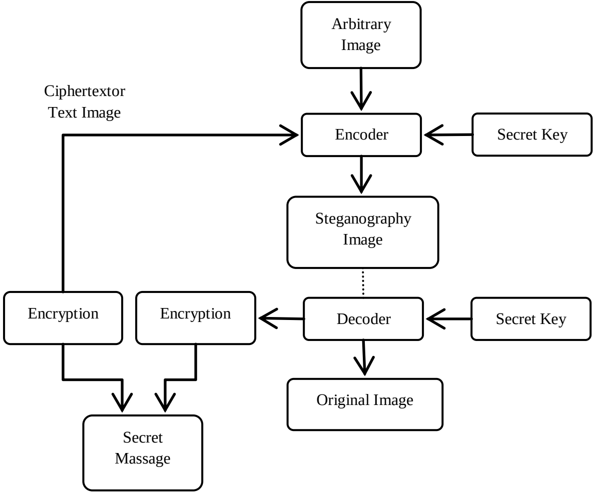


Fig 2: Hiding Secret Message scheme.

3.1 Cryptographic system and Secrete message generate

Cryptographic system Consists of the a secrete message (plaintext), encryption, cipher text, keys, and decryption To ensure secure communication, cryptography essentially transforms and disguises the message that is being transmitted over an open-public channel. Sender can apply the transformation to the sensitive message, or the plaintext, to obtain the transformed message, or the cipher text. This process is called the encryption. Analyzing the cipher text must not reveal the corresponding plaintext. An important property of this kind of transformation is that it must be invertible, but unless a particular secret is known, getting plaintext directly from theCipher text is hard. This secret is often referred to as the key. Finally, the inverse transformation on the recipient side is called the decryption [7, 8]. Fig.1. illustrates this common cryptographic system.

3.2 Discrete wavelet transform (DWT)

The frequency domain transforms being the fundamental tools in the digital signal processing field [9, 10]. The main reason of using frequency domain Steganography is for analyzing signals and it is very secure, hard to detect, flexible and has different techniques for manipulation of its coefficients values. We proposed a Haar-DWT, the simplest DWT [11]. A 2-D Haar-DWT consists of two steps as illustrated in Fig.3. One is the horizontal operation and the other is the vertical one. Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (L) while the pixel differences represent the high frequency part of the original image (H). Step 2: scan the pixels from top to bottom in vertical direction. Perform the addition and subtraction operations on neighboring pixels and then store the sum on the top and the difference on the bottom as illustrated in Figure 3. Repeat this operation until all the columns are processed. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and hence looks very similar to the original image. [12, 13].

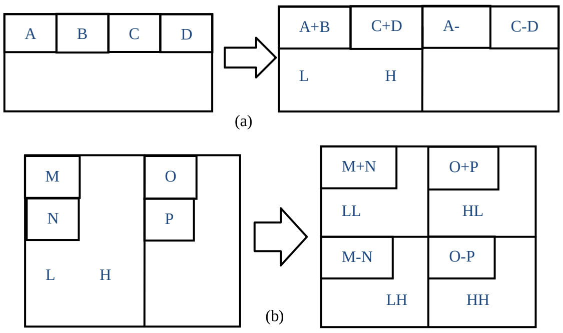


Fig 3: (a)The horizontal operation on the first row, (b) vertical operation.

3.3 Embedding scheme

The block diagram of our proposed method in fig.4, Shows how to hide the secrete message such as text/image in a wavelet domain transformation steganography, adopted for the purpose of high security, good visibility, and no loss of secrete message. The Steps of the embedding scheme proposed.

1. We Embed the information in a high texture of a host image, if the secrete message in text form, then ID bit stream obtained by converting the American Standard code for information interchange (ASCII) into 8 bit binary and link them as a sequence, else if the secrete message a gray scale image, we simply converting each pixel value into 8 bit gray level and link them as a sequence. Encrypt the secret information by using ALHTERBAHN-128 cipher steam before hiding them. Pseudo-random permutation off secrete message is used.

2. Use 2-D wavelet decomposition of gray or colored scale to determine the position and magnitude to adaptively embed the secrete message, and then compute the approximation coefficients matrices.

3. Divided the cover image into the number of joint non-overlapping blocks and calculate the difference value of pixels in each block producing the partitioned difference image (PDI)

to find the associated sub-block pairs at the horizontal, vertical and diagonal direction of various levels as illustrated in Fig.3.
4. Pseudo-random generator used to produce a traversing order for visiting the two pixel blocks for the embedding process.
5. Encode process uses an encrypted stream of secrete message to be hidden in the DWT decomposition levels or sub-bands and accomplished by changing a difference value in one range into any of the difference values in the same range. The encoding is achieved when all the bits of the secrete message are hidden, this process may repeated more than one level.
6. Apply the IDWT (Inverse Discrete Wavelet Transform) using the newly updated sub-band values at difference decomposition levels to obtain the Steganography image, this embedded steps illustrated in Fig. 4.

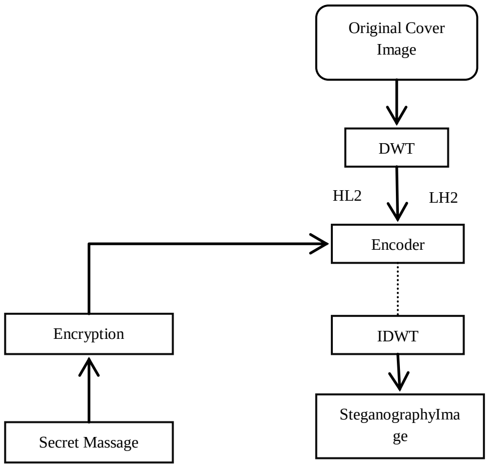


Fig.4. Embedding Secrete message scheme

3.4 Extracting scheme

The extraction process aim is to estimate and obtain reliability of the original image from a possible distortion version of the Steganography image. The extraction process can be carried out by reversing the embedding procedures that is generate the similar random permutations of each embedding sub channel as the encoding by using the same user-provided key and given the correlation coefficient between the given and extracted one to get the output as the original image and the Secrete message, Fig.5 illustrated in extracting process.

4. EXPERIMENTAL RESULT AND DISSCUSION

To show the efficiency, security and robustness performance of our scheme, executive tests have taken place. We perform simulation on five well-known images each with variable parameter size of 512 × 512 Pixel. The Steganography images go through two attaching methods JPEG200 compression and cropping. The original image cameraman and test results of it are shown in Fig 6.The resulting of experiments on other testing images are show in the Table 1.

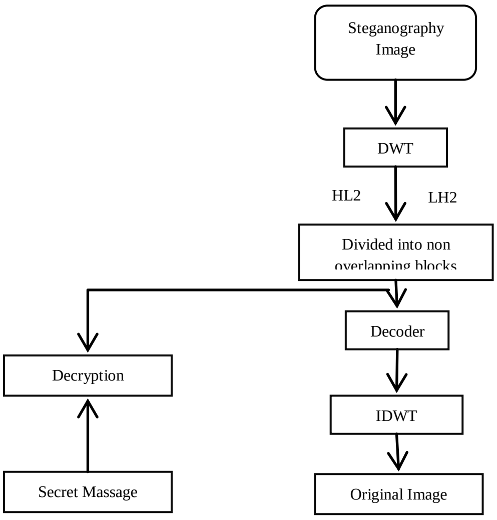


Fig.5. Extracting the Secrete message scheme

Table1. Similarity measures for the "Lena", "Home", "Boat", "Baboon", images.

Image	Camera man	Lena	Home	boat	Baboon
PSNR	45.7933	47.07	34.536	38.536	46.262
NC	0.9370	0.9982	0.9997	0.9200	0.8920
AVERAGE DIF	-0.0685	-0.0539	-0.1833	-0.1833	-0.0894
MAX DIFF	3	13	4	8	3

Here we have used the similarity measures for the various images such as Peak Signal to Noise Ratio (PSNR), is adopted to estimate the dissimilarity between the original and the Steno images and can be defined via Mean Square Error (MSE) in the unit of logarithmic decibel (dB) as follows:

$$PSNR = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{255^2}{MSE} \qquad (1)$$

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)^2 \qquad (2)$$

A higher PSNR indicates that the Steno image is closer to the original one from the perspective of host contents. The host fidelity is acceptable for any PSNR greater than 30 dB, after extracting the secrete message, the normalized correlation coefficient (NC) is computed using the original image and Steganography image to judge the existence of secrete message. It is defined as follows:

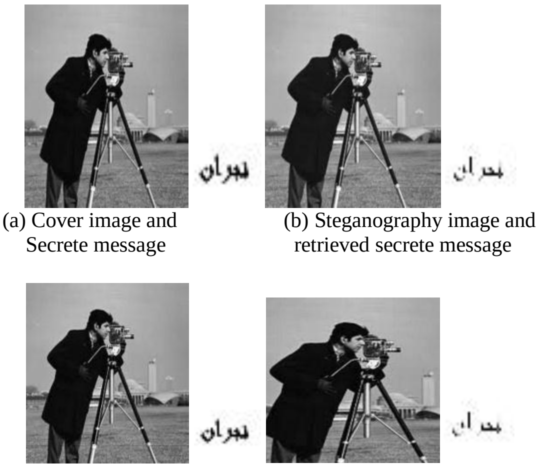
$$NC = \frac{\sum_{i=1}^{n} W(i) \times w^{'}(i)}{\sum_{i=1}^{n} W^{2}(i)} \qquad (3)$$

Where W (i) means the original image which the length is "n", W' (i) mean the extracting hidden image. We have used average difference and Maximum Difference measures for the various images to differentiate between the original image and Steganography image as follows:

$$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x^{'}_{j,k}\right) / MN \qquad (4)$$

$$MD = Max\left(\left|x_{j,k} - x^{'}_{j,k}\right|\right) \qquad (5)$$

Fig.6. shows the Cameraman original image and the Steganography image respectively and it shows the test result of the various attaches such as JPEG200 compression and Cropping. We see that the original image is not distinguishable from the Steganography image.



(a) Cover image and Secrete message

(b) Steganography image and retrieved secrete message

(c)JPEG2000Compress(d) Cropping

Fig.6. Test result of the original image of cameraman

5. CONCLUSION

The emerging techniques in the field of transform domain such as DWT and adaptive Steganography are not an easy target for attaches, especially when the concealed messages are small. We have proposed a new framework for enhancing security system by combining text and image, in which a new digital steganography method based on DWT, shows the effectiveness and robustness of the proposed system. A new metric that measures the objective quality of the image based on the extracted Steganography image bit is introduced in our proposed method. Images after extracting the embedding secrete message is nearly the same with the original image before embedding in aspect of recognition result. This paper also provides a new approach to classify key-based steganography techniques, which are grouped based on the usage of secret keys.

6. REFERENCES

[1] Saraju P. Mohanty 1999."Digital Watermarking: A Tutorial Review," Dept. of Comp Sci. and Eng. University of South Florida Tampa, FL 33620 smohanty@csee.usf.edu.

[2] S. Katzenbeisser, A.P Fabien. Petitcolas, 2000. "Information hiding techniques forSteganography and digital watermarking" editors. p. cm. (Artech House Computing library).

[3] Chung-Li Hou, ChangChun Lu, Shi-Chun Tsai, andWen-Guey Tzeng2011. "An Optimal Data Hiding Scheme With Tree-Based Parity Check," IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 3.

[4] Furht, B., Muharemagic, E., Socek, D.,2005 Multimedia Encryption and Watermarking, Multimedia Systems and Application Series, vol. 28, Springer Science BusinessMedia, Inc.

[5] Wenbo Mao,2004 Modern Cryptography: Theory and Practice, Prentice Hall PTR,, Prentice-HallInc.

[6] William Stallings,2002 Cryptography and Network security: principles and Practice, Prentice HallInternational Inc.

[7] Jae K. Shim, Anique A. Qureshi and Joel G. Siegel, 2000The International Hand book of ComputerSecurity, Glenlake Publishing Company, Ltd.

[8] Cryptography,Wikipedia,http://en.wikipedia.org/ wiki/Cryptography

[9] Poularikas, A.D., 1996"The Transforms and Applications Handbook", CRC Press LLC (with IEEE Press).

[10] Grigoryan, A.M., Agaian, S.S.,2003 Multidimensional Discrete Unitary Transforms:Representation, Partitioning, and Algorithms, Marcel Dekker, Inc., New York.

[11] P. Y. Chen, E. C. Liao,2002"A NewAlgorithm for Haar Wavelet Transform." IEEE Int. Symposium on IntelligentSignal Processing and Communication System: 453-457.

[12] Po-Yueh Chen, Hung-Ju Lin,2006 "A DWT Based Approach for Image Steganography," Int. J. Appl. Sci. Eng., 4, 3.

[13] S. Youssef, A. Abu Elfarag, R. Raouf,2011 "A Robust Steganography Model Using Wavelet-Based Block-Partitionmodification," Int. J. Comp. Sci.& I. T, Vol. 3, No 4.

[14] Huang Daren, L. Jiufen, H.Jiwu and L.Hongmei "A DWT-Based image watermarking algorithm," IEEE Int. Conf. on Multimedia and Expo.

[15] HONG CAI, M.S. 2007 "Wavelet Structure Based Transform: Information Extraction and Analysis," University Of Texas, Dissertation.

[16] Ali Al-Ataby and Fawzi Al-Naima,2010. "A Modified High Capacity Image SteganographyTechnique Based on Wavelet Transform," The International Arab Journal of Information Technology, Vol. 7, No. 4.

[17] Xu Jianyun, A. H. Sung, P. Shi, Liu Qingzhong, 2004 "JPEG Compression Immune Steganography Using Wavelet Transform," IEEE International Conference on Information Technology, Vol.2, pp. 704 – 708.