Enhancing Image Steganography Methods by using New Secret Message Encoding Technique based on Pigpen Cipher (Pigpen Encoding)

Abdelmgeid A. A.
Faculty of Computer and Information science,
Minia University
Egypt

Bahgat A. A.
Computer Science Dept.
Faculty of Science,
Minia University
Egypt

Al-Hussien Seddik Saad
Computer Science Dept.
Faculty of Science,
Minia University
Egypt

Maha Mohamed Gomaa
Computer Science Dept.
Faculty of Science,
Minia University
Egypt

ABSTRACT

Steganography is one of the important information hiding techniques which hides the existence of the message in the cover file. By using steganography, secret messages can be hidden in carriers such as images, audio files, text files and videos. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. Steganography is used to conceal the information so that no one can sense its existence. In this paper the performance of hiding image technique will be enhanced by modifying the secret message itself not the technique of embedding. That is by using a new encoding technique based on the Pigpen cipher that will represent 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.

Keywords

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

1. INTRODUCTION

The security of information is an important issue during the transmission of data over the internet [1]. So to protect information from being stolen there is some ways to do this like encryption and steganography. Encryption is the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully. While steganography is a technique which hides secret information into a cover media or carrier so that it becomes unnoticed and less attractive [2]. Steganography is the art and science of invisible communication which received a lot of concern from the scientific community recently [3]. The term steganography is derived from the Greek words “stegos” meaning “covered” and “grafia” meaning “writing” which means “covered writing” [4].

Steganography techniques tend to hide the existence of the message itself, which makes it difficult for an observer to figure out where exactly the message is; on the other hand the main objective of cryptography is to secure communications by changing the data into a form so that it cannot be understand by an eavesdropper [5]. Steganography provides a kind of data hiding method that conceals the existence of the secret message in the media [6].

Steganography can be divided into different categories based upon the type of cover media chosen (Images, Audio, Video, and Text) [8]. The most frequently used carriers are digital images which is our point of research.

A steganography system can act as shown in Fig. 1. [9]

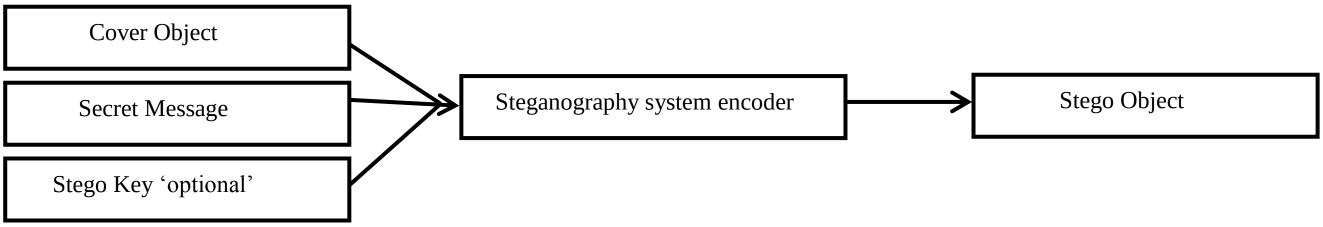


Fig 1: Basic model of steganography

The steganography system consists of the following components:-

- Cover object (carrier): It is the original file into which the required secret message is embedded. It is also termed as innocent file or host file.
- Secret Message (Payload): It is the secret massage that has to be embedded within the cover file.
- Stego Object: It is the final file obtained after embedded the payload into a given cover file. It should have similar properties to that of the cover file.
- Stego key ‘optional’: is a password that may be used to encode the secret information to provide an additional level of security.

The basic steganography system has two processes one for embedding and one for extraction. The embedding process uses a cover object, secret message and embedding algorithm to hide secret message inside cover object to produce the Stego object [10]. The extraction process is much simpler; it is an inverse of the embedding process, where the stego object and extraction algorithm used to get the secret message again [11].

The performance of an image steganography system can be measured using some important factors. One factor is the invisibility of the data, which refers to how difficult it is to determine the existence of a hidden message in the stego image and this can be measured by calculating the PSNR (Peak Signal to Noise Ratio). Other factor is the capacity or MHC (Maximum Hiding Capacity), refers to the maximum information that can embedded in a cover image [5].

2. RELATED WORK

In [2] authors proposed a new image steganography technique called Substitute Last Digit In Pixel (SLDIP), in which the secret message is converted into its ASCII code so each character will be represented in three digits only. Then substitute each 3 digits with the last digit of each pixel. For example if the secret letter is R and the current block contains 255, 200 and 101. The proposed method 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. So the last digit only will be substituted. These digits will be used for extraction process, as every three pixels' last digits will represent a byte in the secret message.

This SLDIP technique has a very high PSNR values and a very high MHC in which each secret byte can be hidden in only three pixels of the cover images.

Also, in [2] authors proposed another method which is Modified SLDIP (MSLDIP). It was able to keep same Maximum Hiding Capacity of the SLDIP Method plus higher PSNR values than SLDIP. It is modifying the substituted step to decrease the difference between the original pixel and the substituted pixel. Using the same example, for embedding the secret message R which equals 082 in ASCII, in the first block (255, 200, and 101), instead of (250, 208 and 102), by using MSLDIP method the block becomes (250, 198 and 102).

3. THE PROPOSED METHOD

In this method the PIGPEN cipher will be used to represent the secret message by using only two digits not three digits as ASCII encoding. The pigpen cipher is a type of a substitution cipher of cryptography, but rather than replacing each letter with another letter, the letters are replaced by symbols [13]. Table 1, shows the ASCII table second part that contains the letters, numbers and some special characters [12].

Table 1. ASCII table second part (32 – 127)

ASCII	Char	ASCII	Char	ASCII	Char	ASCII	Char
032	Space	057	9	082	R	107	K
033	!	058	:	083	S	108	L
034	"	059	;	084	T	109	M
035	#	060	<	085	U	110	N
036	$	061	=	086	V	111	O
037	%	062	>	087	W	112	P
038	&	063	?	088	X	113	Q
039	'	064	@	089	Y	114	R
040	(	065	A	090	Z	115	S
041	)	066	B	091	[	116	T
042	*	067	C	092	\	117	U
043	+	068	D	093	]	118	V
044	,	069	E	094	^	119	W
045	-	070	F	095	_	120	X
046	.	071	G	096	`	121	Y
047	/	072	H	097	A	122	Z
048	0	073	I	098	B	123	{
049	1	074	J	099	C	124	|
050	2	075	K	100	d	125	}
051	3	076	L	101	E	126	~
052	4	077	M	102	F	127	DEL
053	5	078	N	103	G		
054	6	079	O	104	H		
055	7	080	P	105	I		
056	8	081	Q	106	J		

In the PIGPEN cipher the encryption process is made by replacing each occurence of a letter with the designated symbol. The symbols are assigned to the letters using the key shown below in Fig. 2., where the letter shown is replaced by the part of the image in which it is located [13].

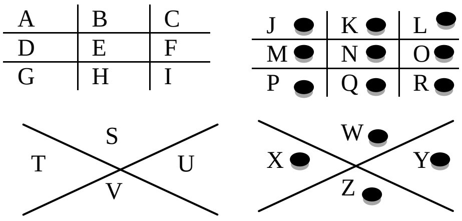
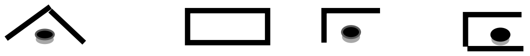


Fig 2: The pigpen cipher symbols

So to represent a word ‘zero’ for example, we replace it with these following symbols:-



So from this method a new encoding technique will be developed for encoding the secret message with smaller number of digits than ASCII. The first step was to list each character (small letters, capital letters, numbers and some special characters) by using the PIGPEN cipher in such tables. Then each table will have a number and also each character within the table will have a number which is the position of it in the table. So each character can be represented by two numbers only.

So, for example to represent letter ‘A’ it can be find in Fig. 3. in table number ‘0’ in the first position so ‘A’ replaced with ’01’. And to represent letter ‘m’ it can be find in table number ‘4’ in position ‘4’ so it replaced by ‘44’ and so on. So for capital letters three tables can be constructed (0, 1, and 2) as in Fig. 3.

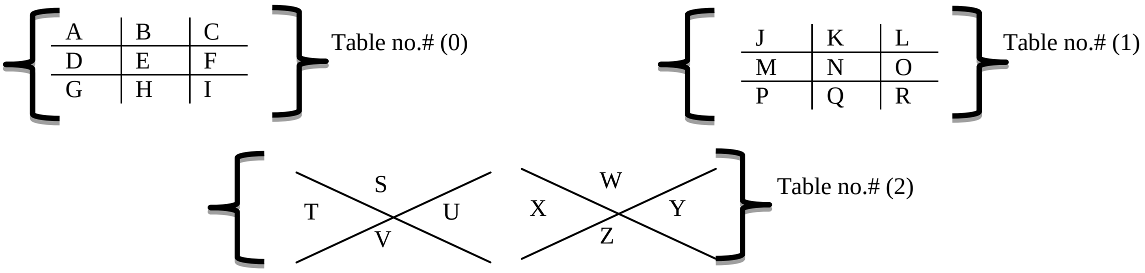


Fig 3: The pigpen cipher tables for capital letters

In table 2, capital letters can be represented by only two digits as follow:

Table 2. PIGPEN table for Capital Letters

PIGPEN	Char	PIGPEN	Char
01	A	15	N
02	B	16	O
03	C	17	P
04	D	18	Q
05	E	19	R
06	F	21	S
07	G	22	T
08	H	23	U
09	I	24	V
11	J	25	W
12	K	26	X
13	L	27	Y
14	M	28	Z

Also, the same will be done with the small letters, numbers and special characters.

Now tables from 0 to 9 can represent all capital letters, small letters, numbers and some special characters. But there are the rest of special characters that may be used in the secret message as in ASCII table, it can be represented by using the other possible combinations of numbers (00,10,20,30,40,50,29,59,89).

Finally, the small letters, numbers and whole special characters are added to the encoding table so the final version of PIGPEN encoding table will be as shown in table 3:-

Table 3. PIGPEN Encoding Table for Numbers, Small and Capital Letters and Special Characters

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	=
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	/		

As shown in the final table, each character can be represented by only two digits not three as in ASCII table. So by using this encoding technique to represent the secret message it can save one third of the required space for embedding capacity. And also this method will enhance the PSNR of the stego image as will be presented in the next section.

4. EXPERIMENTAL RESULTS

The proposed method (PIGPEN) will be tested by taking different messages and different cover images size. Then some comparisons between this proposed method (PIGPEN) results and MSLDIP method results will be done.

The following table shows a comparison of MHC between MSLDIP and PIGPEN methods on different images size:-

Table 4. Comparison of MHC between MSLDIP and PIGPEN methods

Image size (Pixels)	Maximum Hiding Capacity (MHC)	
	MSLDIP	**MSLDIP-PIGPEN**
8 × 8	21 bytes	32 bytes
16 × 16	85 bytes	128 bytes
32 × 32	341 bytes	512 bytes
64 × 64	1,365 bytes	2,048 bytes
128 × 128	5,461 bytes	8,192 bytes
256 × 256	21,845 bytes	32,768 bytes
512 × 512	87,381 bytes	131,072 bytes
1024 × 1024	349,525 bytes	524,288 bytes

As shown in Table 4, after the comparison of MHC between MSLDIP and PIGPEN methods has been done, it has been found that we can save one third of the embedding capacity of the cover image by using the new method (PIGPEN).

Table 5. Comparison between MSLDIP and MSLDIP-PIGPEN methods

Cover Image (256 × 256)	Message Capacity	PSNR	
		MSLDIP	**MSLDIP-PIGPEN**
Lena	5,612 bytes	49,4535	51,1928
Peppers	5,612 bytes	49,0716	51,1954
Plane	5,612 bytes	49,6922	51,1983

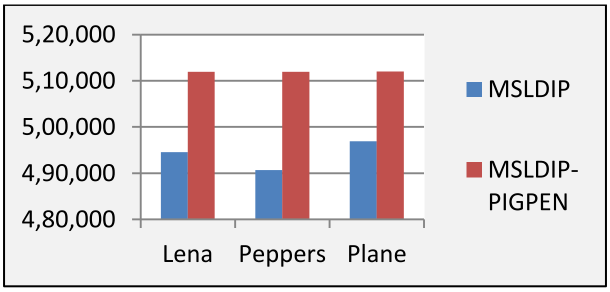


Fig 4: Comparison between PSNR values of Table 5

As shown in Table 5, after hiding the same message length (5,612 bytes) in the cover images (Lena, Peppers and Plane) with the same size (256 × 256) using the MSLDIP method and the proposed method (PIGPEN), it has been found that, the proposed method has higher PSNR values than MSLDIP method.

Table 6. Comparison between MSLDIP and MSLDIP-PIGPEN methods

Cover Image (256 × 256)	Message Capacity	PSNR	
		MSLDIP	**MSLDIP-PIGPEN**
Lena	8,891 bytes	47,4355	49,2988
Peppers	8,891 bytes	47,0708	48,7126
Plane	8,891 bytes	47,5824	49,2077

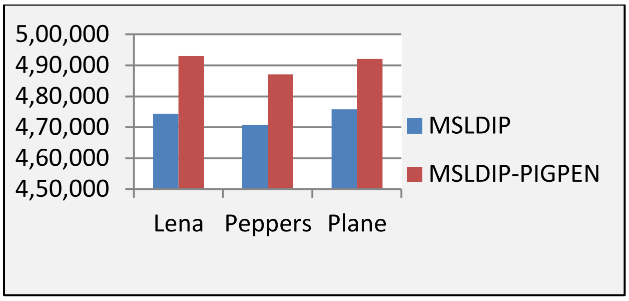


Fig 5: Comparison between PSNR values of Table 6

In Table 6, the same cover images in table 4 has been used, (Lena, Peppers and Plane) with the same size (256 × 256), and change the message length to (8,891 bytes), and after applying the MSLDIP method and the proposed method (PIGPEN), also it has been found that, the proposed method has higher PSNR values than MSLDIP method.

Table 7. Comparison between MSLDIP and MSLDIP-PIGPEN methods

Cover Image (512 × 512)	Message Capacity	PSNR	
		MSLDIP	**MSLDIP-PIGPEN**
Lena	80,023 bytes	43,9930	45,7708
Peppers	80,023 bytes	43,6296	45,4100
Plane	80,023 bytes	43,9988	45,7217

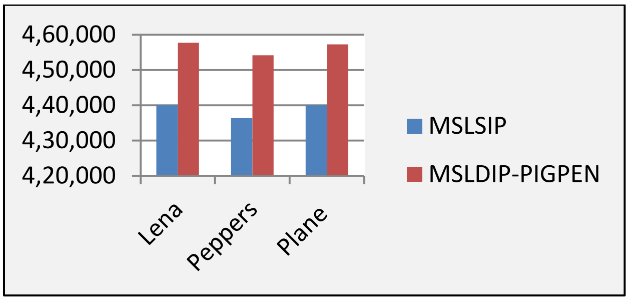


Fig 6: Comparison between PSNR values of Table 7

This time in Table 7, a large secret message (80,023 bytes) and large cover images **(**512 × 512**)** has been used. By using the MSLDIP method and the proposed method (PIGPEN), it has been found that, the proposed method has higher PSNR values than MSLDIP method.

Table 8: Comparison between MSLDIP and MSLDIP-PIGPEN methods

Cover Image Peppers	Message Capacity	PSNR	
		MSLDIP	MSLDIP-PIGPEN
128 × 128	2,717 bytes	46,2509	47,9108
256 × 256	10,871 bytes	46,2134	47,9391
512 × 512	43,483 bytes	46,2160	47,9617
1024 × 1024	130,451 bytes	47,4451	49,1334

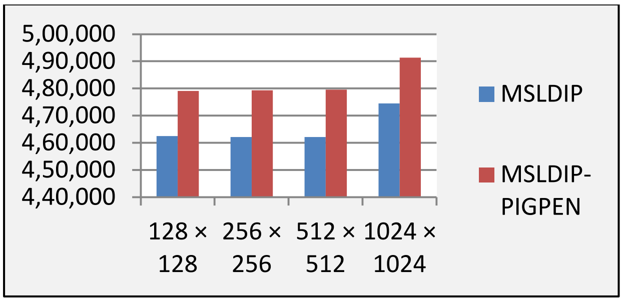


Fig 7: Comparison between PSNR values of Table 8

Finally in Table 8, the same cover image with different sizes and different secret messages has been used, and also it found that, the proposed method has higher PSNR values than MSLDIP method.

5. CONCLUSION AND FUTURE WORK

In this paper a new encoding technique PIGPEN has been proposed which represents each character in the secret message by two digits only not three digits as ASCII encoding. And as a result of that it saved one third of the space required for embedding capacity and also this enhanced the PSNR values as shown in the experimental results section.

As a future work, a try will be made to develop a new technique that use our new PIGPEN encoding method 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 applying the proposed method on frequency domain.

6. REFERENCES

[1] Kavitha, Kavita K., Ashwini K. and Priya D., "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), issn: 2248-9622, Vol. 2, Issue 3, pp. 338 - 341, May - Jun 2012.

[2] Radwan, A. A., Swilem, A. and Seddik, A. H., " 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.

[3] Sushil K., Muttoo S. K., " A Comparative Study Of Image Steganography In Wavelet Dmain ", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 2, Issue. 2, February 2013.

[4] 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.

[5] Shikha S., Sumit B., " Image Steganography: A Review ", International Journal of Emerging Technology and Advanced Engineering, Vol 3, Issue 1, January 2013.

[6] Ahmed T. A., Abdullah M.A., " A Novel Steganographic Method for Gray Level Images", International Journal of computer, information, and System science, and Engineering 3:1 2009.

[7] Seddik, A. H., " Enhancing The (MSLDIP) Image Steganographic Method (ESLDIP Method) ", International Conference on Graphic and Image Processing (ICGIP 2011), Proc. of SPIE, Vol. 8285, 82853i, 2011 SPIE.

[8] Shaveta C. and Himani G., "LSB Embedding in Spatial Domain - A Review of Improved Techniques", International Journal of Computers & Technology, ISSN: 2277-3061 Volume 3, No. 1, Aug, 2012.

[9] Abdul-Sada, A. I., " Hiding Data Using LSB - 3 ", J.Basrah Researches (Sciences), Vol. 33, No.4. (81-88), December, 2007.

[10] Mohammed A. F. H., "Message Segmentation to Enhance the Security of LSB Image Steganography", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012.

[11] 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.

[12] http://www.asciitable.com

[13] http://crypto.interactive-maths.com/pigpen-cipher.html