EXPLORING STEGANOGRAPHY: SEEING THE UNSEEN

Sravya Jarugu

U00299001

EXPLORING STEGANOGRAPHY: SEEING THE UNSEEN

Abstract: *When communicating over an untrusted medium such as Internet, information protection plays a very important role. In the current communication, the two conventional techniques used to cipher or hide information are cryptography and steganography are respectively. To achieve information security there are a number of ways from which cryptography and steganography standout. Cryptography is the area in science which deals with mathematics to encrypt or decrypt any given information or data which is converted to an obscure format. Sending messages that hides the very existence of the communication in the real world is the art and science of secret communication called Steganography. The message is sent in an unintelligible form such that only the receiver can remove the disguise to extract the encrypted text in cryptography. Digital media plays an important role in steganography where data is hidden (embedded) in media files which include image, video, or audio and the file is then transmitted in steganographic systems. This report describes the main existing methods and techniques in steganography that allows us to hide the existence of a message along with steganalysis techniques to counter them. Further, it emphasizes a method of hiding secret messages in the image, by combining steganography and cryptography. To lower the space of representing the characters a new encryption technique is used. Least Significant Bit (LSB) is a method where the message to be sent is embedded and hidden in the message. The quality of images is measured by calculating PSNR and MSE. The proposed system is subjected to LSB and the corresponding PSNR and MSE results when calculated gave better results than simple LSB with higher PSNR lower MSE.*

INTRODUCTION:

Covert communication is one of the most major concerns in today's world. With the growing needs of the secure means to transfer an information via Internet, the process of exchanging information secretly has become valuable due to the increase of data to be exchanged over Internet. Hence, the confidentiality and integrity of data requiring protection of unauthorized access and use of wanton, has led to tremendous growth in the field of data hiding. Systems for protection are divided to steganography which hides or Cryptography which encrypts the information or a mixture of both.

Hiding of such that the detection of messages gets impractical is the art of Steganography. Vast array of secret communication methods can be used to conceal the existence of a message. Data can be hidden either using microdots, character arrangement, digital signatures, invisible inks, covert channels. Using Steganography, information can be hidden in various mediums known as carriers. The carriers can be images, audio files, video files and text files. On the other hand, Cryptography is derived from the Greek words: “kryptós” meaning "hidden" and “gráphein” meaning "to write" - or "hidden writing". It refers to the art of maintaining the secrecy of data by converting it to some other form.

Steganography by itself does not ensure secrecy, but neither does simple encryption. If these methods are combined, however, stronger encryption methods result. Security is achieved when cryptography and steganography are solely used , but in a wide area network such as Internet, it does not withstand security attacks. Hence, Steganography and Cryptography can be combined to hide a secret message. (i.e. If an encrypted message is intercepted, the interceptor will know that the text is an encrypted message. But the interceptor may not know that a hidden message even exists with steganography). This provides two levels of security and with the usage of encryption and combining hashes, integrity and authentication can be achieved.

STEGANOGRAPHY:

In information-hiding systems, there are three different aspects contended with each other: capacity, security and robustness.

Capacity – The total amount of information which can be embedded into a cover medium is called capacity. The cover mediums include image, media file etc.

Security – The inability of an eavesdropper's to detect hidden information is termed as security. Robustness – Resistance to the modification of stego medium (i.e. it should withstand if an adversary tries to destroy hidden information). Steganography is all about embedding a secret message. There are three types of approaches for steganography:

- Pure Steganography
- Secret Key Steganography
- Public Key Steganography

PURE STEGANOGRAPHY:

Pure Steganography is a technique that uses steganography solely but doesn't not combine with any other approaches. It hides information within cover carriers.

SECRET KEY STEGANOGRAPHY:

This technique uses a combination cryptography and steganography where a secret key cryptography technique is dealt with the steganography approach where an encrypted message is hidden within a cover carrier.

PUBLIC KEY STEGANOGRAPHY:

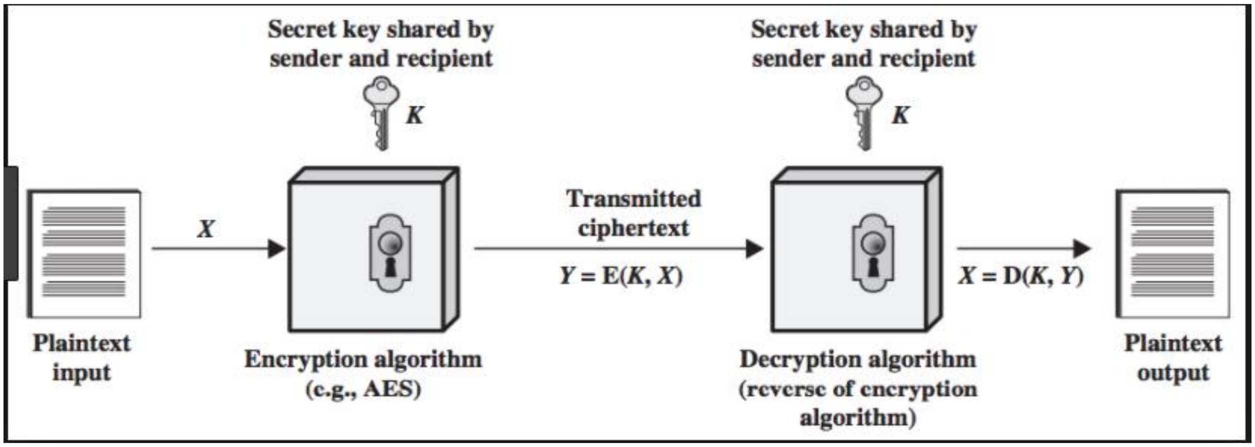
This technique uses a combination cryptography and steganography where a public key cryptography approach is used along with steganography. Encrypt the message with the public key then hide the encrypted within the cover carrier.

CRYPTOGRAPHY:

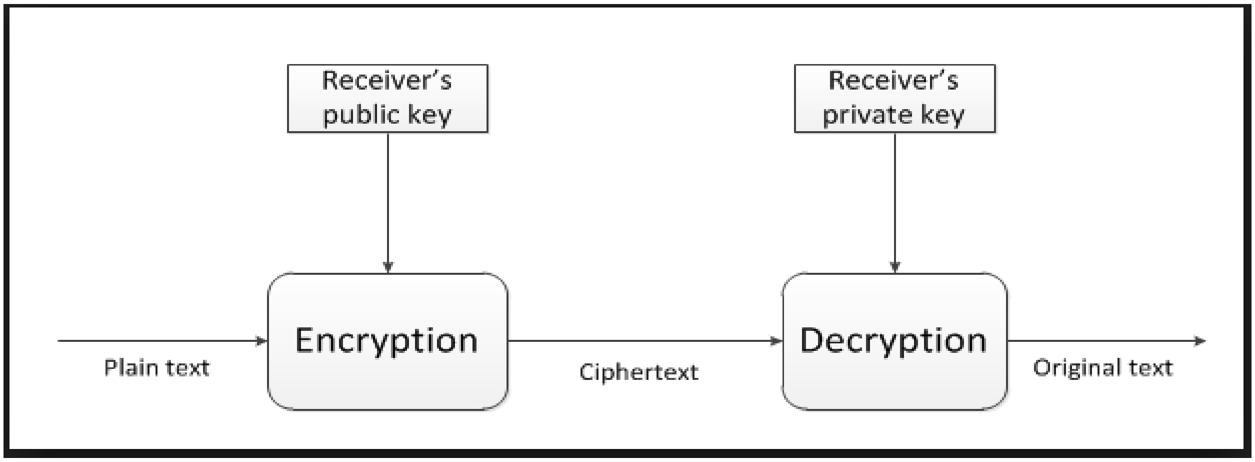
Data cryptography [3] can be described as the scrambling of the content of data to make it unreadable, unintelligible during the transmission or storage called Encryption. Keeping the data secure from unauthorized attackers is the main aim of cryptography. The reverse of this data Encryption is Decryption to retrieve the original data. Plain Text is the original data that is to be transmitted which is readable and understandable by the person. Some encryption algorithms are applied to this plain text which is called as Encryption of the data to get the Cipher text. The cipher text is then decrypted which is called as decryption to retrieve the original data. A cryptosystem provides schemes for both encryption and decryption. Cryptography systems are categorized into symmetric and asymmetric.

- Symmetric-key systems - use a single secret key shared by the sender and the receiver. The sender will encrypt the message using the secret key to generate the cipher text and sends it to the receiver. The receiver will decrypt the cipher-text using the secret key and retrieves the original message.
- Asymmetric-key systems/public-key – These systems relies on two keys – one which is known to the world called a public key and the other which is known only to the recipient of the messages called as the private key.

SYMMETRIC ENCRYPTION


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D(K, Y)
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

ASYMMETRIC ENCRYPTION

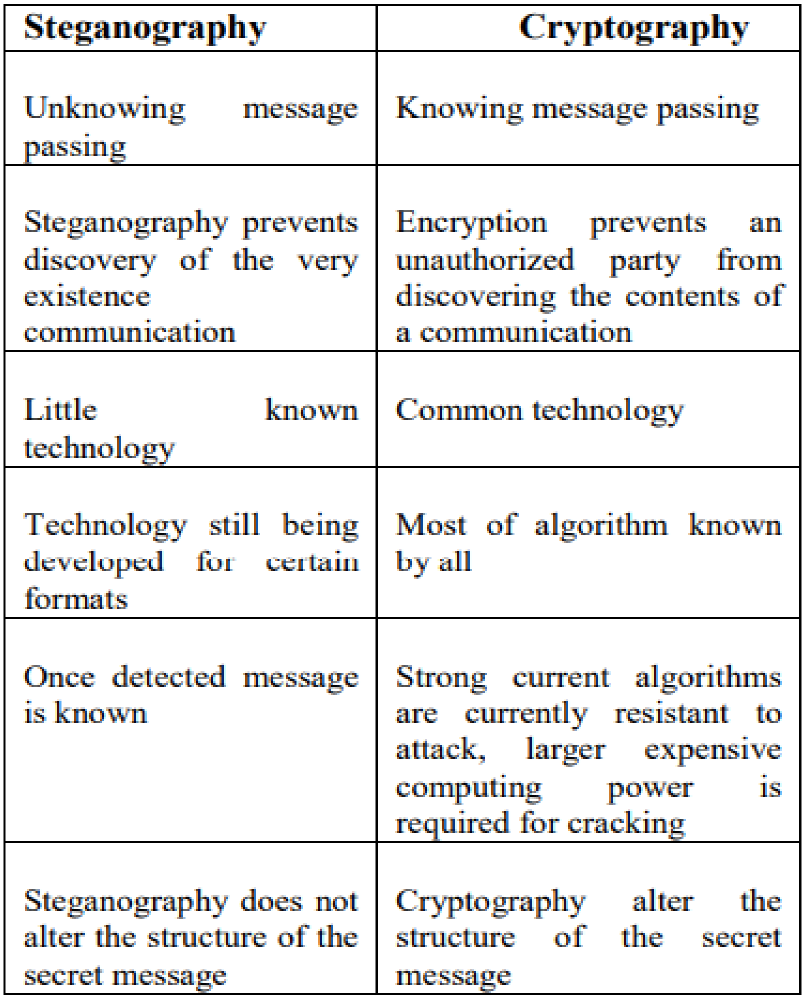


There are some standard methods that use cryptography- Symmetric encryption, Asymmetric encryption, Hash functions and Digital Signatures.

HASH FUCNTIONS:

A hash function [3] over a data of size M will generate a hash value where H = H(M). A hash functions stands good if it is able to generate random outputs which are evenly distributed when a function is applied over a large data set of inputs. The main aim of the hash function is to achieve data integrity. The hash value is usually attached to the message and even a bit change in the message reflects a change in the hash value. A cryptographic hash function is an algorithm for which it is computationally infeasible to find either (a) A data object that maps to a pre-specified hash result or (b) Two data objects that map to the same hash result. For the reasons specified, hash functions are generally used to make sure that data is not changed.

DIGITAL SIGNATURES: A digital signature [3] gives the receiver a reason to believe that the message was created by a known sender (i.e. it assures authentication) and the sender cannot deny having sent the message. Data is embedded together with the Digital Signature and is encrypted with the private key to send it to the other party.



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

The picture above gives the basic difference between Steganography and Cryptography.

STEGANOGRAPHY SYSTEM

It is a mechanism which embeds a secret message [2] ‘m’ in ‘c’ using ‘k’. (Where m = message, c = cover, k = shared secret key). The results in ‘s’ (where s = stego object) that carries the message ‘m’. Therefore stegosystem is defined as a pair of mappings (F,G) with F serves as the embedding function and G as the extraction function. [2]

$$s = F(c,m,k)$$

$$m = G(s,k)$$

If M is the set of all possible messages, then the embedding capacity of the stegosystem is log2 M bits. The embedding efficiency [2] is defined as

$$e = \frac{\log_2 M}{d(c,s)}$$

The set of all cover objects C is sampled using a probability distribution P(c) with c ∈ C, giving the probability of selecting a cover object c. If the key and message are selected randomly then the Kullback-Leibler distance gives the measure of the security of the stegosystem [2]

$$KL(P|Q) = \sum_{c \in C} P(c) \log \frac{P(c)}{Q(c)}$$

The determination of the best embedding function from a cover distribution is an NP-hard problem. The main aim of steganography is to hide a file in another file.

TEXT STEGANOGRAPHY

In this method in the nth letter of every word of a text message the secret message is hidden. Due to the boom in the internet and different types of digital files its importance has decreased. Text files have a very small amount of data hence text steganography using digital files is not used very often.

AUDIO STEGANOGRAPHY

In this method in a medium such as an audio file, the secret message is hidden in an imperceptible manner. The characteristics of stego message that is derived after steganography will be same as the and the host message that is present before steganography. There are a variety of techniques for embedding messages into digital, but it is a very difficult process and is very expensive.

IMAGE/VIDEO STEGANOGRAPHY

In this type of steganography, the secret message is hidden inside a digital image using embedding algorithms and a secret key. Stego image which is the resultant is sent to the receiver. It is then processed by the extraction algorithm using the same key. This stego-image when sent from a sender to the receiver on the other end, an unauthorized person can only notice the transmission of an image but the existence of the hidden message inside the image cannot be guessed. Video Steganography is a technique in which the secret message is hidden inside a video file.

DATA HIDING TECHNIQUES IN IPv4 HEADER

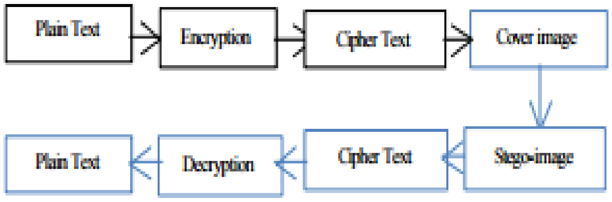
Network uses the jigsaw puzzle analogy for secure transmission of the data. They insinuate to fragment the data into variable sizes instead of fixed length and append each fragment of data with a pre-shared MAC along with a sequence number through which the receiver can authenticate and then combine the fragments to retrieve the original message. Every data fragment is prefixed and also suffixed with a binary 1 and then XOR'ed with a randomly generated number called the one-time pad on the sender side and then transmitted over the network. An exact opposite process of what the sender has followed will be carried out by the receiver upon receiving the message.

LSB [2]

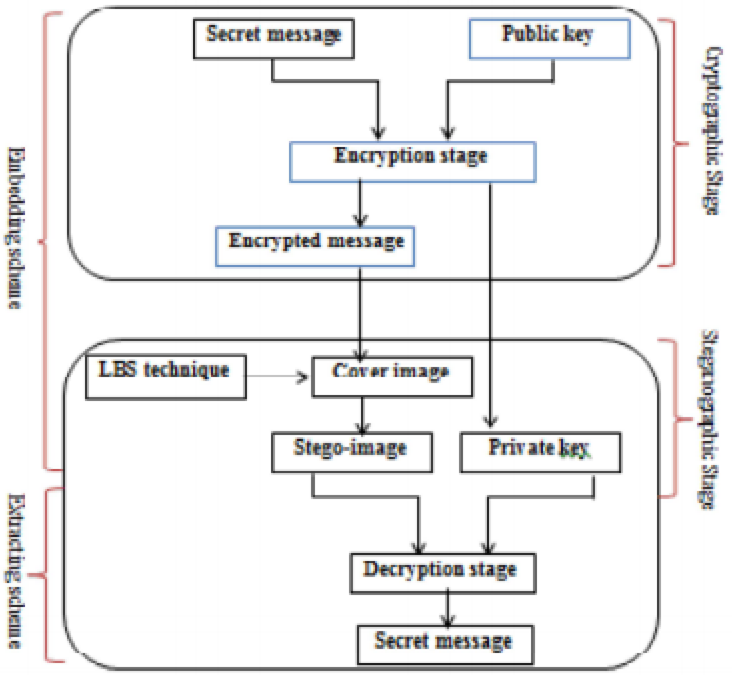
Several steganographic methods have been proposed during the past few years. Most of them are seen as substitution systems that are based on the Least Significant Bit (LSB) technique to encode. Jsteg was the first publicly available steganographic system. In this approach the least significant bit of the DCT coefficients is replaced with the message data. As Jsteg does not require a key, therefore, an attacker knowing the existence of the message will be able to recover it. Due to this simplicity LSB embedding of Jsteg is the most common method implemented today. Using any digital image, LSB replaces the least significant bits of each byte by the hidden message bits.

PROPOSED SYSTEM:

A Simple LSB algorithm along with the techniques of cryptography and steganography is shown in the figure below. The embedding scheme consists of a cryptographic stage and a steganographic stage. In the cryptographic stage, the public key and the secret message are used to produce the encrypted message. In the steganographic stage, the encrypted message concealed in the cover image using LSB technique is used to produce the stego image. While decryption, the private key and the stego-image are used to retrieve the secret message using the extracting scheme. To provide more capacity, robustness, and security cryptography is combined with steganography.



Combination of Cryptography and Steganography ((Encryption/Decryption processes)



General flowchart of LSB algorithm combined with Cryptography and Steganography

Input: cover image + secret message

Output: stego-image + private key

Private Key = P1 + P2 + P3

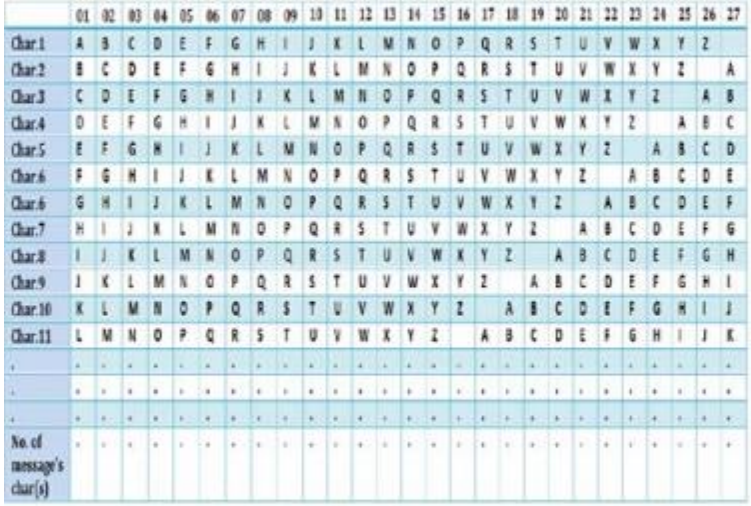
Key parts	Field width	Description
Part1 (P1)	2char.	First letter code in the message
Part2 (P2)	8char.	No. of embedding bits=no. of message characters * 5
Part3 (P3)	8char.	First store position in the image

CRYPTOGRAPHIC STAGE [1]:

- In the cryptographic stage, a code number is assigned to each character in English language. Table 2 is considered as a public key which is known to both the parties.
- 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.

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 2: code numbers given to each alphabet

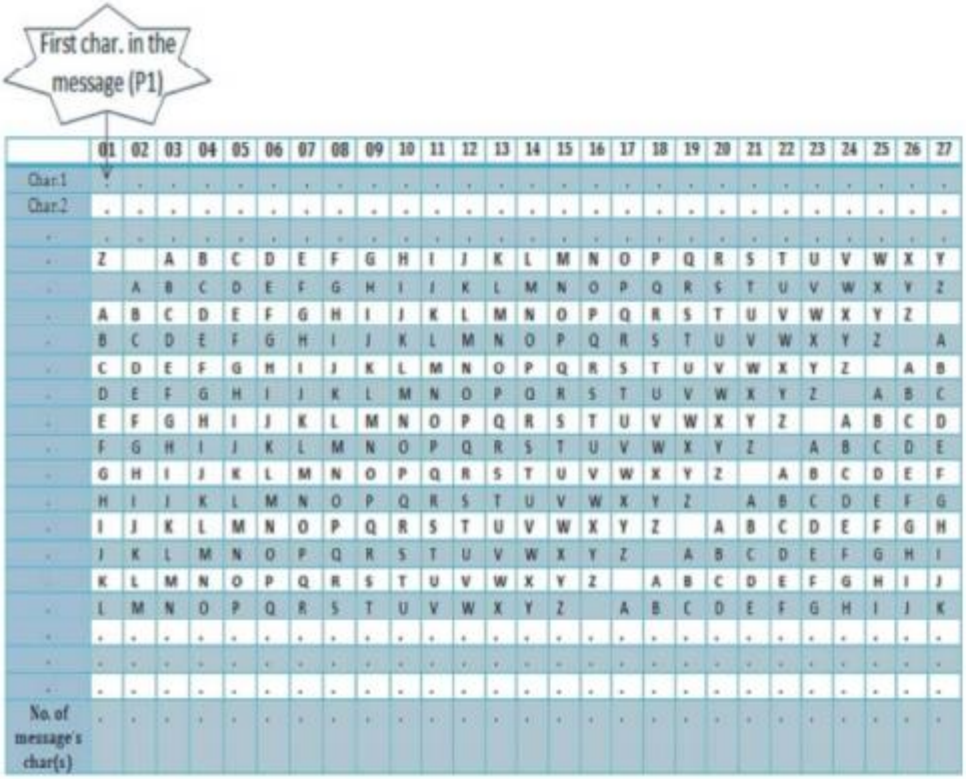


	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Char.1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Char.2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		A
Char.3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	B
Char.4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	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)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Table 3: The general dynamic table

Create Table 3, 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.

- Obtain the decimal code values (i.e. the column numbers) corresponding to each character in the message by applying Table 3. The values range between 1-27.
- Convert the obtained decimal code values to binary code values. For each value five bits are allocated.



First char. in the message (P1)

	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	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
Char.2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	Z		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
.		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
.	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	
.	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
.	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
.	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
.	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
.	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
.	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
.	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
.	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
.	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
.	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
.	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)	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Table 3: General dynamic table

STEGANOGRAPHIC STAGE:

LSB method is used to embed the secret message into the image. The last bit in each pixel of the image is used to conceal the stream of binary code in the cover image resulting in a Stego-image. With this the stego-image and the private key are achieved.

EXTRACTING ALGORITHM [1]:

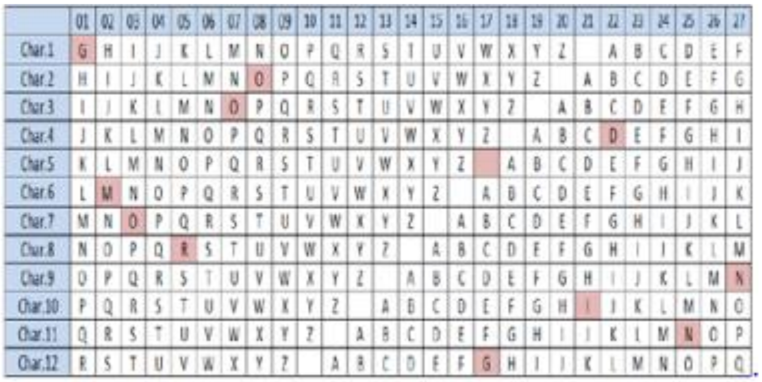
1. Initially read the stego-image and the private key.
2. Retrieve the eighth bit for the image pixels that starts with the first embedding position using the P3 part of the private key until the number of messages's character.
3. Convert each of 5 bits to decimal value by splitting the stream into groups of 5-bits.
4. Using the Table 2 to find the first character in the secret message corresponding to the code value of the P1 of the private key.
5. Using the first character create Table 3.
6. Retrieve each character corresponding to the decimal value code from one row of Table 4 and continue sequentially until all the secret message characters are retrieved. This is the extraction operation.

APPLYING THE PROPOSED METHOD:

Embedding Steps:

Assume to encrypt “GOOD MORNING” message:

1. The first character in the secret message is ‘G’. According to Table 2, the code number that corresponds to ‘G’ is 07 which is the first part of the private key P1.
2. Create Table 4 using Table 3 starting from the first character in the message, ‘G’ such that the number of rows in the table equal to the number of characters in the message where the number of columns is 27.



	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

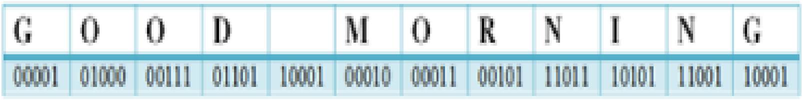
Table 4: A dynamic table that starts from the first character in the message

3. Using Table 4, obtain the decimal values corresponding to each of the characters in the message. The values range between 1-27 as shown in Table 5.

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

Table 5: Decimal values for each character in the message

4. Convert the decimal values obtained to a binary value. Assign five bits to each decimal value as shown in Table 6.



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

Table 6: Binary values specific to the message

5. The secret message is embedded into the image by using LSB method. The eighth bit of the pixel is used to conceal the message binary code.

EXTRACTING STEPS: Apply the following steps to extract the text from the image.

1. The first store position is retrieved by the P3 part of the private key.
2. From P2 part of the private key retrieve the number of bits.

3. Start with the known position in the part P3 of the private key until P2. The eighth bit in each pixel of the stego-image will be retrieved.
4. From this extract the binary code from the stego-image as:

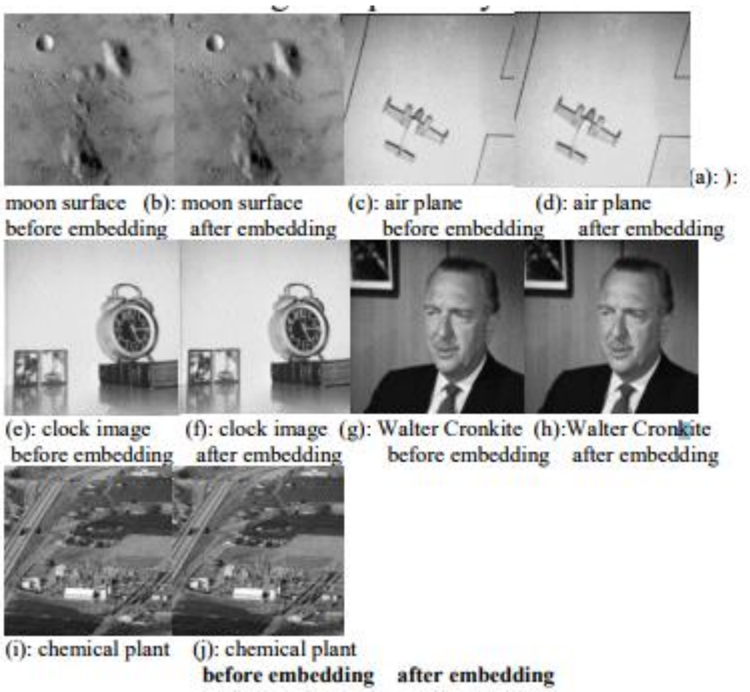
   00001 00001 00111 01101 10001 00010 00011 00101 11011 10101 11001 10001
5. Convert each of the five bits into their corresponding decimal value and the output of these will be :

   00001 00001 00111 01101 10001 00010 00011 00101 11011 10101 11001 10001

   1 8 7 22 17 2 3 5 27 21 25 17
6. According to P1 and Table 2, the first character in the message is known that is “G”
7. After the creation of Table 5, which starts with letter ‘G’, the extraction operation is performed by retrieving each character corresponding to the decimal value from one row of the Table 4 sequentially until getting the secret message.

EXPERIMENTAL RESULTS:

Experimental tests were performed on grayscale and true color images of size 256*256 and the same message is used for all tests. The eighth bit is used to hide the secret message in each host image. Successful results were achieved, for grayscale and true color images. Below are the host images used before and after embedding using the proposed method.



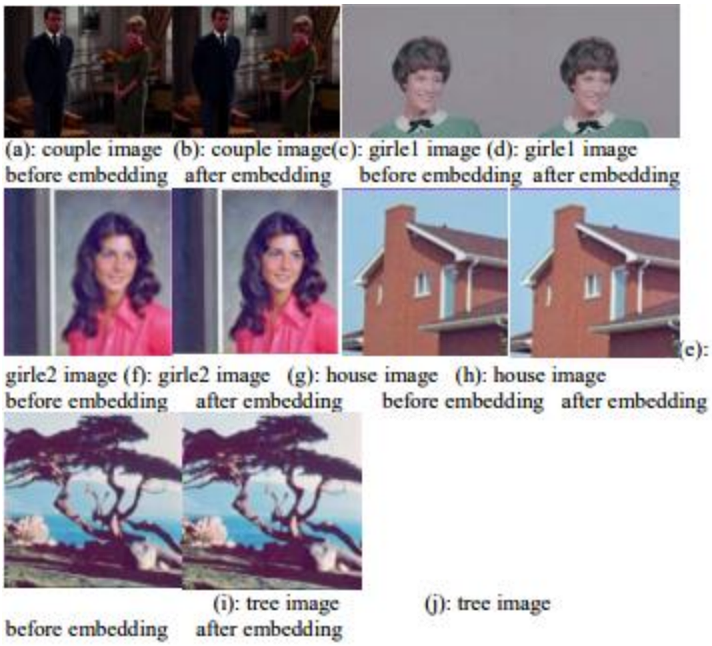
(a):):

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

Gray scale images that were used to embed the secret message



(a): couple image before embedding (b): couple image after embedding (c): girle1 image before embedding (d): girle1 image after embedding (e): girle2 image before embedding (f): girle2 image after embedding (g): house image before embedding (h): house image after embedding (i): tree image before embedding (j): tree image after embedding

Five true color images that were used to embed the secret message

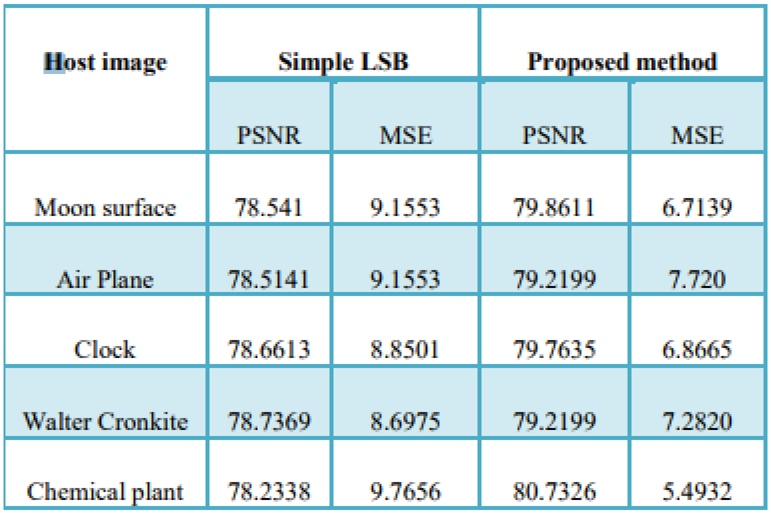
PERFORMANCE MEASUREMENT:

PSNR [2] considered as the most accurate metrics to judge imperceptibility. In addition, MSE is the other metric function, which can be used to estimate the robustness of the stenographic method. The capacity, which is the maximum amount of messages embedding in an image, measured by equation (1) and equation (2).

$$\text{PSNR} = 10 * \log\left(\frac{255^2}{MSE}\right) \qquad (1)$$

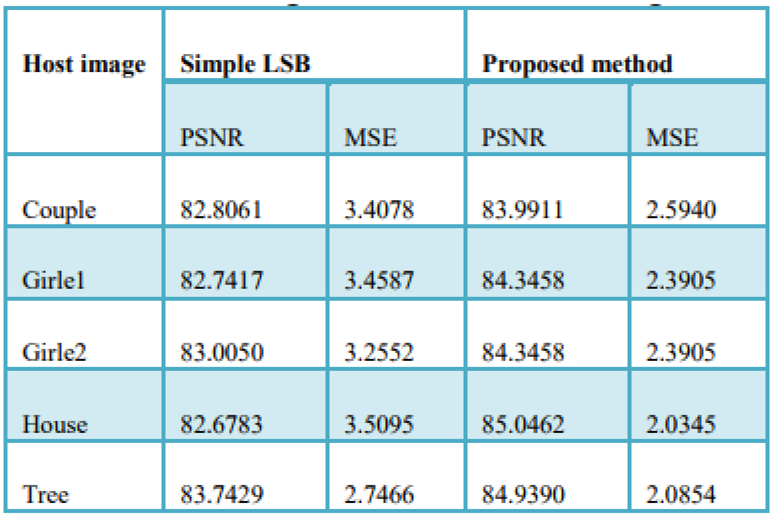
$$\text{MSE} = \sum_{i=1}^{x}\sum_{j=1}^{x}\frac{\left(\left|A_{ij}-B_{ij}\right|\right)^2}{x * y} \qquad (2)$$

Where A represents the original message. B, represents the cover image and x,y represent the number of rows and columns of the original and cover images. Using the simple LSB method, the maximum capacity for 256*256 gray and true color images with 65536 and 198808 [reference 1] bytes are 9362.2 and 28086.8 respectively. Using the proposed method, that has cryptography combined with steganography, the maximum capacity for the same images are 13107.0 and 3931.6 respectively.



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

PSNR and MSE results when secret message is embedded into grayscale images [reference 1]



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

PSNR and MSE results when secret message is embedded into true color images [reference 1]

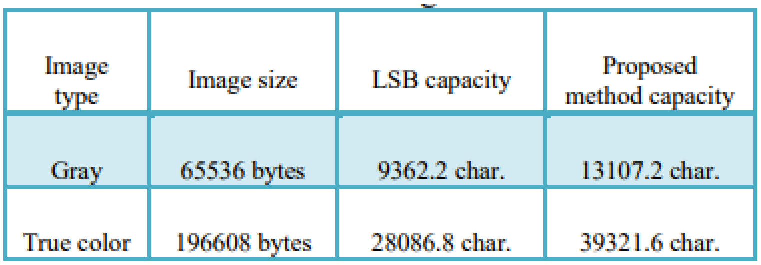


Image type	Image size	LSB capacity	Proposed method capacity
Gray	65536 bytes	9362.2 char.	13107.2 char.
True color	196608 bytes	28086.8 char.	39321.6 char.

Comparison of the capacity between simple LSB and the proposed method

For grayscale and true color images

ADVANTAGES OF THE PROPOSED METHOD:

1. The proposed method provides two levels of security and increases the strength of the algorithm as it combines both cryptography and steganography.
2. The capacity is increased as each character is represented by five bits.
3. In this method, characters have been converted to numbers. It is possible to have the same character represented in different codes and different characters represented in the same code. This increases security and robustness against attacks.
4. A simple, short and easy to understand private key is used to extract the message.

CONCLUSION:

The review presented is the combination of cryptography and steganography to achieve higher levels of security. Encryption only obscures the meaning of the message, but not its existence. Therefore, Steganography that hides the existence of a message is used to supplement encryption. Ensuring security of the data is one of the biggest challenges for computer users. Hence, in the current study, a simple LSB method is used to embed the secret message into the image and the last bit in each pixel is used to conceal the message in binary code**. When the message is encrypted using some cryptographic algorithm and hidden into a message using steganography, even if the attacker gets aware of the steganographic technique, he needs t know the cryptographic decoding key to retrieve the secret information. This provides two layers of security.** Satisfactory results are obtained when the proposed method is tested on a sample of grayscale images and true color images resulting in high level of capacity, higher PSNR for security and lower MSE for robustness against attacks.

DISCUSSION POINTS:

- As explained, a simple LSB used the sequential concealment technique to embed the message into an image. This can be further improvised by using some technique for random concealment to hide the secret message into the image.
- To improve the randomness of the LSB embedding position we encrypt the message which control the embedded position such that the hidden information cannot be extracted without the corresponding private key. To prevent the forgery of the hidden information, we can also add a digital signature to authenticate such that only the rightful person can extract the information. Consider the scenario where we can use digital signatures. The sender will first sign the message and can then encrypt using RSA algorithm explained in [3]. Using some source code generate the public key and the private key for encryption and decryption.

  ENCRYPTION PHASE:

  The sender can send a control message M by encrypting with his own private key to produce the cipher text d1(M), then with the recipient’s public key e2 to do the second encryption generating cipher text e2(d1(M)). After embedding this encrypted secret message in the image we can derive the stego-image.

DECRYPTION PHASE:

After the receiving end, the receiver will decrypt using his private key for the first time to restore the cipher text d1(M), (i.e. d2(e2(d1(M))) = d1(M)) and then with the sender's public key to do the second decryption to get the control message M (i.e. e1(d1(M)) =M).

REFERENCES:

1. http://www.wseas.us/e-library/conferences/2014/Malaysia/ACACOS/ACACOS-17.pdf - HAYFAA ABDULZAHRA, ROBIAH AHMAD1, NORLIZA MOHD NOOR Department of Engineering, UTM Razak School of Engineering and Advanced Technology, UTM Kuala Lumpur, 54100 Jalan Semarak, Kuala Lumpur Malaysia.

2. https://www.researchgate.net/publication/230773060_Combining_Steganography_and_Cryptography_New_Directions - Combining Steganography and Cryptography: New Direction, Khalil Challita and Hikmat Farhat Computer Science Department Notre Dame University - Louaize, Lebanon kchallita,hfarhat@ndu.edu.lb

3. Cryptography and Network Security – Seventh Edition, By William Stallings

4. https://pdfs.semanticscholar.org/4953/6d47887d5c8de44d2d50bc9067cfe377d601.pdf - Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding, Hayfaa Abdulzahra Atee, Robiah Ahmad and Norliza Mohd Noor 1 23, Foundation of Technical Education, Baghdad, Iraq 1, Department of Engineering, UTM Razak School of Engineering and Advanced Technology, 2,3.UTM Kuala Lumpur, 54100 Jalan Semarak, Kuala Lumpur, Malaysia

5. http://docsdrive.com/pdfs/ansinet/jas/2010/1650-1655.pdf **-** An overview given by B.B Zaidan, A.A Zaidan - Faculty of engineering multimedia university, Jalan Multimedia and A.A Alfrajat, H.A Jalab - faculty of Computer Science and Information Technology, University Malaya.