Research Article

Novel Technology for Secure Data Transmission Based on Integer Wavelet Transform and Particle Swarm Optimization

1S. Thenmozhi and 2Dr. M. Chandrasekaran
1Anna University,
2GCE, Bargur, Tamilnadu, India

Abstract: Steganography is the art and science of embedding hidden messages in a carrier medium such that no one apart from the sender and intended recipient even realizes that there is a hidden message. Mediums can include image, video and audio. The main goal of steganography is to maintain secret communication between two parties. There are many techniques available to achieve steganography. This study provides a robust and secure image steganography method to conceal secret image in digital cover image without incurring any perceptual distortion. The technique is based on Integer Wavelet Transform (IWT) and Particle Swarm Optimization (PSO) in transform domain. The transform domain is employed to increase the robustness of the image steganography method. Integer wavelet transform evades the floating point precision problems of the wavelet filters. To achieve high security, an encryption mechanism utilizing PSO is proposed. The secret message to be transmitted is normalized and then embedded into the cover image using IWT and the key generated by PSO. The proposed method is tested on various cover and secret images. The experimental results substantiate that PSO in IWT domain can improve the quality of stego image effectively without any compromise in histogram and statistical analysis. The proposed method also maintains good perceptual quality in Stego image and greater security.

Keywords: Histogram analysis, image steganography, integer wavelet transform, particle swarm optimization

INTRODUCTION

Currently, people tend to exchange huge amount of data through internet. However, data transfer through internet will increase the risk of illegal and unauthorized access. Information hiding is a technique for concealing most important data into digital multimedia and this technique has been broadly applied to many fields such as ownership identification, tamper proofing and secret data transmission (Katzenbeisser and Petitcolas, 2000). Different methods have been developed recently for information hiding. Watermarking and steganography are two most important branches of information hiding technology (Petitcolas et al., 1999). Watermarking is mainly used to protect the author’s property right and maintains high robustness against unauthorized usage. It also assures that the embedded information can be successfully extracted from the watermarked signals (Shih and Wu, 2005; Zhang and Wang, 2005). On the other hand, Steganography is used to protect important and sizable volume of data during transmission. Steganography also aims to increase the embedding capacity and keeping the secret data unnoticeable to the viewers (Chan and Cheng, 2004; Chang et al., 2002; Lai and Chang, 2006).

The word Steganography is originally composed of two Greek words steganos (secret) and graphy (writing) which means "covered writing". Steganography is defined by Markus Kahn as follows, “Steganography is the art and science of communicating in a way which hides the existence of the communication”. Steganography is the process of embedding secret data within public information. Image based steganography is the most common system used since digital images are widely used over the Internet and Web (Tian, 2003). Digital image steganography is a technique of secret communication that aims to convey a huge amount of information secretly by hiding the very existence of information in some other medium such as image, audio or video. The main objective of steganography is to avoid some unintended observer from stealing or destroying confidential information and aims to avoid the intervention of non-communicating parties to this kind of communication (Mandal and Sengupta, 2010).

A number of Steganographic approaches exist for embedding secret message in an image files, these approaches can be classified according to the format of the cover image or the method of embedding (Al-Ataby and Al-Naima, 2010; Tolba et al., 2004; Wang et al., 2001). Image hiding techniques can generally be categorized into spatial domain methods and frequency
domain methods. Spatial domain methods directly embed secret messages into the gray scale values of image pixels, while the frequency domain methods embed secret messages into the transformed coefficients of the cover-image (Cox et al., 1997).

The Least Significant Bit (LSB) is an example of spatial domain method. Till now, LSB is the most preferred method used for data hiding, because it is easy to implement, offers high hiding capacity and provides easy way to control the quality of stego object, but it is low in robustness and imperceptibility. Example for data hiding using LSB can be found in research (Chan and Cheng, 2004; Change et al., 2008; Zayed, 2005). Transform domain techniques are used to overcome the low robustness and imperceptibility problems found in LSB substitution method. There are variety of transforms used for data hiding and the most widely used transforms are DFT, DCT, DWT. Algorithms using DCT can be found in research (Noda et al., 2006; Tseng and Chang, 2004; Westfeld, 2001). Most recent researchers are directed to use of DWT and the examples of using DWT can be found in research (Chen and Lin, 2006; Lai and Chang, 2006).

The advantages of transform domain approaches over spatial domain are their noise tolerance and having more processing possibilities but they are computationally complex, slower and lesser in payload.

The challenge in this study is to find a best method to embed a secret message in an image without degrading the image quality and to provide better resistance against stego analysis process. The objective of this study is to examine the quality and robustness of the stego image after using the proposed image steganography scheme to hide a secret image into the cover image in the transform domain. This study proposes a novel image hiding technique with the use of PSO to hide data into IWT coefficients of the cover image in order to overcome the drawbacks of spatial domain. It also increases the robustness as much as possible. From the results, it is observed that the proposed image steganographic technique can embed the secret message effectively without degrading the quality of cover image.

LITERATURE REVIEW

Reversible data hiding method is proposed by Tian (2003) which is based on difference expansion. In this method, the host image is divided into a series of non-overlapping and neighboring pixel pairs. The difference of each pixel pair is doubled. The parity of the embedding secret bit is modified using doubled difference value. Ni et al. (2006) have developed a method based on histogram shifting to embed secret data reversibly. The peak point of the image histogram is selected and the pixel values in the range from its right one to the zero point are increased by one to create one vacant histogram bin for embedding. The number of secret bits embedded depends on the pixel number of the peak point in the histogram. The information of the peak point and zero point are required in the procedure of extracting the embedded data and recovering the host image. Tai et al. (2009) have presented a binary tree structure that can be utilized to predetermine the peak point used for embedding secret messages. Consequently, only the level of the binary tree must be shared by the sender and the receiver. Kiamini and Fazli (2008) have presented a novel method to embed the message into the cover image so that hackers cannot notice the existence of the data. The proposed algorithm uses the basic concept of the LSB method. In order to improve the quality and security of the image, the cover image is split into n blocks of 8*8 pixels and the message into n partitions. For finding the optimal solutions the technique uses Particle Swarm Optimization (PSO) Algorithm. The result shows that this method is better than the JPEG and Quantization Table Modification method. Elbeltagi et al. (2005) present Hierarchical Structure Poly-Particle Swarm Optimization (HSPPPSO) approach using the hierarchical concept. In the bottom layer of this structure, parallel optimization is performed on the poly particle swarm that increases the searching domain in the top layer, every particle in the bottom layer is considered as single particle swarm. The best position found by the particle in the lower layer is considered as the best position of the single particle in the top layer. The optimization result of top layer is used by the lower layer. The results show that HSPPPSO performs better than PSO. Zeng and Jiang (2010) proposes a cooperative line search Particle Swarm Optimization (CLS-PSO) algorithm by combining the basic PSO with local line search technique. The performance of this hybrid algorithm is evaluated using four nonlinear optimization problems. The result shows that CLS-PSO is better than basic PSO. Nasiriet et al. (2008) have developed a technique for detecting the lips in the color images using PSO. PSO is used to find optimized solution. The objective of this method is that the lip has high values of Cr and low values of Cb. The results shows that this method achieved 92% correction rate as compare to previous approach and 11% increase in lip detection. Bedi et al. (2013) proposed a technique to conceal information in spatial domain using PSO the PSO is used to find the best location to conceal data in the cover in spatial domain also achieved a distortion tolerance.

PRELIMINARIES

Integer wavelet transform: Wavelet domain allows us to conceal data in regions that the Human Visual System (HVS) is less sensitive to such as the high resolution detail bands HL, LH and HH. Embedding secret data in high resolution bands allows us to increase robustness while maintaining good visual quality. In Discrete Wavelet Transform, the used wavelet filters have floating coefficients so that, when we conceal data in their coefficients, any truncations of
the floating point values of the pixels which are the integers, may lead to failure of data hiding system. Thus the perfect reconstruction of original image becomes difficult. However, with the introduction of IWT which maps integers to integers and the output can be completely characterized with integers (Lee et al., 2007; Ni et al., 2006). The coefficients in IWT are represented by finite precision numbers which allow lossless encoding. IWT is more efficient approach than DWT to perform lossless compression. IWT is used to overcome the problems in DWT and it can reconstruct the cover image without loss of information through forward and inverse wavelet transformation (Xuan, 2002). Due to the difference mentioned between DWT and IWT, the LL band in the case of IWT appears to be a close copy with smaller scale of the cover image while in case of DWT the resulting LL band is distorted slightly as shown in Fig. 1.

If the original image A is M pixels high and N pixel wide, the level of each of the pixel at (i, j) is denoted by Ai, j. The IWT coefficients are given by:

\[ LL_{i,j} = \lfloor (A_{2i,2j} + A_{2i+1,2j}) / 2 \rfloor \]  
\[ HL_{i,j} = A_{2i+1,2j} - A_{2i,2j} \]  
\[ LH_{i,j} = A_{2i,2j+1} - A_{2i,2j} \]  
\[ HH_{i,j} = A_{2i+1,2j+1} - A_{2i,2j} \] 

The Inverse IWT coefficients given by:

\[ A_{2i,2j} = LL_{i,j} - \lfloor HL_{i,j} / 2 \rfloor \]  
\[ A_{2i,2j+1} = LL_{i,j} + \lfloor (HL_{i,j+1}) / 2 \rfloor \]

where, \( 1 \leq i \leq M/2, 1 \leq j \leq N/2 \) and \( \lfloor \rfloor \) denotes floor value.

**Particle swarm optimization:** Particle Swarm Optimization (PSO) is one of the latest methods that have been proposed in the computational intelligence area. It has been developed by Kennedy and Elberhart (1995) and it is a population based stochastic optimization model which is generated after the social behavior of bird flocks or fish schooling. This technique can be applied where a problem is given and its solution can be obtained in many ways. PSO does not require any gradient information of the function to be optimized uses only primitive mathematical operators and is conceptually very simple (Tiwari and Gajbhiye, 2013). A population of individuals defined called “particles”. Each particle has a position, a velocity and memory. Value of the objective function for these individuals represents their positions. Each particle moves free in the search space with a certain degree of freedom and randomness, looking where the objective function is much better. Each particle has the capacity to dig into the past for its best position and to share its current performance with other particles of the swarm. The individual's best solution is called the particle’s best or the local best and the best solution among all the neighbors are called global best. The real particle swarm optimization method shows every particle like a potential solution of a problem in n-dimensional space. The modification in particle local best and global best can be defined as the velocity...
value. Velocity of each particle is upgraded by using the following Eq. (9) and the every particle updated its position by Eq. (10).

\[
V_{r}(t+1) = W \times V_{r}(t) + c_1 \times \text{rand1} \times (P(t) - X_{r}(t)) + c_2 \times \text{rand2} \times (g(t) - X_{r}(t))
\]

(9)

\[
X_{r}(t+1) = X_{r}(t) + V_{r}(t+1)
\]

(10)

where,

- \( W \) = The Non negative inertia factor
- \( V_{r}(t) \) = The velocity of particle
- \( X_{r}(t) \) = The current position of particle
- \( c_1 \) = Therelativeinfluenceofthe cognitive component
- \( c_2 \) = Therelativeinfluence of the social component
- \( P(t) \) = pbest of particle
- \( g(t) \) = gbest of the group
- \( \text{rand1} \& \text{rand2} \) = The random numbers used for maintain the diversity of the population and the uniformly distributed in interval \([0, 1]\).

The major steps of the PSO are given below:

- **Step 1**: Randomly initialize each particle (np) with initial position and initial velocity.
- **Step 2**: Initialize constants \( c_1 \), \( c_2 \), \( \text{rand1} \), \( \text{rand2} \), \( W \) and iteration
- **Step 3**: Evaluate fitness function \( f \) using particle \( p \). If the fitness of the current particle is smaller than itsprevious best (pbest) fitness, replace pbest by the update pbest.
  \[ \text{pbest} = p(t) \text{ if } f(p(t)) > \text{pbest} \]
- **Step 4**: For each particle, if its fitness is smaller than the best (gbest) of all the particles, update gbest.
  \[ \text{gbest} = g(t) \text{ if } f(g(t)) > \text{gbest} \]
  where, \( f(t) \) is the objective function to be optimized.
- **Step 5**: Update particle velocity using Eq. (9)
- **Step 6**: Update particle position using Eq. (10)

The process is updated till the certain termination condition is found. When the process stops, the pbest and gbest are determined.

**PROPOSED STEGANOGRAPHY TECHNIQUE**

The proposed image steganography scheme aims to hide a secret image in to the cover image in the transform domain so that the stego image thus produced is good in quality and also more robust. The proposed algorithm is based on both IWT and swarm intelligence, this way of embedding secret message takes full merits of swarm intelligence and IWT. PSO and IWT can guarantee the perceptual invisibility of stego image.

The proposed framework for embedding a secret image in a cover image in the frequency domain is shown in Fig. 2. Cover image is preprocessed using histogram modification. This modification is used to step the overflow during embedding process. The algorithm also applies normalization on the secret image. Embedding process involves merging of the integer wavelet decomposition of the cover image and the normalized version of secret image. This normalized pixel values are fed as input to embedding.

![Fig. 2: Framework for embedding a secret image in a cover image](image1)

![Fig. 3: Framework for extracting a secret image from stego image](image2)
unit which results in reconstruction of the transformed image with better accuracy compared to direct integer values of the pixels as input. The detailed steps for embedding secret image data in a cover image are presented below followed by the corresponding algorithm:

**Input:** An M×N cover image, key and a secret message or image.

**Output:** An M×N stego image.

**Algorithm:**
1. Reading images: Read the cover image I (M X N) and the secret image S (P X Q) to be hidden.
2. Normalize the secret image.
3. Perform histogram modification on the cover image. It is used to prevent overflow or underflow that happens when the customized values in integer wavelet coefficients produce stego-image pixel values to exceed 255 or to be smaller than 0. This problem is found to be caused by the values near 255 or 0 (Shejul and Kulkarni, 2011; Kennedy and Eberhart, 1995). The problem can be solved by mapping the lowest 15 grayscale levels to the value of 15 and the highest 15 grayscale levels to the value 240.
4. Transform cover image into the transform domain using 2D Haar integer wavelet transform resulting LLI, LHI, HLI and HHI.
5. Encrypt the subbands using PSO and generate key. In order to encrypt the subband using PSO, Set the following parameters for PSO:
   - Np - Number of particles,
   - iters - Maximum no. of iterations,
   - iw - Inertia weight factor,
   - c1 and c2 - Cognitive and social acceleration factors,
   - r1 and r2 - Random numbers in the range (0, 1).
6. Embed the secret image into the encrypted cover image.
7. Finally, apply the inverse integer wavelet transform on the image to restore it to the spatial domain.

**Secret image extraction:** Figure 3 illustrates the extraction procedure for the proposed method at the receiver side. The secret image can be extracted from the stego image by the reverse process of embedding. This process uses value found with PSO in the embedding phase as extraction key. With the help of the key the secret image data can be extracted. The extracting procedure can be divided into three steps described as follows:

**Input:** An M×N stego-image and key.

**Output:** A secret message or image.

**Algorithm:**
1. After receiving the stego image, transform stego image into the transform domain using 2D Haar integer wavelet transform resulting LLI, LHI, HLI and HHI.
2. Decrypt the subbands using key obtained using PSO during embedding phase.
3. Extract the secret image from the subbands
4. Denormalize the secret image to get original version of secret image.

**EXPERIMENTAL RESULTS AND DISCUSSION**

The performance of the proposed technique has been evaluated and implemented using MATLAB 7.10. The efficiency of the algorithm is recorded, tabulated and compared with other techniques. The results with different cover images and secret images are shown. Original cover and secret images are shown in Fig. 4 and 5. Six cover images boat, blue hills, cameraman, Lena, mixed fruit and peppers Fig. 4a to f, each of size 512×512 are considered for testing the algorithm. The secret images considered are “butterfly”, “ice-cream” and “deer” Fig. 5a to c, each of size 256×256. The “butterfly” is embedded in “lena and peppers”. The resultant stego image is shown in Fig. 6a and b. The “ice-cream” is embedded in “boat and blue hills”. The “deer” is embedded in “mixed fruit” and “cameraman”. The resultant stego image is shown in Fig.6c and d. In all the cases, the mean PSNR value of stego images is 50.05 dB. Table 1 compares the PSNR value of the stego image in the proposed method and in the other existing methods. In all these the cover image considered is “lena” and the secret images used are of comparable sizes. The average PSNR value in the proposed method is much higher than that in the other methods.
Quality measures: The proposed algorithm is tested with different cover and secret image. The quantitative performance of the proposed steganography algorithm is evaluated based on Mean Square Error (MSE) and Peak signal to Noise Ratio (PSNR) as expressed below:

\[
MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|I(i,j) - I'(i,j)|^2}{M \times N}
\]

(11)

\[
PSNR = 10 \log_{10} \frac{255^2}{MSE}
\]

(12)

where, I-original image, I'-stego image and MXN-size of the image. PSNR is measured in decibels (db) and the bigger the PSNR value is, the better the stego image.

Simulation results: Table 2 provides the details of the performance of stegananography algorithm on various test images and is graphically represents in Fig. 7 and 8.
Fig. 8: PSNR of the stego image for the proposed framework algorithm. Figure 8 shows the PSNR of Stego image with difference cover and secret image of the proposed algorithm.

Comparison with existing approaches: The proposed approach is compared with existing approaches given by authors Hsieh et al. (2001), Ali et al. (2010), Shejul and Kulkarni (2011), Bhattacharya et al. (2011), Ioannidou et al. (2012), Mandal Sengupta (2010) and Parul et al. (2014). The comparison is shown in Table 1.

Figure 9 shows a graphical comparison of proposed approach and other existing approaches. It is clear from the graph that the PSNR value of the proposed method is high than other methods. This comparison concludes superiority of the proposed technique.

Stego analysis: The histogram analysis plays a very important role in image steganography. The histogram analysis is performed on both cover image and stego image. Six cover images used in system simulation. Figure 10 shows the histogram of the cover image and stego image. There is no significant change in the stego image histogram compared to the histogram of the cover image. Thus, it is robust to some statistical attacks and difficult to infer that secret image is hidden. From the histogram analysis, it is inferred that the proposed image steganography technique can embed the secret image without making changes in the histogram.

CONCLUSION AND FUTURE ENHANCEMENT

In this research, a novel method for image steganography algorithm that uses IWT and PSO is presented to increase the security and the imperceptibility of the cover image after embedding. The secret data of various sizes are embedded into the cover image after normalization. The quantitative performance of the proposed technique is analyzed. The MSE and PSNR values vary depending on the amount of secret data embedded in the image. Better PSNR and low MSE values are obtained with the proposed algorithm. The proposed image steganography technique tries to overcome the demerits of previous image steganography approaches. Analysis of the algorithm is accomplished by comparing the proposed approach with other existing approaches. From the empirical results, conclusion can be drawn that the proposed technique is superior in terms of high PSNR and security. The proposed algorithm is applicable on gray scale image and color images but not applicable on...
audio, video and other biometric. Yet, the future work focuses to apply algorithm on audio and videos.

REFERENCES


