

Securing Image Steganography Based on Visual Cryptography And Integer Wavelet Transform

Yasir Ahmed Hamza

Department of Computer Science, Computer and IT Faculty, Nawroz University, Duhok, Iraq

Abstract : The increased use of internet communication has given rise to the field of image steganography and made it necessary to secure digital content. Current image steganography techniques lack novelty and are based on using traditional cryptography solutions for secret image that is embedded in cover image. This research paper proposed and implemented a new method to secure embedded secret image using visual cryptography. A two level integer wavelet transformation technique was applied on the cover image to obtain the coefficients which were used later during the secret image embedding process. The experimental results indicated that high invisibility was achieved for secret image and the ability to embed more than one secret image within the cover image. Also, the use of visual cryptography eliminated the need for permutation process which would otherwise be required for secret image.

Keywords: Cryptography, Image Steganography, Integer wavelet transform, Stego-image, Visual Cryptography.

I. INTRODUCTION

Data communication is one the essential function of the Internet, because of the ease of data transportation and the capability of transferring data over long distances. In spite of the numerous benefits offered by the Internet, there are still many challenges associated with data communication. One of the toughest challenges is data intrusion where adversaries would change content and manipulate data. Therefore, a number of solutions have been implemented to maintain the confidentiality of data. One of which is data encryption. Encryption involves converting human-readable data to unreadable form using one of cryptographic algorithms. An intruder trying to access data, would need to know the encryption algorithm used along with secret key.

On the other hand, there is another way to protect data by embedding data within other data which is known as hidden writing or steganography. In this method, one of the multimedia elements are used (e.g. image, text, video or audio) as a cover media and use a special algorithm to embed confidential data within it. The cover is then sent to the other party. This, in turn, is the process of extracting confidential data through the use of an extraction algorithm.

The word steganography is originally a Greek word; *stegos* means cover and *grafia* means writing [1, 2]. When words are gathered, the result is covered writing or hidden writing. Historically, steganography has been used by Greeks. So when someone wants to send a secret message to his son-in-law, he shaved the head of one of the trusted slaves and put the secret message as a tattoo on his head and waited until his hair grew; then he would send him to the destination with the secret message [1, 2]. Secret (Invisible) ink is another way of steganography where ancient Romans found a way to write between lines using a secret ink [2]. Secret ink was also used during the World War II.

Steganography differs from cryptography in that cryptographic techniques are designed to preserve the secrecy of data; while steganography techniques are used to maintain the existence of confidential data [1, 2, 3]. According to [1] steganography can be made more powerful by combining it with cryptographic techniques. Nowadays, there are a lot of algorithms proposed for data hiding due to an unprecedented amount of research carried out in this area.

In this research study, I will propose a novice method based on using visual cryptography and steganography. The proposed method will be applied on digital color images to build a system that is capable of maintaining data confidentiality within cover image. For this purpose, I will be using a confidential image and embed it within a cover image. Before embedding the confidential image, I will apply an algorithm called (2 out 2 share) which involves inputting an image, splitting it to two secret share, and then split each secret share into two shares. The process involves breaking down the cover image into three layers (Red, Green, and Blue). I will then apply a method called two level integer wavelet transform (IWT) on the blue layer. The result of this application is four sub-bands (Low-low sub-band (LL), High-low sub-band (HL), Low-high sub-band (LH), and High-high sub-band (HH)). Then each share will be embedded within each sub-band. The end result for this process will be stego-image.

On the other side, the extraction process requires taking the stego-image as an input, split into three channels (Red, Green, Blue), and then take blue layer and apply two level integer wavelet transform on it. As

mentioned previously, the result will be four sub-bands; those four sub-bands will be used to extract the secret shares. Then I will combine these shares with each other which will result in a confidential image as output.

II. IMAGE STEGANOGRAPHY

Images have become the most frequently used object in the field of data hiding [1, 2]. This is due to the possibility of random access to any pixel within the image. In addition, images can preserve the secret content and make it difficult for the naked eye to distinguish manipulation in cover image that used during embedding process [2]. Therefore, the usage of images in the field of data hiding can be considered as one of the hot topics. To hide the secret content within the cover image there are several methods used, the most important are [1, 2, 4]:

- 2.1 Spatial Domain (Least Significant Bit): it is the simplest method to embed secret data in the cover image [1]. This method is based on using one or more of the bits that represent the least significant bits of the cover image pixel value. Therefore, we can embed one bit form the secret data in each pixel value of the cover image. For example, if we have a color image, we can divide it into three channels (red, green, and blue), and then embed one bit of secret data within each color pixel value separately. The disadvantage of this method is that when the cover image falls in adversary's hands, he/she can easily extract each least significant bit form cover image pixel value and determine the content of embedded confidential data.
- 2.2 Transform Domain: in this method, secret data embedding process is done in image frequency domain [2]. Therefore, transformation is applied on cover image to obtain the coefficients of cover image. Some or all of these coefficients can be used during the secret data embedding process. This method can be used to design a more powerful image steganography system. One advantage of this method is that it keeps confidential data in the area of the cover image that are susceptible to image processing attacks (e.g. cropping, image compression...etc). There are different types of image transformation that are used (e.g. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT)). Another type of transformation that maintains the reversibility of the cover image is called Integer Wavelet Transform (IWT).
- 2.3 Spread Spectrum: in radio communications, spread spectrum is used to transfer data under the noise level for any given frequency [2]. In order to use this method in the data hiding field, the spread treats cover image as noise or trying to add pseudo-noise to it [2]. Therefore, the secret data is spread through the cover image secretly, which makes it difficult to detect [1]. During the embedding process, the confidential data is embedded within noise and then it's combined with the cover image. The power of confidential data as signal is less than that of the cover image. Therefore, without accessing the original image, embedded confidential data cannot be visible to the human eyes or by computer analysis [1].

There are four main objectives that need to be considered when designing a steganography system [3, 5]:

- Imperceptibility: it means preventing the naked eye to detect the presence of other data included in the cover image.
- Security: in the event that the cover image suffers an attack, the system to protect confidential data from the attack.
- Embedding Payload: the amount of data that can be concealed within the cover image without affecting the quality of the cover.
- Robustness against attack: the possibility of maintaining the confidential data in the event that the cover image suffers image processing operations such as filtering, compression, rotating...,etc.
-

III. Visual Cryptography

This cryptographical method is used to encrypt writing materials (e.g. typed text, handwritten notes or pictures etc.) visually [6]. This method maintains the confidentiality of such data optimally. During the encryption process data is converted into a set of transparent images that are called shares. During the deciphering process, shares are stacked one above the other to obtain the original image. Therefore, the deciphering process is performed using the human visual system. One advantage of this method is that it does not need complex computations.

Decipher Algorithm [7]: Suppose that we have a binary (Black and White) image and we want to apply a (2 out 2 share) visual cryptography on it. We need to perform the following steps:

- Determine the number of shares, in this algorithm need to generate two secret shares..
- Take each pixel form the original image and check the pixel color:
 - If pixel color is white, then randomly choose a pair of pixels and place it into the first share and the offset is placed in the second share. As shown in Table 1.
 - If pixel color is black, then randomly choose a pair of pixels and place it into the first share and the offset is placed in the second share. As shown in Table 1.
- Repeat the above steps until taking all the values of the original image.

➤ The result of this algorithm will be two secret shares.

Each one of them is not given any information about the original image, but when you stack those secret shares together we get the original image. Note that all white colors are represented by a pair of pixels (one white and one black).Whereas, all the black colors are represented by a pair of pixels (one Black and one Black).

Table 1: Construction of (2 out 2 share) Visual Cryptography

| Pixel | White | | Black | |
|--------------------------|-------|-----|-------|-----|
| | 50% | 50% | 50% | 50% |
| Share-1 | | | | |
| Share-2 | | | | |
| Stack Share-1 and Share2 | | | | |

IV. Integer Wavelet Transform

According to [3], they proposed a steganography technique used to embed multiple confidential images with its keys in cover image. This technique is based on using IWT. As a result of this method no visual difference between stego-image and cover image existed. Also peak signal-to-noise ratio (PSNR) was very good. [4] Proposed a data hiding technique based on using IWT. During the embedded process, the secret image hides in IWT coefficients of cover image by using LSB. The result was high invisibility in stego-image. In [8] a reversible steganography method implemented that was dependent on using IWT and histogram shifting which preserved the visual quality of stego-image. In addition, it kept recovery process lossless. A new technique was proposed by [9] which were based on using combination of DWT and IWT. This method maintained invisibility, high security and robustness.

Typically, wavelet transform cannot reach the reversibility well, due to the transformation process that is based on floating point values [8] . During the decomposition process, it is likely that some of the values of the reconstructed image will change. Therefore, this research has used integer wavelet transform, depending on the concept of the integer to integer mapping that operates on the principle of lifting. This method is similar to the discrete wavelet transform and has the same performance. It is a transformation from a non-linear type [9]. When we apply this transformation on the image, we will obtain four (low-low, high-low, low-high, and high-high) sub-bands. The approximation LL sub-band is close to the original image.

If the original cover image (CI) and the value of each pixel at (i,j) is denoted by CI_{i,j}. The IWT sub-bands can be obtained by applying the following equations [3, 4]:

$$LL_{i,j} = \lfloor (CI_{2i, 2j} + CI_{2i+1, 2j}) / 2 \rfloor \quad (1)$$

$$HL_{i,j} = CI_{2i+1, 2j} - CI_{2i, 2j} \quad (2)$$

$$LH_{i,j} = CI_{2i, 2j+1} - CI_{2i, 2j} \quad (3)$$

$$HH_{i,j} = CI_{2i+1, 2j+1} - CI_{2i, 2j} \quad (4)$$

The inverse IWT can be obtained by applying the following equations:

$$CI_{2i, 2j} = LL_{i,j} + \lfloor HL_{i,j} / 2 \rfloor \quad (5)$$

$$CI_{2i, 2j+1} = LL_{i,j} + \lfloor (HL_{i,j+1}) / 2 \rfloor \quad (6)$$

$$CI_{2i+1, 2j} = LL_{i,j} + HL_{i,j} - HL_{i,j} \quad (7)$$

$$CI_{2i+1, 2j+1} = LL_{i,j} + HL_{i,j} - HL_{i,j} \quad (8)$$

Where, $1 \leq i \leq X/2, 1 \leq j \leq Y/2$ and $\lfloor \rfloor$ denotes floor value.

V. The Proposed Algorithm

As mentioned previously, the proposed steganography algorithm is based on using IWT on the cover image. To increase the security of confidential image, (2 out 2 shares) visual cryptography technique is applied on secret image. The secret image that is used in embedding process has the size 128X128 whereas the cover image size is 512X512. The proposed embedding algorithm works as the following and it's also demonstrated in Fig.1.

5.1 Embedding Process:

- Input the secret image.

- Apply (2 out 2 shares) visual cryptography which will result in two secret shares. Each one has a new size of (128 X265).
- Divide each secret share into two sub-shares.
- Input the original color image as a cover image.
- Divide the cover image into three channels (red, green, and blue).
- Take the blue layer and apply 1st-level IWT which will result in four sub-bands (LL1, LH1, HL1, and HH1).
- Take the LL1 sub-bands and apply 1st-level IWT which will result in four sub-bands (LL2, LH2, HL2, and HH2).
- Embed each sub-share in each of (LL2, LH2, HL2, and HH2) sub-bands of LL1.
- Apply inverse IWT on (LL2, LH2, HL2, and HH2) sub-bands to obtain (LL1) sub-band.
- Apply inverse IWT on (LL1, LH1, HL1, and HH1) sub-bands to obtain the new blue layer.
- Combine the new blue layer with red and green layers to obtain the stego-image.

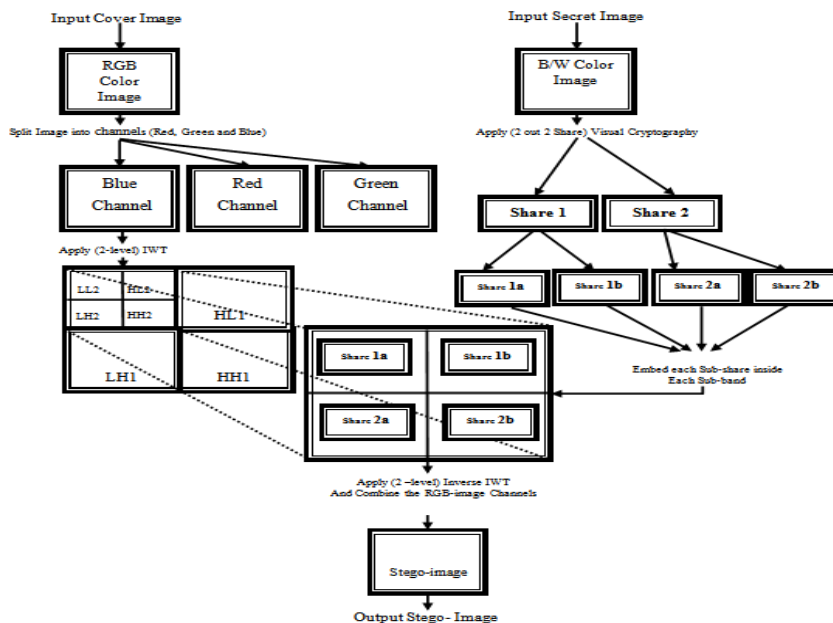


Figure (1): embedding process for the secret image.

5.2 Extraction Process:

To extract the secret image form stego-image, we only need the stego-image for the extraction algorithm. The extraction algorithm works on the principle of blind extraction without the need for the original image. Performing the extraction process requires the following steps and it's also demonstrated in Fig. 2.

- Input the stego-image.
- Divide the stego-image into three channels (red, green, and blue).
- Take the blue layer and apply 1st-level IWT which will result in four sub-bands (LL1, LH1, HL1, and HH1).
- Take the LL1 sub-bands and apply 1st-level IWT which will result in four sub-bands (LL2, LH2, HL2, and HH2).
- Extract each sub-share from each of (LL2, LH2, HL2, and HH2) sub-bands of LL1.
- Combine each sub-share to obtain the original two secret shares.
- Stack the two shares to obtain the secret image.

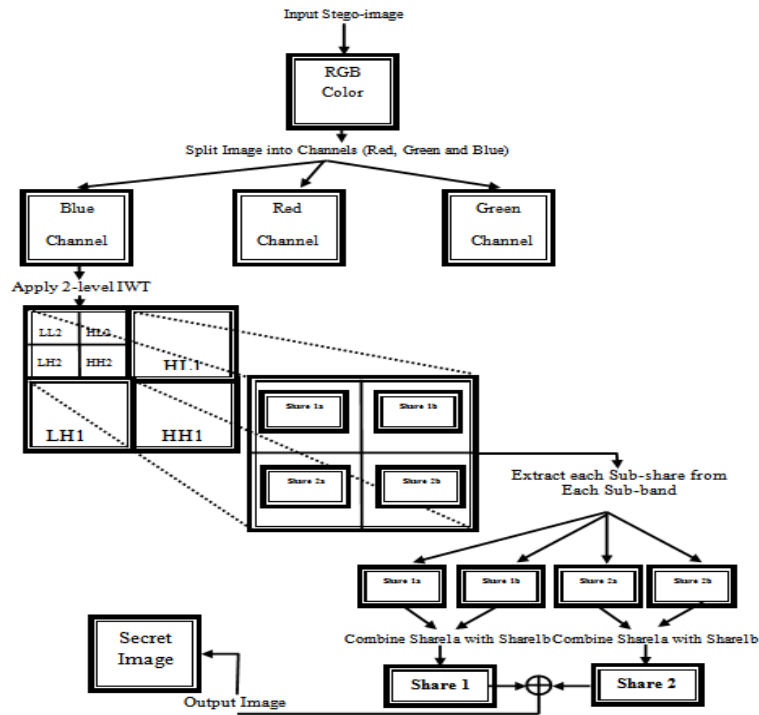
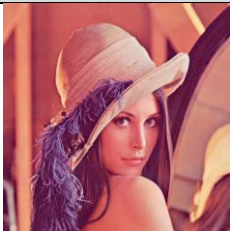
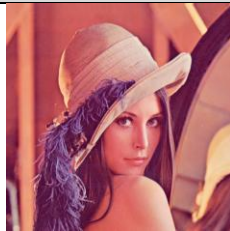
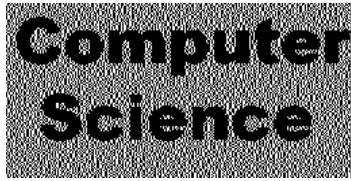
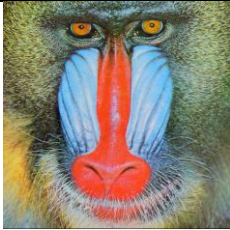
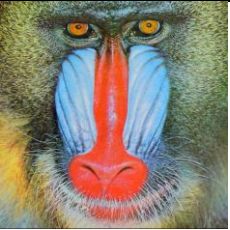





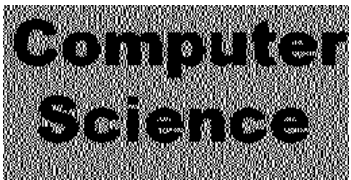


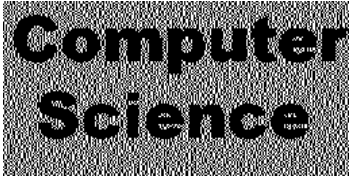
Figure (2): the secret image extraction process.

VI. EXPERIMENTAL RESULTS

The proposed algorithm has been implemented using Matlab R2009a. A graphical user interface was designed for embedding and extracting the secret image from cover image. Four frequently used images of size 512X512 (Lena, Baboon, Monalisa, and Peppers) were chosen to be tested for image steganography. These images are selected to be cover images. The secret image is black and white image of size 128X128, contains the expression “Computer Science”. This secret image is embedded in each cover image. To test the quality of stego-image, two measurements were used; the first measurement is root mean square error (RMSE) while the second one is PSNR. The experimental results show that the tested stego-image maintains high invisibility even when more than one secret image was embedded according to PSNR values. Also, using visual cryptography makes the proposed algorithm not need to use secret key to perform permutations on secret image and this is what makes this method keyless. The test images, stego-images, extracted secret images, RMSE values, and PSNR values are shown in Table 2.

Table 2: Test Images with Their Respective RMSE and PSNR Values

| Cover Image | Stego-image | Extract Secret Image | RMSE | PSNR |
|---|---|--|-------|--------|
|  |  |  | 1.411 | 45.140 |
|  |  |  | 1.412 | 45.133 |

| | | | | |
|---|---|--|-------|--------|
|  |  |  | 1.413 | 45.127 |
|  |  |  | 1.417 | 45.104 |

VII. CONCLUSION

This paper has integrated image steganography with visual cryptography to design and implement a new algorithm. This algorithm is based on using the integer wavelet to transform the cover image into transform domain for obtaining the cover image coefficients. These coefficients were used in secret image embedding process which the (2 out 2 share) visual cryptography was applied on it. The experimental results showed the proposed algorithm maintained high invisibility, high security, and low robustness for secret image. Also, the ability to embed multiple secret images within one cover image. The limitation of the proposed algorithm is that it could not maintain good robustness for secret image against image processing attacks (e.g. filtering, image compression, rotation, .etc) that target stego-image. This limitation can be addressed in future research.

REFERENCES

- [1] T. Markel, J.H.P. Eloff, and M.S. Olivier, "An overview of image steganography", *Proceedings of the Fifth Annual Security South Africa Conference (ISSA2005)*, Sandton, South Africa, 2005.
- [2] N. Hamid, A. Yahya, R. Ahmed, and O.M. Al-Qershi, "Image steganography techniques: an overview", *International Journal of Computer Science and Security (IJCSS)*, Vol.6, Issue 3, 2012.
- [3] S. Hemalatha, Dinesh A.U., A. Renuka, and R.K. Pariya, "A secure and high capacity image steganography technique", *Signal and Image Processing: an International Journal (SIPIJ)*, Vol.4, No. 1, 2013.
- [4] M.F. Tolba, M.A. Ghonemy, I.A. Taha, and A.S. Khalifa, "Using integer wavelet transforms in colored image-steganography", *International Journal of Intelligent Computing and Information Science*, Vol. 4, No. 2, 2004.
- [5] S. Kumar, and S.K. Muttoo, "A comparative study of image steganography in wavelet domain", *International Journal of Computer Science and Mobile Computing*, Vol.2, Issue 2, 2013, pp. 91-101.
- [6] M. Noar, and A. Shamir, "Visual cryptography", *Advances in Cryptography: Eurpocrypt '94*, Springer-Verlag, Berlin, 1994, pp. 1-12.
- [7] S. Chandramathi, K.R. Ramesh, and S. Harish, "An overview of visual cryptography", *International Journal of Computational Intelligence Techniques*, Vol. 1, Issue 1, 2010, pp. 32-37.
- [8] S.K. Jinna, and L.Ganesan, "Reversible image data hiding using lifting wavelet transform and histogram shifting", *International Journal of Computer Science and Information Security*, Vol. 7, No. 3, 2010.
- [9] P. Ganesan, and R. Bhavani, "A high secure image steganography using dual wavelet and blending model", *Journal of Computer Science*, Vol. 9, Issue 3, 2013, pp. 277-284.