A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform

** Prabakaran.G*
Assistant Professor, Dept. of CSE
FEAT, Annamalai University,
Annamalai Nagar,India,
gpaucse@yahoo.com

Bhavani.R
Associate Professor, Dept. of CSE
FEAT,Annamalai University,
Annamalai Nagar, India,
Shahana_1992@yahoo.co.in

Abstract— ***Steganography, the secret image is embedded in the cover image and transmitted in such a way that the existence of information is undetectable. The digital images, videos, sound files and other computer files can be used as 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 results show that the proposed algorithm for modified steganography is highly secured with certain strength in addition to good perceptual invisibility.***

Keywords— ***Steganography, Arnold transformation, Alpha blending, DWT.***

1. INTRODUCTION

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and 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's ultimate objectives and the main factors that separate it from related techniques such as watermarking and cryptography are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data.

The wavelet transform has emerged as a cutting edge technology, within the field of image compression. Wavelet-based coding provides substantial improvements in picture quality at higher compression ratios. Over the past few years, a variety of powerful and sophisticated wavelet-based schemes for image compression have been developed and implemented. Further those Schemes are being designed to address the requirements of very different kinds of applications, e.g. internet, color facsimile, printing, scanning, digital photography, remote sensing, mobile applications, medical imagery, digital library, military application and e-commerce.

2. RELATED WORK

Recent researches are using Discrete wavelet transform (DWT) applied in image compression format (JPEG) 2000 and Motion photographic export group (MPEG)-4 [1, 2, 3]. Chen.P et al.,[1] have proposed secrete message is embedded into the high frequency co-efficient of the wavelet transform while leaving the low frequency co-efficient sub-band unaltered. Ge Xiuhui,et al.,[4] have proposed research on application of Immune digital Water marking Algorithm and find out that wavelet domain has certain robustness against some multimedia processing.

Manjunatha reddy H.S, et al., [5] proposed an approximation band of payload and wavelet coefficient of cover image is fused based an alpha and beta. This method payload capacity increase as the only approximation band of payload is considered. Raja.K.B et al.,[6] have proposed a novel image adaptive steganographic technique in integer wavelet transform domain. Jan Kodovsky and Jessica Fridrich [7] worked out the specific design principles in Steganographic scheme for the JPEG format and their security. Babita Ahuja, et al., [8] proposed for more hiding capacity achieved by Filter Based scheme in Steganography.

Mohamed Ali Bani Younes, et. al., [9] proposed a steganographic approach for hiding. This approach hides the least significant bits insertion to hide the data within encrypted image data. Chang-Chu Chen, et al.,[10] have proposed that data hiding scheme was a modification of the LSB based

steganography using the rule of reflected gray code.

Yang.M, et al., [11] have proposed more hiding data into video processing steganography model. Shaohui liu H.Y., et al.,[12] proposed a Steganalysis technique on the basis of the histogram analysis on the wavelet coefficient for the detection. The approach has given importance on the methods by which the secret message is embedded through quantizing wavelet coefficients. The image statistical features are the important clues to determine whether information is hidden or not in the carrier from the detection process. Chin-Chen Chang et al., [13] proposed a pattern based image steganography in which first the DWT is performed on the digital image, separates the overlapping blocks and then classifies the wavelet coefficient of these overlapping blocks into a several patterns. The secret message is embedded into image by changing the coefficient patterns.

This paper presents a new method for data hiding into the discrete wavelet coefficients of the cover image in order to maximize the hiding capacity overcome the drawback. In addition, the Arnold transformation performed to scramble the secret image and further it should hide into the wavelet coefficients to increase the system security.

The remaining chapter of the paper will be organized as follows; chapter three discuss about the proposed method, Arnold transformation, DWT and implementation of steaganography model. Chapter four describes the experimental results and analysis of proposed steganography method. Chapter five gives the conclusion of the paper and suggests future improvements of the system.

3. PROPOSED METHOD

In our proposed 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.

3.1. Scrambling Based on Arnold Transform:

Arnold transformation is a class of cropping transformation proposed by V. J. Arnold in research of ergodic 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. Set the image pixel coordinates. N is the order of the image matrix, $\mathbf{i}, \boldsymbol{j} \in (0, 1, 2,\ldots, N-1)$ and the Arnold transform is as in (1):

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

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.

3.2. 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 a 1-D sub band decomposition process in which a 1-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. 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 1-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 subband decomposition to the existing LLi subband. This iterative process results in multiple “transform levels”. We refer to the subband LLi as a low-resolution subband and high-pass sub bands LHi, HLi, HHi as horizontal, vertical, and diagonal subband respectively since they represent the horizontal, vertical and diagonal residual information of the original image.

3.3. Implementation of modified steganography model:

The following session describes the implementation of the encoding and decoding process clearly. The encoding process includes DWT, Arnold transformation, Alpha blending, IDWT

and Stego image formation. The decoding process includes DWT, Arnold transformation, Alpha blending, IDWT and Secret image formation.

3.3.1. Encoding process:

During encoding process that the cover image and scrambled secret image (i.e. 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 Figure 3.1.

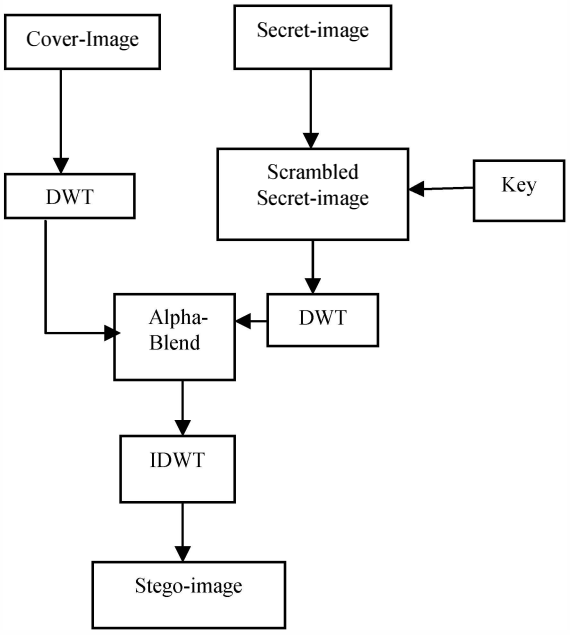

Figure 3.1. Encoding process of modified secure steganography

3.3.1.1. Algorithm for encoding process:

Step1: Preprocessing both the cover image(**C)** (N*N size) and secret image(**S)** (2N*2N size).

Step2: Perform a 2-D DWT at level 1 of the image **C** (N/2 * N/2 size).

Step 3: Apply private key with Arnold transformation on image **S** and get the scrambled secret Image(**SS)**.

Step 4: Again perform a 2-D DWT at level 2 of the image **SS (**N/2 *N/2 size).

Step 5: Extract the approximation co-efficient of matrix (LA) and detail coefficient matrices LH, LV & LD of level 1 of the image **C**.

Step 6: Next extract the approximation co-efficient of matrix LA1 and detail coefficient matrices LH1, LV1 and LD1 of level 1 of the image **SS**.

Step 7: Apply Alpha blending operation on image **C** and image **SS.**

Step 8: Finally, perform 2-D IDWT to form the Stego image **(SI).**

3.3.2. 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 Figure 3.3.

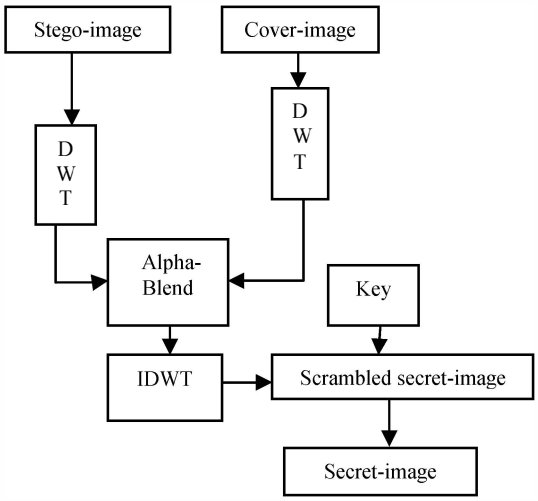

Figure 3.2. Decoding process of modified secure steganography

3.3.2.1. Algorithm for decoding process:

Step1: Received the image **SI**.

Step2: Perform a 2-D DWT at level 1 of the **SI** and known image **C**.

Step 3: Apply Alpha blending on both image **SI** and image **C**.

Step 4: Next separate the wavelet coefficients and take IDWT to reform the **SS**.

Step 5: Finally perform the Arnold transformation with private key and get the original image **S**.

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

To evaluate the performance of the proposed method, we implement the proposed method by using Matlab R2010a and 7.10 version. In our experiment, we have tested 100 general sample images by using this proposed algorithm. In representation purpose we have given Flower.jpg (316X380) and baby.jpg (458x500) are consider as cover images and Route.jpg (560 x 560) is secret image. Implementation purpose the Flower and baby images resize of 300×300 size and then Route.jpg resize of 600x600 size have been considered for our experiment.

We tested the various alpha values in between ranges from 0.05 to 0.01. Fine tuning the embedding strength factor alpha and improve the quality level of stego-image. Then, we tested full secret load 600x600 was embedded into 300x300 size, which is obtained by apply 2 level DWT. The next level of DWT also performed but the approximation band is not clear

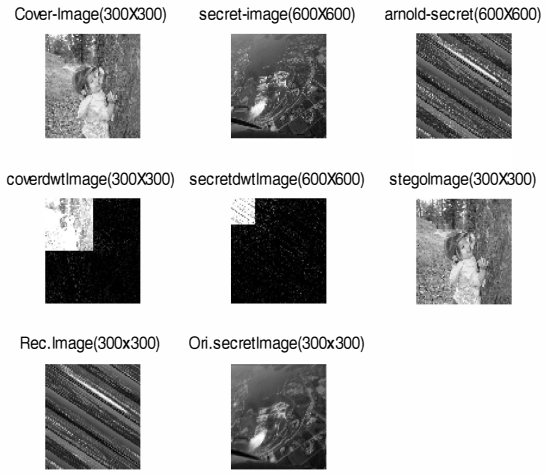

Figure 4.1. Shows a encoding and decoding process of cover image(baby.jpg) and secrete image(Route.jpg).

in the level. The corresponding experimental results should be shown in Figure 4.1.

4.1. Performance Analysis:

The good visual quality of stego images (i.e. images embedded with a secret image) is the most important property of steganography system because it is hard to detect by detectors. We use Peak Signal to Noise Ratio (PSNR) to measure the distortion between an original cover image and stego image.

The PSNR and MSE of cover image verses stego image respectively, the definitions are as follows in (2) and (3)

$$\text{PSNR} = 10\frac{\log_{10}(255)^2}{\text{MSE}}\text{dB} \qquad (2)$$

where

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})^2 \qquad (3)$$

MSE is the mean square error representing the difference between the original cover image x sized M x N and the stego image x' sized M x N, and the $x_{j,k}$ and $x'_{j,k}$ are pixel located at the j^{th} row the k^{th} column of images x and x', respectively. A large PSNR value means that the stego image is most similar to original image and vice versa. It is hard for the Human eyes to distinguish between original cover image and stego image when the PSNR ratio is larger than 30dB.

The other Image quality parameters normalized cross correlation, average difference, structural content, maximum difference and normalized absolute error are taken for our experiment.

Normalized cross correlation (NCC) is defined as in (4)

$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})\frac{1}{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k})^2} \qquad (4)$$

Average difference (AD) is defined as in (5)

$$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})/\text{MN} \qquad (5)$$

Structural content (SC) is defined as in (6)

TABLE-1
COMPARISON OF VARIOUS QUALITY MEASUREMENTS ON COVER IMAGES AND STEGO IMAGE WITH SECRET-IMAGES

Cover-image	Secret-image	MSE	PSNR	NCC	AD	SC	MD	NAE
Deer.jpg 316X 380	Baby.jpg 458 X 500	0.7542	49.320	0.9943	0.5071	1.0115	2.8640	0.0065
Deer.jpg 316X 380	Flower1.jpg 300 X 450	1.0440	47.943	0.9925	0.7435	1.0152	3.1480	0.0078
Deer.jpg 316X 380	Flower2.jpg 564 X 395	0.9249	48.470	0.9949	0.4308	1.0102	3.1760	0.0067
Coconut.jpg 768 X 1024	Flower2.jpg 564 X 395	0.9538	48.336	1.0058	-0.6402	0.9980	3.5540	0.0227
Coconut.jpg 768 X 1024	Flower1.jpg 300 X 450	0.3749	52.391	1.008	-0.3275	0.9983	3.1580	0.0132
Coconut.jpg 768 X 1024	Baby.jpg 458 X 500	0.5754	50.531	1.0050	-0.5639	0.9898	2.7240	0.0174

(PSNR VALUES ARE MEASURED IN DB AND OTHER VALUES ARE IN TERMS OF ERROR RATIO)

$$SC = \sum_{j=1}^{M}\sum_{k=1}^{N} (x_{j,k})^2 / \sum_{j=1}^{M}\sum_{k=1}^{N} (x'_{j,k})^2 \qquad (6)$$

Maximum difference (MD) is defined as in (7)

$$MD = Max\left(\left|x_{j,k} - x'_{j,k}\right|\right) \qquad (7)$$

Normalized absolute error (NAE) is defined as in (8)

$$NAE = \sum_{j=1}^{M}\sum_{k=1}^{N} \left|x_{j,k} - x'_{j,k}\right| / \sum_{j=1}^{M}\sum_{k=1}^{N} \left|x'_{j,k}\right| \qquad (8)$$

The original cover image x sized M x N and the stego image x' sized M x N, and the $x_{j,k}$ and $x'_{j,k}$ are pixel located at the j^{th} row the k^{th} column of images x and x', respectively.

The other image quality measurements compare to cover image and stego image with secret image were measured in terms of error ration. The summary of the image quality measurements with corresponding result of the images used in our study has been illustrated in Table 1.

The image quality factors MSE, PSNR and other quality measurement are observed. The effectiveness of the stego image formation proposed has been studied by calculating MSE and PSNR for the two digital images. The result data shows that for less MSE and High PSNR value. Embedding capacity of the proposed method has been computed which is better than the most cases compared to the existing methods. The MSE and PSNR value is also better than existing methods after embedding of secret image in various coefficient of cover image. Further, steganalysis to compare the quality of recovered secret image with secret image. Normalized cross correlation (NCC) is observed ranges from 0.99 to 1.00. Average Difference (AD) is observed ranges from -0.3 to 0.7. Structural content (SC) is observed ranges from0.97 to 1.01. Maximum Difference (MD) is observed ranges from 1.5 to 3.5. Normalized Absolute Error (NAE) is observed from 0.006 to 0.01.

Inference: Optimal level of PSNR ranges from 35db to 45 db and MSE is as less as possible.

5. CONCLUSION

This work deals with 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.

In future this method can be tested with other wavelet transform techniques with various image quality measurements.

REFERENCES

[1] P.Chen, and H.Lin,"A DWT approach for image steganography", International Journal of applied Science and Engineering", volume.4, 3:pp 275:290,2006.

[2] B.Lai and L.Chang, "Adaptive Data hiding for images based on Haar discrete wavelet transform", Lecture notes in computer science, volume 4319/2006.

[3] M. Yang, M.Trifas, N. Bourbakis, and C. Cushing, "A Robust Information Hiding Methodology In Wavelet Domain", Proceedings of 12th International Conference on Signal and Image Processing", Honolulu, Hawaii, August 2007.

[4] Ge Xiuhui and Tian Hao," Research on application of Immune digital Water marking Algorithm", International conference on computer Science and Software Engineering",2008,pp 806-809.

[5] H.S.Manjunatha reddy ,K. B. Raja, "High capacity and security Steganography using Discrete Wavelets" International Journal of computer Science and Security", volume 3,6: pp.462-472, 2009.

[6] 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.

[7] 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.

[8] Babita Ahuja and, Manpreet Kaur, "High Capacity Filter Based Steganography," International Journal of Recent Trends in Engineering", vol. 1, no. 1, pp.672-674, May 2009.

[9] 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.

[10] 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.

[11] M. Yang, M.Trifas, C. Truitt, and G. Xiong, "Wavelet Domain Video Information Embedding", the 12th World Multi-Conference on Systemics, Cybernetics and Informatics", Orlando, Florida, June 29th - July 2nd, 2008.

[12] H.Y.Shaohui Liu and W.Gao,"Steganalysis of data hiding techniques in wavelet domain", in international conference on image processing", pp 119 -121, August 2004.

[13] C.C Chang, Tung –shou Chen, and H C Hsia,"An Effective image steganography Sheme based a Wavelet transformation and pattern based modification", in international conference on computer networks and mobile computing", pp 115-119, march 2003.

[14] WWW.Wikipedia free encyclopedia, steganography, http://en.wikipedia.org/wiki/Steganography