UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Comparative Study on Image Steganography: Knight Tour and Rivest Cipher Four Algorithms

Tassvini A/P Gunaseharan
School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia
tassvini@gmail.com

Yusliza Yusoff
Applied Industrial Analytics Research Group
School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia
yusliza@utm.my

Submitted: 07/09/2020. Revised edition: 14/10/2020. Accepted: 21/10/2020. Published online: 19/11/2020
DOI: https://doi.org/10.11113/ijic.v10n2.274

***Abstract*—Image steganography is a process of hiding message behind an image file which focuses on protecting the existence of a message secret. There is a security risk in the current image steganography process. Since stego-image will be transferred on unsecured Internet network, attackers will attack and try to decode the message behind the stego-image because of the vulnerable algorithm. Therefore, it is very important to search for a method to make the process of encoding the stego-image more secure. There are many algorithms developed to make the stego-image become more secured. However, the usage of Knight Tour (KT) and Rivest Cipher Four (RC4) algorithms in image steganography are still insufficient although that the algorithms are claimed to be secured and robust. KT algorithm is an easy mathematical technique that can increase the security of hidden information, meanwhile, RC4 is known as a simple algorithm but systematic in cover image programming. In this paper, the performance of KT and RC4 algorithms are observed to measure the security and robustness of JPG image format. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are used to observe the image quality to improve the security factor in the stego-image. From the results, it is found that KT generated better performance compared to RC4.**

***Keywords*—Steganography, Knight Tour, Rivest Cipher Four, security, robustness**

I. INTRODUCTION

In this modern era, data hiding is a principal of increasing security and robustness in digital media. As part of data hiding concept, steganography plays an important role where it has an ability to provide a better security compared to cryptography [1]. Due to high specification of device and Internet speed, people nowadays are not aware on the large amount of sharing images throughout the Internet that may leads to copyright infringement. The are many content copying activities by third party in this digital era resulted to unethical problems.

Steganography is divided mainly into five categories which are; (i) image steganography, (ii) audio steganography, (iii) video steganography, (iv) text steganography and (v) network protocol steganography [2]. In this paper, a comparative study on stego-image using KT Algorithm and RC4 Algorithm are observed. The experimental is conducted on the JPG image format of 24-bit.

There are many steganography techniques being introduced by researchers using different approaches including Discrete Wavelet Transform (DWT), Least Significant Bits (LSB), Discrete Cosine Transform (DCT) and many more [3]. Although there are multiple algorithms to test on security and robustness on image steganography, but still, there is no study that has been done on comparison of KT and RC4 algorithms. KT and RC4 algorithms are to identify which image format has better security and good robustness to produce better image quality.

To examine the results, Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) are chosen as the methods to evaluate the performance of the algorithm in image steganography [4]. MSE is used to analyze image compression quality by calculating the cumulative squared error between the compressed and the original image. Moreover, PSNR represents a measure of the peak error.

II. RELATED WORKS

Steganography in images, can be categorized into two classes which are spatial domain based steganography and the frequency or transform domain based steganography [5]. Fig. 1 shows the methods under steganography based on spatial domain and frequency or transform domain. Spatial domain

technique legitimately controls the pixels of an image. Spatial domain referred to the picture elements of the images which are being controlled to stock the conceal message that is covered up inside the images. Frequency or transform domain images are first transformed to another domain like discrete wavelet transform and any standard embedded techniques are applied to conceal the message. There are basic components in image steganography process, such as capacity, imperceptibility, security, robustness and more. In this paper, security and robustness parameter has been chosen to be evaluated for the stego-image.

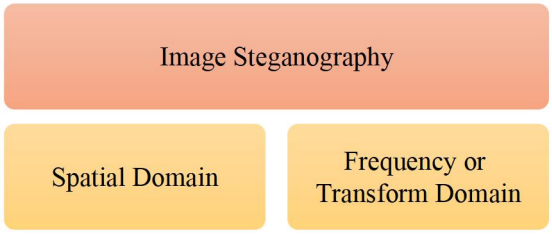


Fig. 1. Image steganography categories

Security is an elements where measure indicates the confirmation of keeping secret messages unreadable for the attackers when it is extracted by attacks. If the secret messages can be seen at the cover image provided or identified in the steganalysis, this convince that the steganography is a failed [6]. Security factor holds a tremendous importance in steganography. Without security, different assaults towards the stego-image will be effectively hacked. Security in steganography implies concealing the secret message procedure should not be known by anybody or raise any doubt from the attackers. The protection measure denotes the guarantee of preserving the name of the game facts unreadable for the adversary when it's far extracted by way of intruders [7].

Robustness factor is to ensure the identity of the message for the receiver despite the fact that stego-file is harmed by any performed incursion within the transmission stage. Besides that, it is also represented as quantity of misinterpretation or distortion that digital cover can able to maintain secret massage safely. Large input data under an estimated scale is known as noise. In image processing the presence of an undisciplined and disastrous perturbation within image also known as noise of a recurrent problem generally known as robustness [8].

There are a lot of enhancement techniques which have been proposed after Least Significant Bit (LSB), for a fine example, LSB replacement. According to Kekre *et al.* (2012) [9]. Most Significant Bit (MSB) of the message image will help us to form a stego-image whereby replacing the LSB of the cover image which would contain the message which means MSB contain most important data of the image compare to LSB. Not limited to LSB, this study compared and observed the betterment of security and robustness of the stego-image.

KT algorithm works just like surface of a chessboard. It divides the image into blocks form and then direct the paths of the knight moving within the image. Finally, the KT will cover the whole image. Meanwhile, RC4 is a stream cipher that provide results in key stream byte at a step. It uses an Initial Permutation Key Stream Generator and Pseudo Random Generator algorithms.

III. Methodology

Fig. 2 shows the overall framework for this study. First step is to find and identify the existing problem by reviewing papers on image steganography.

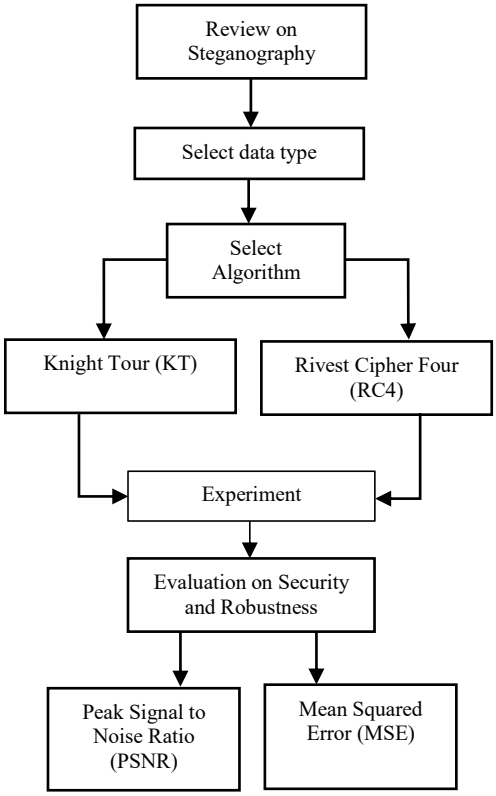
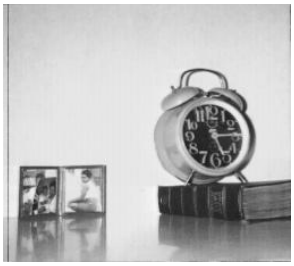


Fig. 2. Overall framework of this study

Then, once the problem is identified, choose the selective data type and suitable algorithm which can be used to ensure the concealment of secret data inside an image without affecting the cover image feature. The experimental is conducted by focusing on two types of algorithms, which are KT and RC4 to assess the performance in the term of security and robustness. Finally, to evaluate and analyze the algorithm performance, PSNR and MSE are used.

A. Data

In this paper, two types of data are used as cover image for the experiment. The pixel size of the image is 256x256. The images are as shown in Fig. 3; Clock.jpg with 24-bit grayscale and Parrot.jpg with 32-bit color mode.



Clock.jpg

Parrot.jpg

Fig. 3. Cover Image

B. Knight Tour (KT)

A pathway or progress of knight depends on each square exactly once around the chessboard in various directions same to the character (L) in KT. Thus, a KT is easy algorithm. Hamilton path also means that path in a graph that visits each vertex exactly once. This technique is applied at the sequence of secret bit stream within the image pixels [7].

This algorithm can be utilized as a technique to embed secret message into the secret image of steganography. Since the search space will be significantly huge even through if we know the starting square of knight's move, by using this technique the high security can be accomplish strong security in steganography.

C. Rivest Cipher Four (RC4)

It is an exclusive algorithm with a byte of key and produce a byte of a cipher text. a byte-oriented stream cipher in with a byte (8-bit) of plain text. Other than that, RC4 is one of the hugely adopted and smooth cipher and according to Jindal (2015) [10, 11], the cipher was developed in 1984 and was anonymously released on news in 1994. RC4 is variable key length stream cipher algorithm.

The advantage of RC4 is systematic in programming. It is simple and rich. RC4 is utilized in bunches of places such as (Secure Socket Layer) SSL, (Wired Equivalent Privacy) WEP and many more. It is the maximum famous stream cipher in life and t is used particularly for random movement.

D. Mean Squared Error (MSE)

In this section, this research discusses about an average prediction of normal squared of the "errors", that is, the distinction in between the estimators what is assessed [12]. The quantity being estimated for the similar units of measurement as the squared of MSE as shown in equation (1). In an acquaintance to standard deviation, taking the square root of MSE allows the root-mean-square error or root-mean-square deviation.

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (1)$$

E. Peak Signal to Noise Ratio (PSNR)

Peak Signal to Noise Ratio (PSNR) as given in equation (2) is used to assess the quality of the image [12, 13]. The higher the PSNR, the better the quality of the compacted, or reassemble the stego-image. It is most easily defined through the mean squared error (MSE).To observe the misinterpretation introduced by the enclosing within the cover image, the Peak Signal to Noise Ratio (PSNR) after enclose was observed for four images. It was found that the quality of PSNR should be high so that it is hardly perceived by human eyes.

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{MSE}\right) \quad (2)$$

Where,

m = width of image
n = height of image
I(i,j) = pixel value of cover image
K (i,j) = pixel value of stego-image

IV. Experimental Results and Analysis

A. Clock.jpg (Grayscale Image)

Table I shows the PSNR reading of KT and RC4 for Clock.jpg cover image. KT algorithm shows a higher reading compared to RC4. Based on the results, KT Algorithm shows a higher reading compared to RC4. As the secret message was embedded, the PSNR value of KT is 89.33 and RC4 is 84.02. Both stego-images are above 40db PSNR and can be considered as good quality image. Resulted that the security and robustness of KT is a bit higher compared to RC4 satisfying that KT is a better algorithm.

TABLE I. PSNR Reading of KT and RC4 for Grayscale Image

PSNR (dB)		
Cover Image Size (256 x 256)	KT	RC4
Clock.jpg	89.33	84.02

Based on Table II, the reading shows zero as the both images has good image quality, as well as has high value of peak signal to noise ratio and also can be concluded that both images are highly distorted images. If the value of mean squared error is zero it is also known as an ideal and most suitable image. It also can be state that if the image depth size is larger and capacity of secret message size is smaller, the stego-image will look similar as cover image and the attacker find difficulties to detect the secret data.

TABLE II. MSE READING OF KT AND RC4 FOR GRAYSCALE IMAGE

MSE (%)		
Cover Image Size (256 x 256)	KT	RC4
Clock.jpg	0	0

B. Parrot.jpg (Colour Image)

Table III shows the results comparison between KT algorithm and RC4 algorithm for 32-bit color JPG image format.

TABLE III. PSNR READING OF KT AND RC4 FOR COLOR IMAGE

PSNR (dB)		
Cover Image Size (256 x 256)	Knight's Tour	RC 4
Parrot.jpg	R = 86. 78	R = 83.31
	G = 84.28	G = 83.77
	B = 85.53	B = 81.41

Based on the results, it can be observed that KT generated better performance for color image format and bit depth. RC4 results are compared to KT algorithm and it is shown that the PSNR value for RC4 is slightly lesser than KT.

TABLE IV. MSE READING OF KT AND RC4 FOR COLOR IMAGE

MSE (%)		
Cover Image Size (256 x 256)	Knight's Tour	RC 4
Parrot.jpg	R = 0	R = 7.12
	G = 0	G = 3.36
	B = 0	B = 9.09

Table IV shows the MSE value reading of KT and RC4 algorithms. Based on table above, value for Knight Tour algorithm and mean squared error for Rivest Cipher is more than 1 which means the algorithm has weakness which the reading of red channel is 7.12, green channel is 3.36 and blue channel is 9.09 when the secret message with 15 byte size is embedded.. KT algorithm has higher peak signal to noise value than RC 4, therefore KT algorithm is considered as better algorithm compared to RC4.

V. CONCLUSION

This is a comparative study on data hiding techniques which based on stego-image quality. This study specifically focused on two different types of algorithms which are KT and RC4. This study measured the image quality with parameter of Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) to obtain better security and good robustness.

From the evaluation results, it is proven that KT has better quality compared to RC4 for image steganography. As a conclusion, Knight Tour is chosen as a better technique for image quality in term of security and robustness.

Overall, KT is a more suitable algorithm to formulate the sequence of the secret bit stream compared to RC4. Besides it is known as a self-developed algorithm, KT is able to determine the path of the knight within the image.

Not limited to KT and RC4, in future, this work can be improvise by examining and evaluating the steganography images with other algorithms which related to security and robustness. Additionally, in term of image quality, the algorithms can be tested on other different types of image format. Besides that, the robustness of the algorithms can be improved by choosing other bits of cover image into consideration. Other factor such as time complexity, capacity, imperceptibility also can be considered to be evaluated by selecting appropriate algorithm or hybrid algorithms to obtain better image processing result.

ACKNOWLEDGMENT

Special appreciation to reviewers for useful advices and comments. The authors greatly acknowledge the UTM Fundamental Research Grant for financial support through grant vot. No. Q.J130000.2551.20H71.

REFERENCES

[1] Kumar, A. and K. Pooja. (2010). Steganography-A Data Hiding Technique. *International Journal of Computer Applications*, 9(7), 19-23.

[2] Bandyopadhyay, S. K., *et al.* (2008). A Tutorial Review on Steganography. *International Conference on Contemporary Computing*.

[3] Bansal, N., *et al.* (2015). Comparative Analysis of LSB, DCT and DWT for Digital Watermarking. *2nd International Conference on Computing for Sustainable Global Development (INDIACom),* IEEE.

[4] Rachmawanto, E. H. and C. A. Sari. (2017). Secure Image Steganography Algorithm based on DCT with OTP Encryption. *Journal of Applied Intelligent System,* 2(1), 1-11.

[5] Kalita, M. and T. Tuithung. (2016). A Comparative Study of Steganography Algorithms of Spatial and Transform Domain. *International Journal of Computer Applications,* 975, 8887.

[6] Denemark, T. D., M. Boroumand, and J. Fridrich. (2016). Steganalysis Features for Content-adaptive JPEG Steganography. *IEEE Transactions on Information Forensics and Security,* 11(8), 1736-1746.

[7] Nie, S.A., *et al.* (2019). The Use of Least Significant Bit (LSB) and Knight Tour Algorithm for Image Steganography of Cover Image. *International Journal of Electrical & Computer Engineering,* 9, 2088-8708.

[8] Isnanto, R. R., R. Septiana, and A. F. Hastawan. (2018). Robustness of Steganography Image Method Using Dynamic Management Position of Least Significant Bit (LSB). *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, IEEE.

[9] Kekre, H., *et al.,* (2012). Comparison between the Basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images. *International Journal of Computer Applications*, 45(1), 33-38.

[10] Kumari, K. L. and K. T. Mattupalli. (2019). Effective Approach to Protect Images by Using Both Cryptography and

Steganography. *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, IEEE.

[11] Jindal, P. and B. Singh. (2015). RC4 Encryption-A Literature Survey*, Procedia Computer Science,* 46, 697-705.

[12] Kini, N. G. and V. G. Kini. (2019). A Secured Steganography Algorithm for Hiding an Image in an Image. *Integrated Intelligent Computing, Communication and Security*, Springer, 539-546.

[13] Goel, S., A. Rana, and M. Kaur. (2013). A Review of Comparison Techniques of Image Steganography. *Global Journal of Computer Science and Technology.*