A MODIFIED SECURE IMAGE STEGANOGRAPHY BASED ON INTEGER WAVELET TRANSFORM AND FUSION TECHNIQUES

PRABAKARAN G., BHAVANI, R. AND LOGANATHAN, R.*
Department of computer science and Engineering, Annamalai University
E-mail: gpaucse@yahoo.com, erloganathan@yahoo.co.in,

Abstract: Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. In this paper, we propose a modified secure steganography scheme hiding a large-size gray image into a small-size gray image. Preprocessing is first performed both on cover and secret images. Arnold transformation is performed on the secret image and the high security and robustness achieved by using this transformation. Integer Wavelet Transform (IWT) is performed in cover image. The cover image Coefficients of the wavelets are altered with the noise within tolerable level. Apply Integer wavelet transformation (IWT) to get the Stego-image. The capacity of the proposed algorithm is increased as the only approximation band of secret image is considered. The extraction model is actually the reverse process of the embedding model. Experimental results show that our method gets stego-image with perceptual invisibility, high security and certain robustness. The MSE and capacity are improved with acceptable PSNR compared to the existing algorithm.

Keywords: Steganography, Arnold transformation, IWT, Fusion techniques, Image quality.

1. INTRODUCTION
Steganography gained importance in the past few years due to increasing need for providing secrecy in an open environment like the internet. 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. Steganography 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, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. Steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message.

1.1. Studies Related to Steganography
H. S. Manjunatha Reddy et al., [1] proposed a scheme embeds a larger-sized secret image while maintaining acceptable image quality of the stego-image and also improved image hiding scheme for grayscale images based on Integer wavelet transform. K. B. Raja et al., [2] have proposed a novel image adaptive stenographic technique in the integer wavelet transform domain called as the Robust Image Adaptive Steganography using Integer Wavelet Transform. According to information theoretic prescriptions for parallel Gaussian models of images, data should be hidden in low and mid frequencies ranges of the host image, which have large energies.

Jan Kodovsky and Jessica Fridrich [3] worked out the specific design principles and elements of steganographic schemes for the JPEG format and their security. L. Y. Por al., [4] have proposed a combination of three different LSB insertion algorithm on GIF image through stegcure system. The unique feature about the stegcure is being able to integrate three algorithms in one Steganography system. By implementing public key infrastructure, unauthorized user is forbidden...
from intercepting the transmission of the covert data during a communication because the stego-key is only known by the sender and receiver.

Gaetan Le Guelvoit [5] proposed a work which deals with public key Steganography in presence of passive warden. The main aim is to hide the secret information within cover documents without any preliminary secret key sharing. This work explores the use of trellis coded quantization technique to design more efficient public key scheme. Chine-Chen chang, et al.,[6] have presented a scheme embeds a larger sized secret-image and also improved image hiding scheme for grayscale images based on wet paper coding.

Chapter five gives the conclusion of the paper and suggests future improvements of the system.

2. PROPOSED METHOD

2.1. Arnold Transformation

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, $i, j \in (0,1,2,..., N-1)$ and the Arnold transform is as in (1):

$$
\begin{bmatrix}
  i' \\
  j'
\end{bmatrix} =
\begin{bmatrix}
  1 & 2 \\
  1 & 1
\end{bmatrix}
\begin{bmatrix}
  i \\
  j
\end{bmatrix} \pmod{N}
$$

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.

2.2. Wavelet Based Steganography

Wavelet transform is used to convert a spatial (or) time domain into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. The wavelet transform is obtained by repeated filtering of the coefficients of the image row-by-row and column-by-column.

2.2.1. Integer Wavelet Transform

Integer to integer wavelet transforms maps an integer data set into another integer data set. This transform is perfectly invertible and yield exactly the original data set. A one dimensional discrete wavelet transform is a repeated filter bank algorithm. The reconstruction involves a convolution with the synthesis filters and the
results of these convolutions are added. In two dimensions, we first apply one step of the one dimensional transform to all rows. Then, we repeat the same for all columns. In the next step, we proceed with the coefficients that result from a convolution in both directions.

Since the integer wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn’t allow perfect reconstruction of the original image. However, with the introduction of Wavelet transforms that map integers to integers we are able to characterize the output completely with integers. One example of wavelet transforms that map integers to integers is the S-transform.

Its smooth (s) and detail (d) outputs for an index n are given in (2) and (3) respectively. Note that the smooth and the detail outputs are the results of the application of the high-pass and the low-pass filters respectively. At the first sight it seems that the rounding-off in this definition of s(n) discards some information. However, the sum and the difference of two integers are either both odd or both even. We can thus safely omit the last bit of the sum since it equals to the last bit of the difference. The S-transform is thus reversible and its inverse is given in equations (4) and (5).

\[
S(n) = \frac{[X(2n) + X(2n+1)]}{2} \quad (2)
\]
\[
d(n) = X(2n) - X(2n+1) \quad (3)
\]
\[
X(2n) = s(n) + \frac{d(n) + 1}{2} \quad (4)
\]
\[
X(2n + 1) = s(n) - \frac{d(n)}{2} \quad (5)
\]

Generally, the 2D S-transform can be computed for an image using equations (6), (7), (8), and (9). Of course the transform is reversible, i.e., we can exactly recover the original image pixels from the computed transform coefficients. The inverse is given in equations (11), (12), (13), and (14). The transform results in four classes of coefficients: (A) is the low pass coefficients, (H) coefficients represent horizontal features of the image, (V) and (D) reflect vertical and diagonal information respectively. During the transform we ignore any odd pixels on the borders.

\[
A_{i,j} = \frac{(I_{2i} + 1, 2j + I_{2i+1},2j)}{2} \quad (6)
\]
\[
H_{i,j} = I_{2i} + 2j + 1 - I_{2i,2j} \quad (7)
\]
\[
V_{i,j} = I_{2i+1,2j+1} - I_{2i,2j} \quad (8)
\]
\[
D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j} \quad (9)
\]
\[
I_{2i,2j+1} = I_{2i} + 1,2j + \left[\frac{H_{i,j} + 1}{2}\right] \quad (10)
\]
\[
I_{2i+1,2j+1} = I_{2i+1,2j} + V_{i,j} - H_{i,j} \quad (11)
\]
\[
I_{2i+1,2j+1} = I_{2i+1,2j} + D_{i,j} - V_{i,j} \quad (12)
\]

Where, \(1 \leq i \leq X/2, 1 \leq j \leq Y/2\)

3. PROPOSED MODEL

3.1. Fusion Encoder

In Fig. 2 show the block diagram of the embedding algorithm. The main idea behind the proposed algorithm is wavelet based fusion. Both cover image and payload is convert into IWT domain. Further, apply IWT on the payload in order to increase the security level.

3.1.1. Algorithm of Data Embedding

Input: Cover Image c and Payload image p.
Output: Stego image s.

(i) Preprocessing on c and p
(ii) Apply Arnold Transformation with secret key into the Payload.
(iii) Transform c and p into 2 levels of decomposition using Haar Wavelet.
(iv) Wavelet fusion of IWT coefficients of c and p.
(v) Inverse transform of all the subbands of the fused image.
(vi) Stego image s is generated.

3.2. Fusion Decoder

In Fig. 3 shows the block diagram for retrieval of payload from the Stego image. The Stego image is normalized, and then IWT is taken. The extraction process involves subtracting the IWT coefficients of the original cover image from the IWT coefficients of the Stego image. It is then followed by decryption of the subtracted
coefficients. Then first step of IIWT on these coefficients is applied followed by second IIWT only with respect to the approximation band of the first IIWT coefficients of the payload.

3.2.1. Algorithm of Data Extraction
Input: Stego Image s.
Output: Payload image p.
(i) Transform s into 2 levels of wavelet decomposition.
(ii) Subtract IWT coefficients of c from IWT coefficients of s to get IWT coefficients of only p.
(iii) Apply IIWT of all the sub bands of p.
(iv) Payload Image is obtained p.

4. PERFORMANCE ANALYSIS
In this section, we evaluate the proposed system from different points of view using various common images. Here we show the same images for evaluation. In these section experimental results of the proposed method are shown based on two good quality images: Icecream (316X380) and Fruitmixer (458X500). Implementation on deer and baby images resize of 300×300 size have been considered for the experiment tested for full embedding capacity.

4.1. Mean Square Error (MSE)
The experimental results obtained are subjected to various statistical techniques to evaluate the performance parameters of steganography images.

\[
MSE = \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{j,k} - \hat{x}_{j,k})^2
\]

Where, \( m \times n \) size of the image with \( j = 0, 1 \ldots M \) & \( k = 0, 1 \ldots N \)

4.2. Peak Signal to Noise Ratio (PSNR)
The Peak Signal to noise ratio (PSNR) is used in experiment to evaluate the quality of the container image and after embedded stego Image.

\[
PSNR = \frac{10 \log_2(255)^2}{MSE}
\]

The some of the image quality measurement has been illustrated in table and corresponding tested results shown in the 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.

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

In future, this technique is applied to multiple wavelet transform and extended to color images.

5. CONCLUSION

In this paper, we have proposed a new enhanced steganography methodology along with a suitable encryption scheme. Real time signals are both time-limited (and space limited in the case of images) and band-limited. Wavelets are localized in both time (space) and frequency (scale) domains. Hence it is easy to capture local features in a signal. Another achievement of a wavelet basis is that it supports multi resolution. Perform an Arnold transform with key on secret image and get the secret cover image. This process gives the more security and robustness to our algorithm.

References


