ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

Enhancement of Image Steganography using a Dynamic Symmetric Key by Arithmetic Coding

[1] Wa'el Ibrahim A. Almazaydeh, [2] H. S. Sheshadri, [3] S.K. Padma
[1] Research Scholar, PET Research Foundation, PESCE, Mandya
[2] PESCE, Mandya, India, [3] Sri Jayachamarajendra College of Engineering, Mysore,India.

Abstract;- **This paper is an enhancement of the image Steganography using a dynamic symmetric key algorithm by applying it on the colored images and using the Arithmetic coding algorithm. However, the Peak Signal to Noise Ration (PSNR) algorithm has been used to compare the results.**

General Terms:- **Steganography, Security, Compression, Symmetric key, LSB, and Zigzag Scanning.**

Keywords:- **Least Significant Bit (LSB), Arithmetic Coding, ASCII code, PSNR, zigzag scanning**

1. INTRODUCTION

In the ordinary sense of the world, the word 'security' means the state of being safe and the measures taken to ensure safety. But safety isn't a goal or an absolute because in spite of using many of the security procedures available there is no 100 percent security. Human beings have been creating and using many safety procedures since ancient times to protect their lives. In the past, only things with physical presence needed protection and security (physical security); for example: a house was used to get protection against the harshness of nature, guards were used to protect places, and weapons were used to protect human beings. Watchtowers, gates, moats, locks, and other forms of protections [3].

Encryption is the most persuasive way to enact data security. It is the process in which information is encoded in such a way that only authorized recipient can decode it. In this, information is changed to make it meaningless for everyone but except for those who obtain special knowledge which authorize them to change information back to its original form. Encryption is important because it consent us to secure and protect the data. This is used to protect the secrets of corporate as well as government's offices. Mainly used to secure the classified information, where as many individuals use encryption to protect their personal information so as to defend themselves against situations like identity theft, cyber crime, etc. There are two types of encryption; they are symmetric encryption and asymmetric encryption. In symmetric encryption, the encryption and decryption keys are the same where as in case of asymmetric encryption there are different keys used for both encryption and decryption [5].

In today's digitized world, due to tremendous increase in electronic communication technology, now it is a real and hard problem to send some sensitive data or information through a secure communication channel. This can be Obtained by means of two techniques. One-Cryptography and second- Steganography. Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. Steganography is an ancient art or practice. Steganography is a branch of information hiding and its main goal is to communicate or transit the data securely in a completely undetectable manner. Literally meaning writing in a cover is the practice of hiding messages within other messages in order to conceal the existence of the original. Steganography refers to data or a file that has been concealed inside a digital image, video or audio file. Examples of its use can be found throughout history, dating as far back as ancient Greece. However, with the digital media formats in use for data exchange and communication today providing abundant hosts for Steganography communication, interest in this practice has increased. Couple this fact with the multitude of freely available, easy to use steganography software tools on the internet, the ability to exchange secret information without detection is available to virtually anyone who desires to do so, and provides unique challenges and opportunities for the security professional [4].

Steganography technologies are a very important portion of the future of security and privacy on open systems such as the Internet. Steganography can be used to hide important data inside another file so that only the parties intended to get the message even knows a secret message exists. In this paper, we review the Steganographic methods and tools in detail. The Steganography methods are very feasible to transit the data without altering it or encrypting and send it in a secure fashion [4].

A Matlab program has been created for this study. It is called (Wa'el-Steganography).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

2. RELATED WORK

This paper is an enhancement technique of the paper "Image Steganography using a Dynamic Symmetric Key" by applying it on the colored images instead of grayscale images and using Arithmetic coding.

Prof. H. S. Aheshadri and Wa'el Ibrahim A. Al-Mazaydeh explained in his paper two techniques for Steganography: the first one is the well known technique which is known as Least Significant Bit, and the second one is the new technique with LSB+KEY. The performances of the results have been compared using the PSNR values of individual algorithms. It is noted that the LSB+KEY algorithm gives better output with respect to the PSNR values [3].

The authors Wa'el Ibrahim A. Almazaydeh, and H. S. Sheshadri presented how to conceal information into an image by using three methods that concentrate on the compression of the data before hiding it into the image and then compare the results using Peak Signal to Noise Ratio (PSNR). The three methods that have been used here are Least Significant Bit (LSB), Huffman Code, and Arithmetic Coding. The performance analysis has been compared [2].

Wa'el Ibrahim A. Al-Mazaydeh explained the Steganography technique in the digital image, and it offers new technique for Steganography using (Least Significant Bit, Zigzag Scanning, and Huffman code). It contains two techniques for Steganography: The first is Least Significant bit, and the second is Least Significant bit and Huffman code. By comparing the results between the two techniques it concludes the LSB+HUFF method is better than LSB method to hide text into image [1].

Dr. Saad Abdual azize AL_ani, Bilal Sadeq Obaid Obaid proposed a new method of hiding data in the cover image. This algorithm is based on converting character to 6 bit, by using b-table compressed to 4 bit and from another side used similarly to value of cover pixel. The receiver gets value of location encrypted by RSA algorithm. There is no data embedded in the cover image [6].

Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda and Mustafa Mamat proposed a simple and an efficient model for calculating secret message that can be embed in an image. This proposed model used Connective Logical (CL) as an algorithm to calculate a new binary number of secret messages while the most significant bit (MSB) of each pixel was used as a key. MSB was a first bit of each pixel and it has a great significant value. Generally the MSB of each pixel calculated with secret message using operator Negation, OR and XOR to produce a new secret message. This new secret message would be embedded in the LSB of pixel. The implementation of this model can produce a low computational complexity of steganography because of the simplicity of the proposed algorithm [7].

Yun-Te Lin, Chung-Ming Wang, Wei-Sung Chen, Fang-Pang Lin, and Woei Lin presented a novel data hiding algorithm for HDR images encoded by the OpenEXR format. The proposed algorithm conceals secret messages in the 10-bit mantissa field in each pixel, while the 1-bit sign and 5-bit exponent fields are kept intact. They recommend an optimal base allowing secret messages to be concealed with the least pixel distortion. An aggressive bit encoding and decomposition scheme is introduced herein, which offers the benefit for concealing an extra bit in a pixel group without incurring pixel distortion. The influence of the message probability is analyzed, and the embedding capacity is further increased by taking advantage of the recommended bit inversion embedding scheme [13].

Dharmesh Mistry, Richa Desai, and Megh Jagad showed that Steganography does not intend to take the place of cryptography but rather support and supplement it. Consider that a message is initially encrypted and then hidden with a steganographic method, it provides a double layer of protection and reduces the chances of the hidden message getting detected [14].

NIELS PROVOS AND PETER HONEYMAN discusses existing steganographic systems and presents recent research in detecting them via statistical steganalysis. Other surveys focus on the general usage of information hiding and watermarking or else provide an overview of detection algorithms [15].

Madhavi V.Kale , Prof. Swati A.Patil proposed steganographic system, Compress ratio is calculated by Huffman Encoding Algorithm. after that Text is hide in image, audio and Video by Least Substitution Method (LSB) and Encrypt by Using Advanced Encryption Standard Algorithm. On the another Hand Receiver receive that that hiding image, audio as well as Video as appear Original Image. After that Receiver Decrypt that Text by using Advanced Encryption Standard Algorithm (AES) and getting Text which is hide by Sender in image, audio as well as video [8].

Amanjot Kaur, Dr. Bikrampal Kaur proposed a novel embedding approach based on k-Modulus Method for colored images. From experimental results it is clear that the proposed technique obtained high PSNR along with good image fidelity for various images which conform k-Modulus Method based image steganography can obtain better security [9].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

R Praveen Kumar, V Hemanth and M Shareef showed that Using LSB technique, embedding huge amount of secret information in not possible. The basic idea of this paper is to embedded huge amount of secret information using LSB technique. To achieve this first the secret information is compressed using wavelet transforms. After compression the bits are encoded using a reversible quantum gate. LSB is one of the best techniques when compared to transformation techniques, because it reduces lots of noise distortion. In cryptography, the intruder can know the existence of the message transferring. By doing this process huge amount of information can be communicated in the covert channel and even the existence of the message is difficult to identify [10].

2.1 Steganography

Figure 1 shows the Steganography technique [1]:

-Secret Message: the information that you want to embed inside the cover media.
-Stegokey: the key used in the Steganography process.
-Cover Media: the medium used in Steganography process such as: image, video, audio, etc.
-Encoding Algorithm: the method used in Steganography process.
-Stego-Media: the medium resulting from adding the secret message into a cover media using Stegokey and encoding algorithm.
-Decoding Algorithm: the method used to extract the secret message from Stego-media using Stegokey.

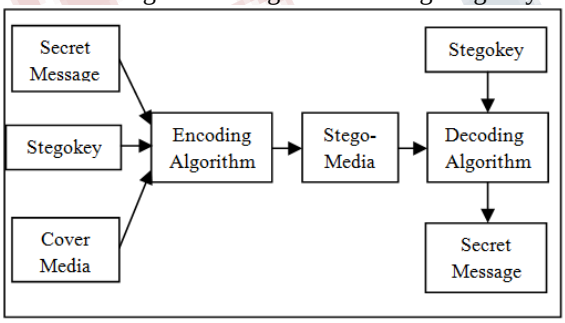

Fig 1: Steganography Technique [1]

2.2 ASCII Code

American Standard Code for Information Interchange (ASCII) is the most common format for characters in the computer systems. In an ASCII code, each alphabetic, numeric, or special character is represented with a 7 bits binary number (a string of seven 0s or 1s). For example the ASCII Code for (A, a, X, $, #) are (65, 97, 88, 36, 35) respectively. In this paper, the ASCII code is used to convert each character of the secret message to the value of ASCII code [3].

2.3 Least Significant Bit (LSB)

The most common technique used for Steganography is the Least Significant Bit (LSB). This study used one bit of Least Significant Bit. It substitutes each bit of the binary text bit with one bit of each pixel in the original image. For example: if we have 8 bytes of data and we want to hide the number 195 which is represented in ASCII code as 11000011, we can use Least Significant Bit (LSB) technique. Figure 2 shows how the LSB technique can be used.

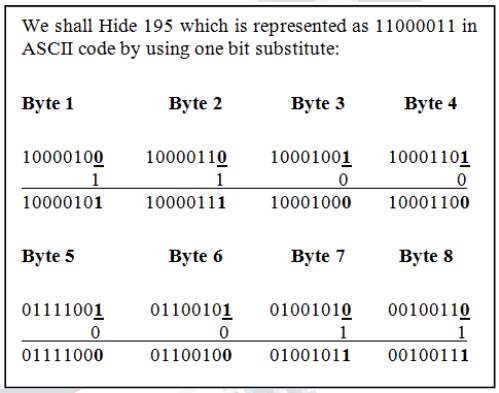

Fig 2: Least Significant Bit (LSB) Technique.

2.4 Zigzag Scanning

This study uses a zigzag scanning method to increase the security that can be achieved by using the Steganography technique. The pixels which will be used to embed the secret message bits are chosen through a method of zigzag scanning. The method of zigzag scanning is elaborated in figure 3 [3].

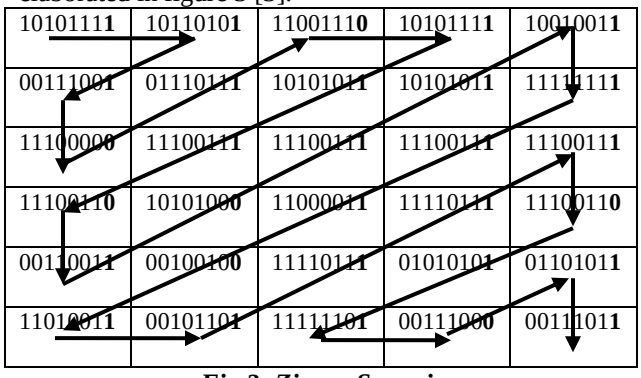

Fig 3: Zigzag Scanning

2.5 Arithmetic Coding

It is most often used when we have to code binary symbols or bits. Each bit begins the coding process. The arithmetic codes generate non-block codes; that is a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

correspondence between source symbols and code words does not exist. Instead, an entire sequence of source bits is allocated to a single code word which defines an interval of real numbers between 0 and 1 [12].
As the number of symbols or bits in the message increases, the interval used to represent it becomes smaller and the number of bits needed to represent the interval becomes larger. Each symbol in the message reduces the size of the interval according to its probability of occurrence. Since the symbols are not coded one at a time, this technique can achieve the highest possible coding efficiency [12].

2.6 PSNR

Peak Signal to Noise Ratio (PSNR) (equation 2) is measured on a logarithmic scale. It depends on the mean squared error (MSE) between an original image and stego image, relative to (2n - 1)2 (the square of the highest-possible signal value in the image, where n is the number of bits per image sample) [11].

$$MSE = \frac{\sum_{M,N} [A(m,n) - B(m,n)]^2}{M \times N} \quad (1)$$

$$PSNR_{db} = 10\log_{10} \frac{(2^n - 1)^2}{MSE} \quad (2)$$

"PSNR can be calculated easily and quickly and is therefore a very popular quality measure, widely used to compare the 'quality' of compressed and decompressed video images" [11].
When the PSNR value is high, the change in the image resolution is low; and when the PSNR is low the change in the image resolution is high. So my goal is to get the high PSNR value.

3. METHODOLOGY

This paper shows two algorithms for image Steganography to hide a secret message in an image using a symmetric key: the first one is image Steganography using a dynamic symmetric key (LSB+KEY) and the second one is the new technique for image Steganography using a dynamic symmetric key and Arithmetic coding (LSB+KEY+ARITH). Figure 4 shows the methodology.
The Arithmetic coding is used for two reasons: the first reason is to reduce the size of the secret message and thus reduce the number of pixels that will need to hide the secret message data in the image and thus get better results for the Steganography process, and the second reason is to give the Steganography process more security.
The results of the two methods have been compared with respect to the Peak Signal to Noise Ratio (PSNR) algorithm between the original image and the stego image.

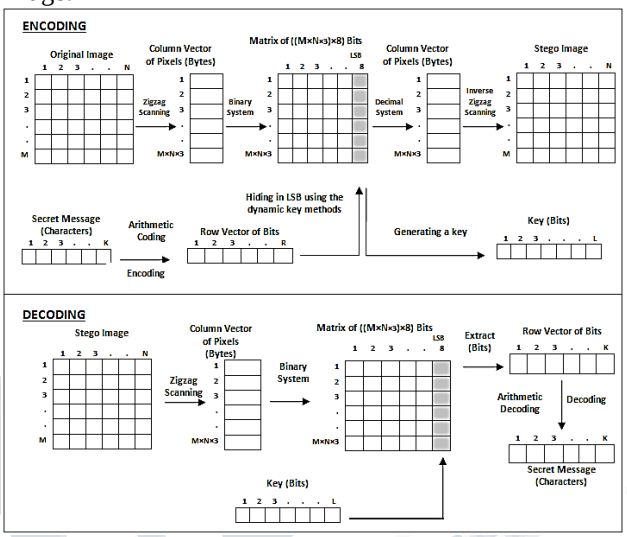

Fig 4: The Encoding and Decoding of this study.

3.1 Image Steganography using a Dynamic Symmetric Key Algorithm

It is also called Wa'el algorithm. This is a new method for image Steganography to hide secret message in an image, it is created and published by (Wa'el Ibrahim A. Almazaydeh). Figure 5 shows the encoding and decoding of the algorithm. This algorithm was used for grayscale images. This paper develops the algorithm to colored images and uses the Arithmetic coding to decrease the size of the secret message.
It converts the image pixels to binary values using zigzag scanning (as shown in figure 4) with size equal to (M×N×3×8) bits, where (M) is the number of rows in the image, (N) is the number of columns in the image, (3) refers to the number of planes (red, green, and blue), and (8) is the number of bits (each pixel in the plane is represented by 8 bits).
Then, gets the two least significant bit of each pixel value according to the position, where the (LSB) position equal to 0 and the bit before LSB position (LSB-1) equal to 1. In a parallel process, the secret message is converted to a row of binary values with size equal (1×K), where K is the number of bits in the secret message. After this, each bit of the secret message is compared with the two bits of the (LSB). Figure 5 shows the encoding and decoding that has been done.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

There are three instances of matching process of the image Steganography using a dynamic symmetric key [3]:
1) If the bit of the secret message matches the position 0 of the (LSB), the key will be 0.
2) If the bit of the secret message matches the position 1 of the (LSB), the key will be 1.
3) If the bit of the secret message doesn't match the first and the second position of the (LSB); we will change the position 0 of the (LSB) to the value of that bit of the secret message and the key will be 0.
At the end of this process, a row vector of bits is created that is present the key. The key refers to the position of the secret message in the stego image. This key, is a shared secret key, between the sender and the receiver; and without this key, the receiver will not be able to get the secret message. The key is considered the base of this method.
The size of the data (secret message) that can be hidden into the image by using this method can be calculated by using the following formula:

$$S1 = (M \times N \times 3) - 27 \quad (3)$$

Where (S1) is the size of the secret message, M is the number of rows in the image, N is the number of columns in the image, (3) is the number of planes, and (27) is represented as: the first seven bits from (1 to 7) are reserved to the Steganography type may be [1, 2, 3, …, 127], for example, when the Steganography type equals 2 means that Steganography process is another Steganography process and etc. The bits from (8 to 27) are the length of the secret message

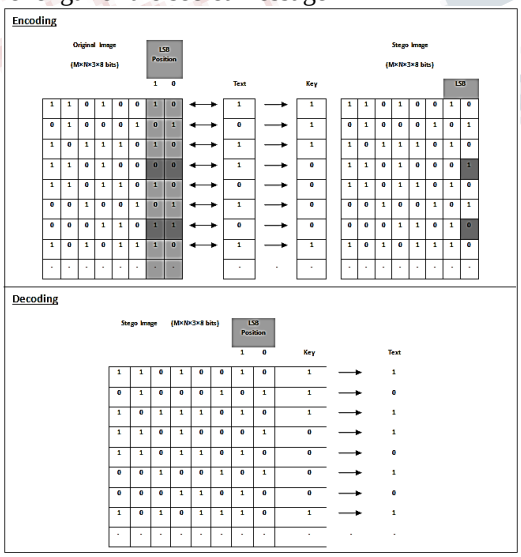

Fig 5: The Encoding and Decoding of the Dynamic Symmetric Key Algorithm.

3.2 Enhancing the Algorithm using Arithmetic Coding

Image Steganography using LSB and dynamic symmetric key using Arithmetic coding algorithm is an enhancing method of the image Steganography using a dynamic symmetric algorithm.
Arithmetic coding is a method to compress the text; it is used here to reduce the size of the secret message. Results obtained from this method are better than the image Steganography using LSB and a dynamic symmetric key.
The size of the secret message after Arithmetic coding process that allowed to be hidden by using this method (LSB+KEY+ARITH) is computed as the following formula:

$$S2 = (M \times N \times 3) - 107 \quad (4.2)$$

Where (S2) is the size of the secret message, (M) is number of rows in the image, (N) is the number of columns in the image, (3) is the number of planes in the colored image, (107) is the number of reserved bits for this algorithm; where the bits from 1 to 7 are of the Steganography type. The bits from 8 to 107 are the length of two variables (A, B, C, D and E) that they are needed for Arithmetic coding compression process.

4. EXPERIMENTAL RESULTS

4.1 The Implementation

An MATLAB program has been developed to implement the algorithms. The program is called (Wa'el-Steganography) relative to the name of the first author of this paper. The images that have been used for implementation the algorithms are colored images (RGB images) of the type (JPEG, PNG, and PMB).
The first time of the implementation of the secret message was one copy of the secret message, the second time of the implementation of the secret message was five copies of the secret message, the third time of the implementation of the secret message was ten copies of the secret message, the fourth time of the implementation of the secret message was fifteen copies of the secret message, the fifth time of the implementation of the secret message was twenty copies of the secret message.

i. Encoding

Petra colored image has been used with size (845×709×3) pixels of type of (JPEG). The secret message that has used is shown in the figure 7. The number of characters of that introduction are (2136) and the number of bits are (14952) bits.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

The following steps explain the encoding process of the (LSB+KEY) algorithm and (LSB+KEY+ARITH) algorithm using the (Wa'el-Steganography) program:

- Pressing on the push button (open image) to choose the Petra image from the bath storage.
- Pressing on the push button (open text) to choose the secret message that is saved as txt file shown in the figure 6. The text also will appear in the text on the program window.
- Opening the Steganography method list to choose the Steganography method (LSB, LSB+KEY or LSB+KEY+ARITH).
- After that, a dialog window will appear to ask the user to save the key. The key is generated from the secret message and the Petra image using the (LSB+KEY) method is shown in the figure 8.
- Then, the stego media will generated and appear in the ego image area.
- Pressing on the push button (Save Stego Image) to save the stego image on the disk.

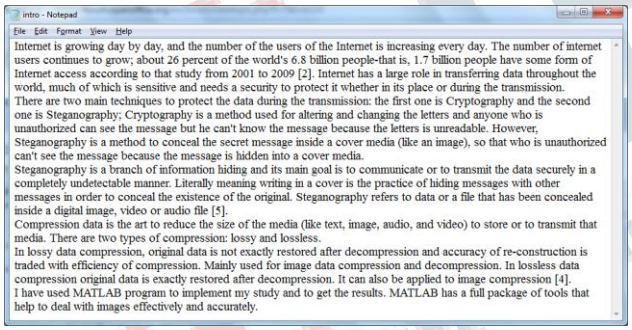

Fig 6: The secret message.

Fig 7: Simulation Results using Matlab GUI (Encoding).

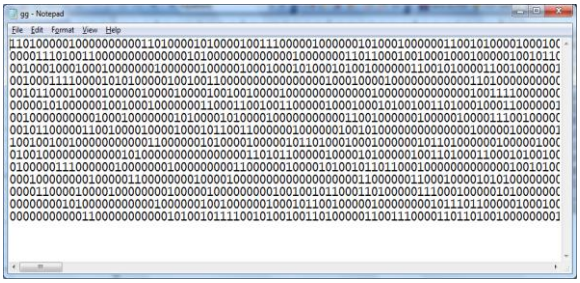

Fig 8: The key.

ii. Decoding

The following steps explain the decoding process of the (LSB+KEY) algorithm and (LSB+KEY+ARITH) algorithm using the (Wa'el Steganography) program that is shown in the figure 9 for decoding process:

- Pressing on the push button (Open Stego Image) to choose the stego image from the bath storage.
- Pressing on the push button (Show). The extraction process will begin to determine which Steganography process has been applied on this image, and hence the data will be extracted from the image.
- Because the stego image that was created depends on the key, dialog window will appear to ask the user to choose the key from the disk storage.
- The user will choose the key fro the disk storage as a text file.
- The extracted data will appear in the text area on the program window.
- The user can save the secret key by clicking on the push button (Save Text) to save it as a text file.

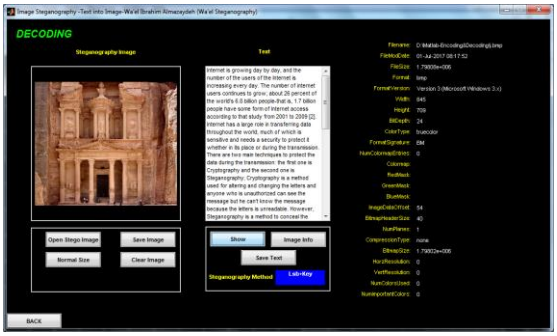

Figure 9: Simulation Results using Matlab GUI (Decoding).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 12, December 2017

4.2 The Results

Figure 6 shows the secret message that has been hidden using the methods: LSB, LSB+KEY and LSB+KEY+ARITH algorithms. Table 4 and Figure 10 shows the results obtained after applying the algorithms.

The maximum size of data (secret message) that can be hidden in this image using the LSB algorithm is:

$$(845 \times 709 \times 3) - 27 = 1797288 \; Bits$$

or

$$1797288 / 7 = 256755 \; Characters$$

The maximum size of data (secret message) that can be hidden in this image using the image Steganography using a dynamic symmetric key algorithm is:

$$(845 \times 709 \times 3) - 27 = 1797288 \; Bits$$

or

$$1797288 / 7 = 256755 \; Characters$$

The maximum size of data (secret message) that can be embedded in this image using the image Steganography using a dynamic symmetric key and Arithmetic coding algorithm after coding process is:

$$(845 \times 709 \times 3) - 107 = 1797315 \; Bits$$

or

$$1797315 / 7 = 256759 \; Charcters$$

Table 4: PSNR values of LSB, LSB+KEYand LSB+ARITH Algorithm.

The number of copies of the secret message	The number of Characters of the secret message	The number of Bits of the secret message	Steganography method		
			(LSB) PSNR	(LSB+KEY) PSNR	(LSB+KEY+ARITH) PSNR
1	2136	14952	71.9532	74.8632	76.5726
5	10680	74760	64.9261	67.932	69.8306
10	21360	149520	61.9287	64.9174	66.9078
15	32040	224280	60.1774	63.1574	65.193
20	42720	299040	58.9292	61.9073	63.942

Figure 10 shows the results (as a chart) for the same values in the table 4.

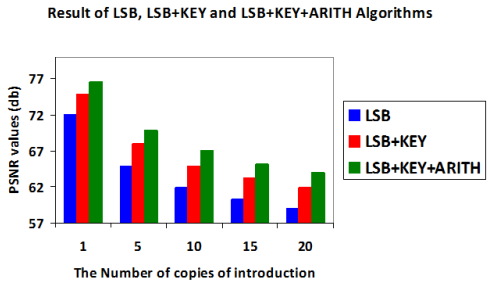

Fig 10: The PSNR of LSB, LSB+Key and LSB+ARITH

5. CONCLUSION

This paper shows a new technique image Steganography that is "Image Steganography using a dynamic symmetric key and arithmetic coding" to hide a secret message in a colored image that is an enhancement technique to the "image steganography using a dynamic symmetric key". This paper also shows and compares the results of the image Steganography to hide a secret message in an image: the first one is the traditional technique that is Least Significant Bit (LSB), the second one is the Least Significant Bit using a dynamic symmetric key (LSB+Key) and the third one is the Least Significant Bit using a dynamic symmetric key and arithmetic coding (LSB+Key+Arith). The performances of the results have been compared using the PSNR values of individual algorithms. It is noted that the enhancing method gives better output from the LSB and LSB+KEY with respect to the PSNR values.

6. REFERENCES

[1] Wa'el Ibrahim A. Al-Mazaydeh. Image Steganography using LSB and LSB+Huffman Code. International Journal of Computer Applications (0975 – 8887), Volume 99– No.5, August 2014.

[2] Wa'el Ibrahim A. Almazaydeh, H. S. Sheshadri. Image Steganography using LSB, LSB+Huffman Code, and LSB+Arithmetic Code. International Journal of Computer Applications (0975 – 8887), Volume 155 – No 11, December 2016.

[3] Prof. H. S. Sheshadri and Wa'el Ibrahim A. Almazaydeh, "Image Steganography using a Dynamic Symmetric Key", 2nd International Conference on Inventive Computation Technologies (ICICT – 2017), organized by RVS Technical campus during August 24-25 2017, IEEE, Coimbatore, India.

[4] Abhishek Koluguri, Sheikh Gouse, Dr. P. Bhaskara Reddy. Text Steganography Methods and its Tools. International Journal of Advanced Scientific and Technical Research, Issue 4 volume 2, March-April 2014, ISSN 2249-9954.

[5] Pramendra Kumar, Vijay Kumar Sharma. Information Security Based on Steganography & Cryptography Techniques: A Review. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014.

[6] Dr. Saad Abdual azize AL_ani, Bilal Sadeq Obaid Obaid. A Steganography Method to Embed Text in Image without Change Structure of Image. INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTER RESEARCH, Volume 3 issue 1 January 2015 Page No.824-828 ISSN :2320-7167.

[7] Siti Dhalila Mohd Satar, Nazirah Abd Hamid, Fatimah Ghazali, Roslinda Muda and Mustafa Mamat. A New Model for Hiding Text in an Image Using Logical Connective. International Journal of Multimedia and Ubiquitous Engineering, Vol.10, No.6 (2015), pp.195-202.

[8] Madhavi V.Kale, Prof. Swati A.Patil. Text Hiding In Multimedia By Huffman Encoding Algorithm Using Steganography. International Journal of Advance Research in Science Management and Technology, Volume 2, Issue 1, January 2016.

[9] Amanjot Kaur, Dr. Bikrampal Kaur. Secure The Secret Information In An Image Using K-MM In Steganography. Journal of Multidisciplinary Engineering Science and Technology (JMEST), ISSN: 3159-0040, Vol. 2 Issue 8, August – 2015.

[10] R Praveen Kumar, V Hemanth, M Shareef. Securing Information Using Sterganoraphy. International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013], IEEE.

[11] Iain E. G. Richardson. H.264 and MPEG-4 Video Compression, The Robert Gordon University, Aberdeen, UK 2003.

[12] Sukhpreet Kaur, Vanita Rani. Designing an Efficient Image Encryption-Compression System using a New HAAR, SYMLET and COIFLET Wavelet Transform. International Journal of Computer Applications (0975 – 8887) Volume 129 – No.15, November2015.

[13] Yun-Te Lin, Chung-Ming Wang, Wei-Sung Chen, Fang-Pang Lin, and Woei Lin. " A Novel Data Hiding Algorithm for High Dynamic Range Images". IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 19, NO. 1, JANUARY 2017.

[14] Dharmesh Mistry, Richa Desai, and Megh Jagad. "Hidden Data Transmission using Image Steganography". International Journal of Computer Applications (0975 – 8887), Volume 130 – No.14, November 2015.

[15] NELS PROVOS AND PETER HONEYMAN. " Hide and Seek: An Introduction to Steganography". IEEE Computer Society, Volume: 99, Issue: 3, May-June 2003.