Enhancing PIGPEN Image Steganography Method by using Zigzag scanning

Abdelmgeid A. A.[1], Bahgat A. A.[2], Al-Hussien Seddik Saad[3], Maha Mohamed Gomaa[4]

ABSTRACT

Steganography is the art and science of writing hidden messages in such a way that no one suspects the existence of the message, a form of security through obscurity. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. In this paper explains the PIGPEN image steganography technique which modifies the secret message itself not the technique of embedding. This technique represents the secret message characters by two decimal digits only not three decimal digits as ASCII encoding. So, it can save one third of the required space for embedding the message in an image. The PIGPEN technique will be enhanced by using the zigzag scanning to increase the security and achieves higher visual quality as indicated by the high peak signal-to-noise ratio (PSNR) in spite of hiding a large number of secret bits in the image.

Keywords: Steganography, Peak Signal-to-Noise Ratio (PSNR), Maximum Hiding Capacity (MHC), Least Significant Bit (LSB), PIGPEN, Zigzag scanning.

1. INTRODUCTION

Since the rise of the internet, one of the most important factors of information technology and communication has been the security of information [1]. By using steganography the security of the information can be accomplished.

The basic steganography system is the compression result of two algorithms, one for embedding and one for extracting. The embedding process is concerned with hiding a secret message in a cover object. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end [2].

The idea of information hiding is not new to history. As early as in ancient Greece there were attempts to hide a message in trusted media to deliver it across the enemy territory. In ancient time, secret information is hidden in the back of wax that covered tablets, scalp of the slaves etc. In the modern world of digital communication, there are several techniques used for hiding information in any medium. The word ‘steganography’ was derived from two Greek words: steganos, which means covered and graphein, which means writing and often refers to secret writing or data hiding [3].

In fact, there are two techniques for concealing the secret message, one is steganography and another is cryptography. Cryptography aims to secure communications by changing the data into a form that an eavesdropper cannot understand which called the cipher text, while steganography techniques on the other hand, tend to hide the existence of the message itself which makes it difficult for an observer to figure out where the message is. In some cases, sending encrypted information may draw attention, while invisible information won't

[4]. The ultimate aim of cryptography and steganography is to make communication secure so it can be said that they are complimentary to each other [18].

There are three steganographic systems [5]:

1. **Pure steganography system**: this technique uses the steganography method only without any other methods.

2. **Secret key steganography system**: this technique uses the secret key cryptography to encrypt the secret message first and then use steganography to hide it within cover object.

3. **Public key steganography system**: also this technique uses the public key cryptography instead of a secret key.

The major objective of steganography is to prevent some unintended observer from stealing or destroying the confidential information. There are some factors to be considered when designing a steganography system:

- **Invisibility**: Invisibility is the ability to be unnoticed by the human.

- **Security**: Even if an attacker realizes the existence of the information in the stego object it should be impossible for the attacker to detect the information.

- **Capacity**: The amount of information that can be hidden relative to the size of the cover object without deteriorating the quality of the cover object.

- **Robustness**: It is the ability of the stego to withstand manipulations such as filtering, cropping, rotation, compression etc. [6].

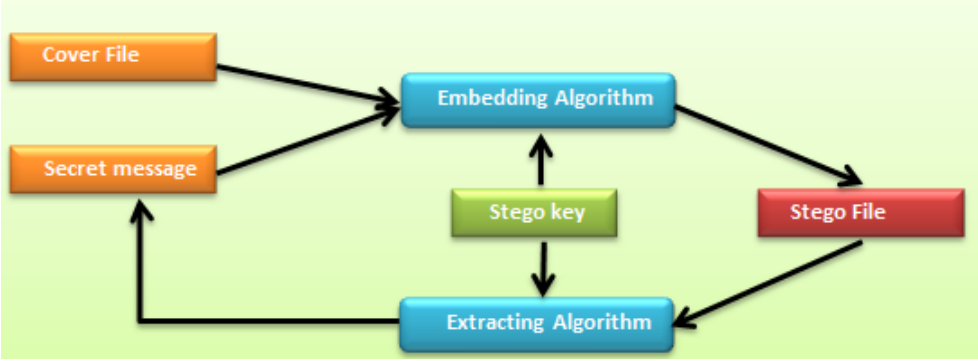

Fig 1: Basic Model of Image Steganography

The main terminologies used in the steganography are the cover file (carrier), secret message (payload), stego file, and stego key according to this Fig 1. [7]

a) **Cover file (Carrier):** It is defined as the original file into which the required secret message will be embedded. It is also termed as innocent file or host file. The secret message should be embedded in such a manner that there are no significant changes in the properties of the cover file.

b) **Secret Message (Payload):** It is the massage that has to be embedded within the cover file in a given steganography model. The payload can be in the form of text, audio, images, or video.

c) **Stego file (stego-object):** It is the final file obtained after embedding the payload into a given cover file.

d) **Stego key**: Is a password that may be used to encode the secret message to provide an additional level of security.

The performance for image steganography can be measured by peak-signal-to noise ratio (PSNR), which measured the similarity between the stego-image and the cover image, represented by the equation 1 [8].

$$PSNR = 10log_{10}(\frac{C^2max}{MSE}) \qquad \textbf{Equation 1}$$

Where **C** is the dynamic range of pixel values, or the maximum value that a pixel can be taken, for 8-bit images; **C**=255, and **MSE** denotes the mean square error, it is measure the difference between the stego image and the cover image, as represented by the equation 2:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \qquad \textbf{Equation 2}$$

Where **M** and **N** are the height and the width of the image, S_{xy} is the x row and the y column pixel in the original cover image, and C_{xy} is the x row and the y column pixel in the reconstructed stego image.

2. PREVIOUS WORK

In [9] the authors proposed a new encoding technique based on the PIGPEN cipher. In which the secret message is converted into its PIGPEN representation code so each character will be represented in two digits only instead of three digits as in ASCII representation. Then substitute these two digits with the last digit of each pixel. The PIGPEN cipher is a type of a substitution cipher of cryptography.

So, for example to represent letter ‘A’ it can be find in table 1 so ‘A’ replaced with ’01’. And to represent letter ‘m’ it can replaced by ‘44’ and so on.

Table 1. PIGPEN Encoding for numbers, small letters and capital letters and special characters [9]

PIGPEN	Char	PIGPEN	Char	PIGPEN	Char	PIGPEN	Char
01	A	31	a	61	0	91	:
02	B	32	b	62	1	92	;
03	C	33	c	63	2	93	<
04	D	34	d	64	3	94	=

PIGPEN	Char	PIGPEN	Char	PIGPEN	Char	PIGPEN	Char
05	E	35	e	65	4	95	>
06	F	36	f	66	5	96	?
07	G	37	g	67	6	97	@
08	H	38	h	68	7	98	[
09	I	39	i	69	8	99	\
11	J	41	j	71	9	00	]
12	K	42	k	72	space	10	^
13	L	43	l	73	!	20	_
14	M	44	m	74	"	30	`
15	N	45	n	75	#	40	{
16	O	46	o	76	$	50	|
17	P	47	p	77	%	29	}
18	Q	48	q	78	&	59	~
19	R	49	r	79	'	89	DEL
21	S	51	s	81	(		
22	T	52	t	82	)		
23	U	53	u	83	*		
24	V	54	v	84	+		
25	W	55	w	85	’		
26	X	56	x	86	-		
27	Y	57	y	87	.		
28	Z	58	z	88	/		

And for example if the secret letter is R and the current block contains 255, 200 and 101. The method in [10] will hide R by representing it in ASCII format, it will equal 082. Then the pixels after substitution will be 250, 208 and 102 instead of 255, 200 and 101.

But by using PIGPEN representation the letter R will be represented by only two digits 19, so just two pixels will be changed. Using the PIGPEN encoding technique to represent the secret message will save one third of the required space for embedding capacity. And also it will enhance the PSNR of the stego image.

3. THE PROPOSED TECHNIQUE

In this technique the PIGPEN Encoding technique will be improved by using the zigzag scanning representation method. Zigzag scanning selects the pixels that will hide secret message inside; so that it can increase the security of the embedding process. Fig 2 shows the basic zigzag scanning process:-

Fig 2: Basic Zigzag Scanning Process

Zigzag scanning is a transformation process from m x n matrix to one array, through zigzag scan reading, as shown in Fig 3. Sorting index started from the top left coefficient and moved in the same direction with arrow in Figure 3, until it ended at the bottom right [11].

The efficiency of zigzag scanning method is that it is able to accelerate the time used for data sorting to group the components from quantified coefficients.

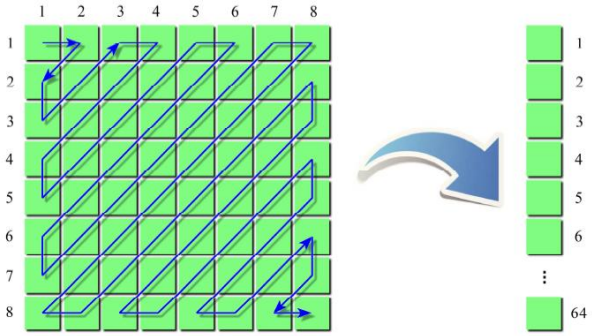

Fig 3: Basic Zigzag Scanning Model

This function is used to rearrange a matrix of any size into a 1-D array by implementing the ZIGZAG SCANNING procedure.
For example suppose '**IN'** specifies the input matrix of any size and '**OUT'** is the resulting zigzag scanned (1-D) vector having length equal to the total number of elements in the 2-D input matrix

$$\mathbf{IN} = \begin{bmatrix} 1 & 2 & 6 & 7 \\ 3 & 5 & 8 & 11 \\ 4 & 9 & 10 & 12 \end{bmatrix}$$

OUT = **ZIGZAG** (**IN**)

OUT= 1 2 3 4 5 6 7 8 9 10 11 12

The proposed system provides means for secure data transmission over the internet. The confidential information is transmitted with additional layer of security. The secret message is represented using PIGPEN encoding technique and then hidden by ZIGZAG scanning technique into the cover image.

Hiding data using ZIGZAG scanning is more efficient than the sequential embedding. The attacker cannot get clues that secret message is hidden in the cover image. If the attacker knows about the existence of secret message, cannot return it without the extraction algorithm.

3.1. Embedding Algorithm: Message Embedding Using Enhanced ZIGZAG-PIGPEN Technique

Input: Cover Image C; Secret Message M.
Output: StegoImage S.
Steps:

1) Split C into 3 channels Red (R), Green (G), Blue (B).
2) Split M into characters; M = {m1, m2, m3 …., mn}.
3) Convert B into 1 - D array Z using ZIGZAG scanning method.
4) Divide Z into blocks Z = {b1, b2, b3...bn} each of which is 2 pixels.
5) Initialize i = 1
6) Take mi from M
7) Convert mi into PIGPEN encoding representation using PIGPEN Encoding method Di = {d1, d2}.
8) Take bi from Z and take Di.
9) Substitute last digit in the 1st pixel of bi with d1 and the last digit in the 2nd pixel of bi with d2.
10) Repeat steps 6, 7, 8 and 9 until the whole M has been embedded in Z.
11) Convert Z again into 2 - D matrix A using Inverse ZIGZAG scanning method
12) Merge the 3 channels R, G, A again to construct the StegoImage S.

3.2. Extraction Algorithm : Message Extraction Using Enhanced ZIGZAG-PIGPEN Technique

Input: StegoImage S, Message Length L.
Output: Secret Message M.
Steps:

1) Convert S into three layers R, G and B.
2) Convert B into 1 - D array Z using ZIGZAG scanning method.
3) Divide Z into blocks Z = {b1, b2, b3...bn} each of which is only one pixel.
4) Initialize i = 1
5) Take bi from Z and make mi = the last digit in bi.
6) Take bi+1 from Z and make mi+1 = the last digit in bi+1.
7) Concatenate mi and mi+1 and convert the string from 'PIGPEN Encoding' format to character again using PIGPEN encoding method.
8) i = i + 1
9) Repeat steps from 5 to 8 until reach the Message Length L (the whole M has been extracted).

4. EXPERIMENTAL RESULTS

The proposed Enhanced MSLDIP-PIGPEN technique will be tested by taking different messages and different cover images size. Then some comparisons between this Enhanced MSLDIP-PIGPEN technique results and other methods will be done.

Table 2: Comparison between LSB-3, Modified LSB-3 Methods and 'Enhanced MSLDIP-PIGPEN' technique

Cover Image (256 × 256)	Message Capacity	PSNR		
		LSB – 3	Modified LSB – 3	Enhanced MSLDIP-PIGPEN
Boat	8,160	39.1132	42.4163	49.5478
Bird	8,160	39.0955	42.4062	49.6381
Flinstone	8,160	39.1188	42.2932	49.1422

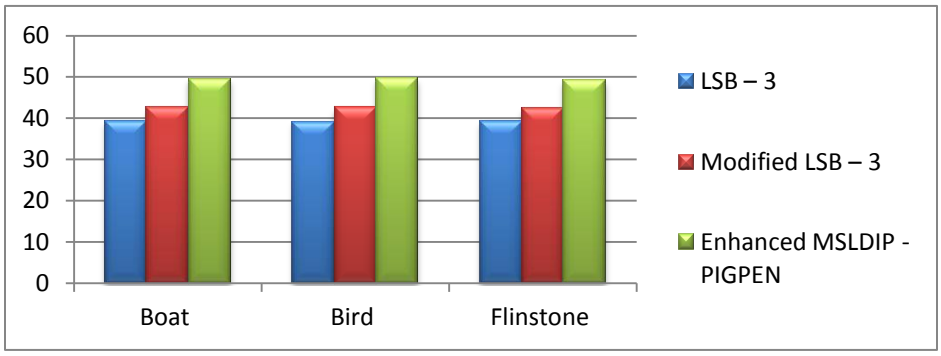

Fig 4: Comparison between PSNR values of Table 2

As shown in Table 2, after hiding the same message length (8,160 bytes) in the cover images (Boat, Bird and Flinstone) with the same size (256 × 256) using the Enhanced MSLDIP-PIGPEN technique and some other methods like LSB-3 and Modified LSB-3 methods it has been found that, the proposed technique has the higher PSNR values than other methods.

Table 3: Comparison between SLDIP, MSLDIP, method in [12] and 'Enhanced MSLDIP-PIGPEN' technique

Cover Image (256 × 256)	Message Capacity	PSNR			
		SLDIP	MSLDIP	Method in[12]	Enhanced MSLDIP-PIGPEN
Boat	6656	44.9953	48.6661	48.894425	50.4389
Baboon	6656	44.9953	48.6638	48.684503	50.1911
Lena	6656	44.9886	48.7596	48.823719	50.4861

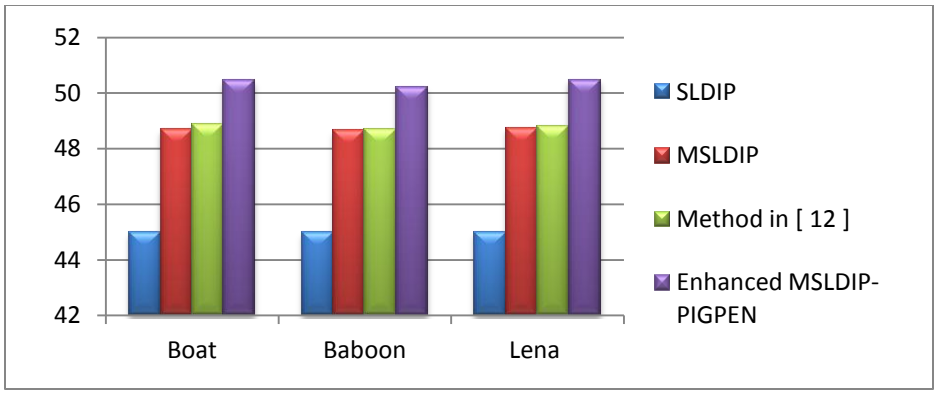

Fig 5: Comparison between PSNR values of Table 3

As shown in Table 3, after hiding the same message length (6656 bytes) in the cover images (Boat, Baboon and Lena) with the same size (256 × 256) using the Enhanced MSLDIP-PIGPEN technique, SLDIP, MSLDIP and method in [12] it has been found that the proposed enhanced technique has the higher PSNR values than other methods.

Table 4: Comparison between method in [14] and 'Enhanced MSLDIP-PIGPEN' technique

Cover Image (512 × 512)	Message Capacity	PSNR	
		Method in[14]	Enhanced MSLDIP-PIGPEN
Lena	10000	38.38	54.7520
Peppers	10000	37.78	54.3006
Lena	4096	42.90	58.4695
Peppers	4096	41.87	58.2275

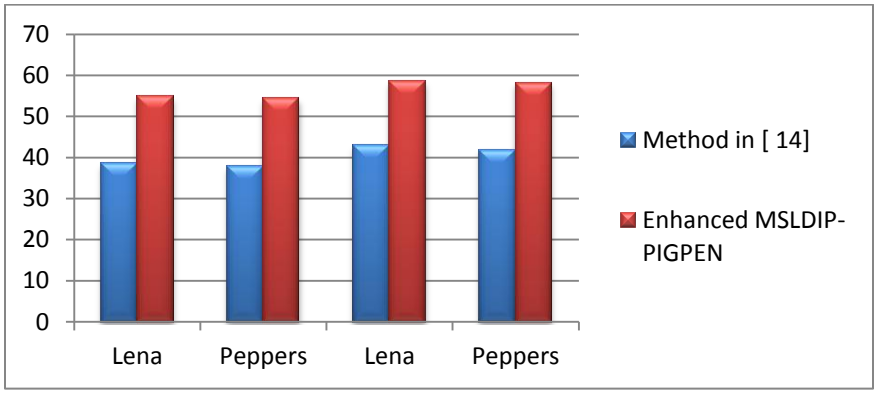

Fig 6: Comparison between PSNR values of Table 4

As shown in Table 4 , after hiding the message length (10,000 bytes and 4096 bytes) in the cover images (Lena and Peppers) with the same size (512 × 512) using the Enhanced MSLDIP-PIGPEN technique and method in [14] it has been found that, the proposed technique has the higher PSNR values than method in [14].

Table 5: Comparison between method in [15], PVD-MSLDIP-MPK Method [16] and 'Enhanced MSLDIP-PIGPEN' technique

Cover Image	Message	PSNR

(256 × 256)	Capacity	Method in [15]	PVD MSLDIP-MPK Method[16]	Enhanced MSLDIP-PIGPEN
Baboon	18,616	33.80	41.7789	45.5299
Lena	13,003	43.56	45.3734	45.7526
Peppers	16,394	36.91	44.1038	45.5470

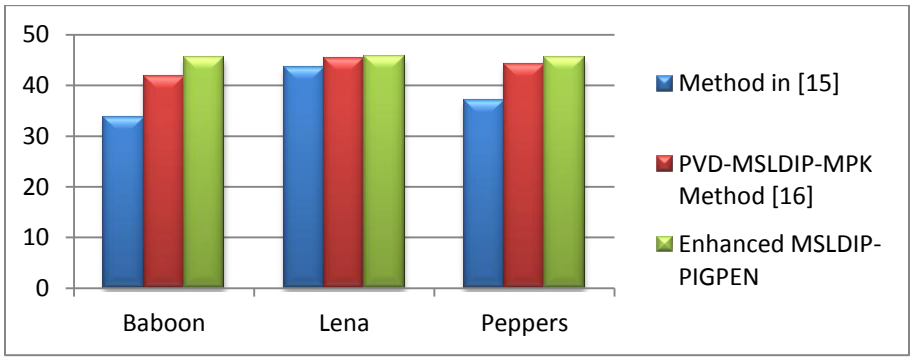

Fig 7: Comparison between PSNR values of Table 5

As shown in Table 5, after hiding different message sizes in cover images (Baboon, Lena and Peppers) with the same size (256 × 256) using the Enhanced MSLDIP-PIGPEN technique, method in [15] and the PVD-MSLDIP-MPK Method [16]. It has been found that, the Enhanced MSLDIP-PIGPEN technique has the higher PSNR values than the other methods.

Table 6: A Comparison between method in [17] and 'Enhanced MSLDIP- PIGPEN' technique

Cover Image (512 × 512)	Message Capacity	PSNR	
		Method in [17]	Enhanced MSLDIP-PIGPEN
Lena	792	45.3672	65.4776
	1702	41.6915	62.2871
	2547	40.0692	60.5866
	4110	37.9555	58.4149
	6075	35.5330	55.1822
	11346	32.6133	53.1541

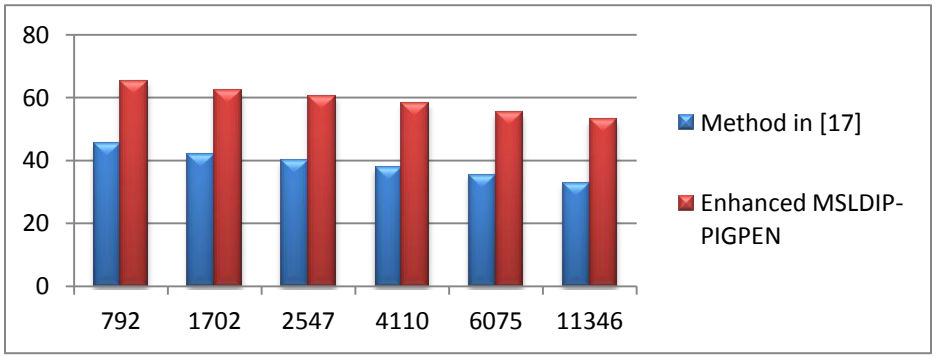

Fig 8: A Comparison between PSNR values of Table 6

As shown in Table 6 after hiding different message sizes (792 - 1702 - 2547 - 4110 -6075 - 11346) bytes in 512 x 512 cover images Lena, using the method in [17] and the Enhanced MSLDIP-PIGPEN technique, it has been found that, the Enhanced MSLDIP-PIGPEN technique has higher PSNR values than the method in [17].

Table 7: A Comparison between method in [9] and 'Enhanced MSLDIP- PIGPEN' technique

Cover Image (256 × 256)	Message Capacity	PSNR	
		Method in [9]	Enhanced MSLDIP-PIGPEN
Baboon	18,616	42.2948	45.5299
Lena	13,003	45.6608	45.7526
Boat	8,160	49.3755	49.5478
Bird	8,160	49.5467	49.6381

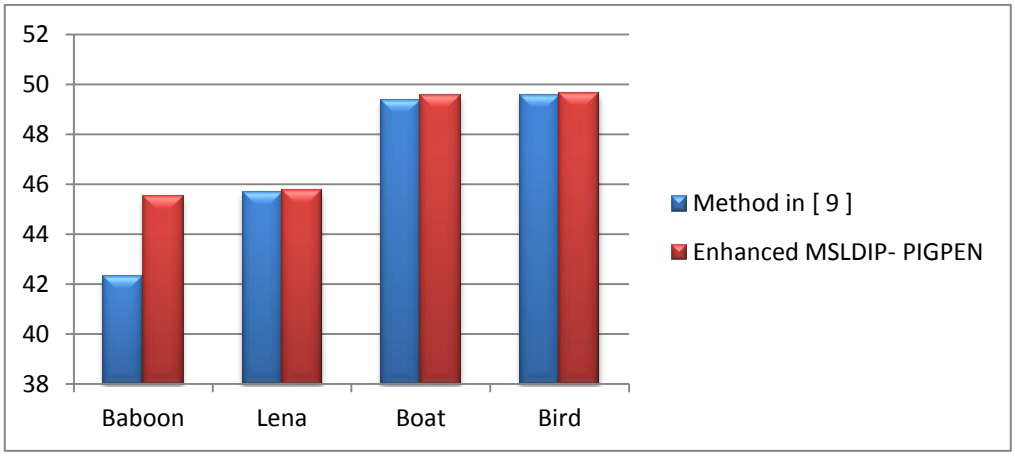

Fig 9: A Comparison between PSNR values of Table 7

Finally as shown in Table 7 after hiding different message sizes (18,616 - 13,003 - 8,160 - 8,160) bytes in (256 × 256) cover images Baboon, Lena, Boat and Bird using the method in [9] and the Enhanced MSLDIP-PIGPEN technique, it has been found that, the Enhanced MSLDIP-PIGPEN technique has higher PSNR values than the method in [9].

5. CONCLUSION AND FUTURE WORK

In this paper a try to enhance the security of the PIGPEN encoding technique has been proposed by using ZIGZAG Scanning, and some comparisons between enhanced technique and some other methods have been done also.

As a future work, a try will be made to develop a new technique that uses our new encoding technique with other image steganography methods to enhance the PSNR values and save more capacity. Also a try will be made to applying the proposed technique on audio and video and a try to improving the security of the proposed enhanced technique by encrypting the secret message before embedding it using any encryption algorithm as RC4 algorithm.

Ethical: NA

Consent: NA

6. REFERENCES

[1] Kanzariya N. K., Nimavat A. V., "Comparison of Various Images Steganography Techniques", International Journal of Computer Science and Management Research, Vol 2, Issue 1, January 2013.

[2] Deepa S., Umarani R., "A Study on Digital Image Steganography ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 1, January 2013.

[3] Stuti G., Arun R., Manpreet K.,"A Review of Comparison Techniques of Image Steganography", IOSRJournal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331, Volume 6, Issue 1 (May - Jun. 2013).

[4] Nagham H., Abid Y., Badlishah A. and Osamah M. A., "Image Steganography Techniques: An Overview", International Journal of Computer Science and Security (IJCSS), Vol. 6, Issue 3, 2012.

[5] Pardeshi, S. M., Sonawane, I. R., Punjabi, V. D., and Saraf, P. A.," A Survey on compound use of Cryptography and Steganoghaphy for Secure Data Hiding", International Journal of Emerging Technology and Advanced Engineering Website, Volume 3, Issue 10, October 2013.

[6] Chandra P. S., Mr. Ramneet S Ch.," A Survey of Steganography Technique, Attacks and Applications ", ijarcsse, Volume 4, Issue 2, February 2014, ISSN: 2277 128X.

[7] Abdelmgeid A. A., Al – Hussien S. S.," Enhancing the Security of SMMWB Image Steganography Technique by using the Linked List Structure (Cover Package Method)", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 7, March 2014.

[8] Rajani and Muhammed T. K. "Data Hiding In Digital Image Processing Using Steganography: A Review." International Journal of Engineering Development and Research. Vol. 2, No. 3, September 2014.

[9] Abdelmegid A. A., Bahget A. A., Al - Hussien S. S., Maha M. G., "Enhancing Image Steganography Methods By Using New Secret Message Encoding Technique Based on PIGPEN cipher (PIGPEN Encoding)", International Journal Of Computer applications (IJCA), Vol. 174, No. 9, September 2017.

[10] Radwan, A. A., Swilem, A. and Al - Hussien S. S, " A High Capacity SLDIP (Substitute Last Digit In Pixel ", Fifth International Conference on Intelligent Computing and Information Systems (ICICIS 2011), 30 June - 3 July, 2011, Cairo, Egypt

[11] Wa'el I. A., "Image Steganography using LSB and LSB+Huffman Code", International Journal of Computer Applications, Vol. 99, No. 5, August 2014.

[12] Abdelmgeid A. A., Al – Hussien S. S., "New Image Steganography Method By Matching Secret Message With Pixels Of Cover Image (SMM) ", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), Vol. 3, Issue 2, Jun 2013.

[13] Marwa M. E., Abdelmgeid A. A., Fatma A. O. "A Modified Image Steganography Method based on LSB Technique." International Journal of Computer Applications, Vol. 125, No. 5, September 2015.

[14] Sara N., Amir M. E., Mohammad S. M., "Secure Information Transmission using Steganography and Morphological Associative Memory ", International Journal of Computer Applications, Vol 61, No 7, January 2013.

[15] G. S. Chandel, P. Halarnkar and K. Dhamejani, "Capacity Increase for Information Hiding Using Maximum Edged Pixel Value Differencing," Springer-Verlag Berlin Heidelberg, pp. 190 - 194, 2011.

[16] Marwa. E. S., Abdelmgeid. A. A. and Fatma. A. O., "Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding," International Journal of Computer Science and Security (IJCSS), Vol. 9, No. 2, PP. 96 - 107, 2015.

[17] S. Kaur, S. Jindal, "Image Steganography using Hybrid Edge Detection and First Component Alteration Technique", International Journal of Hybrid Information Technology (IJHIT), Volume 6, No.5, pp.59-66, ISSN: 1738-9968, 2013.
[18] V. Shukla, A. Chaturvedi, N. Srivastava, "Nanotechnology and cryptographic protocols: issues and possible solutions", Nanomaterials and Energy, Volume 8, Issue 1, June 2019