Performance Analysis of Stegano Data with Improved LSB Substitution using Horse Step Algorithm and Advanced Encryption Standard

Rhishav Poudyal[1], Subarna Shakya[2]
Institute of Engineering,
Tribhuvan University
Lalitpur, Nepal
Email: rhishav.poudyal@gmail.com[1], drss@ioe.edu.np[2]

***Abstract*— The two popular methods of transmitting secret information in very secured way are Cryptography and Steganography. Cryptography scrambles information so it can't be comprehended while the Steganography shrouds the message so that it can't be visible. In this method, first a message is encrypted using an algorithm based on AES cryptographic algorithm or Horse step algorithm which is then embed inside an image using method of Least Significant Bit (LSB) substitution. Digital pictures usually have an oversized quantity of redundant information, thus it's attainable to cover message within image file. Image steganography deals with exploiting restricted power of the human vision where message is hidden within LSB of the image data. This embedding technique relies on the very fact that the LSB bit in an image will be thought of as random noise, and consequently they turn out to be less receptive to any change on the image. Cryptography and Steganography combinedly can enhance the protection of the info embedded. This combinable methodology can satisfy the wants like capability, security and hardiness for secure knowledge transmission over an open channel.**

Keywords—Plain text, Structural Similarity (SSIM), mean square error (MSE), cipher text, peak signal to noise ratio (PSNR), encryption, decryption key, cover image, stego image, Structural Similarity (SSIM)

I. INTRODUCTION

From the dawn of civilization to the highly networked societies, information exchange has always been an important part of our lives. In the current digital era, the fast escalations in digital multimedia system and network have sealed ways that for individuals around to accumulate, utilize and share multimedia system info. Radio communication, telephone communication, mobile communication etc. are the ways of communication in today's world. With the expansion of network, security of information has become a significant concern and therefore data concealing technique has attracted folks round the globe [1]. Such speedy advances in technology have additionally given rise to security threats to people and organizations. Hence, the data security has evolved as a vital and pressing issue not just for people but for business and governments too. In this research, security of data is preserved with the use of cryptography and steganography.

Cryptography and Steganography are two popular methods of sending secret information in a secured way. One shrouds the presence of the message while other twists the message itself by distortion. These are popular methods that control messages keeping in mind the end goal to figure or shroud their reality separately [1]. Steganography is the art of imparting message in a way which conceals the presence of the correspondence [2].Cryptography scrambles information so it can't be comprehended while the Steganography shrouds the message so that it can't be visible.

Data hiding techniques has been challenging nowadays for digital forensic investigators [1]. To ensure that knowledge is secured and doesn't attend unplanned destination, the conception of knowledge activity came up to guard a chunk of data [3]. The Internet provides a communication technique to distribute data to the lots. Therefore, the confidentiality and knowledge integrity are needed to safeguard against unauthorized access and use [4]. Steganography and cryptography are two distinctive data concealing systems, where the message is changed to make it importance cloud to a malevolent people who catch it. Steganography depends on concealing message in unsuspected mixed media information and is for the most part utilized as a part of mystery correspondence between recognized gatherings [5]. The file formats having higher degree of redundancy are more suitable for steganography [6]. Digital images are widely used as cover objects as they bear huge amount of redundant data where steganography can be used. Cryptography simply obscures the integrity of the data in order that it doesn't be to anyone except the creator and the recipient [7]. Privacy is assured by Cryptography while secrecy can be achieved through Steganography [8]. According to [8] "Steganography and cryptography are both used to ensure data confidentiality". However, steganography differs from cryptography within the sense that cryptography focuses on keeping the contents of a message secret whereas steganography focuses on keeping the existence of a message secret [9]. Thus, cryptography shows

ISBN: 978-1-5386-4119-4/18/$31.00 ©2018 IEEE

communication between parties in secure way while steganography makes secret message invisible to others.

II. LITERATURE REVIEW

Advanced Encryption Standard (AES), also known as Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. It has been adopted by the U.S. government and is now used worldwide. RIJNDAEL is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. This research is based on the cryptography technique designed by Nawayoga, Bambang H, Iwan Iwut where they introduced a novel method of cryptography known as Horse Step Algorithm. This method of cryptography exploits 2D matrix to encrypt message. Flexible key, excellent security, efficient and suitable for steganography are some of the features of this algorithm [2]. Cryptography is not only science but also art for securing message. Cryptography becomes interesting due to flexible key [2]. Zhi and Fen [9] proposed method of LSB image steganography, LSB in which secret message was inserted in selected portion of image not in fixed or predefined manner which makes steganalysis difficult. According to Zhang *et al*. [7] "a new method of LSB steganalysis is based on statistical distribution of pixel difference in spatial domain which can be done on high resolution images based on the difference of zero and non-zero values of pixels and also finds the error which is used to determine the steganographic features." Here, Laplacian distribution is used. Further Li *et al.* [8] proposed a method for uplifting wavelet transform image with LSB Information Hiding algorithm. Results proved to be very good security for attacks done invisibly.

III. METHODOLOGY

An image is considered as common type of digital media for steganography as they bear tremendous amount of unwanted or redundant data. Image steganography deals with exploiting restricted power of the human vision where message is hidden within LSB of the image data. This embedding technique relies on the very fact that the LSB bit in an image will be thought of as random noise, and consequently they turn out to be less receptive to any change on the image.

To improve the limit of image steganography and give an indistinct stego picture to human vision, a system for concealing extensive volumes of information is proposed in images by consolidating cryptography and steganography while causing negligible perceptual corruption and to take care of the issue of unauthorized data access.

To increase security of this data, steganography can be embedded with cryptography.

In this method, first a message is encrypted using an algorithm based on cryptographic algorithm then the encrypted message is embedded inside an image using LSB embedding method as LSB substitution alone is not sufficient. The combinational of method will increase the security.

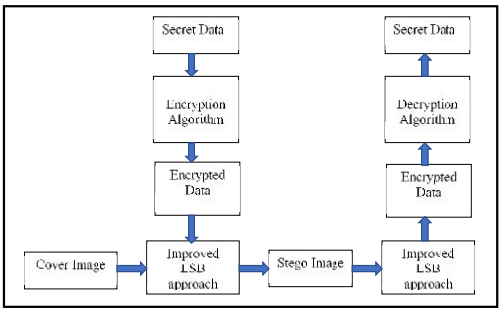

Figure 1: Block diagram of system overview

IV. ALGORITHM

Input: text message, image for data hiding

Output: stego image, message text

1. Read text
2. Encrypt the text into scrambled form using cryptographic algorithm (AES or Horse Step Algorithm)
3. Get the cover image
4. Using the LSB substitution or improved LSB substitution method, embed encrypted message into cover image to obtain stego image
5. Compute MSE, PSNR, SSIM of original and stego image

A. Improved LSB substitution

Only replacement of lower bit with message bit is done in LSB Algorithm but in Improved LSB key known as secret key is inserted to make information secret.

Cover image + secret key + secret information = stego image

Step 1: Take a cover image and divide it into matrices (Red, Green and Blue).

Step 2: Get the secret key and convert it into one dimensional array of bit.

(Secret key and Red matrix plays role only for making decision to allocate the secret information bits either into Green matrix or Blue matrix).

Step 3: Perform XOR operation between each bit of secret key with each LSB of Red matrix. (The resulting XOR value

ISBN: 978-1-5386-4119-4/18/$31.00 ©2018 IEEE

decides whether to hide information on Green matrix or the Blue matrix.)

Step 4: If the XOR value is 1 then replace the LSB of Blue matrix by the first bit of secret information. If the XOR value is 0 then the LSB of Green matrix is replaced by the first bit of secret information and it is continued as until all the bits are hidden.

V. COMPARISION

Digital images often have a large amount of redundant data and for this reason it is possible to hide message inside image file. Image steganography is about exploiting the limited power of the human visual system where information is hidden in the least significant bit of the image data. This embedding method is based on the fact that the least significant bit in an image can be thought of as random noise, and consequently they become less responsive to any change on the image.
Usually, the invisibility of the hidden message is calculated in terms of the Peak Signal-to Noise Ratio (PSNR) [10].

$$PSNR = 10\,log_{10}\frac{255^2}{MSE} \qquad (1)$$

Where mean square error (MSE)

$$MSE = \frac{1}{M*N}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[O(i,j) - O'(i,j)]^2 \qquad (2)$$

Similarity between original message and distorted message can be evaluated using Structural Similarity Index (SSIM) [11] .

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \qquad (3)$$

Where,
μ_x is average of x
μ_y is average of y
σ_x^2 is variance of x
σ_y^2 is variance of y
σ_{xy} is the co-variance of x and y
c_1 and c_2 are the constants

The result also showed the negligible difference in the original image and stego image. The experimental results performed on hiding 4 KB of useful data on 80 KB image size showed that compared with LSB Substitution, Improved LSB substitution has lower MSE and higher PSNR along with higher SSIM. This shows that Improved Least Significant Bit substitution is an improvement over simple Least Significant Bit substitution.

Table 1: Comparative analysis of LSB Substitution and Improved LSB Substitution

Images	LSB substitution			Improved LSB substitution		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM
Image 1	0.017	65.8	0.9991	0.014	66.55	0.9999
Image 2	0.039	62.27	0.9989	0.032	63.13	0.9992
Image 3	0.126	57.12	0.9992	0.087	58.74	0.9998
Image 4	0.003	74.13	0.9993	0.001	76.58	0.9999
Image 5	0.002	74.81	0.9997	0.001	78.05	1
Image 6	0.02	65.16	0.9993	0.015	66.38	0.9998
Image 7	0.004	72.09	0.9992	0.003	73.26	0.9999
Image 8	0.153	56.3	0.9982	0.105	57.93	0.999

VI. RESULTS AND DISCUSSION

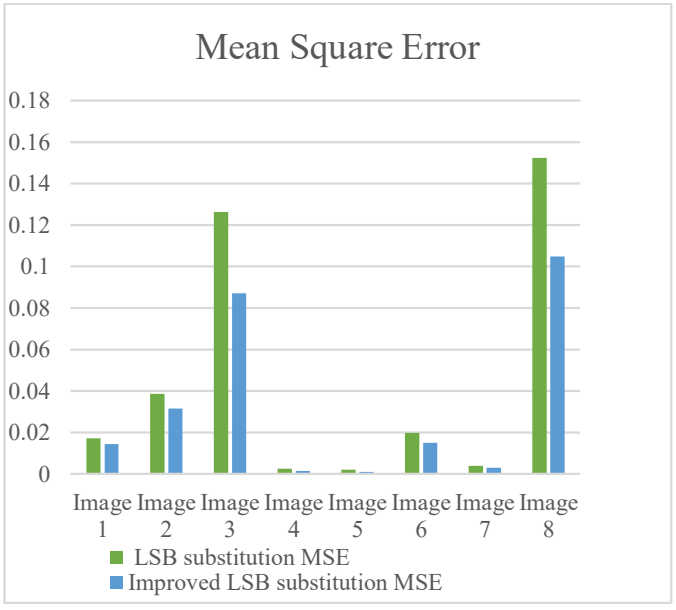

Figure 2: Comparative analysis of Mean Square Error

ISBN: 978-1-5386-4119-4/18/$31.00 ©2018 IEEE

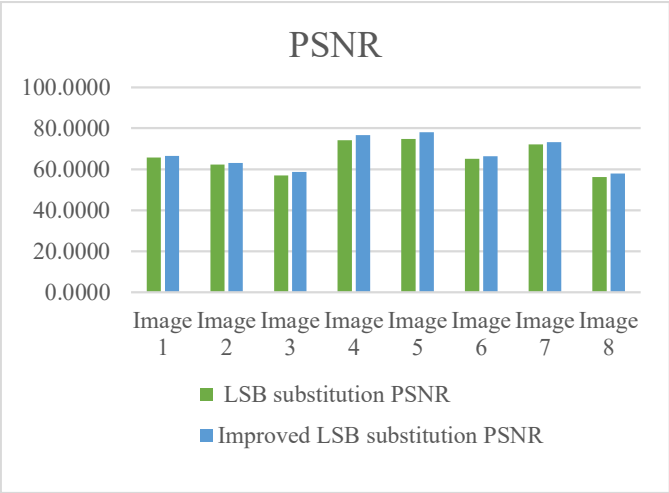

Figure 3: Comparative analysis of Peak Signal to Noise Ratio

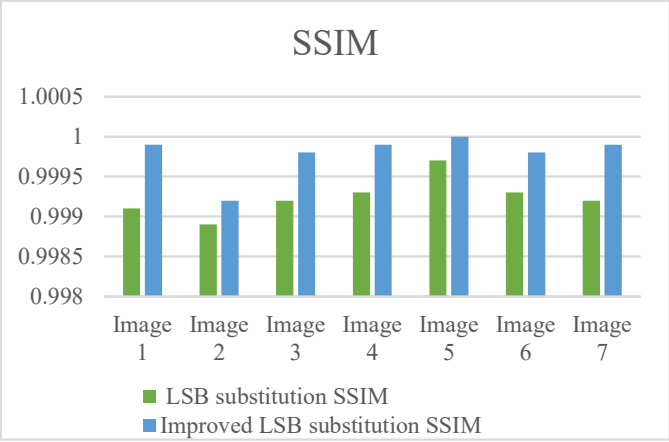

Figure 4: Comparative analysis of Structural Similarity

Figure 2 gives the mean square error of original image along with the message hidden image (stego image) where distortion can be seen more prone to LSB substitution which leads to higher PSNR of the image using improved LSB substitution. Similarly Figure 4 shows that structural similarity of original and stego image which proves that improved LSB substitution has less distortion than the LSB substitution.

VII. CONCLUSION

In this paper an efficient image steganography algorithm has been made more secure with the help of cryptographic algorithms based on AES and HSA cryptographic algorithm. The reason behind choosing AES and HSA is the security as both provides excellent security. AES is the fastest cryptographic algorithm while HSA is the algorithm for variable length key facility. Also, HSA performs great for higher data size. So, among lots of cryptographic algorithms these two are the among the best. The combinational method will increase the security of the data embedded. With the negligible difference in original image and stego image, the embedded information can be transmitted securely. The increase in complexity level in retrieving information further enhances the security of secret data in improved LSB substitution. Compared with LSB Substitution, Improved LSB substitution has lower MSE and higher PSNR along with high SSIM which is shown in Table 1. This shows that Improved Least Significant Bit substitution is an improvement over simple Least Significant Bit substitution. Hence, this combinational methodology provide resistance against various visual and statistical attacks.

Although separately using either cryptography or steganography provides security, combinational method would add multiple security level. HSA algorithm has limitations regarding lower bits of data which can be made faster in future. In this research, cryptographic algorithms are used separately but in future both the algorithm can be implemented together but in a random way. Other methods of cryptography and steganography can be used in future for more data security.

VIII. LIMITATIONS

Data hiding techniques have been used for transmission of secret messages since decades. Ensuring data security is of high concern for users. Since the LSB of image is prone to error, the system can be made more secure by introducing various error recovery techniques. Likewise, for hiding secret information, larger image size is required which can be minimized by replacing other bits at the cost of effective appearance on an image. One of the limitations in symmetric cryptography is the difficulty in transmitting the secret key. Also, the data size plays a great role during data secrecy as higher bits of data needs to be transmitted. So, for this purpose AES operates poorly while HSA is the best option. But HSA too has some limitations as for smaller bits which can be made faster in future. The method can be defined as secured communication providing high level of security.

ACKNOWLEDGMENT

I would like to express my sincere and cordial thanks to distinguished persons who helped in myriad of ways to bring my thesis to this level. I would like to express my profound gratitude and sincere thanks to my supervisor **Prof. Dr. Subarna Shakya** for his continuous supervision, guidance and suggestions throughout the research without whom this paper wouldn't have completed. I would like to extend my sincere thanks for providing me with all the essential co-operation, valuable suggestions for choosing the thesis topic. My heartfelt acknowledgement goes to our respected teachers **Dr. Dibakar Raj Pant, Er. Sitaram Pokharel** and **Er. Hari Prasad Baral** for his guidance and cooperation throughout research.
Finally, I would like to express my sincere thanks to my family and all my friends who always encouraged and supported me.

REFERENCES

[1] W. G. F. J. Xinyi Zhou, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography," IEEE ICIS, 2016.

[2] B. H. I. I. N. Nurwhaju, "Novel Cryptography Using Horse Step Algorithm for More Flexible Key," in *IEEE Asia Pacific Conference on Wireless and Mobile*, 2015.

[3] Rahate, N. D. and Rothe, P. R., "Data Hiding Technique for Security by using Image Steganography," *International Conference on Industrial Automation and Computing (ICIAC),* pp. 33-36, 2014.

[4] Singh, K. M., Singh, L. S., Singh, A. B. and Devi, K. S, "Hiding Secret Message in Edges of the Image," *International Conference on Information and Communication Technology (ICICT),* pp. 238-241, 2007.

[5] Caldwell, J., "Steganography using the technique of orderly changing pixel component," *International Journal of Computer Applications,* vol. 58, no. 6, 2014.

[6] Delahaye, J.P., "Embedded Information, Information Hiding," *Scientific American,* p. 142 46, 1996.

[7] Li, C., Xu, W., Meng, L., Liu, B., Wang, Y. and Wu, L., "Realization of a LSB Information Hiding Algorithm Based on Lifting Wavelet Transform Image," *International Conference on Mechatronic Science, Electric Engineering and Computer,* pp. 1015-1018, 2011.

[8] M. A. Ahmad et al., "Achieving Security for Images by LSB and MD5," *Journal of Advanced Computer Science and Technology Research,* 2012.

[9] T. Morkel and J.H.P. Eloff, "An Overview of Image Steganography," in *Information and Computer Security Architecture (ICSA) Research Group*, 2012.

[10] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio.

[11] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Structural_similarity

ISBN: 978-1-5386-4119-4/18/$31.00 ©2018 IEEE