Analysis of Multiple Data Hiding Combined Coloured Visual Cryptography and LSB

1Halim Maulana, 2Edy Rahman Syahputra
12Department of Information System Sekolah Tinggi Teknik Harapan, Medan-20217, Indonesia
1thekazagami@gmail.com, 2ydeaja@yahoo.com

Abstract. Currently the level of data security becoming a major factor in data transfer. As we know every process of sending data through any medium the risk of that data gets hacked will still be there. Some techniques for securing data such as steganography and cryptography also often used as a solution for securing data. But it does not last long because it has been fou out the weaknesses of the algorithm so that the security be assured. So, in need of variety of new algorithms to be able to protect the data so that data security can be guaranteed. In this study tries to combine two visual algorithms that steganography and cryptography. Where in these experiments will try to secure two pieces of data type that is the type of image data and text data where both the data is regarded as a message so to obtain the correct information receiver should get that two types of data.

1. Introduction
In the communication between the two sides, there is no guarantee that states that the communication occurs has been safe from the threat of a third party. The presence of a third party in a communication can interfere with the comfort of both parties. The third party can retrieve important information from the communication that is going on. This course will be very detrimental to the first and second parties. Based on this was the need for a technique to secure information that is considered important to avoid the threat of a third party. Steganography is an art as well as techniques to hide information such as messages and data on digital media [1]. Securing steganography techniques to hide the message by means of a medium, so that third parties do not suspect messages in the media. Digital media are typically used to hide the message can be text files, digital images, audio, and video. One method of steganography is the Least Significant Bit (LSB) is done by modifying bits including LSB bits in each byte of colour in a pixel. [2][3][4][5]. However, the data security techniques by using steganography methods have emerged many weaknesses and shortcomings in the use of which may cause data to be very unsafe. It can be seen from several previous studies [6][7][8]. In cryptography is also known in the visual cryptography which in visual basic concepts of cryptography works by breaking down an image into sections picture that looks like white noise, but when the parts are united then the hidden image will be displayed [9][10][11]. But based on research-research that past steganography and cryptography techniques are becoming less secure and thus require a breakthrough or other variations in a secure data. In another study [12] conducted a combination of visual methods of steganography and cryptography. In this process, the original image file will be processed by steganography and then encrypted using visual cryptography produce multiple images. In the result, even if the image file managed in the reconstruction process but when done visual cryptography hidden data being lost when detected with a hex editor. The data is lost due to the imperfection of the reconstruction process of visual cryptography. So, it takes a more optimal reconstruction process so that confidential data is not lost either in the form of image or message text. Based on that can be
concluded that both the technique of steganography and cryptography have lack in securing the data so that the data becomes less secure.

2. Proposed Methodology

2.1. LSB Process
Step 1: Read the values of the primary colour components are red, green and blue.
Step 2: Read the text of the message that will be hidden
Step 3: Compares the message size and image size. the process will only run if the size of the image larger than the size of the message.
Step 4: For a character message, all i up to n, perform the checks smallest pixel value of the components of R, G and B by using Operations AND / OR
Step 5: Message Successfully embedded and stego image was generated

2.2 Visual Cryptography Process
Step 1: Read the value of pixels for each - each component of R, G, B
Step 2: Make a histogram for each of the intensity of the main components of the R, G, B of the original image. Wherein for each - each histogram R, G, B has 256 levels of intensity.
Step 3: As we saw in the previous step, each colour component has 256 levels of intensity. From the histogram that have been formed in the previous step will be determined Colour Level of each colour component R, G, B. Where the process of determining the Colour, Level is determined by finding the standard deviation value of the components of R, G, B and Colour Levels are divided into 8 categories as follows.

Category 2 = Value Standard Deviation range 20001-30000
Category 3 = Value Standard Deviation range 15001-20000
Category 4 = Value Standard Deviation range 10001-15000
Category 6 = Value Standard Deviation range 8001-10000
Category 8 = Value Standard Deviation range 5001-8000
Category 16 = Value Standard Deviation range 4001-5000
Category 24 = Value Standard Deviation range 2001-4000
Category 32 = Value Standard Deviation <2000

Step 4: Group the histogram into equal parts. For each colour component X ∈ {R, G, B}, will be made on a histogram of the Nx groups X. To do so, will be determined in advance the color intensity of the boundary between each pair of adjacent groups are defined as K0, ..., KNX -2, In other words, the histogram X will be divided into regions Nx, for example [0, K0), [K0, K1), ..., [KNX -2, 255]. The division is made to make Nx each region has the same size in the area. So, for each group, there will be the same number of pixels in the image are included in each group.
Step 5: Next is the stage of making share. To do so, the authors apply the following method for each primitive colour independently. First, take the k-of-n VCS black-and-white. The basis for Boolean Matrix Bb (for b = 0.1), in Denote Bb= [Bb0, Bb1, ..., Bbm-1]
Bbi shows column i (0=i=m-1) of the Bb. Second, for each color component \( X \in \{R, G, B\} \) done in stages as follows:

1. Assuming if the intensity of the color pixel corresponding to the color components of \( X \) falls in a group of \( k \)-th (where \( 0=k = NX -1 \)) then it will be calculated the probability \( P = k / (NX-1) \).

2. With a probability \( P \), the process will be conducted as follows:
   a. Considering the B0 and randomly select a column, for example, where \( 0=j =m B0J-1 \).
   b. Assume B0J as an n-bit vector. For the first bit will be set in black if the bit value is 1, otherwise it will oversee red/red. The process is repeated until all the pixels have been set with a certain colour to n share.

3. For the probability \( 1-P \), will do a stage like the previous step but by replacing B0 to B1. Based on the value of P, in Table 1 shows a summary of the probability distribution B0 and B1 for groups of individuals. Because columns B0 and B1 is selected at random, then the chances of getting any column in B0 and B1 for the group \( k \) becomes \( k / ((NX -1) m) \) to B0 and \( (1-k / (NX -1)) / m \) to B1. Finally, we have put Share R to the i-th with Share G to the i-th and Share B to the i-th, for \( i = 1, \ldots, n \), to form the final value of i-th share yang comprising components of R, G and B.

3. Encryption and Decryption Process

3.1 Encryption
A. Visual Cryptography

Image file is assumed to be in the process by using visual cryptography steganography has experienced before. We assume each pixel is divided into multiple subpixels, but the human eye still sees the pixel as one pixel. A little review about VCS-based Black & White \((k, n)\). Visual Cryptography process used is to use VCS for coloured image. In assuming that the image \( n \) is the image that will be used to process the VCS. An image of a coloured image will be used to generate n share the image. Image that will be processed using the VCS will be in previously resize with a size of 800 x 600. The stages than encryption algorithms VCS that his adaptation of the results of previous studies [13][14][15][16] which consists of several steps, namely Histogram Generation Determination Quality Colour, Grouping, and Share Creation.

B. LSB bit Encryption

Share 1 and share 2 on visual cryptography get from the process will be used as a medium to hide text messages using LSB techniques. The insertion process is done by first converting messages into binary form and then in binary form will be divided into two parts where the half of the first bit will be inserted in the share1 and the half of the other bits will be inserted in share2 using the AND operation and OR [17] [18].

3.2 Decryption Process
A. LSB Extraction

The LSB bits of the steganography image is extracted at first. Then the last pixel value LSB number is identified to the share positions. The LSB bits of other pixels are arranged according the number identified. The share 1 and share 2 are generated using this LSB extraction.
B. Visual Cryptography Decryption
The obtained shares from the LSB extraction is fed as input to the visual decryption process. The shares are combined by alternating the pixels from each share to generate the secret message image.

4. Experimental Results
At this stage it will be a test to hide a secret message and the secret image by using a combination of algorithms Visual Cryptography and LSB. Suppose there is an image that will fund a message is secured using the algorithm. Then the message will be processed in advance using lsb then continued using visual cryptography techniques.

![Secret Image](image1.png)

![Share1](image2.png)

![Share2](image3.png)

**Figure 1.** (a) Secret Image, (b) Share1 (c) Share2

The output of the algorithm is a combination of two share the image that share 1 and share 2 in which the secret message has been inserted into the two shares to regain a secret message and the secret image in need both share the image. After both share the image collected, to be able to get back data and images is carried out secret decryption process which will generate a secret message that is stored in the secret.txt and will also generate a secret image derived from the share 1 and share 2 which has been in combine.

![Overlapped Image](image4.png)

**Figure 2.** (a) Overlapped Image, (b) Regenerated Secret Message

4.1 Performance Analysis
Various parameters recommended by the researchers to evaluate the performance of visual cryptography Naor and Shamir (1995) suggest two main parameters: pixel expansion and contrast a m. Expansion pixel m refers to the number of subpixels in the resulting shares representing a pixel of the original input image. It presented losses resolution than the original image with the results of the share. Instead a is the relative difference between the combination of the share coming from the white pixels and black pixels in the original image. Pixel expansion that occurs between the original image and share the image it will affect the image quality. In table 1 shows that there is no change of the dimensions of the image, either Height or Weight image of Secret Image, share1, Share2 and Overlapped image, but the image size after the process has been reduced which is significant, but the image restoration still can recognize well as the secret image. From the results obtained in Table 1 it can be concluded that the results are not experiencing visual cryptography pixel expansion [19][20][21]. On the table shows that every visual cryptography scheme has a pixel expansion in addition to algorithms used in this study.

| Tabel 2. Other Visual Cryptography Algorithm |
In tables 3 show that the PSNR for the CVC is the largest compared with VC and EVC, where it is means that the value of the reconstruction will be of high quality. However, MSE that produced very high caused by the insertion of a message contained therein. It also means that the degree of similarity between the secret image and the image in the lower encryption because in the encrypted image does not have enough information about the secret images.

**Table 3. Performance Analysis**

| No. | Author | Year | Sec Image | Exp. | Format |
|-----|--------|------|-----------|------|--------|
| 1   | Yaqi & Shari' | 2005 | 1        | 4 | Base   |
| 2   | Narayana | 2002 | 1        | 4 | Base   |
| 3   | Young-Chang Hsu | 2005 | 1        | 4 | Color  |
| 4   | Z. Zhou | 2006 | 1        | 4 | Base   |
| 5   | T. Jang | 2009 | 1        | 4 | Color  |
| 6   | Indeep Verma & Dr. Vinod | 2012 | 1        | 4 | Color  |
| 7   | Dr. Veer Singh & M. Surya Prakash | 2012 | 1        | 4 | Color  |
| 8   | Proposed Method | 2016 | 1        | 1 | Color  |

**4.2 Histogram Analysis**

In the field of image processing histogram shows the distribution of pixel values in an image. Histogram used attacker (attacker) to perform cryptanalysis by utilizing the frequency of appearance of pixels in the histogram. Attackers hope pixel values that often appear in the plain-image is correlated with pixel values that often appear in the cipher-image. By analysing the frequency of occurrence of pixel values, the attacker deduces the key or the pixels in the plain-image.

**Figure 3. Original and Share Image Histogram Compare**

5. Conclusion
The results from the combination of UCS and LSB algorithm has managed well with can hide the image data and messages and can restore the data with good results. Secret image that retrieved might not like the image to the original before being processed, but they can recognize as the same image. High PSNR value means high quality image generated great surplus of other methods. The value of the Mean Squared Error to be very high due to the message that imbed in the image. However, higher values also mean MSE between the original image and the image is not there a similarity that can be considered as a different picture.

References
[1] Channalli, S & Jadhav, A. Steganography An Art of Hiding Data. International Journal on Computer Science and Engineering. 1(3) (2009) 137-141
[2] Laskar, S.A & Hemachandran, K. High Capacity data hiding using LSB Steganography and Encryption. International Journal of Database Management Systems (IJDMS). 4(6) (2012) 57-68
[3] Champakamala. B.S, Padmini, Radhika.D. K. Least Significant Bit algorithm for image steganography. International Journal of Advanced Computer Technology. 3(4) (2012) 34-38
[4] Gupta, S., Gujral, G & Aggarwal, N. Enhanced Least Significant Bit Algorithm for Image Steganography. IJCEM International Journal of Computational Engineering & Management. 15(4) (2012) 40-42.
[5] Reddy, L.V., Subramaniam & Reddy, C.P. Implementation of LSB Steganography and its Evaluation for Various File Formats. Int. J. Advanced Networking and Applications. 2(5) (2011) 868-872
[6] J. Fridrich &M. Goljan. Practical Steganalysis—State of the Art. Proc. SPIE Photonics Imaging. Security and Watermarking of Multimedia Contents.4675 (2002) 1–13.
[7] Provos, N & Honeyman, P. Detecting Steganographic Content on the Internet. Network and Distributed System Security Symp., Internet Soc. (2002)
[8] Westfeld, A. F5—A Steganographic Algorithm: High Capacity Despite Better Steganalysis, Proc. 4th Int’l Workshop Information Hiding. Springer-Verlag. (2001) 289–302.
[9] Dhole, A.B & Janwe, N.J. An Implementation of Algorithms in Visual Cryptography in Images. 3(3) (2013) 1-5
[10] Noar, M & Shamir, A. Visual cryptography. Advances in Cryptology - EUROCRYPT'94. (1995) 1-12.
[11] I. Kang, G. R. Arce and H. K. Lee. Color Extended Visual Cryptography Using Error Diffusion,” in IEEE Transactions on Image Processing, 20(1) (2011) 132-145
[12] G. Abboud, J. Marean and R. V. Yampolskiy. Steganography and Visual Cryptography in Computer Forensics. Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on, Oakland, CA, (2010) 25-32
[13] X. Wu, D. S. Wong and Q. Li. Extended Visual Cryptography Scheme for color images with no pixel expansion. Security and Cryptography (SECRIPT), Proceedings of the 2010 International Conference on, Athens. (2010) 1-4
[14] F. Liu, C. K. Wu and X. J. Lin. Colour visual cryptography schemes. IET Information Security, 2(4) (2008) 151-165
[15] X. Wu, D. S. Wong and Q. Li. Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion. Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT ’09). (2009) 310-315
[16] S. J. Shyu and H. W. Jiang. General Constructions for Threshold Multiple-Secret Visual Cryptographic Schemes. IEEE Transactions on Information Forensics and Security. 8(5) (2013) 733-743
[17] K. Joshi, P. Dhankhar and R. Yadav. A new image steganography method in spatial domain using XOR," 2015 Annual IEEE India Conference (INDICON), New Delhi. (2015) 1-6
[18] X. Gui, X. Li and B. Yang. Steganalysis of LSB Matching Based on Local Binary Patterns. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on, Kitakyushu. (2014) 475-480.
[19] Chettri, L. Visual Cryptography Scheme Based on Pixel Expansion for Black & White Image. International Journal of Computer Science and Information Technologies. 5(3) (2014) 4190-4193
[20] Kumar, P., Agarwal, S & Shivani, S. Halftone Visual Cryptography with Pixel Expansion through Error Diffusion. International Journal of Information & Computation Technology. 4(14 (2014) 1419-1427
[21] Blundo, C., Cimato, S & De Santis, A. Visual Cryptography with Optimal Pixel Expansion. Theoretical Computer Science 369 (2006) 169-182