Pak. J. Biotechnol. Vol. 13 special issue II **(International Conference on Engineering and Technology Systems (ICET'16) Pp. 116 - 120 (2016)**

A COMPARISON OF SECRET IMAGE HIDE METHODS OF STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Saad Al-mutairi,

Computer Science and Information Technology Faculty, Tabuk University, Saudi Arabia.
s.almutairi@ut.edu.sa

ABSTRACT

During the clandestine data transmission, to protect a secret data from the hackers or intruders is one of the difficult task. In this era, when technology grows, simultaneously the challenges of the technologies also increasing rapidly. In connection with that, while selecting any technology for the particular process, we are in position to check strengthen of the technology towards to the attackers or hackers. In this paper, we have been presenting a comparison statements of different secret image hide methods. To prepare this comparison, we have chosen two popular image hide methods of steganography and visual cryptography. The steganography is a secret image encode method, which will encode a secret image into non-secret cover image. On other hand, visual cryptography is an image hide method. In this method, the original secret image is split into different shares. A single share will not be described the original information. However, the original information can be retained when combining all shares together. In this proposed work, both methods are differentiated based on the different parameters of reconstruction quality, execution time, method strength and complexity.

Keywords: Steganography, Visual cryptography, Secret image, Cover image, Secret Shares.

I. INTRODUCTION

The real meaning of steganography is "a practice of concealing messages/information (image, video, audio, etc.,) within other non-secret massage/information" and it was invented in 1499. Example, a hidden message is an invisible after the encode process, however, may not find any big differences between original and encoded non-secret images in human eye perception. Mostly, this technique is using to send a secret message via non-secret message in defense and telemedicine. This technology can be classified into two different types of encode and decode processes. In encode process, the original secret information and non-secret information are encoding to get a stegano information. The stegano information is an encoded information. This stegano information is sent to the receiver or authenticated person for decoding process. In receiver side, the stegano information is decoding for reconstructing the original secret information and non-secret information. In this decode process, the exact replica of the non-secret image may not be reconstructed but it may reconstruct the exact replica of the secret image.

Tomáš Denemark Denemark et al., [1] have proposed a steganography method in 2016. They used feature sets as a starting point in their paper and extend their design to incorporate the knowledge of the selection channel. This was achieved by accumulating in the histograms a quantity that bounded the expected absolute distortion of the residual. The proposed features could be efficiently computed and provided a substantial detection gain across all the tested algorithms especially for small payloads. Alexandre Santos Brandao and David Calhau Jorge [2] had pro-posed a technique to transmit information efficiently and securely to hide confidential data on apparently innocent messages using a steganography method. The insertion technique was used in the least significant bit (LSB) to insert an image into a digital picture. Artificial Neural Networks were used in the process of reconstruction of encrypted information acting as keys that determine the existence of hidden information [2].

Józef Lubacz, et al., [3] had discussed about basic principles of network steganography, which was a comparatively new research subject in information hiding, followed by a concise overview and classification of network steganography methods and techniques. Keren Wang, et al., [4] had proposed a method for detection of motion vector-based video steganography. The modification on the least significant bit of the motion vector was modeled. The influence of the embedded operation on the sum of absolute difference (SAD) was illustrated. Experiments were carried out on videos corrupted by various steganography methods and encoded by various motion estimation methods, in various bit rates, and in various video codecs. Performance results were also demonstrated and its more favorable for real-world applications.

Another foremost image hiding cryptography method is called Visual Cryptography (VC). The main difference between VC and steganography is that, the steganography is hiding a secret image into non-secret image, however, after encoded process a hidden image will not be visible. In visual cryptography, the original secret image is spit into different shares. While seeing the spilt shares, secret information could not able to predicted. Although, when merging all shares together a secret information may be predicted. Nazanin Askari [8] had presented a new method for processing halftone images that improves the quality of recovered secret images in a VC scheme. The proposed approach had mitigated the two traditional problems in VC of pixel expansion and loss of contrast. Based on this processing stage, this paper had proposed and demonstrated the results of two applications of VC on halftone images, one application in multiple VC, and the second in extended VC. Both applications function were without pixel expansion, with enhanced visual quality of the recovered secret image.

Manimrugan, et al., [5] had proposed a secure medical image Lossless Compression (LC) schemes. In this proposed method, the original input grayscale medical images were encrypted by Tailored Visual Cryptography Encryption Process (TVCE). To generate those encrypted images, four types of processes were adopted which played a vital role. They were claimed that, the proposed technique could be implemented in the field for storing and transmitting medical images in a secure manner. The Confidentiality, Integrity and Availability (CIA property) of a medical image had also been proved by the experimental results [5-7].

From the above words both methods (visual cryptography and steganography) are doing a crucial role in terms of image hiding. However, in this paper, we have presented positive and negative points of both methods. In section II is discusses about steganography and visual cryptography is discussed in section III. Both methods are compared in section IV. Finally, the work is concluded in section V.

II. STEGANOGRAPHY

The steganography is a cryptographic method where a secret image can be hide into inside of the other non-secret image. This method can be classified into two different processes.

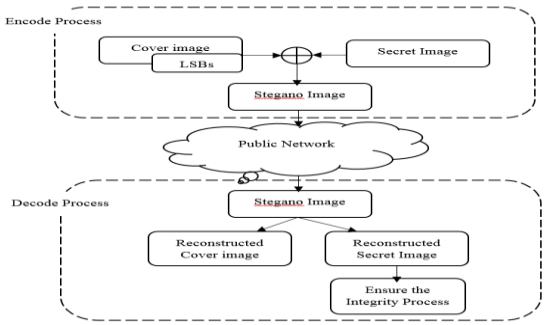


Fig. 1. Overview of the steganography method

One is encode process, in this process, a secret image and non-secret images are together converted as a stegano image (encode image). Another process is decoding process, in this process, a stegano image is decoded for retrieving the secret and non-secret images in figure-1. To encode and decode there are different steps are doing vital roles. Those steps are as follows,

a. Encode process in sender side

1. Get a secret image.
2. Get a cover image.
3. Find the least significant bits in each pixel of cover image.
4. Replace the secret image bits into cover image least significant bits.
5. Prepare the header information.
6. Send the encoded/stegano image to receiver.

b. Decode process in receiver side

1. Get an encoded/stegano image from the sender.
2. Focus on every pixel least significant bits.
3. Reconstruct the secret image from the significant bits of encoded image.
4. Check the integrity constrains to ensure the secret image.
5. If secret image is not an exact replica of the original, then send a request to the sender for resend encoded image.
6. Reconstruct the cover image.

In equation 1, $\sum_{i=0,j=0}^{m,n} A_{i,j}$ is a secret image and $\sum_{i=0,j=0}^{m,n} C_{i,j}$ is a cover image. It means, the original secret image and cover image are encoded. After the encode process, the output of the image is called stegano image $\sum_{i=0,j=0}^{m,n} D_{i,j}$. The equation 2 and 3 are described about, how the secret image bits are encodeed into cover image least significant bits during the encode process.

$$\sum_{i=0,j=0}^{m,n} A_{i,j} \bowtie \sum_{i=0,j=0}^{m,n} C_{i,j} = \sum_{i=0,j=0}^{m,n} D_{i,j} \quad (1)$$

$$\sum_{i=0,j=0}^{m,n} D_{i,j} = \uplus lsp \left\| \sum_{i=0,j=0}^{m,n} C_{i,j}^{1} \oplus \sum_{i=0,j=0}^{m,n} A_{i,j}^{16} \right\| \bowtie \uplus lsp \left\| \sum_{i=0,j=0}^{m,n} C_{i,j}^{2} \oplus \sum_{i=0,j=0}^{m,n} A_{i,j}^{3} \right\| \ldots \bowtie \uplus lsp \left\| \sum_{i=0,j=0}^{m,n} C_{i,j}^{16} \oplus \sum_{i=0,j=0}^{m,n} A_{i,j}^{1} \right\| \quad (2)$$

$$\sum_{i=0,j=0}^{m,n} D_{i,j} = \uplus lsp \left\| \sum_{i=0,j=0}^{m,n} C_{i,j} \oplus \sum_{i=0,j=0}^{m,n} A_{i,j} \right\| \quad (3)$$

The encoded image and given cover image differences will be calculated after the encode process. An important limitation is that, the exact replica of the cover image will not retain from the decode process. Once the reconstruction process is over, the reconstructed secret image is to be tested for assuring the original one or not [12-14]. The main advantage of this method is that, third parties/ intruder can't able to think or identify what is inside of the cover image. Because, there is no differences between cover image and encoded images in human view perception [15-17].

III. VISUAL CRYPTOGRAPHY

This section discusses the foremost cryptography is visual cryptography. The main aim of this crypto system is that, the original secret image is split into unpredictable shares. These shares are may sent to the receiver for reconstruction process. During the reconstruction process every share must be presented. In case during reconstruction process even one share is not presented, the original secret image can't able to retain.

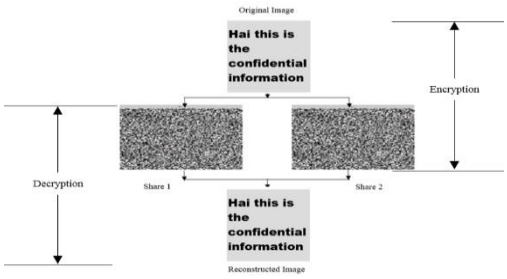
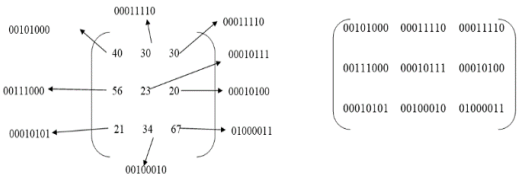


Fig. 2. Flow diagram of visual cryptography

The visual cryptography can be classified into two different processes of encryption and decryption. An encryption, the original image is converted into n number of the shares. These shares are may transfer via network to receiver [8]. In decryption process, to reconstruct the original secret image every share must be presented. Even one share is not presented, we can't able to retrieve the original secret information. This is

the main difference between steganography and visual cryptography.

Fig. 3. 8-bit Binary conversion



There are different steps are involved in encryption and decryption. Those steps are as follows,

a. Encryption process

1. Get the original secret image.
2. Define the reference matrix as given in the figure 4.
3. Convert given secret image pixel into corresponding 8-bit binary.
4. Based on the reference matric of 1 and 0, the corresponding value is substituted in the other share matrixes
5. The output of this process is secret shares and it may send to the receiver

b. Decryption process

1. Get all secret shares from the sender.
2. Use inverse matrix of 1 and 0 for reconstruction process.
3. Take different shares bits and match with reference matrix for retain the original secret information
4. The reconstructed information may apply to the integrity test
5. If the original secret information is not ensure during the integrity test then send the request to the sender to resend the shares.

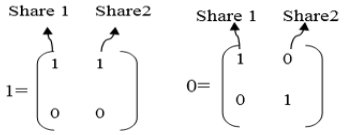


Fig. 4. Reference matrix of 1 and 0 bits for substitution

Many authors have invented the visual cryptography for the different applications. In which Manimurugan et al., [5] have proposed different visual cryptography schemes for different applications. The positive points of their work were that the reconstructed image quality is good.

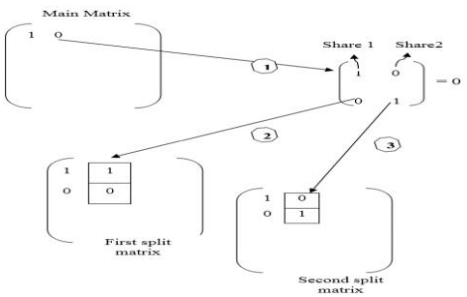


Fig. 5. Secret shares creation process

They have used the same method for medical images. The main objective of their work was that, original medical image was encrypted by tailored visual cryptography and the same encrypted image was compressed by their own proposed lossless compression algorithm [5-7].

$$\sum S^2_{(i,j)} \Longrightarrow Con_{(8bit)}\left[\sum S^2_{(i,j)}\right] \Longrightarrow \sum Bin_{(i,j)} \quad (4)$$

$$\sum Bin_{(i,j)} \oplus \prod_{i,j=0}^{m,n} R_{(i,j)} = \sum Sh^1_{(i,j)} + \sum Sh^2_{(i,j)} \quad (5)$$

The equation 4 and 5 are described about how the original information is converted into corresponding binary values and the same binary image and reference matrices are combined for generating the secret shares of $\sum Sh^2_{(i,j)}$ and $\sum Sh^1_{(i,j)}$. In addition, the figure 5 is illustrated about the share creation process. In this process, the first step is indicating that, from the main matrix a first bit is identified and based on the identified bit the corresponding reference matrix will be chosen. In second step, from the chosen reference matrix, the first column value is placed in first share and second column values of reference matrix are placed in another matrix in third step [9, 10].

TABLE 1: COMPARISON OF STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Image	Steganography			Visual Cryptography		
	Execution time (Sec)		PSNR(dB)	Execution Time (Sec)		PSNR(dB)
	Encode	Decode		Encode	Decode	
1	4.34	3.25	47.36	4.39	3.25	46.33
2	5.324	4.58	48.25	5.56	6.49	45.23
3	4.59	4.36	49.25	5.25	6.11	44.76
4	5.48	4.39	48.59	6.04	5.59	45.16
5	4.48	5.23	49.04	5.05	5.24	44.74
6	4.57	5.12	50.26	5.42	4.57	45.07

IV. COMPARISON AND DISCUSSIONS

In this section, visual cryptography and steganography methods have been compared. For this comparison, we have taken lot of grayscale images. However, in this presentation, we have been enclosing the six grayscale medical images for both methods. Those images are illustrated in figure 6.

In steganography, the CAG image is considering as a cover image. Inside of this image a secret information has been hidden in figure 7. During this encode process, the given cover and secret images are converted into binary. In addition, the cover image least significant bits are replaced by a secret image bits. In figure 8 has been illustrated that, a secret image is CAG in VC.

Fig. 6. The grayscale medical images

This image is segregated into n numbers of shares in an encryption process. In this process, the given secret image is converted as binary and the same binary image is segregated into different shares by reference matrices [11].

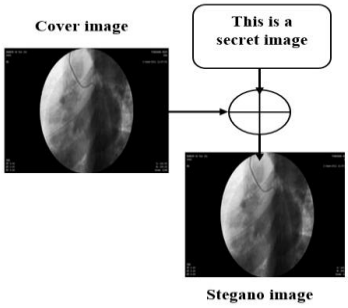


Fig. 7. The encoding process of steganography

TABLE 2: COMPARISON-II OF STEGANO & VISUAL CRYPTOGRAPHY

	Steganography	Visual Cryptography
Strength	4	5
Complexity	3	4
Reconstruction quality	4	3
Pixel expansion	x	4

The table 1 is illustrated about encode, decode and Peak signal to noise ratio (PSNR) performances of both methods. In result, the visual cryptography encryption process time is greater than steganography encodes process time.

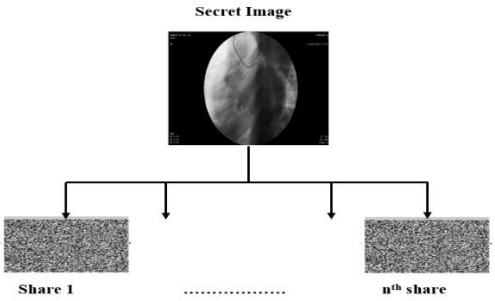


Fig. 8. The encryption process of visual cryptography

This differences are happened due to the pixel substitution in Visual cryptography. Same differences in decode process also. While comparing based on the PSNR, steganography is providing the better result than Visual Cryptography in figure 9.

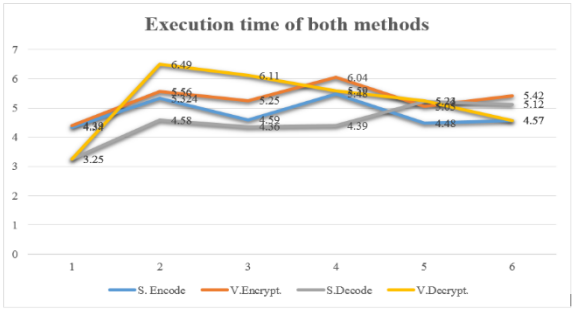


Fig. 9. Execution time comparison

This occurred due the pixel expansion process. In order to improve the quality of the reconstructed image post/pre-processes are doing a vital role in Visual Cryptography (VC).

In table 2 is illustrated that, other parameters of strength, complexity, reconstruction image quality and pixel expansion. We have rated the numbers from 0 to 5. 0 is minimum and 5 is maximum. In this connection, the VC is providing the maximum strength than the steganography. The reason is behind that, when the pixel is expanded, the algorithm strength and complexity will be increased rapidly. In steganography, the least significant pixel only doing an important role to substitute the secret bits. When compared with algorithm complexity both methods are providing the good complexity. However, comparing both, VC is providing higher result than steganography.

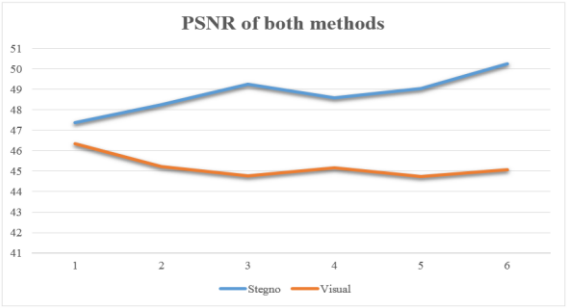


Fig.10. PSNR comparison

About reconstructed image quality steganography is provided the higher result than VC. The reason is, when pixels has expended then it's very hard to retain the original quality of the image.

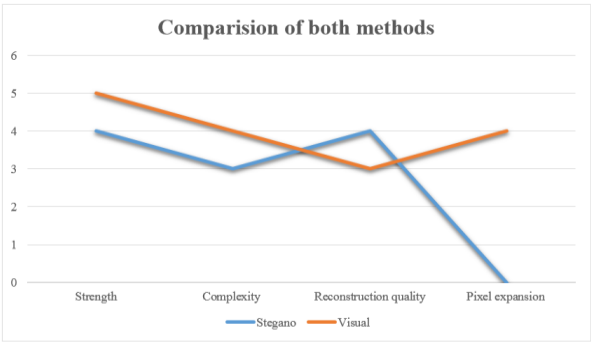


Fig.11. Based on other performances comparison

Very hard to hack the both methods encoded secret images by the intruder or third parties. Finally, in order to pixel expansion the VC is providing the better security than the steganography.

V. CONCLUSION

In this paper, we have presented steganography and visual cryptography performances. In result, every method is providing a fabulous performance in terms of algorithm strength, complexity, reconstruction quality and security. Due to the pixel expansion and reference matrix substitutions the visual cryptography has providing better results. However, the reconstruction of the

image quality is not up to the mark. To improve the reconstruction image quality, it needs pre-or post-process. On other hand steganography also providing good results. When compared with VC its performances are less. Although the reconstruction image quality is higher than the VC.

VI. ACKNOWLEDGMENT

The author would like to thank Tabuk University, Saudi Arabia, all references authors, anonymous reviewers and editors for their valuable supports.

VII. REFERENCES

[1]. Tomáš Denemark Denemark, Mehdi Boroumand and Jessica Fridrich, Steganalysis Features for Content-Adaptive JPEG Steganography. IEEE Transactions on Information Forensics and Security 11(8): 1736 – 1746 (2016).

[2]. Alexandre Santos Brandao and David Calhau Jorge, Artificial Neural Networks Applied to Image Steganography. IEEE Latin America Transactions 14(3): 1361 – 1366 (2016).

[3]. Józef Lubacz, Wojciech Mazurczyk and Krzysztof Szczypiorski, Principles and overview of network steganography. IEEE Communications Magazine 52 (5): 225-229 (2014).

[4]. Keren Wang, Hong Zhao and Hongxia Wang, Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value. IEEE Transactions on Information Forensics and Security 9(5): 741-751 (2014).

[5]. S. Manimurugan and C. Narmatha, Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions. International Journal of Digital Crime and Forensics 7 (1): 26-50 (2015).

[6]. S. Manimurugan, K. Porkumaran and C. Narmatha, The New Block Pixel Sort Algorithm for TVC Encrypted Medical Image. Imaging Science Journal 62(8): 403-414 (2014).

[7]. S. Manimurugan, C. Narmatha and K. Porkumaran, The New Approach Of Visual Cryptography Scheme For Protecting The Grayscale Medical Images. Journal of Theoretical and Applied Information Technology 69 (3): 552-561 (2014).

[8]. Nazanin Askari, Howard M. Heys and Cecilia R. Moloney, Novel Visual Cryptography Schemes Without Pixel Expansion for Halftone Images. Canadian Journal of Electrical and Computer Engineering 37(3): 168 – 177 (2014).

[9]. Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang, Visual Cryptography for General Access Structure Using Pixel-Block Aware Encoding. Journal of Computers 3: 68-75 (2008).

[10]. Yang, C. N., New Visual Secret Sharing Schemes Using Probabilistic Method. Pattern Recognition Letters 25: 481-494 (2004).

[11]. Karakis, R., Guler, I., Capraz, I. and Bilir, E., A Novel Fuzzy Logic-Based Image Steganography Method to Ensure Medical Data Security. Computers in Biology and Medicine 67(1): 172-183 (2015).

[12]. Al Dmour, H. and Al Ani, A., A Steganography Embedding Method Based on Edge Identification and XOR Coding. Expert Systems with Applications 46: 293-306 (2016).

[13]. Tang, M., Zeng, S., Xiaoliang Chen Jie Hu and Du, Y., An Adaptive Image Steganography using AMBTC Compression and Interpolation Technique. Optik International Journal for Light and Electron Optics 127(1): 471-477 (2016).

[14]. Yu Chen Hu, Grey-level image hiding scheme based on vector quantisation. IET Journals & Magazines 39 (2): 202 – 203 (2003).

[15]. D.C. Wu and W.H. Tsai, Spatial-domain image hiding using image differencing, IEE Proceedings - Vision, Image and Signal Processing 147(1): 29 – 37 (2000).

[16]. Xinpeng Zhang, Jing Long, Zichi Wang and Hang Cheng, Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography. IEEE Transactions on Circuits and Systems for Video Technology 26(9): 1622 – 1631 (2016).

[17]. Zhenxing Qian and Xinpeng Zhang, Reversible Data Hiding in Encrypted Images with Distributed Source Encoding. IEEE Transactions on Circuits and Systems for Video Technology 26(4): 636 – 646 (2016).