ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 6 No. 1 March 2020*

Review of Spatial Domain Image Steganography Methods of Handling Random Noise

[1]Yusuf Badamasi*, [2]Mohammed Usman
[1,2]Department of Computer Science,
School of Physical Sciences
Modibbo Adama University of Technology, Yola
Email: ybi4it@gmail.com

Abstract
Steganography is a science of hiding secret information in a carrier. The carrier may be a text file, digital image, audio file or video file. Steganography is used as better alternative for file security than cryptography which only scrambles the content of message. Digital image steganography is widely used than other forms of steganography because of ease of implementation. In most cases, change occurs in the appearance of the career image because anytime a message is hidden in a cover file, random noises are also added in that file due to bit tempering in the replacement process. The secret message bits drastically modify the original bits of the career and hence, make changes to its statistical properties. These change causes distortion to the message containing career and this draws attention of unauthorized person to notice that confidential message was hidden there. This research assessed five (5) methods proposed to address this problem. Three metrics – the image quality, message capacity and achieved Peak Signal to Noise Ratio (PSNR) were employed to evaluate each method. Finally, the results are presented and summarized and the research gap in each method is also identified that serves as basis for future research.

Keywords: Steganography, Cover-Image, Stego-Image, LSB, PSNR, RGB, Message

INTRODUCTION
Information security is one of the major concerns in this era of Information and Communication Technology (Sahoo & Tiwari, 2018). The world now depends more and more on computer systems directly or indirectly for living (Laskar & Hemachandran, 2019). Steganography is the science of hiding a message signal in a host signal. By using steganography, information can be hidden in carriers such as images, audio files, text files and videos (Kaur, Inderjeet and Duhan, 2017). The cover message is the carrier of the message such as image, video, audio, text, or some other digital media. Least Bit Replacement (LBR) is one of the common techniques and implementation of its algorithm seems to be the easiest (Provos & Honeyman, 2013).

The most common threats in a networked system are unauthorized access to data and computer resources. This may cause the loss of confidentiality, integrity, and availability of the information technology assets (Ali & Saad, 2019). Steganography is a technique designed to prevent unauthorised access to data by wrapping them in a carrier as a camouflage and sent over a network to authorized party (Laskar & Hemachandran, 2019).

Steganography method can be implemented with text document, digital image, audio file or video file as cover (Thiyagarajan *et al*, 2013). Steganography approach is also classified into

*Author for Correspondence

two domains – the spatial domain and transformation domain (Mortazavian *et al*, 2016). The spatial domain steganography involves replacement of bits between the confidential message and the carrier where as the transformation domain involves modifying the frequency coefficient of the carrier to create space to hide message (Juneja & Sandhu, 2013). This research is a review of steganography methods of spatial domain, implemented with 24-bit bitmap image. The problem of steganography system is random noise added to stego-image whenever secret message is added making the carrier looks distorted because both the physical and statistical properties of the career changed thereby drawing unauthorized person's attention. Various researches have been conducted to address this issue and this paper reviews some of them.

Figure 1 – A noisy stego-image (Emam, 2016)

The aim of this research is to assess the efficiency of some image steganography methods that are designed to address the problem of random noise. The objectives include:

i. Examine the difference in clarity between the original image and the stego-image of a method using Human Visual System (HVS)
ii. Examine the capacity of each method in message hiding by determining the maximum message size (in bytes) a method can hide
iii. Examine the Peak Signal to Noise Ratio (PSNR) achieved by a method
iv. Draw summary of findings to identify the research gap

SPATIAL DOMAIN IMAGE STEGANOGRAPHY METHODS OF HANDLING RANDOM NOISE

Conventional Least Significant Bit (LSB) replacement method of steganography proposed by Champakamala, Padmini and Radhika (2009) is a common and simple approach to embed information in an image file. The method used 640 X 525 sized RGB image as cover to replace the Least Significant Bits (LSBs) of the cover image (C) with the bits of secret message (M) aimed at reducing noise in the stego-image. Every pixel in 24-bit bitmap image consists of Red, Green and Blue (RGB) colour components and each colour component consists of eight (8) bits. This method simply replaces the last bit of each colour component of pixel with a bit of message until a message is fully embedded. It is easiest to implement but it is characterized by Low PSNR of 19.9987 dB and low quality image that draw intruder's attention to easily sense a secret message is hidden in the stego image. The method also accommodates only 15 bytes or less of message.

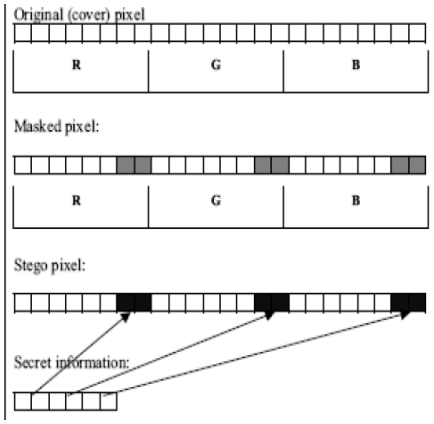


Figure 2 – LSB implementation (Champakamala *et al.*, 2009)

Figure 3 – Original image and stego-image (Champakamala *et al.*, 2009)

Emam *et al* (2016) proposed a random pixel replacement method to hide bits of the secret message. This method pays attention to hiding a message only in blue and green components of the cover image pixels, neglecting red colour component. The hiding is done in 2-1-2 loop fashion where first two bits of the secret message are first hidden in blue colour component and third bit is hidden in green colour component. In the next stage, the next two bits of the secret message will be hidden in the green component and one bit in the blue component. The loop continues in this fashion until every bit of the secret message is hidden in the image. This method achieved high PSNR of 40.434 dB however; the appearance of the stego-image after embedding considerably changes. The method also has good message hiding capacity as it can wrap up to 50 bytes of message length.

Pixel no. in sequence manner	Pixels before embedding				Pixels after embedding	
	Blue pixel	Green pixel	Blue pixel bits	Green pixel bits	Blue pixel bits	Green pixel bits
1	131	137	10000011	10001001	10000001	10001001
2	120	135	01111000	10000111	01111001	10000111
3	106	132	01101010	10000100	01101001	10000101
4	113	131	01110001	10000011	01110000	10000011
5	109	129	01101101	10000001	01101100	10000001
6	111	131	01101111	10000011	01101101	10000010
7	103	127	01100111	01111111	01100100	01111111
8	112	133	01110000	10000101	01110000	10000101
9	108	122	01101100	10000100	01101101	10000101

Figure 4 – Exploiting blue and green component (Emam *et al.*, 2016)

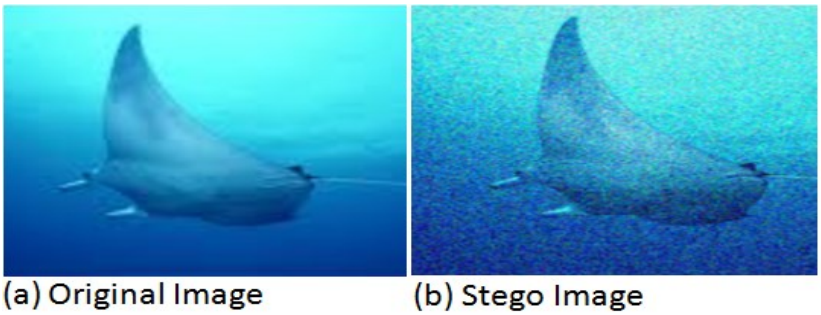


Figure 5 – Original and Stego image (Emam *et al.*, 2016)

Korothan *et al* (2016) proposed a technique that involves hiding secret in a 512 X 484 R G B image. In this technique, embedding is done through replacing the noisy bit of the image with bits of the secret message. From Human Visual System angle, the stego image looks a bit distorted thereby drawing intruder's attention. The PSNR value achieved by this method is 41.131 dB and the method capacity depends on the amount of noisy bits found in the cover to be replaced with message.

Figure 6 – Original and Stego image Korothan *et al* (2016)

Ali and Saad (2019) proposed Secret Message Matching (SMM) method if the embedded bit does not match the LSB of the cover image, then the pixel value of the corresponding pixel is randomly added by ±1. The original image and the stego image looks identical to the Human Visual System and this help reduce suspicion of secret communication. The method achieved 40.1132 dB PSNR but designed to hide only 20 bytes long message.

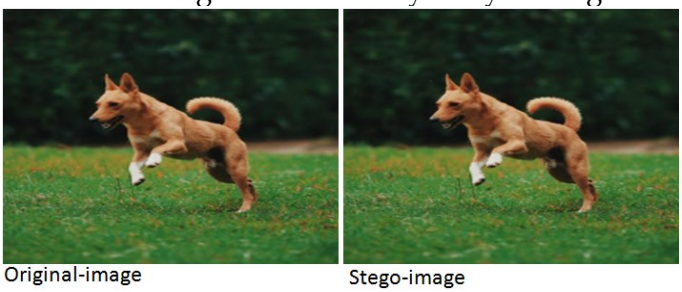


Figure 7 – Original and Stego image

Abdul-Sada (2017) came up with a method that is based on LSB-3 (Third Least Significant Bit) of the cover image by modifying the first and second Least Significant Bit (LSB -1,2) according to the bits of the message. The researcher tried to fill gap he found in two researches. The research exploits the third Least Significant Bit instead of first or second Least Significant Bit and it has achieved great capacity of hiding up to 45 bytes of message and 30.087 dB of PSNR. The original and stego looks a bit different as noise is slightly noticeable to the human eye.

(a) Original Image (b) Stego-Image

Figure 7 – Original and Stego image

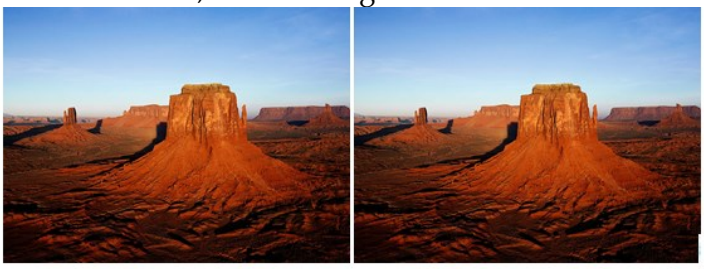
METHODOLOGY

To assess the strengths and weaknesses of the reviewed research articles, this research considers the following metric: Image Quality, Message Capacity, Peak Signal to Noise Ratio (PSNR)

Image Quality

This is assessed using Human Visual System (HVS). Human Visual System encompasses any organ that gives human being the ability to soundly compare and contrast between objects of varying appearance. An image normally changes in look when data are hidden in it. The more differences revealed between the original image and the stego-image, the less secure is the steganography method.

The image before message was hidden and the image after message was hidden will be placed in adjacent in order to notice any difference in the appearance by mere looking. HVS helps in differentiating between the two images. Figure shows two images – one before message was hidden and the other, after message was hidden.



Before message After message

Figure 8 – Original and Stego image

Message Capacity

In steganography, a method that can handle larger message is considered more efficient. This research will determine the maximum length of message a method can handle. A steganography method that can only handle 15 bytes or less of message is considered to be low capacity, 20-30 bytes average capacity and 40 bytes and above are considered high capacity (Provos & Honeyman, 2013).

Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio is an equation that works as metric used in assessing the strength of any steganography method, hence, the higher the PSNR value, the stronger a steganography method. PSNR which is measured in decibel (dB) is a unit of sound used to reveal the degree of difference between the statistical properties of the original image and that of stego-image. High PSNR of stego-image means low chance for an unauthorized person to notice that a confidential message is hidden in the image. According to Alam

(2016), a PSNR in any steganography method is considered low when it is less than 20 dB, average when it is between 30 – 40 dB and high when it is above 40 dB.

$$PSNR = 20 \log(max_i) - 10 \log(MSE)$$

$$MSE = \left(\frac{1}{n}\right)\sum_{i=1}^{n}\left(X_i - X_i'\right)^2$$

Where n is size of image and X_i, X'_i are the value of the pixel in the cover and stego image, respectively.

RESULTS AND DISCUSSION

Based on the result of experimentation of the reviewed methods, it is gathered that the Conventional Least Significant Bit (LSB) replacement proposed by Champakamala, Padmini and Radhika (2009) has lowest PSNR of 19.9987 dB and low quality image. The method also has low capacity to hide message. It can only hide only 15 bytes or less of data.

Random pixel replacement method devised by Emam *et al* (2016) achieved high PSNR of 40.434 dB but poor quality stego-image and has good message hiding capacity of hiding 50 bytes of message. Korothan *et al* (2016) technique has 41.131 dB PSNR but capacity to hide message is variable depending upon the amount of noisy bits found in the cover image. The image quality is low as distortion in stego image is clear from Human Visual System angle.

In Ali and Saad (2019) method, the original image and the stego image looks identical to the Human Visual System and the method achieved 40.1132 dB PSNR but designed to hide only 20 bytes long message. Abdul-Sada (2017) method achieved great capacity of hiding up to 45 bytes of message and 30.087 dB of PSNR. The stego image in this method looks a little bit distorted. The summarized result analysis of the reviewed methods is shown in Table 1.

Table 1: Summary of Results of Reviewed Literatures

Author	Method	PSNR	Image Quality	Capacity
Champakamala *et al* (2009)	Conventional LSB	Low	Low	Low
Korothan *et al* (2016)	Noisy bit substitution	High	medium	Variable
Emam *et al* (2016)	Random substitution	High	Low	High
Ali and Saad (2019)	Matching method	High	High	High
Abdul-Sada (2017)	LSB -3 replacement	Medium	Medium	Low

Future research will address the gap identified in the above researches by proposing a new spatial domain method of steganography that will modify Least Bit Replacement method. The method is expected to achieve higher PSNR, higher image quality and higher data hiding capacity than those achieved by the reviewed methods.

CONCLUSION

Several researches using different methods by various authors have been reviewed. Each of these researches tried to address the problem of random noise in the stego image. Based on the Image quality, message capacity and PSNR, the experimental result of each of the five reviewed techniques indicates the varying degree of PSNR level but none of them achieved a maximum quality and too much complexity against Human Visual System (HVS).

In the future research, a new steganography method should be introduced to fill the above identified gaps found in these previous studies. The future research will aim at addressing the problem of random noise in simple and efficient way and achieving higher PSNR values.

REFERENCES

Abdul-Sada,A. I.(2017). Hiding Data Using LSB-3.*J.Basrah Researches (Sciences)*, *33*(4), 81-88

Alam, I.F. (2016). An investigation into encrypted message hiding through images using SB.*International Journal of EST*, *6*(33), 34.40.

Ali, A.A., &, Saad, A.S. (2019).New image steganography method by matching secret Message with pixels of cover image (SMM). *International Journal of Computer Science Engineering and Information Technology Research, 3*(2), 1-10.

Champakamala, B.S, Padmini, K., & Radhika, D. K. (2009). Least Significant Bit algorithm for image steganography. *International Journal of Advanced Computer Technology*, *3*(4), 34-38.

Emam, M.M., Ali, A.A., & Omara, F.A. (2016). An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. *International Journal of Advanced Computer Science and Applications, 7*(3), 361-366.

Juneja, M., & Sandhu, P.S. (2013). A New Approach for Information security using an Improved Steganography Technique. *Journal of Info.Pro.Systems, 9*(3), 405-424.

Kaur, J., Inderjeet, A., & Duhan, M. (2017). A comparative analysis of steganographictechniques. *International Journal of Information Tech. and Knowledge Management*, *2*, (1), 191-194.

Korothan, J., Kishor, S. & Butey, P. (2016). De-Noise Steganography by Enhancing the Cover Image: A Multi-Level Security Approach. *The International Arab Journal of Information Technology, 13(6),* 851-857.

Laskar, S.A., & Hemachandran, K. (2019). Steganography based on random pixel selection for efficient data hiding.*International Journal of Computer Engineering and Technology, 4*(2), 31-44.

Mortazavian, P., Jahangiri, M., & Fatemizadeh, E. (2016). Low degradation steganography model for data hiding in medical image. *International Journal of Computer Science and Information Technology, 4*(2), 234-240.

Provos, N., & Honeyman, P. (2013). Hide and seek: An introduction to steganography. Retrieved from http://niels.xtdnet.nl/papers/practical.pdf

Sahoo, G., & Tiwari, R.K. (2018). Hiding secret information in movie clip: A steganographic approach. *International Journal of Computing and Applications*, *4*(1), 103-110.

Thiyagarajan, P., Natarajan, V., Aghila, G., Venkatesan, V.P., & Anitha, R. (2013). Pattern based 3D image steganography. Seoul, South Korea: 3D Research center.