IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. V (Nov.-Dec. 2016), PP 92-100
www.iosrjournals.org

Dual Image Steganography Technique: Countermeasure and Analysis

Deepak Kumar Patidar[1],D. Srinivasa Rao[2], G. Sriram[3]
[1]*Research Scholar, MITM, Indore, India*
[2]*Assoc. Prof. of CSE Department, MITM, Indore, India*
[3]*Faculty of Computer Science, School of Distance Education, AU Visakhapatnam, India*
[1]*deepak.patidar007@gmail.com,* [2]*sridas712@gmail.com,* [3]*ram.gopalam@gmail.com*

Abstract: *The Internet has become the most important source of information in today's life which offers the users to exchange information. But the transfer of such information leads to a great security threat. The objective of steganography is to conceal the presence of the message from unapproved party. For concealing confidential data in pictures, there exist a huge classification of steganographic systems some are more difficult than others and every one of them have strong and weak points. In this paper, we proposed LSB (Least Significant Bit) based dual image steganography technique which enables to develop a simple and secure method for securing the digital data. Therefore the proposed technique incorporates dual steganography of data hiding and data recovery process using AES algorithm for high level security. The proposed work involves the LSB embedding based image steganographic technique and AES algorithm to secure the image data from outside intruders and attackers.*

Keywords: *Steganography, Image, Cryptography, AES, DES, Data Security, LSB*

I. Introduction

NOWADAYS, there is a fast advancement of the computer and network technology, people can easily send or receive secret information in various forms to or from almost any remote part of the world through the internet within seconds. In fact, there might be tons of secret information being transmitted and exchanged on the internet at a particular point of time. However, important secret messages may run high risks of leaking out while they are being transmitted or exchanged over some public communication channel. Therefore, how to achieve safe secret communication is an important field of research [1]. Since the beginning of web the security of data is the most key figure data in communication technology. Numerous strategies like cryptography, watermarking and encryption and decoding procedures were produced to secure the data during communication, But still it is insufficient to secure the substance of the confidential message from outside phishers and programmers. There is a need of another system which can keep the presence of the message confidential. In today's information age, the technologies have grown so much that the vast majority of the clients prefer web to exchange information starting with one end then onto the next over the world. So protection in advanced communication is fundamental prerequisite when secret data is being shared between two clients. To provide security, various steganography and cryptography techniques have been used in the past research [2].

A. Steganography

Steganography is the idea of hiding private or sensitive data or information within something that appears to be nothing out of the normal. The word steganography originates from the Greek Steganos, which mean secured or confidential and –graphy mean composition or drawing. In this way, steganography implies secured composing. Steganography is the art and science of concealing data with the end goal that its presence can't be identified and a communication is going on [3]. Confidential data is encoding in a way to such an extent that the presence of the data is covered. Matched with existing specialized strategies, steganography can be utilized to have hidden message exchanges. Steganographic technologies are very important part of the future of internet security and privacy on open systems such as the Internet.

B. Different kinds of Steganography

All computerized file formats can be utilized for steganography, however the formats that are more appropriate having high level of redundancy. Redundancy can be characterized as the bits of an object that provides accuracy which is greater than the required bits for the object's utilization and display [4]. The excess bits of an object are the bits which can be changed without the modification being detected easily [5].

Figure 1 shows the four main categories of file formats that can be used for steganography.

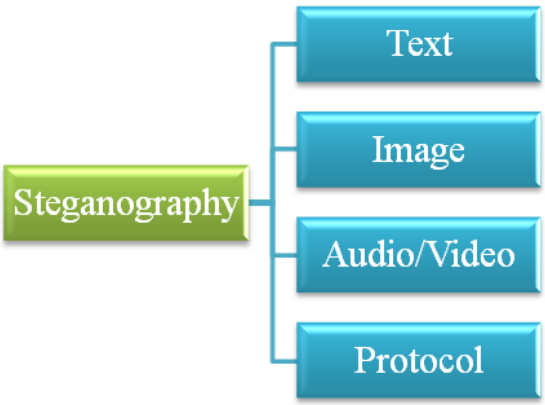


Figure 1: Categories of steganography

Text: Hiding data in content is truly the most imperative technique for steganography. An obvious strategy is to conceal a confidential message in each n^{th} letter of each word of an instant message. The importance of computerized file formats has diminished since the start of the internet [6]. Content steganography utilizing computerized documents is not utilized regularly since content records have a little measure of redundant information.

Image: Given the multiplication of advanced pictures, particularly on the Internet, and given the substantial measure of repetitive bits present in the computerized representation of a picture, pictures are the most well known cover objects for steganography. This paper will focus on concealing a data within a picture in the next sections.

Audio/Video: To hide data in sound records same techniques are utilized as for picture documents. One diverse procedure unique to sound steganography is masking, which misuses the properties of the human ear to conceal data unnoticeably.

A low, however audible, sound gets to be quiet within the sight of another louder audible sound [6]. This property makes a channel to hide data. The pictures are preferable than the sound documents for Steganography as the audio file size is bigger than picture size [7].

Protocol: The term protocol steganography points to the strategy of embedding data inside messages and network control protocols utilized as a part of network transmission [8]. In the layers of the OSI model there exist undercover channels where steganography can be used, for example, the data can be hidden in the fields of the header of TCP/IP packet which are either optional or never used [8].

II. Literature Survey

Rasha Adel Ibrahim et al. [9] worked on Fractal pressure which is done on different divisions of pictures, depending on the way that parts of a picture frequently look like different parts of a similar picture. It requires long encoding time and influences the picture quality. Here an enhanced model incorporating quantized quad trees and entropy coding utilized for fractal picture pressure which results in improving the recovered picture's quality and pressure proportion significantly on different type of pictures and encoding time. Here there reduction in pictures sizes making less encoding time, however poor picture quality. **Hengfu Yang et al. [10]** proposed a novel picture information hiding technique by versatile Least Significant Bits (LSBs) substitution to stay away from unexpected changes in picture edge zones, and additionally to accomplish better quality of the stego-picture. The plan exploits the brightness, edges, and surface masking of the host picture to guess the number k of LSBs for information hiding. Besides, an ideal pixel modification process is utilized to improve stego-picture visual quality obtained by basic LSB substitution technique. To guarantee that the adaptive number k of LSBs stays unaltered after pixel alteration, the LSBs number is figured by the high-order bits rather than all the bits of the picture pixel value. The hypothetical investigations and test comes about demonstrate that the proposed strategy accomplishes higher embedding capacity and better steno image quality compared with some current LSB strategies. **Nouf A. Al-Otaibi et al. [11]** proposed and implemented high security framework appropriate to conceal sensitive text data on PC. The framework concealing techniques includes AES cryptography followed by picture based steganography as two layers to guarantee high security. The study included a few tests to expand the limit inside the steganography layer adopting 1 and 2 least significant bits stego techniques. The study likewise investigates the data dependency and its security impacts by testing it on 30 different fixed size pictures demonstrating interesting attractive results. **Seyed H. Kamali et al. [12]** proposed an alteration to the Advanced Encryption Standard (MAES) to reflect an high level security and better

picture encryption. The modification is done by adjusting the Shift Row Transformation which results in terms of security analysis and implementation are given. Experimental results confirm and demonstrate that the proposed adjustment to picture cryptosystem is highly secure from the cryptographic perspective. The results also prove that with a comparison to original AES encryption algorithm the modified algorithm gives better encryption results in terms of security against statistical attacks. **Satwinder Singh et al. [13]** describes the double layer of security to the information, in which first layer is to encode information using Least Significant Bit picture steganography technique and in the second layer encrypt the information utilizing Advance Encryption Standard Algorithm. Steganography does not replace the encryption of information, rather it gives additional security highlight to it. In this work confidential text message is hiding behind the digital image file and this image file is then encrypted utilizing AES encryption algorithm.

III. Proposed Work

A. Methodology

The data hiding process has two phases shown in figure 2(a) and 2(b).

Phase 1 description- LSB embedding algorithm includes input secret data, cover image1 and get processed and produces Stego image1 then apply AES Encryption algorithm on this image using key 1 and generate encrypted stego image1.

Phase 2 description- The outcome of phase 1 i.e. encrypted stego image1 and cover image2 is taken as an input and processed with LSB embedding algorithm and generates final stegno image, further applying AES Encryption with an input of key2 on final stego image gets final encrypted stego image.

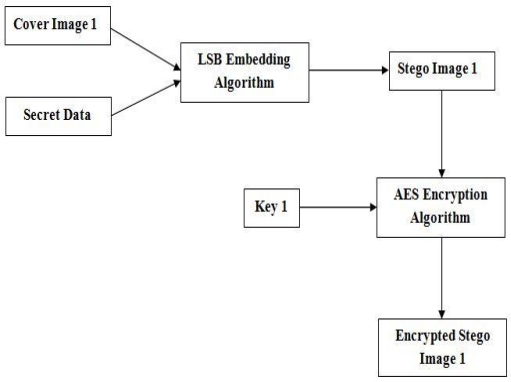
The data recovery process has two phases shown in figure 3(a) and 3(b).

Phase 1 description- The outcome of data hiding process i.e. final encrypted stego image is input to the AES Decryption algorithm and get final stego image by applying key2. On this final stego image we apply LSB recovery algorithm and generate encrypted stego image1.

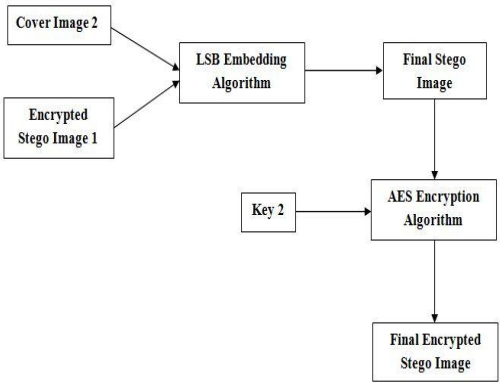
Phase 2 description-

The outcome of phase 1 is input to the second phase where AES Decryption is applied using Stego key1 which generate stego image1, which is given as a input to the LSB recovery algorithm that produce secret data.

This proposed secure image steganography algorithm called double steganography approach in which data secured using dual steganography with dual encryption.

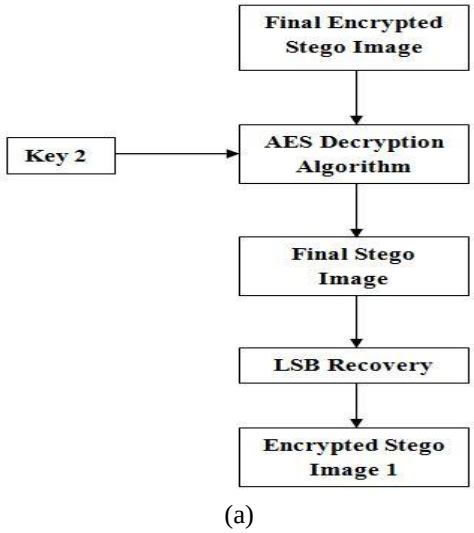


(a)

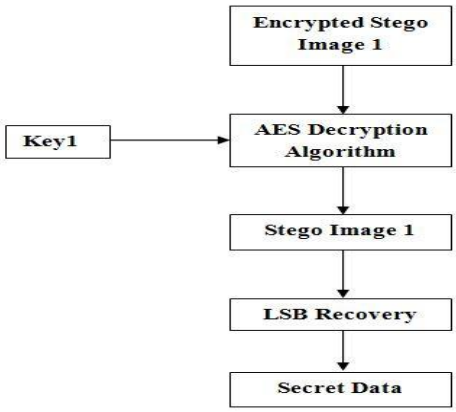


(b)

Figure 2: Figure (a) and (b) shows Data Hiding Process



(a)



(b)

Figure 3: Figure (a) and (b) shows Data Recovery Process

B. Proposed Algorithm

In this section provides the understanding about the processes involved in the proposed cryptographic technique. This section provides the summarized steps of the process for both the required operations.

Table 1: Proposed Dual Steganography Technique

Input: Hide Data H_D, Key_1 & Key_2 of size 128 Bit, Cover ImageI_{C1},Cover Image I_{C2}; ***Output:*** Secret Data D;
Process: **1:**F = readData H_D **2:**I_{C1} = coverImage **3:** stegoImage1 = LSBEmbedding (F, I_{C1}) **4:**Key_1 = stegoKey **5:**encryptedStegoImage1 = AESEncryption (Key_1, stegoImage1) **6:**I_{C2} = coverImage **7:**stegoImage2 = LSBEmbedding (encryptedstegoImage1, I_{C2}) **8:**Key_2 = stegoKey **9:** encryptedStegoImage2 = AESEncryption (Key_2, stegoImage2) **10:**if (Key_{a2} = = Key_2) **11:** decryptedstegoImage1 = AES. decrypt (encryptedStegoImage2, Key_{a2}) **12:**encryptedStegoImage1 = LSBRecovery (decryptedstegoImage1) **13:**if(Key_{a1} = = Key_1) **14:** decryptedstegoImage2 = AES. decrypt (encryptedStegoImage1, Key_{a1}) **15:**D = LSBRecovery (decryptedstegoImage2) **16:**return D

IV. Result Analysis

A. Encryption Time

The amount of time required to encrypt data using selected algorithm is known as encryption time. The comparative encryption time of both traditional and proposed algorithms for cryptography is given using figure 4. In this diagram the X axis shows the file size (in terms of KB-kilobytes) of images used for experiments and the Y axis shows the amount of time consumed for encryption in terms of seconds.

$$\text{Time Consumption} = \text{End Time} - \text{Start Time}$$

Table 2: Time Consumption in Encryption

Data Size (in KB)	Dual Steganography Combined with AES (Time in sec.)	Steganography Combined with DES (Time in sec.)	Steganography Combined with AES (Time in sec.)
10	56110	26194	1146
20	46694	30866	777
30	75812	31481	1163
50	36464	35098	11625
70	28520	23065	11531
100	31548	28795	12598
200	25498	25489	9562

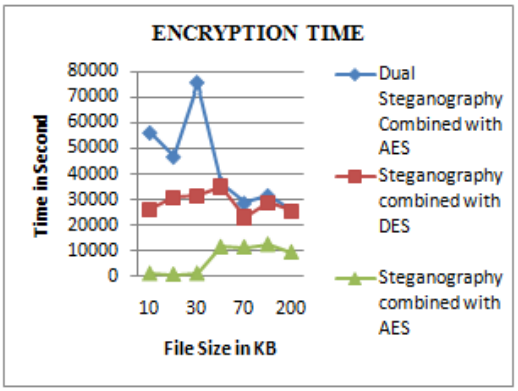


Figure 4: Time Consumption in Encryption

According to the obtained performance of implemented proposed work, traditional algorithm i.e. steganography of hiding information using Advance Encryption Standard and Data Encryption Standard, AES and DES respectively (represented using red and green line) consumes less time for processing of data file as compared to proposed Algorithm (represent by blue line). Additionally with increasing size of data the time consumption of the traditional technique is increase simultaneously while proposed method may vary time according to algorithm. Therefore the proposed technique is less efficient as compared to traditional techniques by means of encryption time.

B. Decryption Time

The amount of time required to recover the original image or data from the encrypted image is termed as decryption time. The comparative time consumption of both traditional and proposed technique is shown using figure 5.

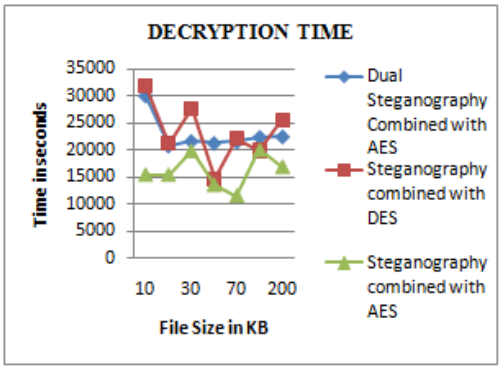


Figure 5: Times Consumed in Decryption Process

Table 3: Time Consumption in Decryption

Data Size (in KB)	Dual Steganography Combined with AES (Time in Second)	Steganography Combined with DES (Time in Second)	Steganography Combined with AES (Time in Second)
10	30040	31697	15491
20	20873	21192	15499
30	21726	27615	19978
50	21367	14685	13634
70	21642	22061	11547
100	22469	19856	20154
200	22568	25487	16985

$$\text{Time Consumption} = \text{End Time} - \text{Start Time}$$

By using above formula we calculated decryption time consumed during process. In this diagram the performance of proposed steganography technique is given using the blue line and the red and green line shows the performance of traditional AES and DES of steganography. For depiction of the performance X axis contains the size of images or text data on which experiments are performed that is given in terms of KB and Y axis shows the time in terms of seconds. The evaluated performance of the techniques shows the proposed algorithm and AES based steganography is much better and efficient than DES based steganography in terms of time complexity. Therefore the proposed technique and AES is much adoptable as compared to DES technique

C. Encryption Memory

The amount of main memory required to execute the implemented encryption algorithms is termed as encryption memory. The figure 6 shows the comparative performance of the both algorithms for the space complexity of encryption. For results demonstration the X axis shows the different experiments performed with the system and the Y axis shows the memory consumption during encryption in terms of kilobytes. To compute the memory consumption the following formula is used.

$$\text{Memory Consumed} = \text{Total Memory} - \text{Free Memory}$$

In order to show the performance of proposed algorithm the blue line is used and the red line, green line shows the performance of traditional algorithms. According to the given results most of the time the memory consumption in both the algorithms e.g. AES and DES are much similar but our proposed algorithm consumes more space compared to AES and DES. In addition of that the space complexity of the algorithms are increases with the increasing size of experimental images.

Table 4: Memory Consumption in Encryption

Data Size (in KB)	Dual Steganography Combined with AES (Memory in KB)	Steganography Combined with DES (Memory in KB)	Steganography Combined with AES (Memory in KB)
10	39.211914	19.598633	39.00098
20	55.18457	24.712891	38.4541
30	72.585938	27.175781	45.24316
50	25.279297	18.581055	37.20215
70	22.392578	20.542969	29.2666
100	31.25895	21.25987	25.12365
200	38.21577	24.3258	27.22598

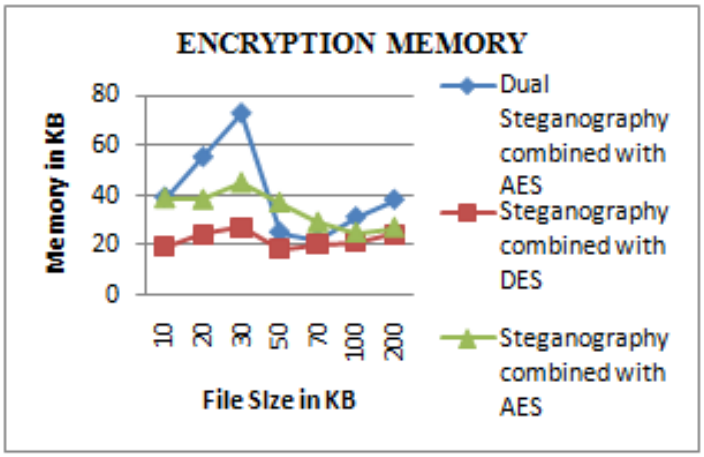


Figure 6: Memory usages during Encryption

Thus as the file size increases the required memory is also increases. According to the system performance the proposed technique is take large space in system while other two methods take little amount of space. Therefore AES and DES approaches much efficient than proposed algorithm.

D. Decryption Memory

The memory consumed during the decryption or recovery of original algorithm is termed here as the decryption space complexity. The comparative outcome of the space complexity is given using figure 7. In this diagram the amount of memory used is given in terms of kilobytes using Y axis and the X axis shows the different experiments performed with the system. The performance of the proposed dual steganography combined with AES algorithm is given here using blue line and the traditional approaches are represented using the red and green lines. According to the known results the proposed cryptographic technique consumes large memory and in consistent manner as compared to the Hybrid Steganography. Thus proposed technique is less adoptable as compared to traditional techniques.

Table 5: Memory Consumption in Decryption

Data Size (in KB)	Dual Steganography Combined with AES (Memory in KB)	Steganography Combined with DES (Memory in KB)	Steganography Combined with AES (Memory in KB)
10	37.350586	19.250977	31.68555
20	63.130859	28.200195	44.2793
30	80.457031	27.936523	50.96777
50	26.146484	23.914063	42.54883
70	24.509766	21.108398	34.56836
100	27.325894	24.32658	25.32568
200	31.258987	26.14987	30.25869

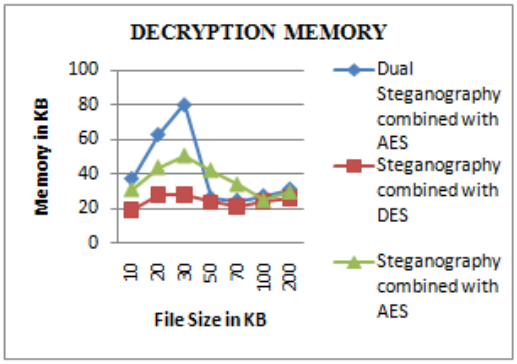


Figure 7: Memory usages during Decryption

E. Mean Square Error (MSE)

The mean squared error (MSE) of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. In figure 8 and table 6, depiction of mean square error of input data images for proposed and traditional method has shown. The Mean Square Error is defined as the square of the difference between the pixel values of the original image and the Stego image and then dividing it by size of the image. In figure 8, proposed image steganography technique shown by blue line and other two traditional approaches are depicted by red and green line. The lower value of Mean Square Error (MSE) signifies lesser error in the Stego image in other words better quality.

Table 6: MSE Values

Data Size (in KB)	Dual Steganography Combined with AES	Steganography Combined with DES	Steganography Combined with AES
10	0.3227109	0.4995313	0.449846
20	0.1156016	0.1329297	0.396492
30	0.2013047	0.5052734	0.254565
50	0.3822031	0.5118359	0.417235
70	0.1302891	0.2456641	0.36752
100	0.351367	0.197305	0.25925
200	0.215986	0.235977	0.35582

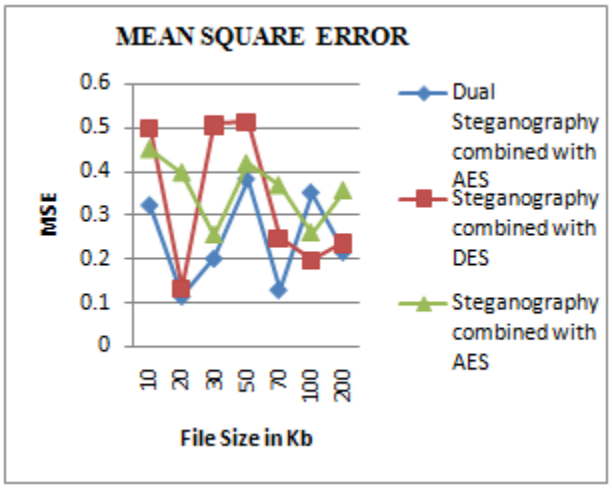


Figure 8: Mean Square Error

F. PSNR (Peak Signal to Noise Ratio)

The PSNR measures the peak signal-to-noise ratio between two images. This ratio is often used as a quality measurement between the original and a compressed image. Higher the PSNR means better the quality of the compressed or reconstructed image. The PSNR value can be calculated as:

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

Table 7: PSNR Values

Data Size (in KB)	Dual Steganography Combined with AES (dB)	Steganography Combined with DES (dB)	Steganography Combined with AES (dB)
10	53.042667	51.145177	51.60016
20	57.501167	56.894584	52.14845
30	55.092265	51.095539	54.07282
50	52.307861	51.039496	51.927
70	56.981724	54.227387	52.478
100	52.673192	54.164578	53.94774
200	57.714856	51.402115	51.84097

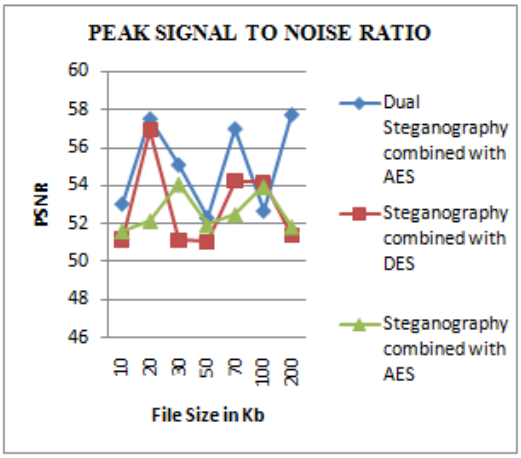


Figure 9: PSNR ratio

Peak signal to noise ratio of both the traditional and proposed techniques for image steganographic technique is given using figure 9. In this diagram the X axis shows the experimental file size and the Y axis shows the obtained PSNR ratio. The figure contains the red and green line to show the performance of the traditional approach and Y axis contains the performance of the proposed technique. The amount of computed PSNR is fluctuating with the image quality therefore that is not depends on the image size that is depends on the quality of image. Proposed algorithm has higher PSNR value which indicates better image quality

V. Conclusion

Security is a primary need of the digital data, different kinds of attacks and malicious programs can harm the data. In addition of that during the network transmission the data is also suspected to be stolen. Therefore different kinds of security techniques are implemented for enhancing the security of the digital data. In various security techniques the cryptography is popular and classical approach of data security. In this presented work the image cryptography is studied in detail and a new security technique using the steganography and data cryptography is proposed. The proposed cryptographic technique is hybrid technique which combines the efforts of both cryptography and steganography. Therefore the technique promises to provide more secure data exchange as compared to single technique implementation of image data security.

References

[1] Muhalim Mohamed Amin "Information Hiding Using Steganography", ethesis, University Technology Malaysia, 2003.
[2] Komal Patel and Sumit Utareja, "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm", International Journal of Computer Applications (IJCA), Volume 63– No.13, February 2013.
[3] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
[4] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", 19th National Information Systems Security Conference, 1996.
[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.
[6] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf
[7] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.
[8] Ahsan, K. & Kundur, D., "Practical Data hiding in TCP/IP", Proceedings of the Workshop on Multimedia Security at ACM Multimedia, 2002.
[9] Rasha Adel Ibrahim, et al., "An enhanced fractal image compression integrating Quantized quadtrees and entropy coding", 2015 11th International Conference on Innovations in Information Technology (IIT), 2015 IEEE.
[10] H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal of Radio Engineering, vol. 18, no. 4, 2009
[11] N. A. Al-Otaibi and A. A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", Lecture Notes on Information Theory, vol. 2, no. 2, (2014).
[12] S. H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, "A new modified version of Advanced Encryption Standard based Algorithm for Image Encryption", proceeding of IEEE International Conference on Electronics and Information Engineering (ICEIE), (2010) August 1-3, Kyoto, Japan.
[13] GNDU RC, Jalandhar. "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm." (2015).