Combining Cryptography and Steganography for Data Hiding in Images

HAYFAA ABDULZAHRA, ROBIAH AHMAD[1], NORLIZA MOHD NOOR
Department of Engineering,
UTM Razak School of Engineering and Advanced Technology,
UTM Kuala Lumpur, 54100 Jalan Semarak, Kuala Lumpur
Malaysia
Email: haifaa_atee@yahoo.com, robiah@ic.utm.my, norliza@ic.utm.my
[1]Corresponding author: robiah@ic.utm.my

Abstract: - Cryptography and Steganography are the two popular methods for secure data hiding and transmission available broadly. The techniques used information in order to cipher or cover their existence respectively. Cryptography is the science of using mathematics to encrypt and decrypt data; the data are converted into some other gibberish form, and then the encrypted data are transmitted. While Steganography is the art and science of hiding communication, a stenographic system, thus embeds hidden content in the unremarkable cover media so as not to provoke an eavesdropper's suspicion. In steganography the secret message embeds in a harmless looking cover such as a digital image file, then the image file is transmitted. The primary purpose of this paper is to improve a new method of hiding secret messages in the image, possibly by combining steganography and cryptography. A new encryption technique is used in order to lower the space of representing the characters. LSB method is used to hide the encrypted message into images. PSNR and MSE are used for measuring the quality of images; the results showed that the proposed method gives better results than simple LSB with higher PSNR lower MSE.

Key-Words: - Cryptography, Steganography, LSB, Data hiding, Stego-image, Private key.

1 Introduction

As digital information and data are transferred over the internet and securing sensitive messages need to discover and developed more often than ever before, new technologies for protecting and securing the sensitive messages needs to realize and develop. Because cryptography and steganography methods always exposed to attacks by Steganalysis, so we constantly need to develop and look for new modes. Cryptography and Steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way, which hides the existence of communication [1]. On the other hand, cryptography is the enciphering and deciphering of data and information with a secret code so it cannot be understood [2]. The Steganography hides the message so it cannot seen.However, cryptography systems can be broadly classified into symmetric-key systems that use a single key, both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message, for instance, might provoke. Suspicion on the part of the recipient while an invisible message created with steganographic methods will not. However, steganography can be useful when the use of cryptography is illegal. Where cryptography and strong encryption are barred, steganography can avoid such policies to pass the message secretly. However, steganography and cryptography differ in the way they are judged. Cryptography fails when the "enemy" is able to access the content of the cipher message, while steganography fails when the "enemy" detects that there is a secret message present in the steganographic medium.

The combination of these two methods will enhance the security of the data embedded. This combined will satisfy the requirements such as capacity, security, and robustness for secure data transmission over an open channel.

The difference between cryptography and steganography is a significant issue, and outlined by Table 1.

Table 1 Comparison between steganography and cryptography

Steganography	**Cryptography**
Unknowing message passing	Knowing message passing
Steganography prevents discovery of the very existence communication	Encryption prevents an unauthorized party from discovering the contents of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithms are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

Even though both methods provide security, this study proposes to combine both cryptography and steganography methods into one system in order to provide strong security, by using two levels of data encryption. After the data encryption done, the cipher text will hide inside the image using an LSB steganographic technique. The new encryption technique used five spaces to represent each character in the message and five pixel to conceal each character in the image.

2 Related Work

In recent years have seen a rapid growth of communications security and the threat of a trespasser gain access to secret information has been an ever present concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat. Both these techniques received more attention from the research community. The reason of this growing interest is due to the combined of these two techniques together are often achieved higher levels of security [3]. Ushl et al., [4] proposed an encrypting system, by combine's techniques of cryptography and steganography with data hiding. Instead of using a single level of data encryption, the message is encrypted twice. Conventional techniques have been used for this purpose. Then the cipher is hiding inside the image in the encrypted format for further use. It uses a reference matrix for the selection of passwords depending on the properties of the image.

Bharti and Soni [5] proposed a novel scheme based on steganography and cryptography to embed data in color images. This method shows its larger capacity for hiding data than other methods without loss of imperceptibility integer wavelet transform and Genetic algorithm. The method is very efficient, especially when applied to those images whose pixels are scattered homogeneously and for small data. Marwaha and Paresh [6] used traditional cryptographic techniques to achieve data encryption and visual steganography algorithms have been used to hide the encrypted data. Multiple cryptography proposed where the data was encrypted into a cipher and the cipher will be hidden into a multimedia image file in the encrypted format.

Umamaheswari[7] compress the secret message, encrypt it by the receiver's public key along with the stego key, and embed both messages in a carrier using an embedding algorithm. Kandar, and Maiti [8] proposed a technique of well-known k-n secret sharing for color images using a variable length key with share division using random numbers. Bairagi [9] describes how such an even-odd encryption based on ASCII value is applied and how encrypted message converting by using Gray code and embedding of picture that can secure the message and thus makes cryptanalyst's job difficult.

3 Proposed Scheme Items

The research proposed a new method of embedded secret message into image; it is combined between cryptography and steganography in order to provide higher capacity, robustness, and security. The proposed algorithm is designed based LSB (Least Significant Bit) method to hide encrypted message into image.

Input: cover image + secret message
Output: stego-image + private key

The private key is an important item in the proposed scheme, It consists of three parts as shown in Table 2.
Private Key = P1 + P2 + P3

Table 2 Private key elements

Key parts	Field width	Description
Part1 (P1)	2char.	First letter code in the message
Part2 (P2)	8char.	No. of embedding bits=no. of message characters * 5
Part3 (P3)	8char.	First store position in the image

A pictorial description of the proposed scheme which combined concepts of cryptography and steganography is shown in Figure 1.

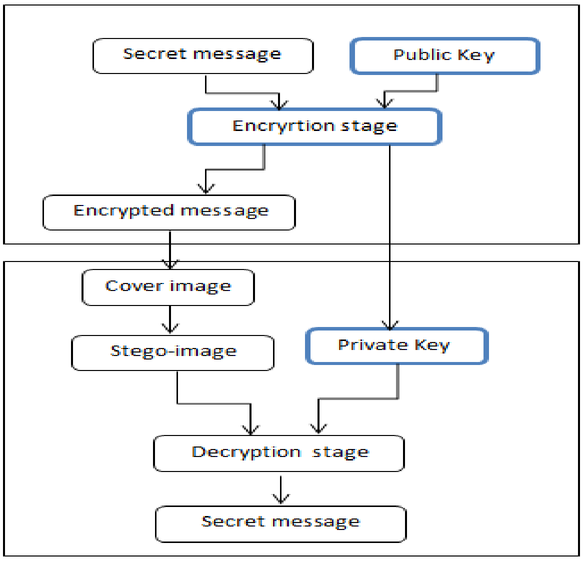


Fig.1 The general flowchart of proposed scheme

4 Embedded Algorithm

Cryptography and steganography are the two main stages of embedding algorithm.

4.1 Cryptography Stage

1.Create Table 3 which assigns a code number to each character in the English language (we can use random order for letters and space character or for numbers from 1 to 27). Table 3 considered as a public key which should be known to both parity.

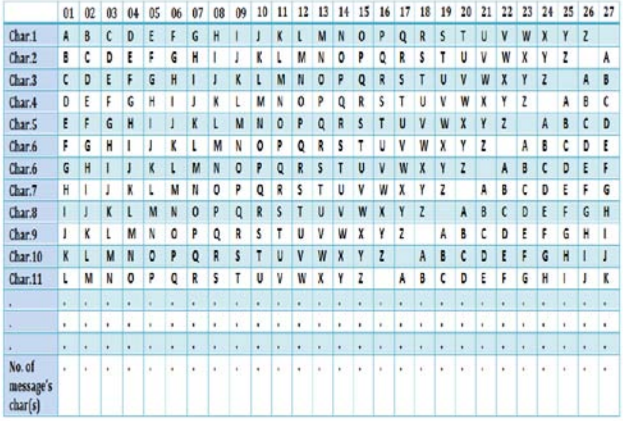
Code No.	Char.	Code No.	Char.	Code No.	Char.	Code No.	Char.
01	A	08	H	15	O	22	V
02	B	09	I	16	P	23	W
03	C	10	J	17	Q	24	X
04	D	11	K	18	R	25	Y
05	E	12	L	19	S	26	Z
06	F	13	M	20	T	27	SPACE
07	G	1	N	21	U		

Table 3 Code numbers of English language

2.Based on Table 3, the first part of the private key (P1) equals to the corresponding code for the first character in the secret message.

3.Create Table 4 which is the number of columns is 1 to 27, and the row's number equals to the number of message's characters. The first row starts with the first character in the message and continue alphabetically for other rows and columns.

Table 4 The general dynamic table



	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Char.1	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	
Char.2	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
Char.3	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
Char.4	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
Char.5	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
Char.6	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
Char.6	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
Char.7	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
Char.8	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
Char.9	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
Char.10	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
Char.11	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
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
No. of message's char(s)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

4.Apply Table 4 to obtain a decimal code values (i.e. column numbers) that corresponding to each character in the message. The values range between 1 to 27.

5. Convert decimal code values to binary code values. Five bits for each value.

4.2 Steganography Stage

1. The simple LSB method used to embed the secret message into the image; the last bit in each pixel used to conceal the stream of binary code in the cover image.

2. Stego-image and private key are achieved.

5 Extracting Algorithm

1. Read the stego-image and the private key.
2. Retrieve the eighth bit for the image pixels that starts with the first embedding position using P3 of the private key until the number of message's character (P2 of the key).
3. Split the stream of bits into groups of 5 bits; then convert each 5 bits to decimal value.
4. Use Table 3 to find the first character in the secret message which is corresponding to the code value of the P1 of the private key.
5. Use the first character to create Table 4.
6. Based on Table 4, extracting operation is performed by retrieving each character corresponding to the decimal value code from one row of Table 4 and continuing sequentially until getting all secret message characters.

6 Applying Proposed Method

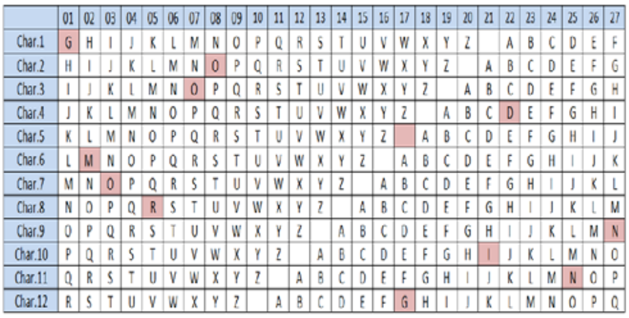
6.1 EmbeddingSteps

Assume to encrypt "GOOD MORNING" message:

1. The character "G" is the first character in the secret message. According to the Table 3, the code number that corresponding to "G" is 07. This is the first part P1 of the private key.

2. From Table 4, create Table 5 starting from the first character in the message "G" so that the number of table's rows equals to the number of message's characters, while the number of columns is 27.

Table 5 The dynamic table which starts with the first item in the message



	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Char.1	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
Char.2	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
Char.3	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
Char.4	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
Char.5	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
Char.6	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
Char.7	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
Char.8	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
Char.9	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
Char.10	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
Char.11	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
Char.12	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

3. Apply Table 5 to obtain the decimal values (i.e. column numbers) which corresponding to each character in the message, the value ranges between 1 to 27 as shown in Table 6.

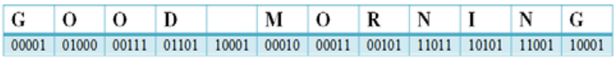
Table 6 Decimal values of the specific message

G	O	O	D		M	O	R	N	I	N	G
1	8	7	22	17	2	3	5	27	21	25	17

As seen, there are three "O" in the original message, but each one of them is coded with different codes, Furthermore, the code 17 assigned to "G" and "SPACE" characters. These properties, provide strength for the proposed algorithm.

4. Convert decimal value to a binary value. Five bits are assigned to each decimal value (i.e. 2^5 is used to represent all characters) as shown in table7.

Table 7: Binary values of the specific message



G	O	O	D		M	O	R	N	I	N	G
00001	01000	00111	01101	10001	00010	00011	00101	11011	10101	11001	10001

5. Embed the secret message into the image by using the LSB method. The eighth bit in each pixel uses to conceal the message binary code.
6. Stago-image and private key are achieved.

6.2 ExtractingSteps

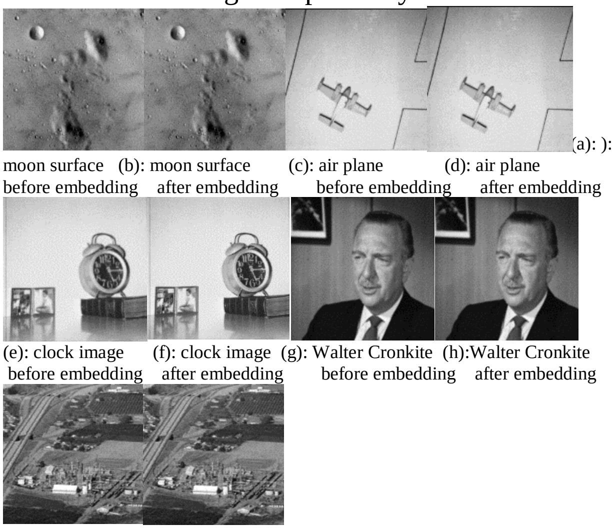
To extract the text from the image; apply the following steps:

1. Retrieve the first store position by the part P3 of the private key.

2. Retrieved thenumber of bits that will be known by part P2 of the private key.
3. Start with the known position in the part P3 of the private key until P2 (the number of message character), the eighth bit in each pixel of the stego-image will be retrieved.
4. Retrieve the binary code from the stego-image as below:
   000010000100111011011000100010000110010111011101011100110001
5. Convert each five bits to decimal value as below:
   1 8 7 22 17 2 3 5 27 21 25 17
6. According to the P1 and Table 3, the first character in the message will be known "G".
7. After creating Table 5 which starts with the letter "G", the extraction operation is performed by retrieving each character corresponding to the decimal value from one row of the Table 5 sequentially until getting the secret message.

7 Experimental Results

Experimental tests performed on grayscale and true color images of size 256*256, same message used for all tests. The eighth bit is used to hide the secret message in each host image. Good and encouraged results are achieved, for grayscale and true color images. Different host images are used, which are shown in Figures 2 and 3 before and after embedding using the proposed method. Tables 8 and 9 show the PSNR and MSE values resulting from embedding the secret message into the grayscale and true color host images respectively.

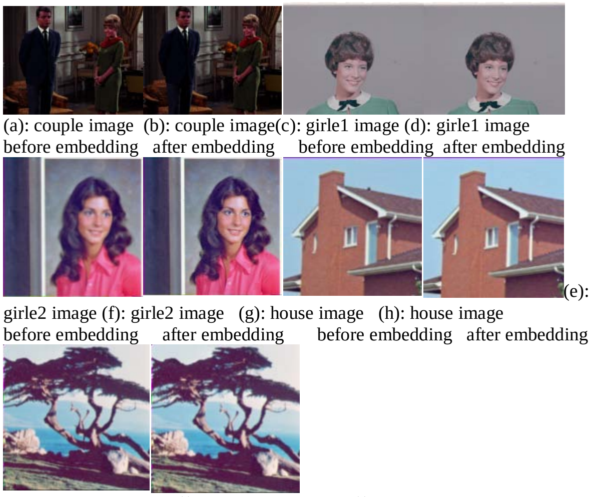


(a):):
moon surface (b): moon surface (c): air plane (d): air plane
before embedding after embedding before embedding after embedding

(e): clock image (f): clock image (g): Walter Cronkite (h):Walter Cronkite
before embedding after embedding before embedding after embedding

(i): chemical plant (j): chemical plant
before embedding **after embedding**

Fig.2 The five grayscale images that were used to embed the secret message



(a): couple image (b): couple image(c): girle1 image (d): girle1 image
before embedding after embedding before embedding after embedding

(e):
girle2 image (f): girle2 image (g): house image (h): house image
before embedding after embedding before embedding after embedding

(i): tree image (j): tree image
before embedding after embedding

Fig.3 The five true color images that were used to embed the secret message

Table 8 The PSNR and MSE results of embedding secret messages into grayscale host images

Host image	**Simple LSB**		**Proposed method**	
	PSNR	MSE	PSNR	MSE
Moon surface	78.541	9.1553	79.8611	6.7139
Air Plane	78.5141	9.1553	79.2199	7.720
Clock	78.6613	8.8501	79.7635	6.8665
Walter Cronkite	78.7369	8.6975	79.2199	7.2820
Chemical plant	78.2338	9.7656	80.7326	5.4932

Table 9 The PSNR and MSE results of embedding the secret message into true color host images

Host image	**Simple LSB**		**Proposed method**	
	PSNR	MSE	PSNR	MSE
Couple	82.8061	3.4078	83.9911	2.5940
Girle1	82.7417	3.4587	84.3458	2.3905
Girle2	83.0050	3.2552	84.3458	2.3905
House	82.6783	3.5095	85.0462	2.0345
Tree	83.7429	2.7466	84.9390	2.0854

In the simple LSB method, the maximum capacity for 256*256 gray and true color images with 65536 and 198808 bytes are 9362.2 and 28086.8 respectively, while in proposed method, which combines between cryptography and steganography, the maximum capacity for same images are 13107.0 and 39321.6 respectively, as shown in Table 10. Fig. 4 illustrates the comparative capacity diagram for LSB and the proposed method.

Table 10 The capacity comparison between simple LSB and proposed method for grayscale and true color images

Image type	Image size	LSB capacity	Proposed method capacity
Gray	65536 bytes	9362.2 char.	13107.2 char.
True color	196608 bytes	28086.8 char.	39321.6 char.

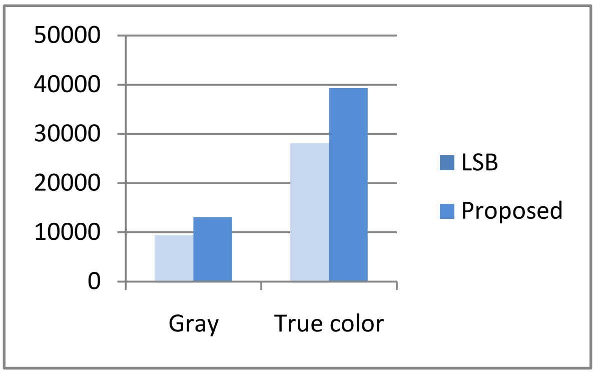


Fig.4 Comparing the capacities of the LSB and proposed method

8 Advantages of Proposed Method

1. Cryptography and steganography are combined in order to increase the strength of the algorithm.
2. A new encryption method is proposed, in this method each character represented by five bits only, while in conventional LSB each character represented by seven bits. That means increasing the capacity.
3. Characters have been converted to numbers where it is possible that the same character represented in different codes, and may be different characters can be represented in the same code. This increases the security and robustness against the attacks.
4. Simple, short, and effective private key used to extract the secret message.

9 Conclusion

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. The present study is designed to combine the features of both cryptography and steganography, which will provide a higher level of security. It is better than the technique used separately. Simple LSB method was used to embed the secret message into the image. The last bit in each pixel used to conceal the message binary code. The future work will be on including the small letters, symbols, and numbers from 0 to 9 in the Table 3.

AcknowledgmentThe authors would like to thank the Ministry of Higher Education (MOHE) Malaysia and Universiti Teknologi Malaysia (UTM)under grant Vote GUP 08J28 for the financial support provided throughout the course of this research.

References:

[1] Rajyaguru, M. H., Combination of Cryptography and Steganography With Rapidly Changing Keys,*International Journal of Emerging Technology and Advanced Engineering*, Vol.2, No.10, 2012, pp 329-332.

[2] Manoj, I. V. S., Cryptography and Steganography. *International Journal of Computer Applications* (0975–8887), Vol.1, No.12, 2010,pp 63-68

[3] Sherekar, S. S., Thakare, V. M., and Jain, S., Critical Review of Perceptual Models for Data Authentication,*Emerging Trends in Engineering and Technology (ICETET)2nd International Conference, 2009*, pp. 323-329. IEEE.

[4] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, 0*Computer Science and Network Technology (ICCSNT), International Conference,* Vol.2, No.2.11, 2011 ,pp. 1017-1020.IEEE.

[5] Bharti,P.,and Soni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,*International Journalof Computer Applications*,Vol.58,*No.*18,2012,pp1-5

[6] Marwaha, P., Visual cryptographic steganography in images,*Computing, Communication and Networking Technologies (ICCCNT), International Conference , 2010*,pp 1-6. IEEE.

[7] Umamaheswari, M., Sivasubramanian, S. and S. Pandiarajan S., Analysis of Different Steganographic Algorithms for Secured Data Hiding,*IJCSNSInternational Journal of Computer Science and Network Security,* Vol.10, No.8, 2010, pp 154-160.

[8] Kandar. S, and Maiti. A., Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number, *Internationa Journal of Computer Applications* (0975 – 8887) Vol.19, No.4, 2011, pp 35-40.

[9] Bairai, A. K., ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security,ISSN 2078-5828 (Print), ISSN 2218-5224 (Online), Vol.01,No.2,2011, pp 37-41, Manuscript Code: 110112.