New Technique for Encoding the Secret Message to Enhance the Performance of MSLDIP Image Steganography Method (MPK Encoding)

Abdelmgeid Amin Ali
Associate Professor, Dept. of Computer Science
Faculty of Science, Al - Minia University, Egypt

Al – Hussien Seddik Saad
Assistant Lecturer, High Institute for Engineering and Technology (H.I.E.T) Al – Minia, Egypt

ABSTRACT
Steganography is a Greek origin word which means "hidden writing". Steganography word is classified into two parts: Steganos which means "secret or covered" (where you want to hide the secret messages) and the graphic which means "writing". It is one of the most important techniques of data hiding. By using steganography, secret messages can be hidden in carriers such as images, audio files, text files and videos. In this paper we tried to enhance the performance of the image steganography technique by modifying the secret message itself not the technique of embedding. That's by using a new encoding technique that we called it Mobile Phone Keypad encoding or MPK encoding, that can 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. Finally, we are hoping to globalize this new MPK encoding technique to be used in the field of steganography.

General Terms
Image steganography, Secret message encoding, Data hiding

Keywords
Steganography, SLDIP Method, MSLDIP Method, Peak Signal-to-Noise Rate (PSNR), Mean Square Error (MSE), Least Significant Bit (LSB).

1. INTRODUCTION
There are many digital multimedia transmissions on the network and there could be some important data that needs to be protected during transmission. Therefore, how to protect the secret messages during transmission becomes an important research issue. In fact, the problem is how to protect secret message from being stolen during transmission and there are two ways to solve this problem. One way is encryption, which refers to 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. Another way is steganography , which is our point of research, and this is a technique which hides secret information into a cover media or carrier so that it becomes unnoticed and less attractive [1]. The word steganography comes from the Greek Steganos, which means covered or secret and Graphy which means writing or drawing [2,3]. It can be defined as the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises that guaranteed by a cryptosystem. So, it can be said that the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present [4].

Actually, there has been a rapid growth of interest in the subject of steganography over the last ten years and that's for two main reasons. Firstly, the publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products; an appreciation of new market opportunities created by digital distribution is coupled with a fear that digital works could be too easy to copy. Secondly, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages [4].

One of the oldest examples of steganography dates back to around 440 BC in Greek History. Herodotus, a Greek historian from the 5th Century BC, revealed some examples of its use in his work entitled "The Histories of Herodotus". One elaborate example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaved and the message that commanded a revolt against the Persians was revealed [5]. In this example, the slave was used as the carrier for the secret message, and anyone who saw the slave as they were sent to Aristagorus would have been completely unaware that they were carrying a message. As a result of this, the message reached the recipient with no suspicion of covert communication ever being raised.

A basic model for steganography as shown in Fig 1, consists of the following :- [6, 7]

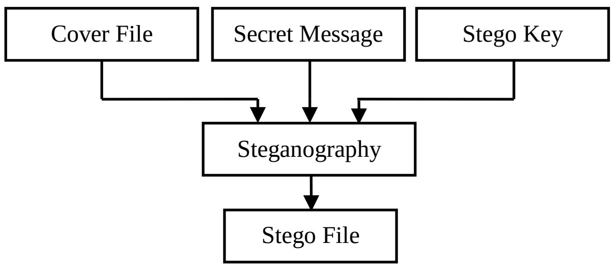

Fig 1: Basic model of steganography

• Cover file (Carrier): It is defined as the original file into which the required secret message is embedded. It is also termed as innocent file or host file.

• Payload (Secret Message): It is the secret massage that has to be embedded within the cover file in a given Steganographic model. The payload can be in the form of text, audio, images, or video [8].

• Stego 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.

• Stegokey: is a password that may be used to encode the secret information to provide an additional level of security.

Now, after a basic model of steganography has been looked at, the rest of this section will discuss basic types of it. There are two types, linguistic and technical steganography [6].

Technical steganography can be classified into: image, audio, video and text steganography [6]. But this paper will concentrate only on image steganography as it is our point of research. An important note is that, image steganography itself is divided into spatial domain and frequency domain steganography [9].

So, what are the most important aspects affecting image steganography and its usefulness? The most important aspects are the Capacity and the invisibility. Capacity refers to the amount of data bits that can be hidden in the cover image, invisibility is to hide a secret message in the pixels of the image in such a manner that the Human Vision System (HVS) is not able to distinguish between the original and the stego-image [1].

Because of these main aspects of image steganography, all steganographers (authors) try to enhance and develop new image steganography techniques that either with a very high PSNR (Peak Signal-to-Noise Ratio) values (invisibility) or with a very high MHC (Maximum Hiding Capacity).

But while searching on the internet it has been found that almost all of spatial domain image steganography proposed methods make use of Least Significant Bits (LSBs) - which is simple approach to embed information in an image, as an example, applying LSB technique to each byte of a 24-bit image, three bits only can be encoded into each pixel, as each pixel is represented by three bytes [10] - but with little changes in the steps such as using indicator pixels, using indicator channel, counting number of 1's in the first four Most Significant Bits (MSBs) or embedding more than 1 bit in each pixel and so on. So, the core process of embedding in these methods was LSB embedding.

Because of this, a big effort has been done to get out from the LSB method and two methods have been proposed that didn't embed data by using the LSB method but by using the last decimal digit in each pixel using the ASCII representation of the secret message, not the binary representation.

The first method was called Substitute Last Digit In Pixel or (SLDIP) [1], then it has been modified to become Modified SLDIP (MSLDIP) [1]. From the results tables of these methods it can be said that, the proposed methods have a very high PSNR values and very high MHC compared to current image steganography methods. This MSLDIP method which has been proposed is the method that the new MPK encoding technique will be applied on. Now, These two previously proposed methods will be discussed in the next section.

2. RELATED WORK

In [1] a new image steganography technique called Substitute Last Digit In Pixel or (SLDIP) has been proposed, in which the cover image is divided into non overlapping blocks each contains three pixels only and the secret message is converted into its ASCII code which means each character will be represented in three digits only. As an 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. As shown in [1], a cover image of size 512 x 512 can hold data up to 87,381 bytes which approximately equals to 699,050 bits in only one layer. Also the results showed that after embedding a secret message of size 82,407 bytes in a cover image of size 512 x 512 the PSNR value was 40.04469 which is a very high PSNR and this means that the two images are undistinguishable because the PSNR was higher than 37 [1].

Also, in [1] The second proposed method was Modified SLDIP (MSLDIP), which was the modified version of the SLDIP method. It was able to keep same Maximum Hiding Capacity of the SLDIP Method plus higher PSNR values than SLDIP. So, after embedding a secret message of the same size 82,407 bytes in the same cover image with the same size 512 x 512 the PSNR value was 43.84178 which is a very high PSNR and also, it is higher than the PSNR value of the SLDIP method.

After Modifying the SLDIP to become MSLDIP, a try to enhance the performance of the MSLDIP image steganography technique has been done to develop an enhanced version of the SLDIP Method and it has been succeeded in modifying the embedding steps and an Enhanced SLDIP (ESLDIP) method [6] has been proposed that has a PSNR and MHC values larger than both SLDIP and MSLDIP. But this method uses a combination between ASCII (decimal) and binary digits in representing the secret message, see [6], and because of this reason, the new MPK encoding technique won't be applied on it.

In this paper, a try to modify the secret message itself before embedding it in the cover image has been done (i.e. preprocessing step) instead of modifying the embedding technique. But the question was " How to modify the secret message to enhance the performance of the technique ?".

As said before, the secret message in SLDIP and MSLDIP methods have been represented using the ASCII (American Standard Code for Information Interchange) code, as an example the letter R will be equal to 082 not 82, in order to be able to retrieve the secret message, all the letters have to have the same length, and because there are some letters such as m equals to 109. It means that each character in the secret message must be represented by three digits. This means if the secret message was 1000 characters, it will be represented by

3000 digits to be embedded in the cover image or it needs 3000 pixels to be hidden. So, the only way to modify the secret message is by shrinking the number of digits needed to represent it.

As known, the ASCII table [13] is divided into three parts:

- 0 - 31 Control Codes.
- 32 - 127 standard, implementation independent characters.
- 128 - 255 non-standard characters (special symbols).

Actually, in our daily life we are dealing with the second part only that contains letters, numbers and some special characters (i.e. all keyboard buttons). So, we need only the second part from the ASCII table as shown in Table 1:-

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		

So, as said before, what is needed is to modify or develop a new encoding technique that able to shrink the number of digits representing the secret message.

Before discussing the new MPK encoding technique, some previous image steganography methods will be discussed that encode the secret message in such a way that enhance the performance of the image steganography techniques.

3. LITERATURE REVIEW

In [11], the authors said that, they will take from English language 24 (from a to z) characters, plus the ten digits (from 0 to 9) and the space character, so totally they got 35 characters.

First of all, from a to z are 26 characters not 24, so the total will be (26 characters + 10 numbers + 1 space) 37 not 35 characters). Then they said that "*each character in the message can be coded by six random code and these codes will be stored in table called code table known by each sender and receiver*. " Finally, the random codes will be embedded in some how.

In this method, the authors tried to make a new code table that contains small letters, space and numbers from 0 … 9. But if the secret message contains capital letters or some special characters such as @ in an email address, the algorithm will fail and the code table will be useless. Moreover, the coding table should be sent to the receiver because this coding table not global as ASCII table, and should be sent to each receiver that will receive the message. Also there will be another problem that each character will has six random codes which mean these codes are not constant as each time the algorithm will generate them. So, the table will be needed each time with the stego image, and this will be not effective and suspicious to do.

In [4], the author said that, " *an English message text is written by using the alphabetic characters of the English language (which are 26 letters ('a'...'z')). Some other special characters are useful to use in writing messages which are giving the reader a good understanding of the message. Some of these characters that are adopted in this study: ('space character', '.', ',', '(' , ')' , '"'). Therefore, the total numbers of characters that are used to write a message become 32 characters. This means that at least 5-bits are needed to represent these 32-characters in any digital system.* "

But here, the same mistakes have been happened in this table. If the secret message contains numbers from 0 … 9, any other special characters or capital letters, the whole table will be fail also. Another problem is that, the table must be sent to each receiver in order to know the encoding of the character.

Then he said that, " *The main operation of the algorithm in this proposed research is to map each 4-cases from ($2^7 = 128$) of the 7 Most Significant Bits (MSBs) in a pixel to one of the 32-cases of the characters in the message. The algorithm's goal for using 4-cases instead of one case is to increase the probability of finding the matched pixels in the image that are mapped to a character in the message*." So, it can be said that this algorithm is close to the previous method, but a big problem is that, in the coding table (Mapping table) if the sequence (no. of characters in the table) exceeds 31 the table will fail because the binary representation will be 8 digits and the algorithm works with 7 digits only. So, the table can't be expanded to hold capital letters and other characters.

In [12], the authors proposed a method that take the cover image, secret message and secret key, then transfers the secret message into text file, then convert the text file into a zip text file (Compressed File) and convert zip text file to binary codes. Finally the message is embedded by using 2 LSBs. The author here used the zip file for securing the secret message, also it has been compressed but the problem is that the stream of binary digits will be too long also. So, the same encoding problem hasn't been solved as the author converted the secret message into to binary.

After reviewing these few techniques; which dealing with the secret message; that have been hardly found, because almost all papers deals with the steganography technique itself not the secret messages, the next section will discuss and explain in details the new proposed MPK encoding technique.

4. THE PROPOSED MPK ENCODING

While thinking of a way to modify the secret message it has been found that each character in the mobile phone can be represented by only two digits not three as ASCII encoding. So, the decision has been taken to work on this to develop a new encoding technique for encoding the secret message with smaller number of digits than ASCII and also to call it MPK (Mobile Phone Keypad) encoding.

As an example, by using your mobile phone you will find that the letter a (Small letter) can be typed by pressing the key no.# (2) in the keypad only one time and the letter b (Small letter) can be typed by pressing the key no.# (2) for two times and so on.

So, the first step was to represent the letters from a … z (Small Letters) by two numbers, the first will be the key no.# and the second will be the number of presses on that key. As an example the letter a will be represented as 2 1 and the letter z will be represented as 9 4 (will be read as nine - four separated not ninety four as decimal) and so on. So, an encoding table for small letters from a … z can be constructed as shown in Table 2 :-

Table 2. MPK table for small letters

MPK	Character	MPK	Character
2 1	a	6 2	n
2 2	b	6 3	o
2 3	c	7 1	p
3 1	d	7 2	q
3 2	e	7 3	r
3 3	f	7 4	s
4 1	g	8 1	t
4 2	h	8 2	u
4 3	i	8 3	v
5 1	j	9 1	w
5 2	k	9 2	x
5 3	l	9 3	y
6 1	m	9 4	z

So, by this new MPK technique each small letter can be represented by two digits only not three as ASCII. But a full encoding table should be constructed to be able to represent the whole secret message not only the small letters. So, the numbers from 0 … 9 should be added to the new encoding technique.

Returning to the mobile phone keypad, by pressing the key no.# (0) for two times you will type the number 0, pressing keys from no.# (2) to number (8) for four times except key no.# (7) the numbers from 2 to 8 except for 7 will be typed. The keys no.# (7) and (9) will be pressed for five times to type numbers 7 and 9 , that's because these buttons hold four characters not three.

Now, the capital letters should be added to the encoding technique. By using the mobile phone you can press the key (#) to make the letters capital or small but here the rest of presses to nine times can be used, i.e. if letters A, B and C needs to be typed, instead of adding the (#) before 2 1 and 2 2 and 2 3, the number of presses 2 5, 2 6 and 2 7 can be used to represent capital letters and so on. So, the table now will hold the small letters, capital letters and numbers as shown in Table 3:-

Table 3. MPK table for numbers, small and capital letters

MPK	Char	MPK	Char	MPK	Char	MPK	Char
0 2	0	*4 2*	*h*	6 4	6	8 4	8
2 1	*a*	*4 3*	*i*	6 5	M	8 5	T
2 2	*b*	4 4	4	6 6	N	8 6	U
2 3	*c*	4 5	G	6 7	O	8 7	V
2 4	2	4 6	H	*7 1*	*p*	*9 1*	*w*
2 5	A	4 7	I	*7 2*	*q*	*9 2*	*x*
2 6	B	*5 1*	*j*	*7 3*	*r*	*9 3*	*y*
2 7	C	*5 2*	*k*	*7 4*	*s*	*9 4*	*z*
3 1	*d*	*5 3*	*l*	7 5	7	9 5	9
3 2	*e*	5 4	5	7 6	P	9 6	W
3 3	*f*	5 5	J	7 7	Q	9 7	X
3 4	3	5 6	K	7 8	R	9 8	Y
3 5	D	5 7	L	7 9	S	9 9	Z
3 6	E	*6 1*	*m*	*8 1*	*t*		
3 7	F	*6 2*	*n*	*8 2*	*u*		
4 1	*g*	*6 3*	*o*	*8 3*	*v*		

An important note is that, the key no.# (1) is a special case that it contains a lot of special characters, so 1 7 will represent the number 1.

Finally, the last modification is that the whole special characters that can be used during secret messages should be added as in ASCII table. The special characters in the mobile phone are included in the button (*) , but it can't be represented by a digit so, the presses in between the used presses can be used to hold the special characters. These presses include the following:-

(0 0 , 0 1 , 0 3 , 0 4 , 0 5 , 0 6 , 0 7 , 0 8 , 0 9 , 1 0 , 1 1 , 1 2 , 1 3 , 1 4 , 1 5 , 1 6 , 1 8 , 1 9 , 2 0 , 2 8 , 2 9 , 3 0 , 3 8 , 3 9 , 4 0 , 4 8 , 4 9 , 5 0 , 5 8 , 5 9 , 6 0 , 6 8 , 6 9 , 7 0 , 8 0 , 8 9 , 9 0)

In Table 4, the final version of the MPK table that contains the same characters as ASCII second part table but represented by two digits.

Table 4. Comparison between MPK and ASCII encoding

MPK	ASCII	Char	MPK	ASCII	Char	MPK	ASCII	Char
0 0	032	space	3 8	064	@	5 8	096	`
0 1	033	!	2 5	065	A	2 1	097	a
0 3	034	"	2 6	066	B	2 2	098	b
0 4	035	#	2 7	067	C	2 3	099	c
0 5	036	$	3 5	068	D	3 1	100	d
06	037	%	3 6	069	E	3 2	101	e
0 7	038	&	3 7	070	F	3 3	102	f
0 8	039	'	4 5	071	G	4 1	103	g
0 9	040	(	4 6	072	H	4 2	104	h
1 0	041	)	4 7	073	I	4 3	105	i
1 1	042	*	5 5	074	J	5 1	106	j
1 2	043	+	5 6	075	K	5 2	107	k
1 3	044	,	5 7	076	L	5 3	108	l
1 4	045	-	6 5	077	M	6 1	109	m
1 5	046	.	6 6	078	N	6 2	110	n
1 6	047	/	6 7	079	O	6 3	111	o
0 2	048	0	7 6	080	P	7 1	112	p
1 7	049	1	7 7	081	Q	7 2	113	q
2 4	050	2	7 8	082	R	7 3	114	r
3 4	051	3	7 9	083	S	7 4	115	s
4 4	052	4	8 5	084	T	8 1	116	t
5 4	053	5	8 6	085	U	8 2	117	u
6 4	054	6	8 7	086	V	8 3	118	v
7 5	055	7	9 6	087	W	9 1	119	w
8 4	056	8	9 7	088	X	9 2	120	x
9 5	057	9	9 8	089	Y	9 3	121	y
1 8	058	:	9 9	090	Z	9 4	122	z
1 9	059	;	3 9	091	[	5 9	123	{
2 0	060	<	4 0	092	\	6 0	124	|
2 8	061	=	4 8	093	]	6 8	125	}
2 9	062	>	4 9	094	^	6 9	126	~
3 0	063	?	5 0	095	_			

As shown in the final table, each character can be represented by two digits only not three digits. So, the 1000 characters secret message will be represented by only 2000 digits which means 2000 pixels needed to be modified, not 3000 pixels. That means MPK method saved 1000 pixels which will enhance the PSNR of the stego image and also save a lot of capacity.

So, it can be said that by using the new proposed MPK encoding technique, one third of the required space for embedding capacity can be saved.
So, how to evaluate the new MPK encoding technique in the field of steganography? in the next section the MPK will be applied on the (MSLDIP) method and make a comparison between the results of (MSLDIP - MPK) method and our previously proposed (MSLDIP) method without modifying the method itself or any of its embedding steps, to decide whether modifying the secret message by using the new MPK encoding will enhance the performance or it won't.

5. EXPERIMENTAL RESULTS

Now, the new proposed MPK encoding technique will be tested by taking different messages and different cover images then MSLDIP using MPK (MSLDIP - MPK) and the original (MSLDIP) without MPK will be applied.

The obtained MHCs and PSNRs results are recorded and can be summarized in the following tables:-

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

Table 5. Comparison of MHCs between original (MSLDIP) and (MSLDIP – MPK) Methods

As shown in Table 5, after the Comparison of MHCs between original (MSLDIP) and (MSLDIP – MPK) methods has been done, it has been found that one third to the embedding capacity of the cover image has been added by using the original MSLDIP and MPK. So, the MPK encoding technique has proved its efficiency in the embedding capacity.

Cover Image (256 x 256)	Message Capacity	PSNR	
		MSLDIP	MSLDIP-MPK
Lena	6,656 bytes	48.68009	50.58189
Baboon	6,656 bytes	48.68028	50.15226
Boat	6,656 bytes	48.35419	50.24284

Table 6. 1st Comparison between (MSLDIP) and (MSLDIP – MPK) Methods

As shown in Table 6, after hiding the same message length 6,656 bytes in the cover images (Lena, baboon, boat) with size (256 x 256), using the (MSLDIP) and (MSLDIP – MPK) methods, it has been found that, the (MSLDIP – MPK) method has higher PSNR values than the (MSLDIP).

Table 7. 2nd Comparison between (MSLDIP) and (MSLDIP – MPK) Methods

Cover Image (256 x 256)	Message Capacity	PSNR	
		MSLDIP	MSLDIP-MPK
Boat	8,192 bytes	47.77530	49.36969
Bird	8,192 bytes	47.61975	49.54604
Flinstone	8,192 bytes	47.54466	49.25001

Also in Table 7, after hiding the same message length 8,192 bytes in the cover images (boat, bird, flinstone) with size (256 x 256), using the (MSLDIP) and (MSLDIP – MPK) methods, it has been found that, the (MSLDIP – MPK) method has higher PSNR values than the (MSLDIP).

Table 8. 3rd Comparison between (MSLDIP) and (MSLDIP – MPK) Methods

Cover Image (512 x 512)	Message Capacity	PSNR	
		MSLDIP	MSLDIP-MPK
Lena	75,836 bytes	44.23179	45.99333
Baboon	82,407 bytes	43.84178	45.36410
Peppers	75,579 bytes	43.95254	45.74744

In Table 8, a decision has been made to use large secret messages as shown in the table and (512 x 512) cover images. By using the (MSLDIP) and (MSLDIP – MPK) methods, it has been found that, the (MSLDIP – MPK) method has higher PSNR values than the (MSLDIP).

Table 9. 4th Comparison between (MSLDIP) and (MSLDIP – MPK) Methods

Cover Image Baboon	Message Capacity	PSNR	
		MSLDIP	MSLDIP-MPK
(128 x 128)	2,560 bytes	46.71704	48.37757
(256 x 256)	10,211 bytes	46.84267	48.32637
(512 x 512)	40,990 bytes	46.86696	48.36563
(1024 x 1024)	163,724 bytes	46.84914	48.44889

Finally in Table 9, the same cover image with different sizes and different secret messages have been used, and also the results are that the (MSLDIP – MPK) method has higher PSNR values than the original (MSLDIP).

6. CONCLUSION AND FUTURE WORK

In this paper a new encoding technique has been proposed that is called Mobile Phone Keypad encoding (MPK) for secret message that represent each character in the secret message by two digits only not three digits as ASCII encoding, which means it saved one third of the required space for embedding. This in turn enhanced the Maximum Hiding Capacity (MHC) of the cover image as shown in Table 5, also as a result of this the PSNR values have been enhanced as shown in the tables from Table 6 to Table 9 in the experimental results section. So, it can be said that, the new MPK encoding technique proved its efficiency in shrinking the number of digits needed to represent the secret message characters.

As a future work, we will try to develop a new image steganography method that make use of the new MPK encoding technique instead of ASCII encoding technique to obtain better results from shrinking the number of digits that represent the secret message characters as shown in the previous section.

7. REFERENCES

[1] 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.

[2] Shatnawi, A. M. A., " A New Method in Image Steganography with Improved Image Quality ", Applied Mathematical Sciences, Vol. 6, no. 79, 3907- 3915, 2012

[3] Bandyopadhyay, S. K. and Chakraborty, K., " Image Steganography Using DNA Sequence ", Asian Journal Of Computer Science And Information Technology, 50 – 52, 1:2 (2011).

[4] Husainy, M. A. F., " Image Steganography by Mapping Pixels to Letters ", Journal of Computer Science, 5 (1) : 33-38, ISSN 1549-3636, 2009.

[5] Kaur, J. and Kumar, S., "Study and Analysis of Various Image Steganography Techniques", IJCST Vol. 2, Issue 3, September 2011.

[6] 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.

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

[8] Swain, G. and Lenka, S. K., " A Novel Approach to RGB Channel Based Image Steganography Technique ", International Arab Journal of e - Technology, Vol. 2, No. 4, June 2012.

[9] Anu, Rekha and Praveen, " Digital Image Steganography ", International Journal of Computer Science & Informatics, Volume-I, Issue-II, 2011.

[10] Ghosal, S. K., " A New Pair Wise Bit Based Data Hiding Approach on 24 Bit Color Image using Steganographic Technique ", IEMCON 2011, organized by IEM in collaboration with IEEE on 5th and 6th January, 2011.

[11] Alnawok, F. and Ahmed, B., " Multi-Segment Steganography Technique ", The International Arab Journal of Information Technology, Vol. 5, No. 3, June 2008.

[12] Ibrahim, R. and Kuan, T. S., " Steganography Imaging System (SIS): Hiding Secret Message inside an Image ", Proceedings of the World Congress on Engineering and Computer Science 2010, Vol. I, WCECS 2010, October 20-22, San Francisco, USA.

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