IJESMR

International Journal OF Engineering Sciences & Management Research

A NOVEL DIGITAL IMAGE STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM.

Sudhakar Murugesan*, Edward Danso Ansong, Nivash Thirunavukarasu
Lecturer, Department of Information Technology,
Valley View University, Techiman Campus,
Ghana, West Africa

KEYWORDS: Discrete wavelet.

ABSTRACT

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message, This can be achieve by concealing the existence of information within seemingly harmless carriers or cover, the text, image, video, audio, etc can be used as a carrier to embed the information. In this paper, we propose a modified secure and high capacity based Steganography scheme of hiding a large-size secret image into a small-size cover image. Arnold transformation is performed to scrambles the secret image. Discrete Wavelet Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego image. We have investigated the performance of our scheme by comparing various qualities of the stego image and cover image, the modified Steganography is highly secure with certain strength in addition to good perceptual invisibility.

INTRODUCTION

Steganography is the art and science of writing hidden message for communicating secret data in an appropriate multimedia carrier, e.g., image, audio, video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data and it has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit, Steganography ultimate objectives and the main factors that separate it from related techniques such as watermarking and cryptography is undetectability, robustness and capacity of the hidden data. For spatial domain watermarking methods, the processing is applied on the image pixel values directly. In other words, the watermark is embedded in image by modifying the pixel values. The advantage of this type of watermarking is easy and computationally fast. The disadvantage is its low ability to bear some signal processing or noises. For frequency domain methods, the first step is to transform the image data into frequency domain coefficients by some mathematical tools e.g. FFT, DCT, or DWT. Then, according to the different data characteristics generated by these transforms, embed the watermark into the coefficients in frequency domain. After the watermarked coefficients are transformed back to spatial domain, the entire embedding procedure is completed. The advantage of this type of watermarking is the high ability to face some signal processing or noises. However, methods of this type are computationally complex and hence slower. The second category of data hiding is called Steganography. The methods are designed to embed some confidential data into some cover-media such as texts, voices, images, and videos. After the confidential data are embedded, they are then transmitted together with the cover-media. The major objective is to prevent some unintended observer from stealing or destroying those confidential data.

There are two things to be considered when designing a Steganography system: (1) Invisibility: Human eyes cannot distinguish the difference between the original image and the stego-image. (2) Capacity: The more data an image can carry the better it is. However, large embedded data usually degrade the image quality significantly. How one can increase the capacity without ruining the invisibility is the key problem. The design of a Steganography system also can be categorized into spatial domain methods and frequency domain ones. The advantages and disadvantages are the same as those we mentioned about watermarking methods earlier. The proposed Steganography method is described in details step by step. Some numerical examples are illustrated as well. Experimental results and analysis are demonstrated. Finally some concluding remarks are provided.

LITERATURE REVIEW

Literature Survey on Methods in the JPEG Domain

Jan Kodovský, Jessica Fridrich[1] presented "Influence of Embedding Strategies on Security of Steganography Methods in the JPEG Domain" embed a secret message so that its very presence in the stego object cannot be proved. Thus, the main requirement of steganography is undetectability, which, loosely defined, means that no algorithm exists that can determine whether an object contains a hidden message

Literature Survey on Least Significant bit Technique

Babita Ahuja [2] presented "High Capacity Filter Based Steganography" we present an image based Steganography algorithm named as High Capacity Filter Based Steganography (HCFBS) that combines Least Significant Bit (LSB) method for data hiding, and the filtering techniques for image enhancement.

Mohammad Ali Bani Younes, [3] presented "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion" in Steganography technique will be used to send the secret information along with an encrypted image. A number of horizontal and vertical blocks at the sender side will be generated, and then mixed with the encrypted image before transmitting it to the receiver. The receiver will need this information to reconstruct the same secret transformation table after extracting the secret information from the encrypted image. Instead of sending the whole secret transformation table, which is usually big, only the secret information is sent. In this approach, the binary representation of the hidden data is used to overwrite the LSB of each byte within the encrypted image randomly. This method will be expected to spread hidden information within encrypted image data randomly based on the secret key before transmission. The values of the correlation and entropy before and after the insertion process are expected to be the same. Thus, it will be used to reduce the chance of the encrypted image being detected and then enhance the security level of the encrypted images. Furthermore, this information will be used to enable the receiver to reconstruct the same secret transformation table after extracting hidden data and hence the original image can be reproduced by the inverse of the transformation and encryption processes

Problem Definition:

- Secrete message is embedded into the high frequency co-efficient of the wavelet transform while leaving the low frequency co-efficient sub-and unaltered.
- Application of Immune digital Water marking Algorithm and find out that wavelet domain has certain robustness against some multimedia processing.

Image based Steganography algorithm named as High Capacity Filter Based Steganography (HCFBS), that combines Least Significant Bit (LSB) method for data hiding, and the filtering techniques for image enhancement

PROPOSED METHOD

We use two processes. The first one is encoding and second one is decoding process. In encoding, we apply Arnold transform with key on secret image and get the scrambled secret image. This process gives the more security and robustness to our algorithm. Apply DWT on the cover image and scrambled secret image in order to increase the security level. The alpha blending matrix is obtained, by the addition of wavelet coefficients of respective sub-bands of cover image and scrambled secret image. Alpha factor is increasing the embedding strength factor. Once the Alpha blending operation is done, we apply the inverse discrete wavelet transform (IDWT) and get the stego image. The decoding process is actually the reverse process of the embedding model. The DWT performed on the stego-image and known cover image. Then alpha blending performed on both images and applies inverse discrete wavelet transform on Alpha blend image and gets the scrambled secret image. Finally, perform Arnold transformation with key to recover the original secret image. The encoding and decoding process clearly exposed idea about our model.

SYSTEM ARCHITECTURE

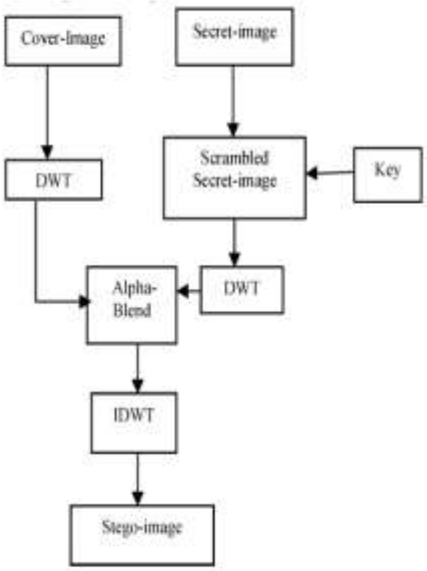
Functional architecture is an architectural model that identifies the functions and their interactions for the corresponding system needs, this method we used two processes. The first one is encoding and second one is decoding process. In encoding, we apply Arnold transform with key on secret image and get the scrambled secret image. This process gives the more security and robustness to our algorithm. Apply DWT on the cover image and scrambled secret image in order to increase the security level. The alpha blending matrix is obtained, by the addition of wavelet coefficients of respective sub-bands of cover image and scrambled secret image. Alpha factor is increasing the embedding strength factor. Once the Alpha blending operation is done, we apply the Inverse discrete wavelet transform (IDWT) and get the stego image. The decoding process is actually the reverse process of the embedding model. The DWT performed on the stego-image and known cover image. Then alpha blending performed on both images and applies inverse discrete wavelet transform on Alpha blend image and gets the scrambled secret image. Finally, perform Arnold transformation with key to recover the original secret image. The encoding and decoding process clearly exposed idea about our model.

The following modules can be extracted. They are,

- ➢ Implementation of modified Steganography model
    - Encoding
    - Decoding
        - ▪ Scrambling Based on Arnold Transform
    - ▪ Discrete wavelet transform
        - ▪ Alpha Blending
    - Noise Attack

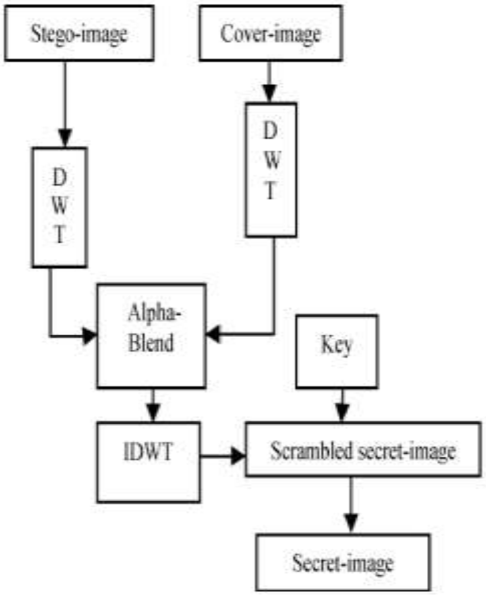
Encoding Process

The encoding process that the cover image and scrambled secret image with key was reassigned by DWT transform and then by alpha blending process. Next, IDWT was performed to reform the stego image. This secure stego image was transfer to any communication media. The secret key and alpha blending operation gives more security in our model. The schematic representation of encoding process was given in Fig: 1.1



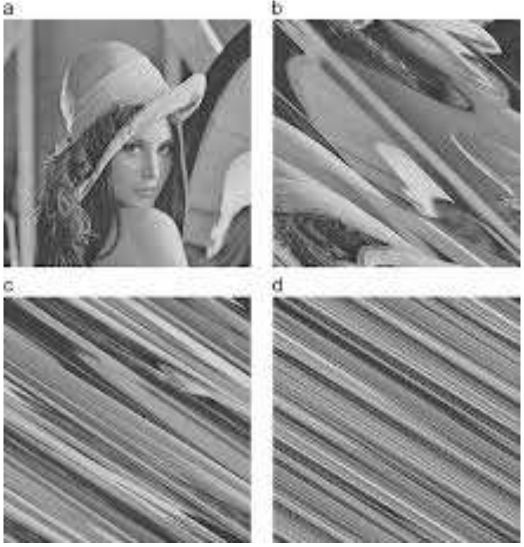
Decoding Process

The recover stego image and known cover image was reconstructed with DWT transform and followed by alpha blending process. Next, IDWT was performed to rebuild the scrambled secret image. Finally the secret key was applied to get the original secret image. The schematic representation of decoding process was given in the Fig:1.2



Scrambling Based on Arnold Transform

Arnold transformation is a class of cropping transformation proposed by V. J. Arnold in research of Random theory, We put digital image as a matrix, which will become chaotic after Arnold transform .The discrete digital image is equivalent to a class of special matrices in which there is a Correlation between elements, Arnold transformation of this matrix and then a new matrix can be obtained in order to achieve image scrambling processing. Fig:1.3 shows the Arnold transformer scrambled image.



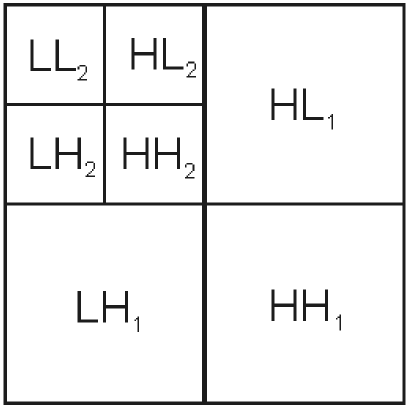
Set the image pixel coordinates. N is the order of the image matrix, i, j € (0, 1, 2. . . N -1) and the Arnold transform is

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \text{ (Mod N)}$$

The above transformation is one-to-one correspondence; the image can do iteration, iteration number can be used as a secret key for extracting the secret image. This transformation gives more security and robustness to our algorithm.

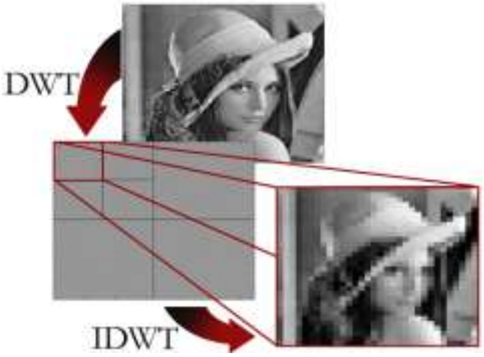
Discrete wavelet transform

Wavelets are functions defined over a finite interval and having an average value of zero. The basic idea of the wavelet transform is to represent any arbitrary function (t) as a superposition of a set of such wavelets or basis functions. These basis functions or baby wavelets are obtained from a single prototype wavelet called the mother wavelet, by dilations or contractions (scaling) and translations (shifts). The wavelet-based transform uses an I-D sub band decomposition process in which an I-D set of sample is converted into the low pass sub band (Li) and high-pass sub band (Hi).Where I represents level of decomposition mentioned in fig: 1.4



The low-pass sub band represents a down sampled low-resolution version of the original image. The high-pass sub band represents residual information of the original image. In 2-D sub band decomposition, the entire process is carried out by executing I-D sub band decomposition twice, first in one direction (horizontal), then in the orthogonal (vertical) direction. For example, the low-pass sub band (Li) resulting from the horizontal direction is further decomposed in the vertical direction, leading to LLi and LHi sub bands. Similarly, the high pass sub band (Hi) is further decomposed into HLi and HHi.

After one level of transform, the image can be further decomposed by applying the 2-D sub band decomposition to the existing LLi sub band. This iterative process results in multiple "transform levels". We refer to the sub band LLi as a low-resolution sub band and high-pass sub bands LHi, HLi, HHi as horizontal, vertical, and diagonal sub band respectively since they represent the horizontal, vertical and diagonal residual information of the original image.



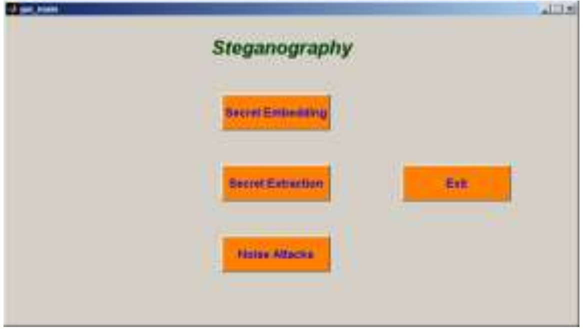
Alpha Blending

Alpha blending is the process of combining a translucent foreground color with a background color, thereby producing a new blended color. The degree of the foreground color's translucency may range from completely transparent to completely opaque. If the foreground color is completely transparent, the blended color will be the background color. Conversely, if it is completely opaque, the blended color will be the foreground color. Of course, the translucency can range between these extremes, in which case the blended color is computed as a weighted average of the foreground and background colors. Fast graph provides alpha blending functions that work on RGB color values, on direct color bitmaps, and on direct color virtual buffers. The alpha blending functions do not work when a 256-color virtual buffer is active.

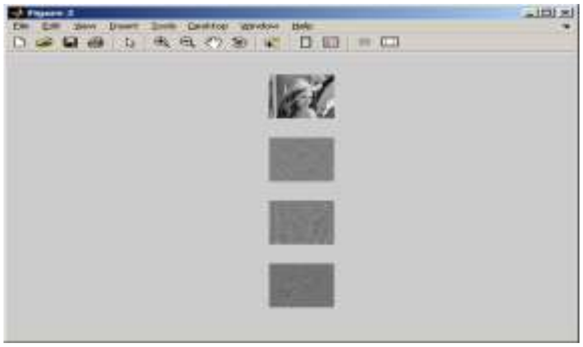
EXPERIMENTAL RESULTS

PROCEDURE FOR ENCODING PROCESS

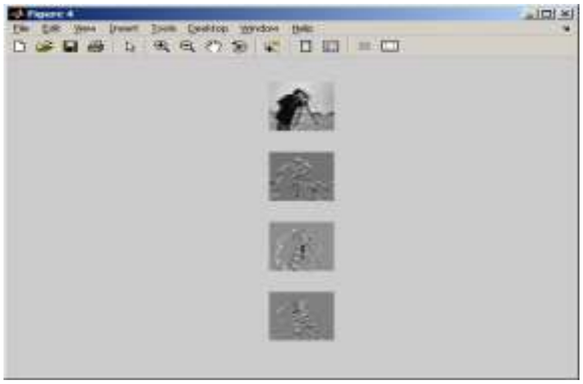
The cover image is scrambled using discrete wavelet transform for hiding the secret image in the low sub band, secret image is converted in to matrix and the new matrix can be obtained in order to achieve image scrambling processing, the image can do iterations, the iteration key can be used as secret key for extracting the secret image, inverse digital wavelet transform was performed to reform the stego image, it can be transfer to any communication medium. This feature can be used for a hiding the secret image in the cover image at low sub band.



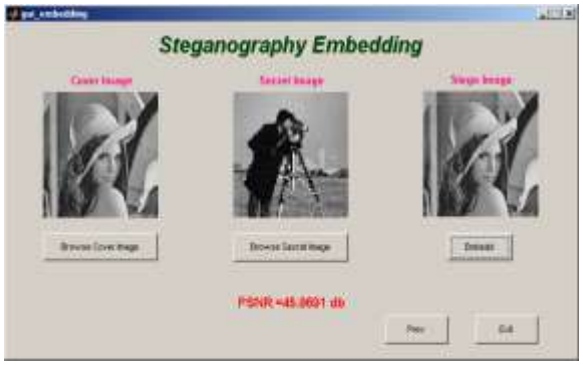
Structure for Encoding, Decoding & Noise Attacks.



Scrambling cover image



Scrambling secret images with key

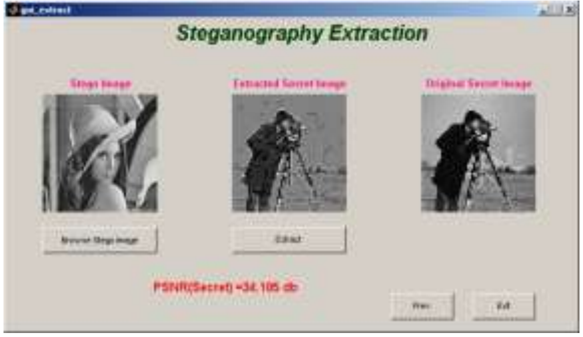


PSNR =45.8691 db

Secret image Embedded with cover image to stego image

Procedure for Decoding Process

The stego image and known cover image was reconstructed with discrete wavelet transform which is followed by Alpha blending process, inverse discrete wavelet transform was performed to rebuild the scrambled secret image. Finally the secret image was applied to get the original secret image for decoding process.



PSNR(Secret) =34.105 db

Extracting secret images from stego image

CONCLUSION

Thus the paper has brought in a clear view of the techniques for Steganography in discrete wavelet transform as associated to gray scale image. A new and secure Steganography method for embedding secret image into cover image without producing any major change has been proposed. In addition, this method gives more capacity and high security to transfer images in communication field. Experimental results show that our method gets stego-image with perceptual invisibility, high security and certain robustness.

REFERENCES

1. Jan Kodovsky, Jessica Fridrich "Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain" Proceedings of SPIE, the International Society for Optical Engineering", vol. 6819, pp. 681902.1-681902.13, 2008.
2. Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography," International Journal of Recent Trends in Engineering", vol. I, no. I, pp.672-674, May 2009.
3. Mohammed Ali Bani Younes and Aman Jantan, "A New Steganography Approach for Images Encryption Exchange by Using the Least Significant Bit Insertion," International Journal of Computer Science and Network Security", vol. 8, no. 6, pp.247-257, 2008.
4. K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K.R.Venugopal,L. M.Patnaik, "Robust Image Adaptive Steganography using Integer Wavelets" International conference on Communication Systems Software", pp. 614-621, 2008.
5. Chang-Chu Chen, and Chin-Chen Chang, "LSB-Based Steganography Using Reflected Grey Code, "The Institute of Electronics, Information and communication Engineers Transaction on Information and System", vol. E91-D (4), pp. 1110-1116, 2008.