International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 2 (2020), pp. 345-354
© International Research Publication House. https://dx.doi.org/10.37624/IJERT/13.2.2020.345-354

Digital Colour Image Steganography for PNG Format and Secured Based on Encoding and Clustering

Arshiya Sajid Ansari[1], Mohammad Sajid Mohammadi[2], Syed Sohail Ahmed[3]

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia.

[2]Department of Information Technology, College of Computer Qassim University, Saudi Arabia.

[3]Department of Computer Engineering, College of Computer Qassim University, Saudi Arabia.

*ORCIDs: 0000-0001-5375-0188 (Dr. Arshiya sajid), 0000-0002-3082-5068 (Mr. Sajid),
0000-0001-5489-9099 (Dr Sayed sohail)*

Abstract

Security has become the top priority in any system of computers application, online systems application etc. as millions of users are using Internet. This research paper proposes an algorithm for implementation of Information Security System using PNG (Portable Network Graphics) images. With the best of our knowledge, very few works are there in literature on PNG image steganography domain. Thus proposed algorithm has applied on PNG image with the unique concepts, like data capacity pre-estimation, generated unique key, double encryption of generated key (at hidden location), clustering of cover image and data scattering to embed secret data. The proposed algorithm transfers securely, more than 40 thousand bits on Internet using PNG image. Information can be the any type of data like picture image, video, audio or text in the form of bits. This research provides secure way of information communication and reduces the possibilities of the attack like cropping and brute force attack during transmission over internet. The proposed research will provide better capacity and security as compared to previous PNG image format works. Moreover, comparative results for the proposed algorithm is very promising for PNG cover image format. Steganalyzer tool is also used to check the performance evaluation against cropping and brute force attack.

PSNR (Peak Signal to noise Ratio): PSNR is an visual quality indicator of an image. It shows the perceptible quality for any image in unit decibels (dB). Higher PSNR indicates better quality of stego image. PSNR Value almost 30 to 35 dB or higher indicates the acceptable image quality.

Keywords: Steganography, PNG Image Format, Data Hiding, Security.

I. INTRODUCTION

Information security is a hot topic nowadays. Steganography is an art of secure transmission of messages from a sender to a receiver. It should ensure that nobody should realize the existence of secret message. Only the authorized receivers should extract the secret information. To achieve such target secrecy, the secret message (data/ object file) is concealed in some media (cover media) and send over the network, at destination, the receiver receives this embedded file called stego file (stego process = data + cover media image) where the secret information from cover medium is extracted (unstego process).

When secret data get embedded in cover medium it produces distortion in cover medium which can affect image PSNR. If the visual quality deteriorates it can attract the attention of eavesdroppers. A noise can be avoided by selecting the right intensity choice of pixel. We can insert the data value in the texture of the image or in its edges. Sharp changes in the pixels can visualize the distortion in the cover image. Thus the decision of amount of embedding data is complex. In this work of steganography, we are concentrated our focus on PNG image type only though it can be done on JPEG BMP, TIFF or other mage formats. T Steganography algorithm must fulfil the technical requirements as shown in Figure 1.

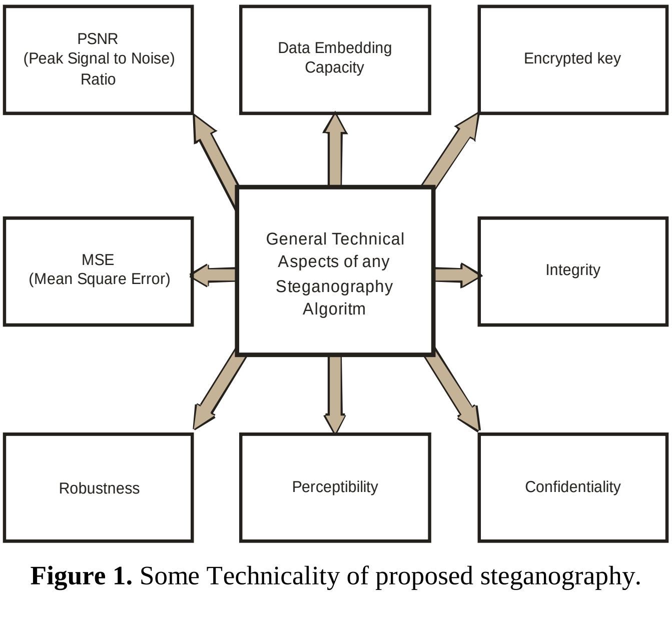


Figure 1. Some Technicality of proposed steganography.

Encrypted Key (Stego key): This key is used for getting back the embedded data at the receiver's side while unstgo the stego image.

Confidentiality: The Stego file must be confidential, only the intended recipient should be able to read the message, others should not be doubtful on it. Its perceptibility (should not attract the eavesdropper attention).

Integrity and robustness: Data must be correct, should remain unchanged in the process of embedding and retrieving from stego file while robustness indicates that stego image must stand hard against of attacks.

MSE (Mean Square Error): It is an error between input original cover image and output Stego images. There exists an inverse relationship between MSE and PSNR metric, lower the MSE value specifies lower difference between input and output images; in our ISS algorithm, we have tried to address

PNG (Portable Network Graphics) is a pallets based file format. PNG stands for Portable Network Graphic, having .png file extension. It is useful when we need small loss less data compression file format to store image repeatedly. As it is a lossless bitmap image format and an open format developed in 1996. It is specially designed for transferring images on Internet to store graphics on website. It does not support animation. For animation support we have APNG image format. Although APNG does not considered as an official PNG extension, APNG is backward compatible to the basic image format. An application program supporting PNG (but not APNG) will be still able to play an APNG file, but, just a single image can be seen, not the full animation completely.

PNG supports number of colours plus variable levels of transparency. PNG supports indexed colour, grey scale and RGB images. It also has 24 bit RGB or 32 bit palette based images RGB colours, grayscale and Full colour based non palette based RGB images. To reduce the size of image, Image Alpha mac tool can be used. We can reduce the size of PNG images up to 11.2:1 compression ratio.

At this point, the following query may come up in the mind of the reader: What is the benefit of having a proposed image Steganography algorithm that works on PNG cover image formats? We can answer this question through the following points (which in turn give the ground for having an algorithm like this proposal).

Having the option to use PNG as cover images provides flexibility and simplicity for the Internet or mobile user to transmit images online.

Capacity of a cover image can vary based on the image format. Based on the data size, network bandwidth and allowable distortions, proposed scheme can adaptively select the best PNG cover image to hide data.

We have used MATLAB software tool for this research work since MATLAB provides simulation environment for doing numerical computations with matrices and vectors and work best with any type of image format. To test the results, colour images from all type of camera and a database named BOSS base ver.1.1 that contains 10,000 pixels' images. A Steganalyzer Ben4D tool shows promising results of our project performance evaluation against attack.

Contribution

Thus, this paper advances the state-of-art in image Steganography in two ways:

- Introducing a unique algorithm (called ISS) that can be used specially on PNG images.
- The concept of clustering and sub clustering are used to embed data bits to enhance security of each location of embedded data, scattering to embed secret data for data hiding.
- Double encryption on shared key (hidden location) which eliminate the chances of bout force attack.
- Data is secure even after Cropping of image i.e. cropping attacks can be handled.
- It is showing promising results when compared with other similar methods on PNG images.

The remaining paper is organized as give here. Section 2 focuses on abstract of literature review from 1999 till now. Section 3 gives the abstract description of the proposed method. Section 4 elaborates the experimental results. Finally, we conclude the work in Section

II. LITERATURE REVIEW

Today's real world Internet steganography is highly prone to attack by cyber-criminal or prisoners. This chapter review, how the Steganography methods has progressed day by day to improve security, how the different authors tried to implement the Steganography for different domain, how can the database be used in the progress of accuracy of results and in ease of the Steganography experimentation analysis process. This section introduces literature of Steganography methods for PNG image formats.

The basic building block of any PNG image excluding first 8 bytes is nothing but *chunk*. [1] These Chunks could be easily detected by human eye, can be tested and can be manipulated by computer programs.

As shown in figure 2 each chunk of PNG block has similar 4 byte length in "Big-endian" format. as with all inter values in PNG stream) a 4-byte chunk type ranging from 0 byte to 2147483647 bytes of data and a CRC value(cyclic redundancy check) of 4-byte long.

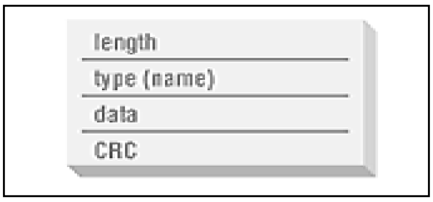


Figure 2. PNG chunk structure

Palette-based images are also called as colour mapped images or indexed-colour images. These images use the PLTE chunk, supported palette entries like 2, 4, 16, or 256 maximum which are based on four different pixel depth bits viz. 1, 2, 4, and 8 bits.

- PNG FORMAT VARIENT TYPES

Palette-Based

Palette-Based with transparency

Grayscale

Grayscale with Transparency

Grayscale with Alpha channel

RGB

RGB with transparency

RGB with Alpha Channel

The Simplest PNG

Figure 3 shows a simplest PNG file.

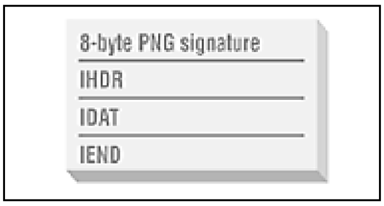


Figure 3. Layout of the simplest PNG.

It is made up of PNG signature of 8 byte size and only three chunk types IHDR Image Header Chunk, IDAT Image Data chunk, and IEND END Of Image chunk. The first chunk is IHDR always that includes all fine details about the image type, its size in height and width, compression, pixel of depth, interlacing method and filtering methods, it has an alpha (transparency) channel or not and also if it is a true colour, grayscale, or colour mapped (palette) image.

We generally hide secrete data in random chunks. This chunk should add before/ after IDAT chunks. IDATA chunk should be uninterrupted as per the standard. Two different methods can be applied to PNG images for hiding the secret massage bits. The embedding can be done in image data of PNG images. The image data mode of embedding provides the high capacity of data hiding but it is more difficult to implement data security. Here in image data mode variety of numbers of bits can be embed in it. For example: a single bit, 2 bits, 3 bits as maximum as up to 7 bits per pixel could cause no visual distortion of PNG image. Another method is to use pallets to hide the secrete data bits. As palette size is less in PNG image, it provides less capacity to store the data bits in it. For example, 256 colour Palette can mix only 210 bytes. If we try to but more than this capacity, it will cause the perceptibility of image to be decree. Encoders can hide the message bits in palettes of PNG by ordering the colours of the palette in some way or the other. Works proposed in [2,3] are based on palette-based PNG images using palette mode operation to insert the data bits. Manipulation operation such opening, updating and saving generally do not disturb the order of colours in PNG image palette based, hence it is robust for steganography; however [4,5,6] presented data mode PNG Steganography for storing secret data. Literature [2-11] reveals that image data mode insertion provides better capacity as compared to data insertion in palette mode.

Table 1. Summary of PNG Stegangraphy Algorithm with Dataset used

Reference / Target Image format	Year	Basic approach	Data used
Oktavianto , B., Purboyo, T. W., & Saputra, R. E[12] / PNG	2017	In this research author has used spectrum method and LSB method for steganography They find the value of RGB pixel by dividing the image in 3x3 pixel blocks first and converting it into binary form to insert characters.	3x3 pixel PNG image & characters data.
Rojali, Salman, A. G., & George.[5] / PNG	2017	Another research presents steganography by the Vigenere Chiper with directory based compression method and LSB method.	18 kb is used as secrete data Flower, Birds and sand images are used.
Wai Wai Zin [4]/PNG	2013	They have used a fusion of BBs (Blum Blum Shub), RC4 algorithm and LSB technique for steganography.	Text has used and secrete message and Water lilies Msg PNG image.
Chen, Yung-Fu et al. [3] /PNG	2009	Here in this research For training the Palette K-means clustering is used and for measuring the distance between pixels Euclidean distance is used.	PNG Images like Baboon, Lena, and Pepper of Size 512×512.
Fridrich Jiri [2] / PNG	1999	They inserted 1 pixel to one bit data. For inserting a bit here closest colour has been chosen in randomly selected pixel with seed and shared key.	"Mandrill" (baboon) image of size 512×512.

III. METHODOLOGY, DESIGN, AND IMPLEMENTATION

All experiments are done using MATLAB software tool to implement this research algorithm. To test the results, colour images from many types of camera and BOSS base database is used.

III.I Functional block diagram of proposed Algorithm

This proposed research algorithm presents new enhanced Information Security System using PNG images. The proposed algorithm provides high data security. We are using PNG image format since it provides better security as compared to BMP format [5].

In this section, we describe our proposed image Steganography algorithm for a PNG Image. Figure 4 shows the functionalities of our method using a block diagram. First, our algorithm reads a cover PNG image and hidden data (say an image also), then it extracts the 'pixels from the IDAT header from the PNG cover image. Without any type conversion, like colour to grayscale or binary, our algorithm can directly work on pixels' data got from PNG IDATA header, to manipulate them.

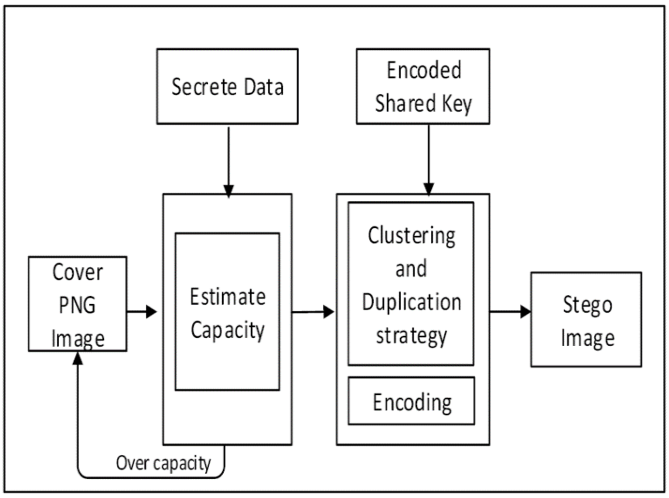


Figure 4. Functional block diagram of proposed algorithm

Data capacity pre-estimation, firstly before start embedding in given image, our algorithm pre-calculate the capacity of given cover image by its row column size and number of cluster and sub-cluster and decide whether given data can be encapsulated in giver cover image or not? if the data is more it will ask for bigger OR another cover image. If cover image has capacity to hide the data based on number of bits it can store. Maximum we can store 5- 6 bits as it would not disturb the image visual quality or perceptibility of image.

III.II Clustering

The concept of clustering and sub clustering ids used to embed data bits to enhance security of each location of data scattering and duplication to embed secret data for data hiding. As shown in Figure 5 some configurable number of bits from every pixel header is extracted to use it as a parameter for a function which generates some values. This generated value is used for address regrouping for all the entries that has same features. All the pixels in same cluster could be geographically scattered as shown Fig. 6. This phenomenal is helping the image to reduce possibilities of attacks. On the other side, clustering is regrouping the pixels with same predefined features and in our case will also be used to store portion of watermark data that has specific criteria which help retrieval and adds robustness of the data hiding process. If we have more uniform distribution of image pixel in cluster more robustness is achieved against attack.

In this paper, this function is taken as simple as concatenating three bits from each. Thus we have address of 9 bits which can address 512 cluster entries in The clustering function clusAdd(x,y,z) should be chosen so as to achieve maximum possible uniform distribution.

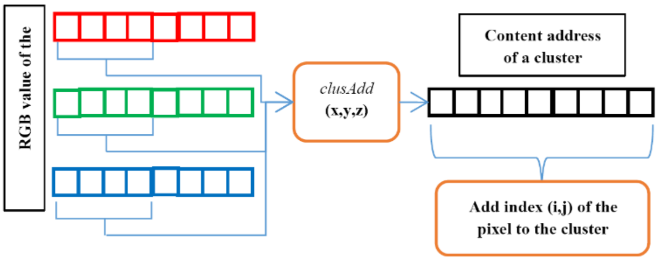

RGB value of the
clusAdd (x,y,z)
Content address of a cluster
Add index (i,j) of the pixel to the cluster

Figure 5. Clustering Method

The clustering processes used for all pixels and create there indexes in cover image. Based on size the cluster is divided into sub clusters. Same portion of secrete data is held by all clusters. is going .

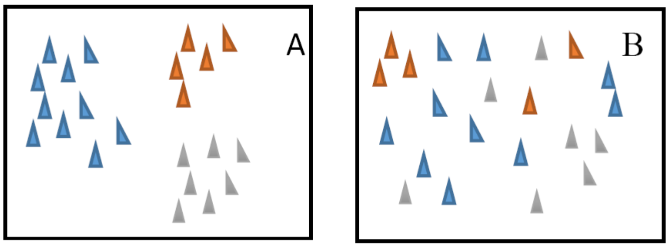
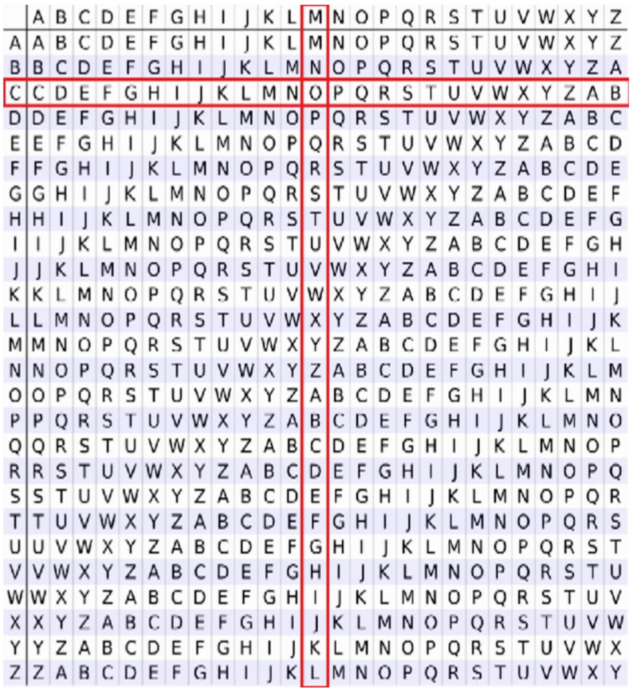


Figure 6. Geographic (A) vs. Dispersal (B) clustering

The Pixel Clustering is studied in details in [13-15]. In the Pixel Clustering, a set of pixels having the same features are declared to be in the same cluster. These features are used to address this group of pixels. In both sender and receiver end a shared key is used to find location or R or G or B of RGB colours of PNG image to hide the data bits. Proposed algorithm then generate a character -set key using randomization function. This key is doubled encrypted using Vigenère cipher technique to make it more secure from the III.III Key encryption and proposed algorithm Vigenère cipher encryption method to provide strong security to our generated key. Mechanism: (Use ASCII or any representation)



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 7. Encryption matrix

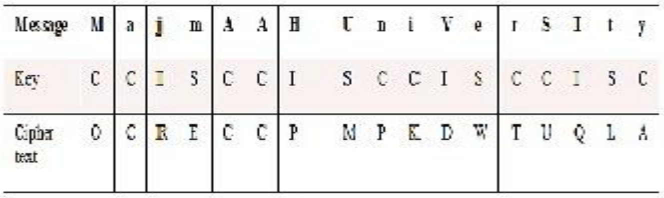
From mono-alphabetic family

- Encryption
    - Key - column
    - Message - row
    - Cipher -cross section
- Decryption
    - Key - column
    - Cipher - cross section
    - Message - row
- Encryption
- Key - **CCIS**
- Cipher text - *Ocreccp Mpkdwtuqla*

Example:

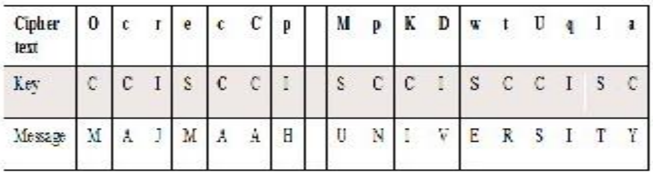
Message - Majmaah University

Table 2. Encryption



Message	M	a	j	m	A	A	H	U	n	i	V	e	r	S	I	t	y
Key	C	C	I	S	C	C	I	S	C	C	I	S	C	C	I	S	C
Cipher text	O	C	R	E	C	C	P	M	P	K	D	W	T	U	Q	L	A

Table 3. Decryption



Cipher text	O	c	r	e	c	C	p		M	p	K	D	w	t	U	q	l	a
Key	C	C	I	S	C	C	I		S	C	C	I	S	C	C	I	S	C
Message	M	A	J	M	A	A	H		U	N	I	V	E	R	S	I	T	Y

Data is embedded using the proposed scheme. The algorithm generates clusters and then sub-clusters and a shared doubled encrypted key. It then stores stego file along with this shared key in these sub clusters in turn clusters. An exactly reverse process is applied to recover data back at the receiver side. Our algorithm supports up to only 24 bit PNG format.

IV. EXPERIMENTAL RESULT ANALYSIS

The performance of the proposed algorithm has experiment and evaluate over different range of input parameters, such as on PSNR (Peak Signal to noise Ratio), MSE (Mean square Error), The correlation coefficient (NC) and Steganalyzer (Ben 4D) tool. For experimentations of this ISS algorithm, we are inserting 1 to 8 numbers of bits per pixel in the block of sub-clusters as shown in table 4. We took secrete data image of solder. It has 15160 bits of data. We tested our algorithm on different PNG cover images of different sizes. All cover images along with their sizes are shown in Figure 8.

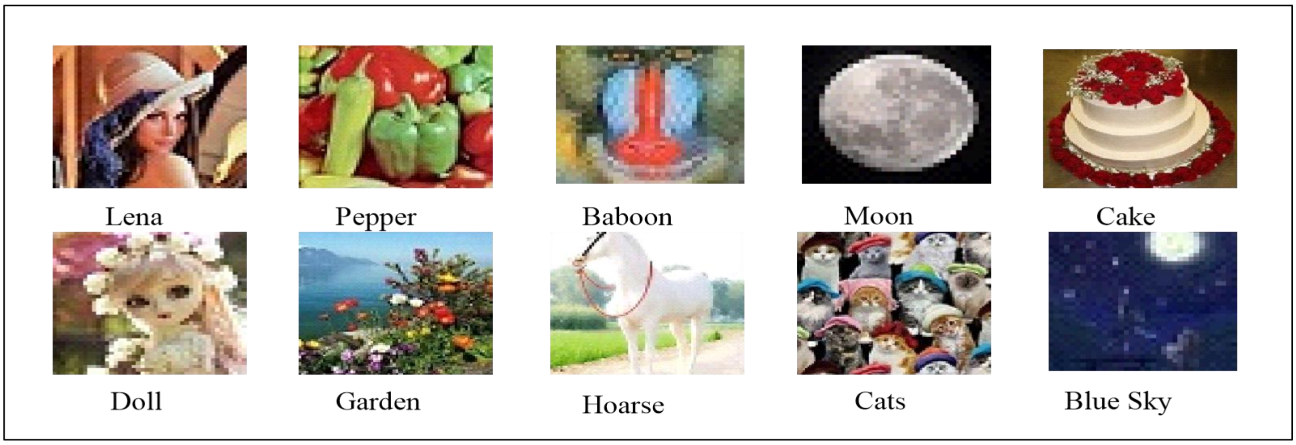


Figure 8. Some example of PNG cover images used in experimentations: Lena, Pepper, Baboon, Moon (512 × 512), Doll and Blue Sky (480 × 480), Garden (544 × 544), Cats (456 × 448).

Algorithm: *Proposed Algorithm*

Input: PNG Cover Image, Secret Data, Shared key.

Output: Secured PNG Stego Image.

```
1.  Begin
2.  Read and calculate the capacity of PNG Cover Image in bits.
3.  Calculate secret image data sizes in bits.
4.  Repeat for each pixel
5.  Generate clusters and sub cluster with error check bit from each pixel data from IDATA header.
6.  Generate the shared key.
7.  Generate first level key generation through randomisation.
8.  Apply Vigenère cipher method as second level encryption on key. 9. Embed the n number of bits in each cluster and sub cluster pixel
10. For each cluster in clusters set:
11. For each block in the cluster:
12. blockEmbedd (scCounter,data,block)
13. Save new values of pixels back into the cluster and sub cluster
14. Embed the encrypted key.
15. End
```

Some are resized to 512 × 512 dimensions while others images are kept as is in size.

For experimentations of proposed algorithm, we have taken soldier image (data length 15160 bits) as a secret data image as shown in figure 9.

Figure 9. Secrete data image of solder to be embed in Lena Pepper and baboon etc. images.

For simplicity, we took only one image 'Garden' as a cover image for illustration purpose here with NC=1(described shortly)

The two important performance measures indicator equations are utilized.

1. The correlation coefficient (NC) given in equation (1) is used to measure the similarities between the embedded and extracted secret data:

$$\mathrm{NC} = \frac{\sum_{x}\sum_{y} osd(x,y)\, esd(x,y)}{\sum_{x}\sum_{y} osd^{2}(x,y)} \qquad (1)$$

   where,

   osd is the actual secret data and *esd* is the extracted secret data.

2. Peak Signal to Noise Ratio (PSNR): It is used to evaluate and find the differences between original image and the cover image. Peak Signal to Noise Ratio (PSNR) indicator is given by Equation (2).

$$\mathrm{PSNR} = 10\log\left(\frac{\max\left(ci^{2}(x,y)\right)}{\frac{1}{MxN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left(ci(x,y)-si(x,y)\right)^{2}}\right) \quad (2)$$

Where *ci* is the cover image and *si* is the stego_image.

Figure 10 shows output stego images of Garden cover image for all possible bit embedding (Biti) where i = 1 to 8. Their corresponding PSNR outputs are shown in Table 4. (With dashed column). If we look at two bits (Bit2) in Table 4 we see that for the same size images Lena, Pepper, and baboon, PSNR are slightly different based on color or other parameters, while the difference in PSNR slightly changes for other images based on their size, edges and fine details. Up to four or five bit (Bit4) or (Bit5), PSNR is in the acceptable range but beyond five bits insertion (Bit4), we can see that value of PSNR starts to decay which is not acceptable.

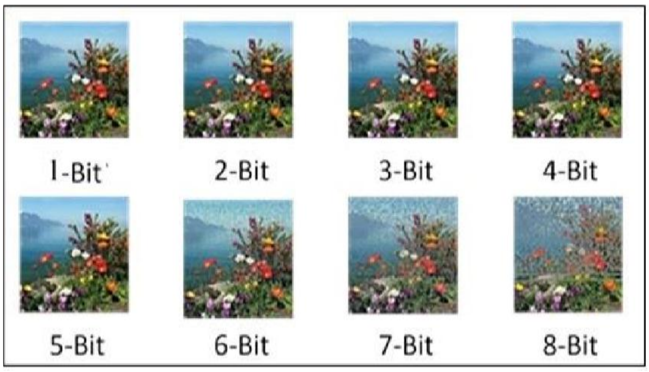


Figure 10. Output results of the ISS Algorithm 'Garden' as the cover image with different bit size insertion.

Table 4. Bit/Bits Insertion Result of algorithm in terms of PSNR for different Images.

No. of bits	**PSNR In (dB)**										
Size / (Bit_i)	Lena 512 **x** 512	Pepper 512 × 512	Baboon 512 × 512	Fruit Plate 512 × 512	Moon 512 × 512	Cake 496 × 536	Doll 480 × 480	Garden 544 × 544	Hoarse 544 × 544	Cats 456 × 448	Blue sky 480 × 480
(Bit_1)	68.45	67.09	67.38	67.38	64.59	64.58	64.87	64.38	64.43	65.00	64.76
(Bit_2)	57.41	57.18	57.39	57.44	57.31	57.30	56.58	57.30	57.18	56.15	56.23
(Bit_3)	51.89	51.89	51.89	51.71	51.90	51.88	51.57	51.60	51.60	51.11	51.32
(Bit_4)	46.28	46.28	46.28	46.31	46.28	46.40	45.53	47.04	47.04	45.72	45.53
(Bit_5)	41.25	41.25	41.25	41.26	41.25	41.40	40.33	42.20	42.20	39.67	40.33
(Bit_6)	36.16	36.16	36.16	36.11	36.16	36.13	35.53	35.93	35.93	34.67	35.53
(Bit_7)	29.80	29.80	29.80	29.31	29.80	29.79	30.07	29.62	29.62	29.84	30.07
(Bit_8)	23.73	23.69	23.69	23.56	23.69	23.67	24.00	23.76	23.76	24.26	24.00

Table 5. PSNR In dB comparison with other methods for PNG images as cover media

Cover Image Size 512×512	Proposed Method		YUNG Method [2]	Fridrich Method [2]	EZ-stego Method [2]
Lena		68.45	36.95	31.28	14.23
Baboon		67.38	35.86	30.64	14.55
Pepper		67.09	34.09	25.98	21.68

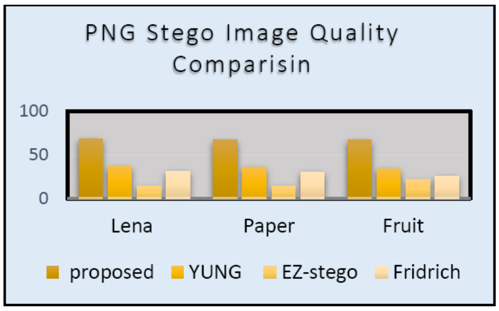


Figure 11. A comparative graph measuring performance in terms of PSNR (PNG images).

Their output stego images are shown in figure 9 (only three images are shown for simplicity).

The proposed research algorithm has been tested over number of colour PNG formats images. Soldier image is used on different images as a payload data as shown in figure 9.

The capacity of every color PNG cover image is different according to colors, size, edges and contrast, and number of cluster found. For the same data length and cover images size Lena, Pepper and baboon PSNR is slightly different based on color or other parameters. The algorithm does not accept any cover image for which data length exceeds expected data.

Table 5 show comparisons of our algorithm results for PNG image format with other methods like CHEN et al. Scheme, EZ-stego and Fridrich Scheme given in [2]. Here also our method outperforms others. With their resultant comparative graph is shown in figure 11.

IV. I Blocks Dispersal Rate and cropping Attack

As proposed in [14-15] for pixels in each cluster, we used the blocks distribution over each cluster in this research as the area covered by the cluster's blocks in the cover image. And we have shown the sub cluster– holding the similar data – dispersal rate (SCDR) in the equation below as the area covered by the sub cluster's blocks throughout the area of each cluster in cover image.

$$\mathrm{SCDR}_c = \frac{\left(x_{max_{sc}} - x_{min_{sc}}\right) * \left(y_{maxs_c} - y_{min_{sc}}\right) * 100}{\left(x_{max_c} - x_{min_c}\right) * \left(y_{max_c} - y_{min_c}\right)}, (3)$$

In Figure 12 the cluster distribution rate of the clusters in Lena with one address value and one LSB bit stripped out is shown.

In Figure 13 number of sub-clusters per cluster in Lena with the exactly same settings is shown.

The Figure 14 provides the SCDR in Lena with the same settings.

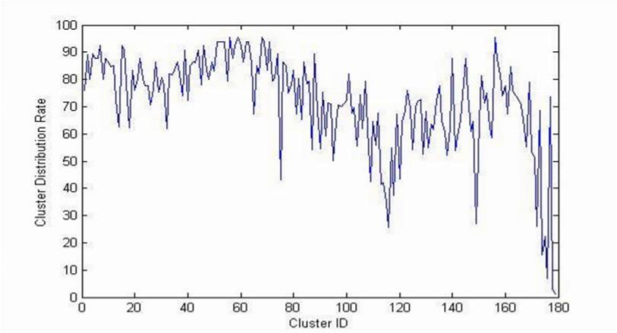


Figure 12. Lena Cluster Distribution Rate

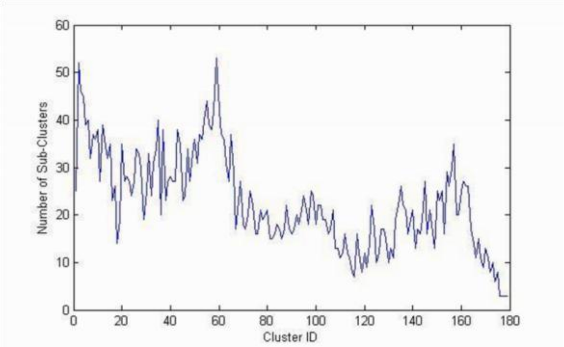


Figure 13. Lena Number of Sub-Clusters per Cluster

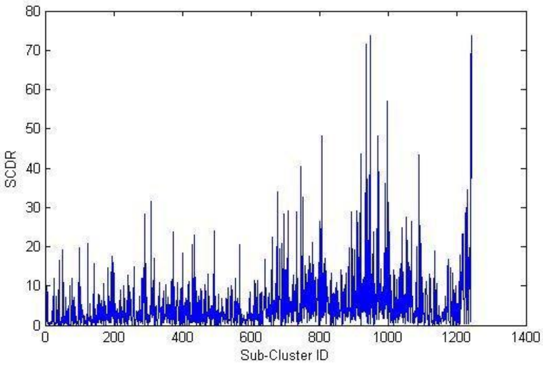


Figure 14. Lena Sub Clusters Dispersal Rate

The sender can run using different settings to choose which is the best image and configuration that may handle the stego data with the best distribution.

The sender finds the best configuration settings and can decide best distribution of data in stego file. These settings could be sent with the encrypted key. The low SDCR valued sub-clusters may not be used depending on data size.

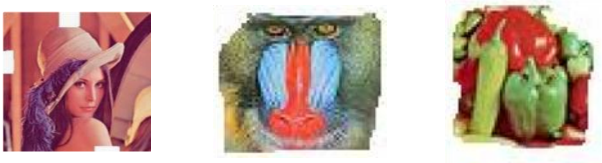


Figure 15. Cropped images

For the images that can hold the stego data or a considerable part of it and without attack, the stego data is extracted without any lose (NC =1).

After embedding the data, the stego image has been cropped as showed in Figure 15. The NC of the extracted data is shown in Table 5 below.

Table 5. NC after cropping

Cropped Image	NC of extracted data
Lena	1
Baboon	0.98
Pepper	0.94

There is no change in the data and it is not affected when using Lena as cover image as because the number of sub-cluster is considerable with high SCDR. The crop may happen in an area that contains entire sub-clusters which may result on lose of that data. Due to that, the sender can decide of using only the sub-clusters that have high SCDR and then report this decision in the transferred double encrypted key.

V. CONCLUSION

The proposed algorithm has use different PNG mages as cover media by utilizing proposed algorithm.

In addition, we have shown concepts like capacity pre-estimation, clustering sub clustering, double encryption and data duplication to embed good amount of secret data. To the best of our knowledge, the proposed algorithm is the first Steganography algorithm that can utilize cover images of PNG format type for embedding high capacity of data and robust against attach. This way, the applicability of the proposed method is much wider that other reported works in this image format domain.

In future work we could do a comparative analysis of Portable Network Graphics (PNG) and Scalable Vector Graphics (SVG) Image Formats for steganography. SVG images format could prove to be a better choice to increase the efficiency of steganography techniques.

ACKNOWLEDGMENT

This work is supported by Scientific Research Deanship of Qassim University Saudi Arabia under the Project ID: COC-2018-1-14-S-3958. The authors are highly thankful of SRD Qassim University for such support.

REFERENCES

[1] www.libpng.org › pub › png › book › chapter08

[2] Fridrich.J, (1999), April.” A new steganographic method for palette-based images”. In PICS pp. 285-289.

[3] Chen, Yung-Fu, Show-Wei Chien, and Hsuan-Hung Lin. (2009),"True colour image Steganography using palette and minimum spanning tree". WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering. Ed. Lifent Xi. No. 3. World Scientific and Engineering Academy and Society.

[4] Zin, Wai. "Message Embedding in PNG File Using LSB Steganographic Technique. November such support. (2013)". International Journal of Science and Research (IJSR) Volume 2.

[5] Rojali, Salman, A. G., & George. (2017, August). "Website-based PNG image steganography using the modified Vigenere Cipher, least significant bit, and dictionary-based compression methods". In AIP Conference Proceedings (Vol. 1867, No. 1, p. 020059). AIP Publishing.

[6] Ansari AS, Mohammadi MS, Parvez MT. A Comparative Study of Recent Steganography Techniques for Multiple Image Formats. International Journal of Computer Network and Information Security. 2019;11(1):11

[7] Ansari AS, Mohammadi MS, Parvez MT. JPEG Image Steganography based on Coefficients Selection and Partition. International Journal of Image, Graphics & Signal Processing. 2017 Jun 1;9(6).

[8] Kumar, Dr. Sushil, (2017). "A TQWT Based Approach for Image Steganography", Mathematical Sciences International Research Journal Vol 6 Issue 1 ISSN 2278 – 8697.

[9] Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez, (2017),"JPEG Image Steganography based on Coefficients Selection and Partition". International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.9, No.6, pp.14-22, 2017.DOI: 10.5815/ijigsp.2017.06.02

[10] Suryawanshi, G.R., and Mali, S.N. (2015). "Study of Effect of DCT Domain Steganography Techniques in Spatial Domain for JPEG Images Steganalysis". International Journal of Computer Applications, 127(6), pp.16-20.

[11] Mishra, R., Mishra, D., Ranjan, A., and Gupta, H. (2015). "A Survey on Secure Image Steganography based on F5 Algorithm". IJEIR, 4(2), pp.344-347.

[12] Kaur, M. and Kaur, G. (2014).” Review of Various Steganalysis Techniques”. (IJCSIT) International Journal of Computer Science and Information Technologies, 5(2).

[13] Ghasemzadeh, H., & Kayvanrad, M. H. (2017).” A Comprehensive Review of Audio Steganalysis Methods”. arXiv preprint arXiv:1701.05611.

[14] Oktavianto, B., Purboyo, T. W., & Saputra, R. E. (2017).” A Proposed Method for Secure Steganography on PNG Image Using Spread Spectrum Method and Modified Encryption”. International Journal of Applied Engineering Research, 12(21), 10570-10576.

[15] Ansari AS, Mohammadi MS, Uthman, MT “Digital colour image steganography for nonspecific format and secured based on Clustering.” IJCSNS International Journal of Computer Science and Network Security, VOL.19 No.4, April 2019.

[16] M.T. Ben Othman, CAM-based Digital Image Watermarking Revisited, WSEAS Transactions on Systems 07/2014, vol. 13, pp. 510-519.

[17] M.T. Ben Othman, New Image Watermarking Scheme based on Image Content Addressing Method, 13th WSEAS International Conference on Applied Computer and Applied Computational Science ACACOS'14, Kuala Lumpur, Malaysia, April 23-25, 2014.

[18] Mohamed TB. Novel image clustering based on image features for robust reversible data hiding. International Journal of Fuzzy Systems and Advanced Applications. 2015:1-8.

[19] Li B, Wang M, Li X, Tan S, Huang J. A strategy of clustering modification directions in spatial image steganography. IEEE Transactions on Information Forensics and Security. 2015 Sep;10(9):1905-17.

AUTHORS' PROFILE

Dr. Arshiya Sajid Ansari has received her B.E degree in Computer Technology from the Yashwantrao Chavan College of Engineering, Nagpur University, India and M. Tech. in Computer Engineering from the NMIMS University, Vile Parle Mumbai, India. She has completed her Ph.D. from Noida International University NCR Delhi Noida, India. She has 12 years of experience in teaching field. Her research areas of interests are image processing and data warehousing. She is a lifetime member of ISTE.

Mr. M. Sajid Mohammadi has completed his B.E degree in Computer Technology from the Yashwantrao Chavan College of Engineering, Nagpur University, India. He did his M. Tech.Computer Engineering from the NMIMS University, Vile Parle Mumbai, India. He is pursuing his Ph.D. from Noida International University NCR Delhi, India. He has total 16 years of experience including 1.5 years' industrial experience in Reliance Petroleum Mumbai and 14.5 years of teaching experience. He is currently working as Lecturer in Computer Engineering Department, Qassim University Saudi Arabia. His research interest includes Image Processing, Information Hiding, and Information/Network Security. He was a member of Saudi Internet Scientific Society for the year 2017-18.

Dr. Syed Sohail Ahmed received the BS and MS degrees in computer engineering from University of Engineering & Technology (UET) Taxila, Pakistan, in 2005 and 2007, respectively. He completed his Ph.D. from University of Sydney (CSIRO). He has 14 years of experience in teaching field. His research areas of interests are signal processing and Wireless networks. He is a lifetime member of PEC.