Message Concealment in Digital Image based on Steganography

Moh Moh Myint Zin
University of Computer Studies, Yangon
mohmohmz@gmail.com

Abstract

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. The art of sending and displaying the hidden information has received more attention and faced many challenges. Digital steganography exploits the use of a host data to hide a piece of information in such a way that it is imperceptible to a human observer. Wavelet transform that map integers to integers allow perfect reconstruction of the original image. In this paper, the steganography techniques are used to conceal the message in the digital images. Hence, this system embeds the message bitstream into the LSB's of the integer wavelet coefficients of a true-color image. And this system also applies the RSA algorithm to get more authentication and protecting content owner's right. In this proposed system, the original and stego-images are difficult to segregate by the human eyes. The performance of the proposed system is evaluated using the peak signal to noise ratio (PSNR).

Keywords: Steganography, Integer Wavelet Transform (IWT), RSA Cryptosystem

1. Introduction

The development of information technologies makes it convenient for people to transmit mass data through Internet. It also provides vast opportunities for hackers to steal valuable information. Therefore, security becomes an important issue. This increasing dependency on digital media has created a strong need to create new techniques for protecting these materials from illegal usage. One of those techniques that have been in practical use for a very long time is Encryption. The basic service that cryptography offers is the ability of transmitting information between persons in a way that prevents a third party from reading it.

In the digital steganography, exploits the secret message is hided or embedded in media content, so that it is imperceptible to a human observer, but easily detected by a computer. The principal advantage of this is that the content is inseparable from the hidden message.

In an image steganographic system, a message is embedded in a digital image by the stegosystem encoder which uses a key. The resulting stego-image is transmitted over a channel to the receiver where it is processed by the stegosystem decoder using the same key.

There has been a lot of research on developing techniques for the purpose of placing data in the images. Some techniques are more suited to dealing with small amounts of data, while others to large amounts. Some techniques are highly resistant to geometric modifications, while others are more resistant to non-geometric modifications, e.g., filtering. Those methods for the embedding of messages into cover images fall into two main categories: high bit-rate data hiding and low bit-rate data hiding, where bit-rate means the amount of data that can be embedded as a portion of the size of the cover image.

The most common and simplest form of high bit-rate encoding is the least significant bit insertion (LSB). This method embeds the message into one or more least significant bits of some selected pixels. Not every pixel is suitable for being changed. Changing the values of some pixels may result in a degradation of the quality of the original object. The advantages of the LSB method include the ease of implementation and high message payload.

This system includes embedding the message by modulating coefficients in a transform domain, such as the Integer Wavelet Transform (IWT) by using LSB insertion. The transformation can be applied to the entire image or to its subparts. And to get more authentications the RSA algorithm is used for the encryption the secret key. Finally, PSNR is used to measure the invisibility of the hidden messages.

In this paper, IWT is used over the cover image to conceal the secret message. The next section explores the overview of the steganography and IWT. In the section 3, the RSA key generation is described. Then the proposed system is presented. And the last section analyzes the experimental results by the PSNR based on the various message lengths.

2. Steganography

Steganography is not only the art of information hiding, but also the art and science of hiding the fact that communication is taking place. It utilizes the typical digital media such as text, image, audio, video and multimedia as a carrier for hiding private information in such a way that the unauthorized person cannot detect or even notice the presence of the communication. In this way, steganography allows for authentication, copyright protection, and embedding of messages in the image or in transmission of the image. Most of the existing steganographic algorithms are performed in pixel domain as it provides more embedding space, reliability and controllability in encoding and decoding of the hidden message.

Steganography differs from cryptography in that it provides secrecy of the data being sent. The advantage of steganography over cryptography is that messages do not attract attention to themselves. Plainly visible encrypted messages will arouse suspicion. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties. So,when a cryptographic message is steganographically concealed, it is indecipherable and undetectable.

Steganography can be used in many areas of life and work such as to hide a secret chemical formula or plans for a new invention, in the non-commercial sector to hide information that someone wants to keep private, to prevent unauthorized persons from becoming aware of the existence of a message, etc.

2.1. Integer Wavelet Transform

The wavelet transform (WT) has gained widespread acceptance in signal processing and image compression. Because of their inherent multi-resolution nature, wavelet-coding schemes are especially suitable for applications where scalability and tolerable degradation are important. Wavelet transform is used to convert a spatial 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 used in many applications such as engineering and scientific applications, in scalable lossless image coding applications, region of interest coding in medical images to reduce the cost while meeting the diagnostic quality requirements, digital communications, biomedical signal processing, medical imaging, matrix computation, digital signal compression, and video-conferencing , etc.

The used of wavelet filters have floating point coefficients. Thus, when the input data consist of sequences of integers as images, the resulting filtered outputs no longer consist of integer which doesn't allow perfect reconstruction of the original image. So, the wavelet transform that maps integer to integer can be able to characterize the output is integer.

The integer wavelet transform (IWT) is efficient approach for lossless compression. Lossless means digitally identical to the original images and only achieve a modest amount of compression. The advantages of integer wavelet transform is better identification of which data is relevant to human perception because of that can be give higher compression ratio.

One example of the integer wavelet transform is S-transform that is based on the Haar wavelet transform. Its smooth (s) and detail (d) outputs for an index n are given in equations 1(a) and 1(b) are the results of the applications of the high-pass and low-pass filters respectively. It is not an integer transform. To build integer transform, the rounding-off definition is used over the equations of sum (smooth) and difference (detail). It is seems that it discards some information but the sum and the difference of two integers are either both even or both odd. So that is safely omitting the last bit of the sum, since it is equal to the last bit of the difference. The S-transform is reversible and its inverse is given in equations 2(a) and 2(b).

$$s(n) = \left\lfloor \frac{x(2n)+x(2n+1)}{2} \right\rfloor \quad \text{.....1(a)}$$

$$d(n) = x(2n) - x(2n+1) \quad \text{.....1(b)}$$

$$x(2n) = s(n) + \left\lfloor \frac{d(n)+1}{2} \right\rfloor \quad \text{.....2(a)}$$

$$x(2n+1) = s(n) - \left\lfloor \frac{d(n)}{2} \right\rfloor \quad \text{.....2(b)}$$

For the construction of the 2D S-transform, suppose that the original image (I) which has Y pixels wide and X pixels high and the color level of pixels located at position i and j is denoted by $I_{i,j}$ is computed by the following equations.

$A_{i,j} = \lfloor (I_{2i,2j} + I_{2i+1,2j})/2 \rfloor$ (A=low-pass coefficient)

$H_{i,j} = I_{2i,2j+1} - I_{2i,2}$ (H=horizontal coefficient)

$V_{i,j} = I_{2i+1,2j} - I_{2i,2j}$ (V=vertical coefficient)

$D_{i,j} = I_{2i+1,2j+1} - I_{2i,2j}$ (D= diagonal coefficient)

The inverse is given by the following equations.

$$I_{2i,2j} = A_{i,j} - \lfloor H_{i,j}/2 \rfloor$$

$$I_{2i,2j+1} = A_{i,j} + \lfloor (H_{i,j} + 1)/2 \rfloor$$

$$I_{2i+1,2j} = I_{2i,2j+1} + V_{i,j} - H_{i,j}$$

$$I_{2i+1,2j+1} = I_{2i+1,2j} + D_{i,j} - V_{i,j}$$

where $1 \le i \le X/2$, $1 \le j \le Y/2$

Note that the presented transforms are not computed using integer arithmetics, since the computations are still done with floating point numbers. However, the result is guaranteed to be integer due to the use of the floor function and hence the invertetibility is preserved. The integer wavelet transform is applying to the lena image is as shown in Figure 1.

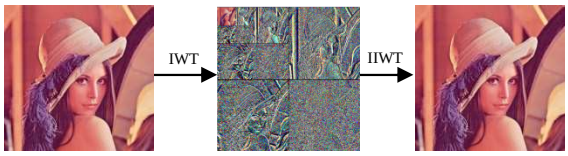


Figure 1. Lena Image Applying Integer Wavelet Transform

3. RSA Cryptosystem

Cryptography enables to store sensitive information or transmit it across insecure networks. It concerned with message confidentiality and intended to ensure the secrecy and authenticity of messages. In cryptography, the encryption and decryption algorithms are public, anyone can access them. The key are secret. So they need to be protected. Cryptography algorithms can be divided into two groups: symmetric-key cryptography algorithm and asymmetric-key cryptography algorithm. Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. In asymmetric-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption.

RSA is the asymmetric-key cryptosystem and it support encryption and digital signature and most widely used public key algorithm. It is relatively easy to understand and implement. RSA is used in security protocol such as IP data security, transport data security, email security, terminal connection security, etc. In Figure 2, the block diagram of the RSA algorithm is shown.

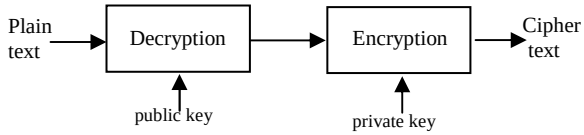


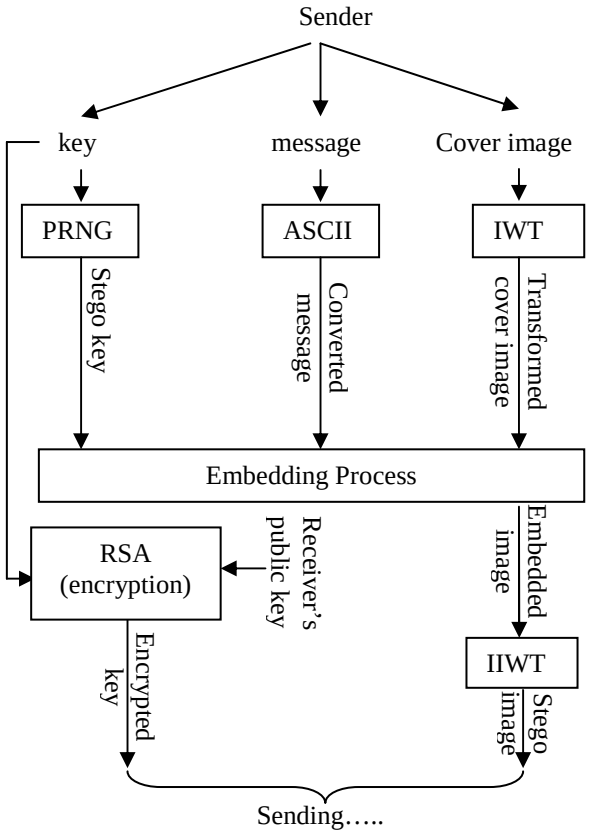
Figure 2. Block Diagram of RSA Algorithm

3.1. RSA Key Generation

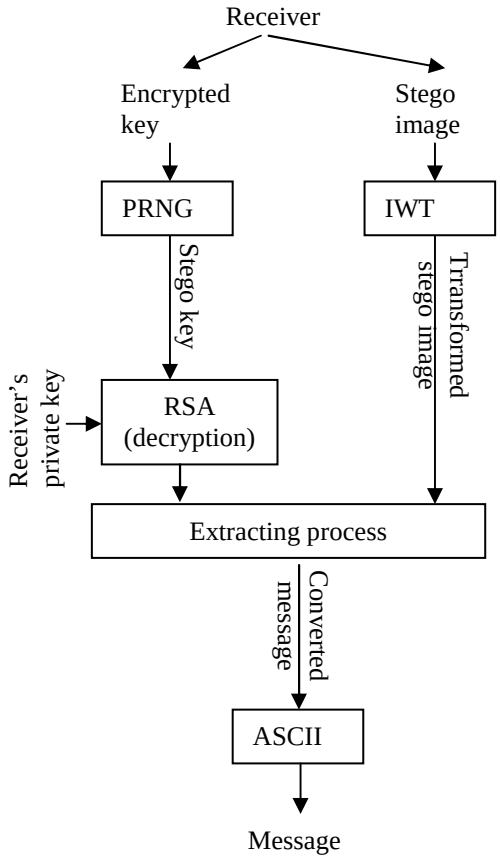
The key generation starts by finding two distinct prime numbers p and q. At first, pseudo random number generator (PRNG) is used to generate random numbers, and then they are tested for primality and will be regenerated until prime numbers are found. The p and q must same length in bits, must not be equal, and they should not be close to each other. Compute modulus n = p*q and $\Phi(n) = (p - 1)(q - 1)$. The n will be stored for later as it is part of the public key. To have 1024 bit public key, then p and q are about 512 bits each. Choose a random integer e, $e < \Phi(n)$ and greated common divisor, $\gcd(e, \Phi(n))$, then compute the integer d, $d=e-1 \bmod \Phi$. Then the key pairs of (n,e) is the public key and (d,e) is the private key.

4. The Proposed System

The wavelet transforms that maps integers to integers in the field of image steganography allowed the embedded message to be recovered without loss. The 2D S-Transform is applied on each color plane of the colored cover image. Then the secret message bit streams is stored in the least significant bits of the transform coefficients. The RSA cryptosystem with 1024 bits key length is used to encrypt the secret key. And the resulted stego-image and the encrypted key are transmitted over a channel to the receiver of the other site. The proposed system is as shown in Figure 3.



(a) The Embedding Process



(b) The Extracting Process

Figure 3. System Overview

4.1. The Embedding Process

Firstly, the secret message is converted by the ASCII code for each character into an 8-bit binary representation, and the concatenating as a sequence. The next step is the cover adjustment is concerned with applying Integer Wavelet Transform on the cover image. The cover image is the color image and it has three color planes: red, green and blue, so the wavelet transform is performed on each color plane separately.

The pseudorandom permutation is used for the secure selection scheme. The permutation generator uses the stego key and produces as the different sequences of the set. The embedding process stores the message bits in the least significant (LSB) of the IWT coefficients of the cover image. This system use the four sub-bands of the image transform for embedding. After embedding process, the stego image is produced by applying the Inverse Integer Wavelet Transform (IIWT) on the modified coefficient.

Finally, the stego key is encrypted by the RSA algorithm using the receiver's public key to get more authenticity. The size of the secret message can embed to the cover image is depended upon the cover image. If the image has MxN pixels, the size of the message is (3*M*N)/8 characters. The cover image and the secret key are given by the user. And the stego-image and the encrypted key are sending to the receiver.

4.2. The Extracting Process

Firstly, the receiver's private key is used in the RSA algorithm to decrypt the secret key. And then reverse the embedding operation starting from applying the IWT on each color plane of the stego image, then select the embedding coefficient. Then the extracted bits are converted into its original form.

5. The Experimental Results

The high bit-rate data hiding can be provided the maximum possible payload and the embedded data must be imperceptible to the human observer. Any modifications to the files, such as conversation of the file type, add the noise, crop the stego image, etc. is expected to remove the hidden bits from the file because the data bits are hidden in the LSB of the cover image.

The invisibility of the hidden message can be measured in terms of the Peak Signal-to-Noise Ratio (PSNR). In this paper, to evaluate the imperceptible of the proposed system, several sizes of images are tested based on the various message lengths by the PSNR.

PSNR is used to be a measure of image quality and is useful to access image imperceptibility which can be evaluated using subjective evaluation techniques involving human observers. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40dB and above.

$$\text{PSNR} = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right)$$

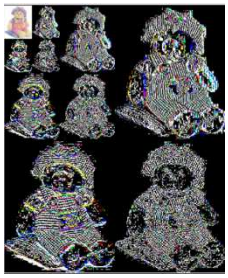
$$\text{PSNR} = 20 \log_{10} \left(\frac{MAX_I}{RMSE} \right)$$

$$\text{MSE} = \frac{1}{xy} \sum_{x,y} (p(x,y) - \hat{p}(x,y))^2$$

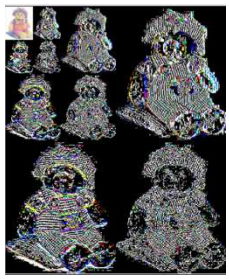
$$\text{RMSE} = \sqrt{\frac{1}{xy} \sum_{x,y} (p(x,y) - \hat{p}(x,y))^2}$$

where,
(x,y) is the coordinate of the original image,
p(x,y) is the pixel of the cover image,
$\hat{p}$ (x,y) is the same pixel in the stego image,
MSE is the mean square error,
RMSE is the root mean square error as a measurement criterion, and
MAX_I is the maximum of image pixels (255 pixels).

(a) Bear (379x456)



(b) Transformed cover image



(c) Embedded image

(d) Stego image

Figure 4. Resulted Images of the Embedding Process

To compare the cover image and the stego image use the Figure 4(a) that shows the color image of bear and Figure 4(d) that shows the resulted stego image after embedding the message of 96 kbits based on 4 bits per pixel. The RMSE and PSNR measured on Figure 5(b) are 1.074 and 47.504 respectively. As shown in above information, the difference between the covered image and stego image is barely distinguishable by the human eye.

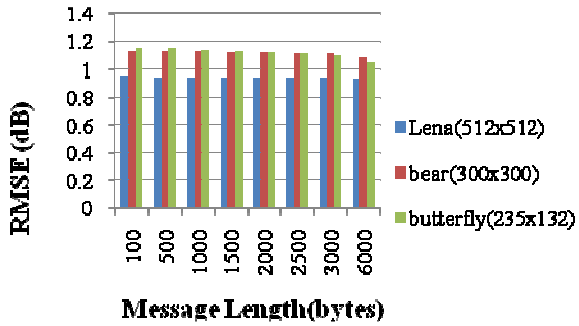


Figure 5. RMSE Values Change over Various Message Length

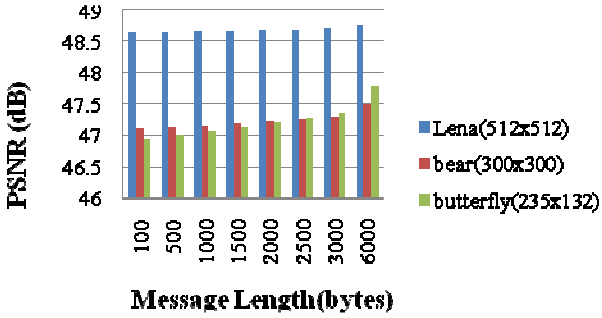


Figure 6. PSNR Values for Various Message Length

Figure (5) shows the results of RMSE values and Figure (6) also shows the results of PSNR values change over various message lengths and sizes of the cover images.

5. Conclusions

This system allows the perfect reconstruction of the original image by using the Integer-Wavelet-Transform. And the message embedded in the cover image is more secure than others because the data are embedded in the random bits generating by the PRNG and the key for this PRNG (stego-key) is encrypted by the RSA algorithm. The proposed algorithm deals with true-color images and applies the S-Transform on each color plane separately. According to the experimental result, the cover image and the stego image are difficult to distinguish by the human eye.

So, this system can be used to transfer message or copyright protected images in the governmental departments, such as Immigration, Police and Military and all where secret communication is essential. In addition, this system makes the stegoanalysis be more complicated and difficult to detect the stego image by combining the steganography and cryptography algorithms.

7. References

[1] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt “Digital Image Steganography: Survey and Analysis of Current Methods”, School of Computing and Intelligent Systems, Faculty of Computing and Engineering University of Ulster at Magee, London.

[2] A. R. Calderbank, I. Daubechies, W. Sweldens, B. Yeo, “Wavelet Transforms That Map Integers to Integers”, Applied and Computational Harmonic Analysis (ACHA), 1996.

[3] B. Dunbar, “A detailed look at Steganographic Techniques and their use in an Open-Systems Environments”, SANS Institute 2002.
[4] C. Mulcahy, Ph.D. “Image Compression Using The Haar Wavelet Transform”, Spelman Science and Math Journal.
[5] F. Khan and A. Abdul-Aziz Gutub “Message Concealment Techniques using Image based on Steganography”**.**
[6] G. Xuan1, Y. Q. Shi2, Z. C. Ni2, J. Chen1, C. Yang1, Y. Zhen1, J. Zheng1, **“**High Capacity Lossless Data Hiding based on Integer Wavelet Transform**”,** ISCAS 2004.
[7] H. Manjunatha Reddy, K B Raja, “High Capacity and Security Steganography Using Discrete Wavelet Transform”, international journal of computer science and security (ijcss).
[8] J. Cummins, P. Diskin, S. Lau and R. Parlett, “Steganography And Digital Watermarking”, copyright © 2004.
[9] N. Provos and P. Honeyman, “Hide and Seek: An Introduction to Steganography”, IEEE Security and Privacy, 2003, pp.32-44.
[10] P. Riikonen, “RSA Algorithm”, 2002.
[11] R.J.E. Merry, “Wavelet Theory and Applications”, Eindhoven, June 7, 2005.
[12] S. Areepongsa , Y. F. Syed , N. Kaew-kamnerd , and K. R. Rao, “Stegano-graphy For A Low Bit-rate Wavelet Based Image Coder”, The University of Texas at Arlington, Box 19016, TX 76019.
[13] S. Channalli, A. Jadhav “Steganography An Art of Hiding Data”, International Journal on Computer Science and Engineering Vol.1(3), 2009, pp.137-141.