International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Survey on Steganography with Cryptography

Ankita Khare[1], Bhavana Gupta[2]
[1]Research Scholar, [2]Guide, Oriental College of Technology,

Abstract: **Technology today evolves at a faster pace than it could have been predicted. The benefit of these brisk changes has not diminished the concerns for security of data. This survey comprises of the experimental results of Digital Image steganography with encryption based on Rubik Cube Principle (2016) that validate the supremacy of this methodology compared to other existing ones in terms of imperceptibility, toughness and with reasonable embed capacity. It is also found to be more resistant to steganalysis.**

Keywords: **Cryptography, Steganography, Encryption, Decryption,**

I. INTRODUCTION

Steganography equation is as shown in Figure1.

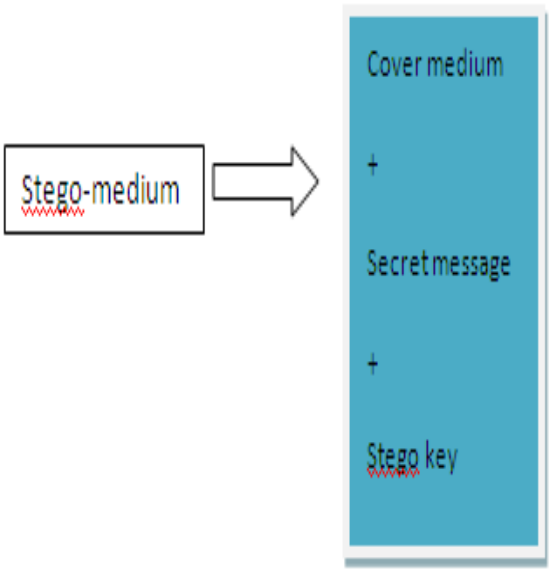

Figure 1: Steganography System

Steganography equation today everybody wants to send secret message for their privacy. The secret data of message is known as embedded data. The message is mainly hide in message which known as cover-text or cover-image or cover audio, which results in the stego-text or other stego-object. A secret-key is used to secure and control the hiding process so that any unauthorised person must not detect the hidden data. Some properties that are used in creating the digital data for hiding message is: Imperceptibility: In this property one cannot define difference between the stego image and original image.

Embedding Capacity: It defines how much amount of information can be embedded in the original without changing the quality of an image. Robustness: It defines the degree that is used to demolish embedded information without demolish the original image.

Steganography can be classified in three categories:

Text Steganography: It protects the text behind some other text file. It is a tricky form of steganography as the amount of redundant text to shield the information message is scant in text files. Examples of text steganography techniques are selstive hiding, HTML web pages etc.

Image steganography: Most commonly used techniques of steganography are image steganography because of the limitation of the Human visual System (HVS). The vast range of color the human eye cannot detect and any insignificant change in the quality of an image that results from steganography.

Audio Steganography: It is another difficult form of steganography as humans are easily able to detect even a minute change in the quality of audio.

II. LITERATURE SURVEY

Many active researchers have proposed various methods to embed the information message after encryption. Some researchers hide message contained by any document or text file or even sound file whereas others use image files.

Now-a-days everyone works on steganography systems to cover their objects using images. I have examined numerous such algorithms and lots of techniques that have been projected to conceal the secret data at the back of cover image without leaving any sort of mark.

Ibrahim et.al(2011) In this paper, A new set of algorithm is designed by the author for hiding data in images by means of Steganography. Here, in this algorithm binary codes and image pixels are used to hide data. In this method, for Maximising the data storage capacity, It is firstly converted into Zip file and then to the binary codes. The application of this algorithm system is called Steganography Imaging System (SIS). Then the viability of the proposed algorithm is tested to observe, whether it is viable or not. Algorithm, when applied and tested with the naked eyes, it remains unchanged and can not be noticed. When the stego images are tested using PSNR value. The PSNR value of those images observed higher and hence, this method of data hiding is very viable and liable for hiding our data from getting leaked[1].

Khaled Loukhaoukha et.al.(2012) A new design has been created using Rubik's cube principle. In the proposed algorithm, the author has shuffled and mixed the data with its identical but different data using the Rubik's cube method.XOR operation is applied to intermix the image data in rows and columns by applying two secret keys. In this method of data encryption, the time taken for hiding data is comparatively less and the method is also very liable as well as viable as per the data security, data encryption and its capability to defend its data from the various attacks of data hacking. The experiment shows tremendous results and is used in the real time application for communication applications [2].

Seetaiah Kilaru et.al.(2013) This paper put a light how to propose novel algorithm planted on the toy principle Rubik cube. Here, XOR operator along with two secret keys is used to design algorithm. The results also showed that the proposed algorithm is efficient in cases of eye sensitivity and key sensitivity. The main reason behind this algorithm is to produce confusion between the original and encrypted images in most possible manner. XOR operator is applied to rows and columns of an image in such a way that using the same key. After that key is flipped and applied again to the same number of rows and columns to reconstruct the image [3].

Devi, Kshetrimayum Jenita et.al. (2013) In this set, The image based steganography that combines Least Significant Bits techniques and pseudo random encoding technique on images for improving the security of the communication, is proposed. In this method, the Least Significant Bits (LSB) of the cover image is replaced with the Most Significant Bits (MSB) for hiding out the communication data without actual distortion or destruction of image data property. This LSB-based technique is the most efficient and challenging method for getting hacked as it is difficult to differentiate between the cover-object and stego-object, if few LSB bits of the cover object are changed or replaced with another bits. In the Pseudo-Random technique, keys in random are used. In the embedding process, Pseudo-Random Number Generator is needed, as seen in the study [4].

Navneet Kaur et.al. (2014) Many observations and reviews been given on digital steganography methods in this paper. The comparison of Least Significant Bit based Steganography, Discrete Cosine Transform based Steganography and Discrete Wavelet Transform based steganography have been made and their advantages and disadvantages are discussed[5].

A.K. Gulve et.al. (2014) this paper put a light on all the important aspects of Steganography and data encryption. The LSB steganography technique in images can be made more complicated by further using combination of Cryptography and Pseudo-random number generator.

The given method provides security of both data hiding and data encryption. The use of Pseudo-Random Number sequence helps the message bit to spread across 3 (4th, 5th and 6th) LSB's randomly, without the proper key. It is most difficult and almost impossible to detect the exact address of the LSB which holds the message bits. By using only a single RBG component from the pixel, the distortion created by Steganography is negligible, But at the cost of capacity to hold the data is high [7].

Sangivalasa et.al.(2015) In this paper the author is dealing with implementation of security measures for images based on the principles of Rubik's cube. In this paper the image is encrypted by scrambling of pixels and performing XOR operations and it is decrypted in the same way. This technique enables improved procedure for ensuring security for the image files that are being transmitted exactly every second. Before mentioned algorithms are efficient and have been constantly tested for actual results, but, the ethical aspect of the solution must not be forgotten. The techniques mentioned above need to be implemented decently to produce required results without breaching any established security protocols [8].

B. Srinivasan et.al. (2015) a new method has been made by adding up the three security channel in digital data image by wrapping up the message in digital image. For many different cover images and secret images this approach was executed and tested. Through their PSNR values the final stego-image and original image are compared. In this set of paper a new algorithm named, Non-uniform segmentation algorithm have been introduced named Non-Uniform Block Adaptive Segmentation on Image (NUBASI). The key function of the given algorithm is to create various numbers of segmented images with different dimensions, for embedding the secret messages. The Author used LSB replacement method. An arbitrary pattern is preferred by an algorithm Random Pattern Number Generator (RPNG). A great result is observed by using this method on Original image and stego-image PSNR values [9].

Ashwini B. Akkawar et.al. (2016) In this paper, the important aspects of a new steganography technique for embedding both text or image in cover images by using LSB & Link List method is used and implemented. This steganography technique is completely based on pixels. The secret messages are embedded directly into 24- bit colour image. In this method, two ways are provided for embedding the secret data inside cover image such as sequential encoding and random encoding for both text & image. For the purpose of data security, encryption technique is used with a user-defined key. RGB image format is used to enhance the quality of the stego image.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Both of this encoding technique works successfully using this hybrid method and hides the text data & image in cover images efficiently. By using same method, Audio or Video can also be used as cover object but it increases the payload capacity of secret data [10].

III. Experimental Analysis

In most of the research work, the authors have tried to implant some secret message within any cover file in an encrypted form so that no one will be able to pull out the actual secret message. Some standard steganography method is used in the cover file. Here, I have experimentally evaluated DISE based on Rubik's Cube principle.

3.1 Evaluation method and experimental result of Digital Image steganography with encryption based on Rubik Cube Principle (2016):

Encryption plays an important part in information security. Therefore, it is necessary to evaluate the performance of encryption and decryption algorithms. The evaluation is done on three parameters: encryption time of algorithm, avalanche effect and PSNR value.

3.2Encryption time of Digital Image steganography with encryption based on Rubik Cube Principle (2016):

Encryption time of any algorithm is the time required to encrypt the file.

Table 1:
Encryption time of Digital Image steganography with encryption based on Rubik Cube Principle (2016)

Digital Image steganography with encryption based on Rubik Cube Principle (2016)	
File Size in KB	**Encryption Time in seconds**
5.57 KB	0.234
15.3 KB	0.364
27.4 KB	.504

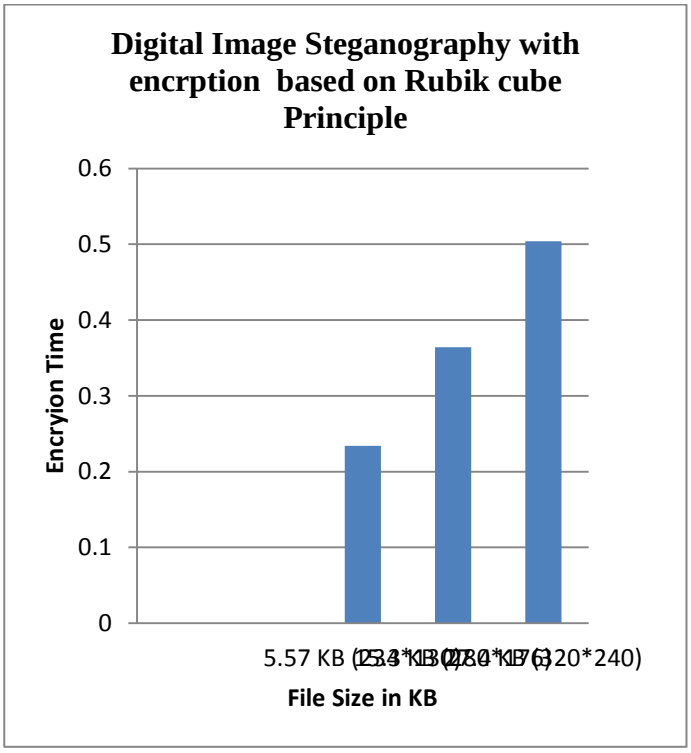

Figure 2: Encryption time of Digital Image steganography with encryption based on Rubik Cube Principle (2016)

It is clear from the table 3.1 & figure 3.1 that the encryption time increases with the increase in file size. 5 KB file requires 0.234 second to encrypt. 15KB file require 0.364 second to encrypt.

3.3 Avalanche effect

It is an enviable property in which if you change a one bit in input then its lead to a major bit change in output of cipher text A property of some cipher systems in which a small change in the input results in a very large change in the output.

Table 2:
Avalanche effect of Digital Image steganography with encryption based on Rubik Cube Principle (2016)

File Size in KB	**Avalanche Effect**
	Digital Image steganography with encryption based on Rubik Cube Principle (2016)
Single bit change in key	**48.63%**

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

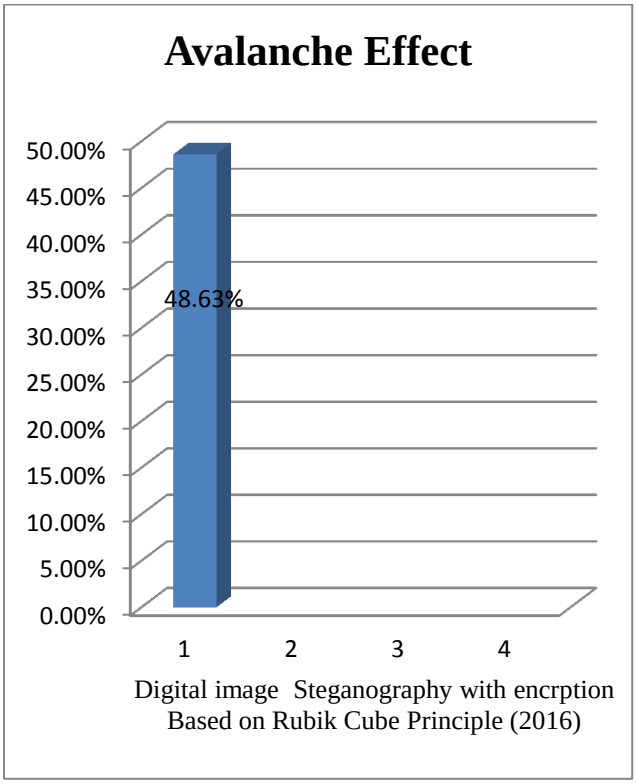

Figure 3: Avalanche Effect of Digital Image steganography with encryption based on Rubik Cube Principle (2016)

3.4 Peak Signal to Noise Ratio

Peak signal to noise ratio is a term used to find ratio between the highest possible value of an input signal and the rate of distorting noise that affects the quality of its representation. PSNR is usually expressed in terms of decibel.

Table 3:
PSNR Value of Digital Image steganography with encryption based on Rubik Cube Principle (2016)

File Size in KB	PSNR Value
	Digital Image steganography with encryption based on Rubik Cube Principle (2016)
1 KB	52.644

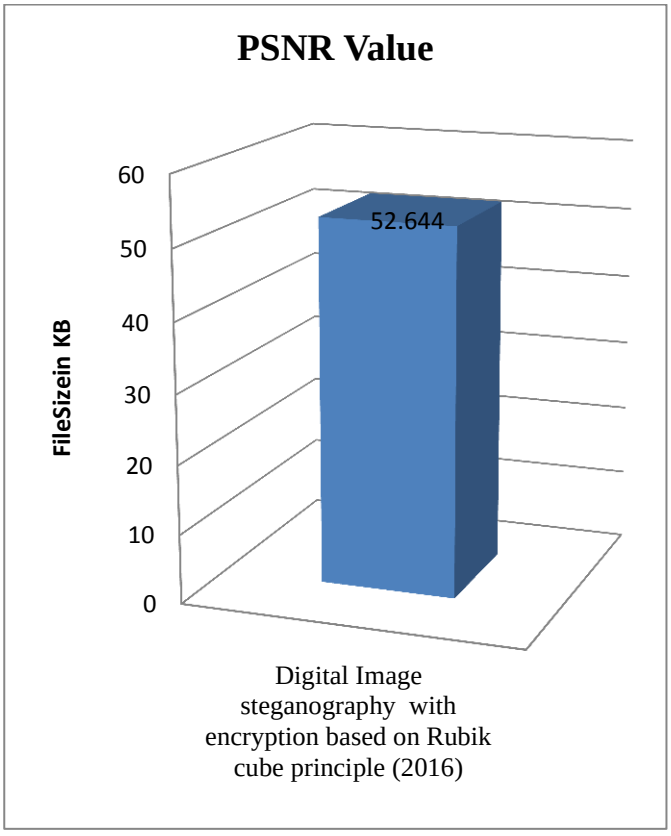

Figure 4: Peak Signal to Noise Ratio of Digital Image steganography with encryption based on Rubik Cube Principle (2016)

Experimental results of Table 3 and figure 4 show that PSNR value of base paper algorithm for 1KB file is 52.644

IV. Conclusion And Future Work

With the projectile like evolution of technologies in computer and internet, data security is an important concern in today's life. Authors have proposed steganography system that is joint with encryption algorithm that is based on rubik's cube principle used to kept information secret. If somebody wants to extact that message, it would be sturdy to decrypt secret image due to confusion and diffusion properties of the encryption algorithm combined with large key space.

In this paper I have experimentally evaluated the paper Digital Image steganography with encryption based on Rubik Cube Principle (2016) by using dot net based on parameter, Execution time, avalanche effect, Peak to signal noise ratio.

Evaluation results show that the algorithm takes less execution time and avalanche effect to encrypt file but having High PSNR Value. In future work this weakness can be overcome by developing new algorithm.

Secret image can be perfectly hidden in cover image. The proposed steganography systems are tested using visual attack and Chi square analysis.

REFERENCES

[1] Ibrahim, Rosziati, and Teoh Suk Kuan. "Steganography algorithm to hide secret message inside an image." arXiv preprint arXiv:1112.2809 (2011).

[2] Loukhaoukha, Khaled, Jean-Yves Chouinard, and Abdellah Berdai. "A secure image encryption algorithm based on Rubik's cube principle." Journal of Electrical and Computer Engineering 2012 (2012).

[3] Kilaru, Seetaiah, et al. "effective and key sensitive security algorithm for an image processing using robust Rubik encryption and decryption process."University of Birmingham, ISSN (Print) 2 (2013): 2278-8948.

[4] Devi, Kshetrimayum Jenita. "A secure image steganography using LSB technique and pseudo random encoding technique", National Institute of Technology-Rourkela, 2013.

[5] Kaur, Navneet, and Sunny Behal "A Surveyonvarious types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology 11.8 (2014): 387-91.

[6] Thakre, Ketki, and Nehal Chitaliya "Dual Image Steganography for Communicating High Security Information" ,International Journal of Soft Computing and Engineering (IJSCE) 4.3 (2014).

[7] Gulve, Avinash K., and Madhuri S. Joshi. "An image steganography algorithm with five pixel pair differencing and gray code conversion." International Journal of Image, Graphics and Signal Processing 6.3 (2014)

[8] Sirisha, M., and S. V. V. S. Lakshmi. "Pixel Transformation based on Rubik's Cube Principle.", International Journal of Science and Technology 8.S7 (2015): 228-235.

[9] Srinivasan, B., S. Arunkumar, and K. Rajesh. "A novel approach for color image, steganography using nubasi and randomized, secret sharing algorithm." Indian Journal of Science & Technology 8.S7 (2015): 228-235.

[10] Ashwini B. Akkawar, komal B. Bijwe "Hybrid approach for Embedding Text or Image in Cover Images", International journal of innovative research and science, engineering and technology, vol. 5, Issue 5, May 2016.