RESEARCH ARTICLE OPEN ACCESS

Enhancement the Security and Efficiency of Video Steganography Using Frame Selection, Data Compression and Encryption

Hasan Milad [1], Ola Haydar [2], Ali Diab [3]

[1] M.Sc., Department of Computer and Control Engineering, University of Albaath,
[2] M.Sc., Department of Computer and Control Engineering, University of Tishreen,
[3] M.Sc., Department of Computer and Control Engineering, University of Albaath - Syria

ABSTRACT

In recent times, the importance of digital communication over the Internet has increased rapidly. Accordingly, data security becomes a vital issue, as there are many hackers who want to access others' private data and steal or modify it. Hence, hiding information appeared as a way to hide the existence of secret data within another cover. This cover could be an image, audio, and video. Using the video as a cover to hide secret data is safer against hacker attacks compared to other multimedia due to its relative complexity compared to other types and because of the redundancy of data that allows it to be included in a large amount of secret data in addition to the fact that video streaming over the Internet is very common over the Internet and therefore it is unlikely that Be suspicious of hackers.

This paper offers three levels of security: compression, encryption, and steganography. In this search, a colour or grayscale image can be hidden within a video. At first, the secret image is compressed using an algorithm Deflate, the header information is encrypted and then the header always is hidden in first frame and the secret data are hidden into the selected number of video frames after finding an optimal algorithm to find the best frames for hiding. Therefore, there is an extra safe. Thus, reduces the chance of the hidden message being detected. Which offer the best ratio MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) Comparison with other research.

Keywords — Video Steganography, Deflate, LSB, Robustness, MSE, and PSNR.

I. INTRODUCTION

Steganography is a process that involves hiding what is important Information (secret information) inside the data (cover) to protect the message from unauthorized users. Mixed data (secret information and the cover) which called as “Stego Objects” will see the human visual system (HVS) as single piece of data because HVS will not be able Find out that there is a small change to your cover data. This cover could be any type of data format such as text, audio, image and video[1].

Any successful steganography system must consider three very important criteria: imperceptibility, capacity, Robustness[1].

- **capacity**:

The amount of secret data that can be hidden into the cover without affecting on it.

- **Imperceptibility**:

To reach high embedding efficiency, we need to have a low modification rate in the jacket and high quality of

The cover data. When information hiding is unrecognizable, this reduces the attacker's chance of finding the hidden data. This can be adjusted by measuring the MSE and PSNR values.

However, any distortion of the cover data after the embedding process will increase the attention of the attackers. In traditional steganography, capacity and non-perception clash. Increasing the capacity of confidential data will reduce the quality of the Stego videos, which then weaken the lack of awareness. Both factors should be considered. Decisive factors depend on the steganography algorithm and user requirements.

- **Robustness**

The steganography is robust when the receiver can

extract the secret data from the cover correctly without any distortion or lack of data. Therefore, this factor measures the ability of the algorithm to resist attacks and process signals that could be noise signals, filters, or compression[2].

II. STEGANOGRAPHY VS ENCRYPTION

In general, security systems are consisting of cryptography and information hiding as shown in Fig. 1

At first we should we should note the basic difference between Steganography and cryptography is the art of hiding the existence of data by embedded it into other cover, but cryptography is another word for "coding”, it is just to turn it into an indecipherable message using a secret code. To improve the security of information system, Steganography and encryption can be combined.

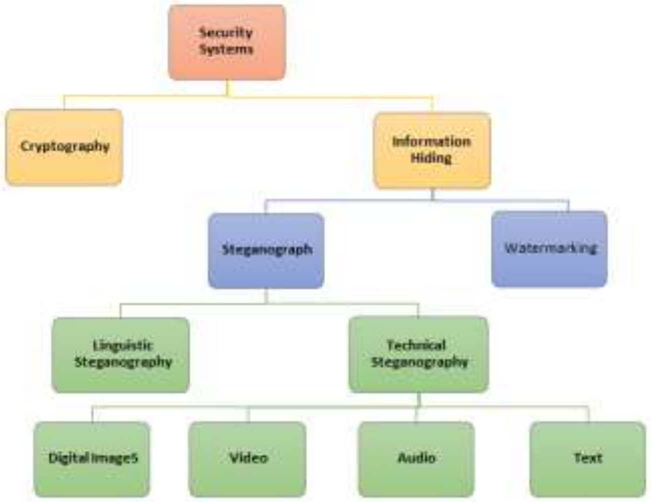

Fig. 1 Disciplines of system systems

PROPOSED METHOD AND DESIGN

The proposed method is presented by two stages, the first stage is to embed the secret image after compressed it into a video, and the second stage is to extract the secret image from the video to ensure that the process is going true and finally we will calculate the MSE, PSNR.

A. *Embedding Stage*

RGB image (secret image) will be hidden in a video(.avi), starting hiding at Hidden Key which is a position that sender choose it at the begin of the programme. Fig. 2 depicts the flow diagram for proposed embedding stage.

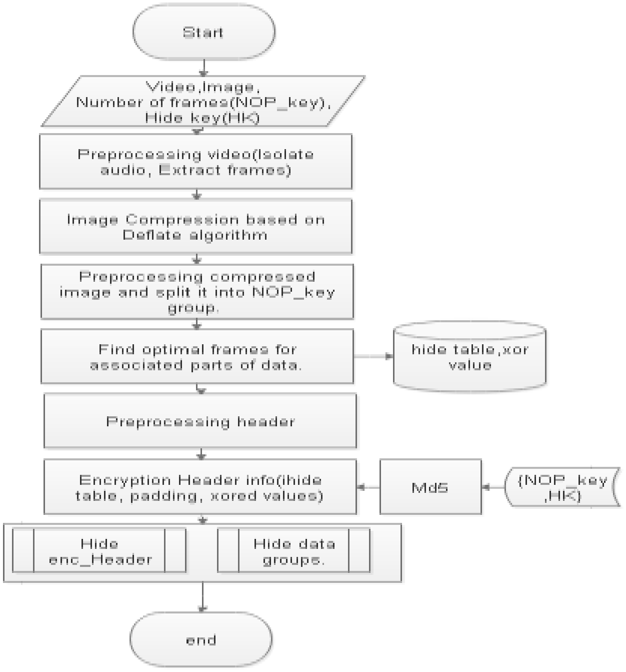
Start
Video,Image, Number of frames(NOP_key), Hide key(HK)
Preprocessing video(Isolate audio, Extract frames)
Image Compression based on Deflate algorithm
Preprocessing compressed image and split it into NOP_key group.
Find optimal frames for associated parts of data.
hide table,xor value
Preprocessing header
Encryption Header info(hide table, padding, xored values)
Md5
(NOP_key ,HK)
Hide enc_Header
Hide data groups.
end

Fig. 2 flow diagram for proposed embedding stage

1) ***Inputs:***

We enter the image, the video to be hidden with and the keys values:

- Key that determines where to start hiding data in frame.
- Key that determines the number of frames that will be used to hide within.

2) ***Pre-processing video:***

In this stage will be isolate audio and extract video frames.

3) ***Compression image:***

The secret image will be compressed by deflate algorithm. This algorithm shown in Fig. 3.

Deflate is two-stage lossless data compression algorithm that uses the combination of LZ77 and Huffman coding. This will take advantage of both the algorithms. It is a popular compression method that was originally used in the well- known Zip and Gzip software and has since been adopted by many applications [6][3].

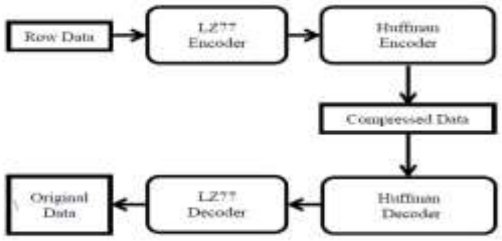

Fig. 3 Deflate algorithm

4) ***Pre-processing compressed image:***

After compression is completed, the output (compressed image) is processed and converted to binary in respect to become divisible by the number of frames, which entered.

5) ***Find optimal frames for Hiding:***

We will find the optimal frames to hide each group of data, through calculating P(F1), the probability of appearing the bit [1] in the pixels that will be hidden by, starting from the hide key value, as well as calculating P(G1), the probability of bit [1] in each of the data group separately in the secret compressed image. These values will be arranged in descending order, as shown in Table 1, 2.

For example:

- Data length=1000.
- Number of parts/frames (NOP) =5.

- Hide Key (HK) = 20

Each group consists of 200 bits. As shown in Table 1 and

TABLE I

FINDING OPTIMAL FRAMES FOR HIDING STEP 1

Frame number.	Sum LSB in frames from 2 to last starting from HK (SUM_1F).	Sorted SUM_1F.	Index of sorted frames. (Index_F)	Portability of ones in each frame. P(G1)	Sum LSB In each group (SUM_1G).	Sorted SUM_1G.	Index of sorted Groups (Index_G)	Portability of ones in each frame. (P(F1))
2	10	195	8	0.975	80	200	4	1
3	160	190	7	0.95	20	170	6	0.85
4	30	160	3	0.8	140	140	3	0.7
5	90	150	6	0.75	200	90	5	0.45
6	150	90	5	0.45	99	80	1	0.4
7	190	30	4	0.15	170	20	2	0.1
8	195	10	2	0.05	3	3	7	0.015

We perform comparison between portability of bit [1] for **nop**(entered key) frames and portability of bit [1] for groups.

TABLE II

SELECTING OPTIMAL FRAMES FOE HIDING AND GENERATE HIDE-TABLE STEP 2

Hide_table				Xorvalue	
Index_F	**a=P(F1)**	**Index_G**	**b=P(G1)**	**a>.5&b<.5 or <.5&b>.5**	
8	0.975	4	1	0	
7	0.95	6	0.85	0	
3	0.8	3	0.7	0	
6	0.75	5	0.45	1	Reduce difference.
5	0.45	1	0.4	0	

6) *Pre-processing Header:*

Convert header into stream of bits.

7) *Encryption Header information:*

The data is encrypted depending on the key generated by the md5 algorithm, which gives a different encryption key with the slightest change in the input represented by the values of the two local keys. Thus, any small change in income is equivalent to a very large change in the output, so the attacker would not be able to penetrate the system if he entered a hidden key close to the original key.

The encryption is performed using xor.

8) *Hiding the Header's data:*

Hiding the encrypted header always in first video frame starting with hide key(HK).

9) *Hiding the secret data:*

Hiding the encrypted header and the secret data groups using the LSB.

B. *Extraction stage*

The extraction stage is the reverse of the embedding stage as shown in Fig. 4.

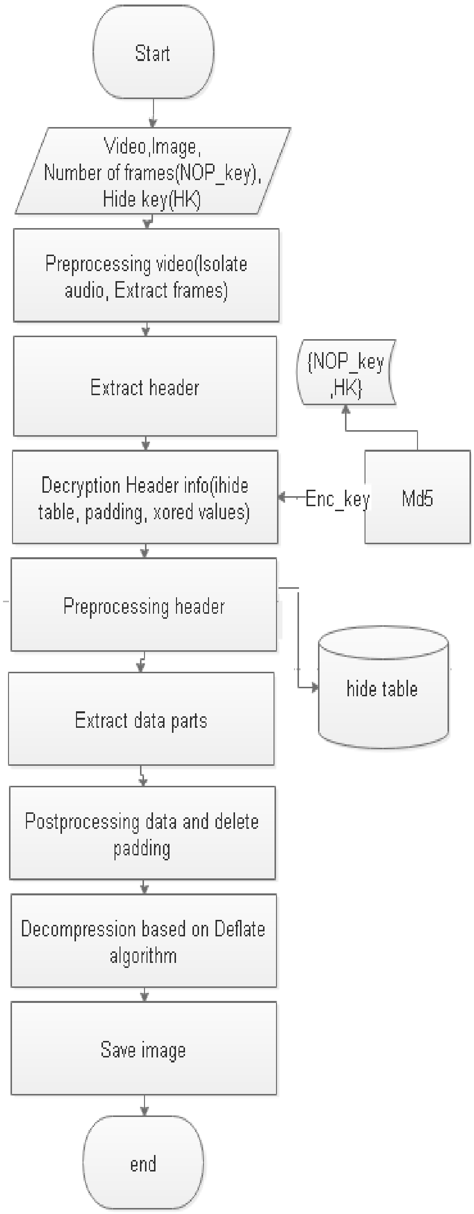
Start
Video,Image,
Number of frames(NOP_key),
Hide key(HK)
Preprocessing video(Isolate audio, Extract frames)
Extract header
{NOP_key ,HK}
Decryption Header info(ihide table, padding, xored values)
Enc_key
Md5
Preprocessing header
hide table
Extract data parts
Postprocessing data and delete padding
Decompression based on Deflate algorithm
Save image
end

Fig. 4 flow diagram for proposed extraction stage

III. EXPERIMENTAL RESULTS AND ANALYSIS

Some experiments are carried out to prove the efficiency of the proposed method where simulation is done on Matlab 2015; video (.avi) is used as the cover video to hide an RGB image to form the stego-video. With the experimental study, we noticed that the visual differences between the original cover frames and stego frames are hardly detected with naked eyes. In addition, by noticing the histograms for original cover frames and stego frames, there is not a visual difference between them, as shown as in Fig. 5 and Fig. 6.

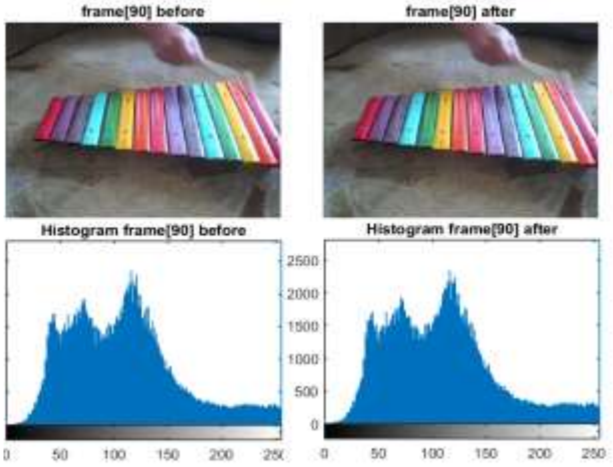

Fig. 5 frame90 and its histogram before embedded and after (Lena)

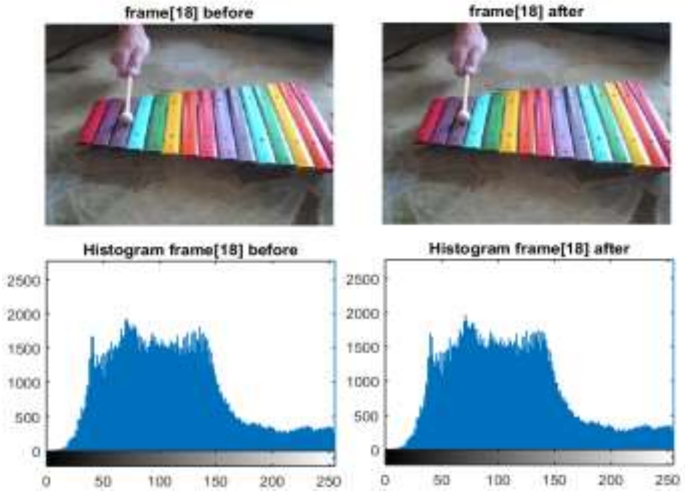

Fig. 6 frame18 and its histogram before embedded and after (Lena)

MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) [4] are two common quality measurements to detect the difference between the cover video and the stego-video.

MSE is the averaged pixel-by-pixel squared difference between the cover- video and the stego-video.

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{h}[C(i,j,k)-S(i,j,k)]^2}{m \times n \times h}$$

$$\mathrm{PSNR} = 10 * Log_{10}\left(\frac{MAX_C^{\,2}}{MSE}\right)\ (dB)$$

C, S represent carrier and stego-frame respectively and both m and n indicate the frame resolutions, and h represents the RGB colours (k = 1, 2, and 3).

Following Table 3 presents the information of used video.

TABLE III

THE INFORMATION OF USED VIDEO

Image	Frame Dimensions	Number of frames(max)
drop.avi	256*240	153
flame.avi	256*240	80
xylophone.avi	320*240	141

Following Table 4 presents the information of images.

TABLE IV

THE INFORMATION OF USED IMAGES

Secret Image		Image Dimensions	Size(KB)
Colored	Barbara.png	512*512	31.5
	Lena.png	512*512	500
	Baboon.png	512*512	55.4
	Peppers.png	512*512	32
	Airplane.png	512*512	27.2
	Clock.png	768*1024	62.5
Grayscale	Cameraman.png	64*64	2.65
	Cameraman.png	128*128	7.39
	Cameraman.png	158*158	10.5
	Cameraman.png	256*256	37.8

Following Table 5 presents the values of MSE and PSNR when hiding different RGB images in a video (.avi),

Table 6 presents the values of MSE and PSNR when hiding different Grayscales images in a video (.avi).

We notice that the results are very convenient, and this refers to the success of the proposed method.

TABLE V

COMPARISON OF MSE, PSNR VALUES IN COVER FRAMES VIDEO AND STEGO FRAMES VIDEO USING COLORED IMAGES

Video	Colored Secret Image (512*512)	Proposed Work	
		MSE (avg)	PSNR (avg)
Xylophone.avi (NOP=max-1, HK=1)	Barbara	0.0705	62.427
	Lena	0.0398	62.188
	Baboon	0.0447	61.689
	Peppers	0.0345	62.812
	Airplane	0.03	63.416
	Clock	0.704	59.725
drop.avi (NOP=max-1, HK=1)	Barbara	0.0424	61.908
	Lena	0.0448	61.665
	Baboon	0.0505	61.153
	Peppers	0.0386	62.312
	Airplane	0.0332	62.955
	Clock	0.0803	59.152
flame.avi (NOP=max-1, HK=1)	Barbara	0.0815	59.183
	Lena	0.0862	58.949
	Baboon	0.0987	58.363
	Peppers	0.0748	59.551
	Airplane	0.0635	60.134
	Clock	0.1534	56.472

TABLE IV

COMPARISON OF MSE, PSNR VALUES IN COVER FRAMES VIDEO AND STEGO FRAMES VIDEO USING GRAYSCALES IMAGES

Video	Grayscale Secret Image (512*512)	Proposed Work	
		MSE (avg)	PSNR (avg)
Xylophone.avi (NOP=max-1, HK=1)	Barbara	0.0158	66.191
	Lena	0.0131	66.991
	Baboon	0.0146	66.532
	Peppers	0.0109	67.8
	Airplane	0.0097	68.279
	Clock	0.023	64.568
drop.avi (NOP=max-1, HK=1)	Barbara	0.0145	66.529
	Lena	0.0152	66.344
	Baboon	0.0168	65.893
	Peppers	0.0126	67.15
	Airplane	0.0113	67.61
	Clock	0.0257	64.069
flame.avi (NOP=max-1, HK=1)	Barbara	0.0305	63.406
	Lena	0.0318	63.225
	Baboon	0.035	62.809
	Peppers	0.0265	64.009
	Airplane	0.0238	64.466
	Clock	0.0507	59.725

Table 7, Fig. 7, 8 present the values of MSE and PSNR when the size of embedded image increases. It is noticed that the reduction in PSNR is very slight as compared with the increases in the size of embedded image; this suggests that the quality of the cover frames remains almost constant when the size of embedded image increases. Therefore, the proposed method has been shown a good performance.

TABLE VI

MSE AND PSNR VALUES OF STEGO VIDEO WITH INCREASING PAYLOAD

Amount of Data Embedded or Payload (graysclae)	MSE (avg)	PSNR (avg)
Camera man 64*64	0.0002	84.343
Camera man 128*128	0.0009	78.605
Camera man 158*158	0.0013	77.118
Camera man 256*256	0.0031	73.207

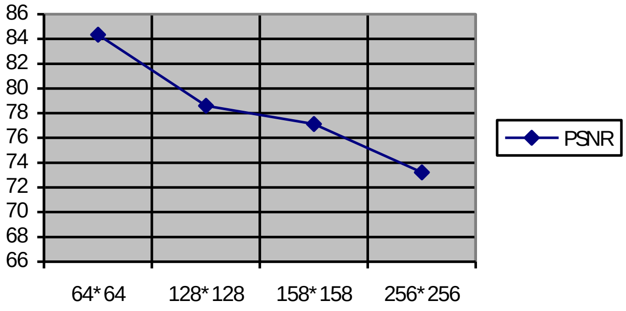

FIG. 7 PSNR VALUES of Stego video with increasing payload

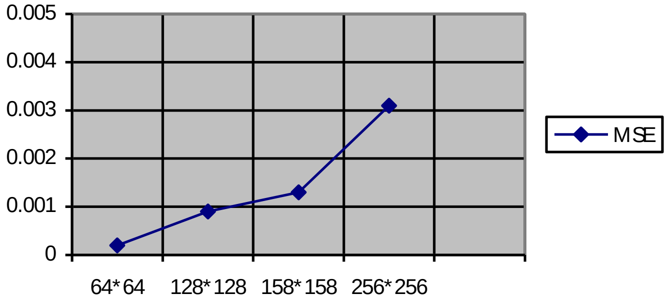

Fig. 8 MSE values of Stego video with increasing payload

We compared the previous studies[5], that hide text in video and where it compare his results with the results of spatial domain method, as it shown in Table 8 and in Table 9 comparison between two study[6] HLSB and LSB. Compared to results which are obtained the proposed method improved the results significantly,

TABLE VIII

COMPARISON OF MSE, PSNR VALUES OF PREVIOUS STUDY

Video	PSNR (spatial domain method)	MSE (spatial Domain method)	PSNR [5]	MSE [5]
Drop.avi	44.34	0.34	54.39	0.236
flame.avi	42.66	0.34	60.21	0.061

TABLE IX

COMPARISON OF MSE, PSNR VALUES FOR PREVIOUS STUDY (HLSB AND LSB)

	HLSB		LSB		
Video	PSNR	Avg. MSE	PSNR	Avg. MSE	Secret Message 640*480
Drop.avi	44.34	0.34	48.65	0.42	
American footbal	45.67	0.34	52.34	0.52	
Flame.avi	42.66	0.34	48.56	0.38	

IV. CONCLUSION

In this paper, steganography algorithm is improved a aimed at hide the colored or grayscale image into a video. Our system provides three levels of security: compression, encryption and steganography, the results show that the human visual system (HVS) will not be able Find out that there is any small change to cover video, the proposed method gives very good PSNR and MSE values.

For future work, we will study providing a video steganography algorithm that focuses on special parts of the video as carrier for data hiding instead of using entire video. Such a method will lead to enhance the quality of steganograms and the resistance against attacks.

Design video steganography algorithm that find optimal frames to hide in using artificial neural networks.

REFERENCES

[1] R. J. Mstafa and K. M. Elleithy, “Compressed and raw video steganography techniques: a comprehensive survey and analysis,” *Multimed. Tools Appl.*, vol. 76, no. 20, pp. 21749–21786, 2017, doi: 10.1007/s11042-016-4055-1.

[2] R. J. Mstafa, K. M. Elleithy, and E. Abdelfattah, “Video steganography techniques: Taxonomy, challenges, and future directions,” *2017 IEEE Long Isl. Syst. Appl. Technol. Conf. LISAT 2017*, 2017, doi: 10.1109/LISAT.2017.8001965.

[3] O. Haydar and K. Aboukassem, “Enhancement the Efficiency of Data Hiding Using Data Compression and Dividing Data,” *IJCST*, vol. 7, no. 4, pp. 84–88, 2019.

[4] Y. He, G. Yang, and N. Zhu, “A real-time dual watermarking algorithm of H.264/AVC video stream for video-on-demand service,” *AEU - Int. J. Electron. Commun.*, vol. 66, no. 4, pp. 305–312, 2012, doi: 10.1016/j.aeue.2011.08.007.

[5] C. Science, C. Science, and C. Science, “Data Hiding Using Video Steganography -A Survey,” vol. 5, no. 6, pp. 206–213, 2015.

[6] K. Dasgupta, J. K. Mandal, and P. Dutta, “Hash Based Least Significant Bit Technique for Video Steganography(Hlsb),” *Int. J. Secur. Priv. Trust Manag. (IJSPTM)*, vol. 1, no. 2, pp. 1–11, 2012, doi: 10.5121/ijsptm.2012.2201.

[7] Amit JainKamaljitI Lakhtaria, "COMPARATIVE STUDY OF DICTIONARY BASED COMPRESSION ALGORITHMS ON TEXT DATA", International Journal of Computer Engineering and Applications. Issue II, May 14, Vol. VI.

[8] Rupali Bhardwaj and Vaishali Sharma, “Image Steganography Based on Complemented Message and Inverted bit LSB Substitution”, Procedia Computer Science, Vol.93, 2016

[9] 3hyrki AlakuijalaEvgeniiKliuchnikov, Zoltan Szabadka, and Lode Vandevenne "Comparison of Brotli, Deflate, Zopfli, LZMA, LZHAM and Bzip2 Compression Algorithms"．Google Inc． 2015

[10] Dalvir KaurKamaljeetKaur, "Analysis of Lossless Data Compression Techniques", International Journal of Computational Engineering Research．Issue 4，2013，Vol. 03．

[11] GOELRANA,KAUR,M "A Review of Comparison Techniques of Image Steganography"． IOSR Journal of Electrical and Electronics Engineering． Issue 1，2013，Vol. 6．

[12] Mohammed Al-lahamIbrahiemM. M. El Emary, "Comparative Study between Various Algorithms of Data Compression Techniques", IJCSNS International Journal of Computer Science and Network Security．No.4，April 2007，Vol. 7．

[13] Pratiksha SethiV.Kapoor“A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography” ． International Conference on Computational Science． Issue 5，2017，Vol. 5．

[14] Prithwish DasSupriyoRay and Atanu Das, "An Efficient Embedding Technique in Image Steganography Using Lucas Sequence", Modern Education and Computer Sience MECS． No.09，8 September 2017，Vol. 09.

[15] Gaurav , “A New Method for Image Steganography Using LSB and MSB”, International Journal of Recent Research Aspects, Vol. 2, Issue 4, 2015.

[16] SinghAmritpalSingh and Harpal, "An Improved LSB based Image Steganography Technique for RGB Images, IEEE,2015.

[17] Sushil Sharma and Ishpreet Singh Virk, “Image Steganography using Two’s Complement”, International Journal of Computer Applications, Vol.145, No.10, 2016

[18] Biswajita Datta, Upasana Mukherjee and Samir Kumar Bandyopadhyay, “LSB Layer Independent Robust Steganography using Binary Addition”, Procedia Computer Science, Vol.85, 2016

[19] Orooba Ismaeel Ibraheem Al-Farraji, “NEW TECHNIQUE OF STEGANOGRAPHY BASED ON LOCATIONS OF LSB”, International Journal of Information Research and Review, Vol. 04, Issue 1, 2017.

[20] Prithwish Das, Supriyo Ray and Atanu Das, “An Efficient Embedding Technique in Image Steganography Using Lucas Sequence”, Vol.09, No.09, 2017.

[21] Bhoomika Parmar, Rakesh Kumar, “High PSNR Based Image Steganography”, International Journal on Recent and Innovation Trends in Computing and Communication, Vol.5, Issue 10, 2017.

[22] Ashwini W, Nagraj Kyasa, “The Improved Image Steganography with Encryption Method and to Overcome the Compression Technique”, International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 5, 2017.

[23] Pratiksha Sethi, V. Kapoor, “A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography”, International Conference on Computational Science, 2016.