International Journal of Mechanical Engineering & Computer Sciences, Vol.1, Issue 1, Jan-Jun, 2017, pp 01-11

HYBRID KNAPSACK PUBLICK KEY CRYPTOGRAPHIC-STEGANOGRAPHY SYSTEM

DR.ENG. SAAD M. KHALEEFAH AL-JANABI.
Assistant Professor ,
Al-Turath Colledge University,
Baghdad-Iraq

www.arseam.com

ABSTRACT

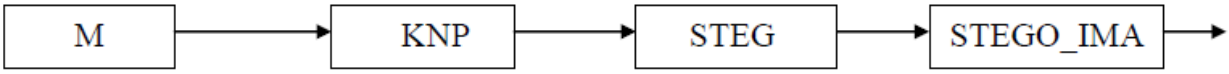
In this system we made a combination between a cryptography and steganographic we use the technique which is called least significant bit (LSB). A cryptographic system which we used it is a knapsack public key crypto system . First we used the cryptographic system to generate the ciphertext and second is the steganography which is embedded the ciphertext in it . In this paper we gave explanation of this hybrid system and gave a computer example to represent the system .In this case we strengthen the knapsack system by the steganography system.

KEYWORDS *:Knapsack , Steganography ,Cryptography , public key.*

INTRODUCTION:

In this way of combination we used first the knapsack procedure which is a part of public key for ciphering and then we embed the secret message in the covering image . We used the technique least significant bits (LSB) which is technique used in steganography we got a stego-image for the cipher-text which is the output of cryptography and then transmit in the channel to the receiver .as shown in fig (1).

At the receiver , first of all we extract the bits of cipher-text from stego-image by using the steganography to extract the bits of the secret message which embedded in the cover image .then we use the deciphering procedure of the Knapsack to obtain the original message .as shown in fig(2).



Fig(1). Block Diagram for Transmitter

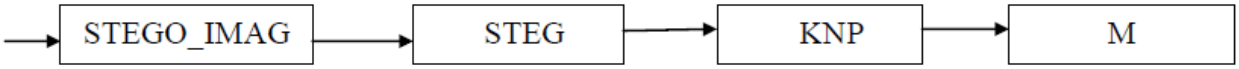


Fig (2). Block diagram for receiver

2 . STEGANOGRAPHY:

Steganography is the art and science of communication in a way which hides the existence of the communication .in contrast to cryptography , where the enemy is allowed to detect intercept and modify message without being able to violate certain security premises guaranteed by a cryptosystem [1].

Stegaography is derived from greek means "covered writing ".

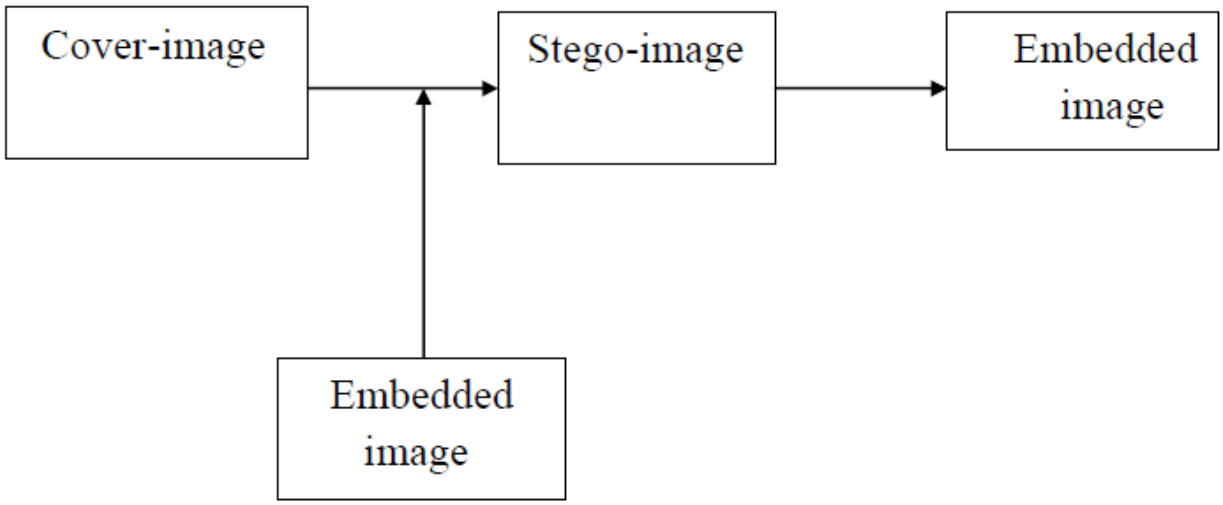


Fig (3). The Steganographic System.

2.1 STEGANOGRAPHY TECHNIAUES:

Information hiding techniques are receiving much attention today. The main advantage for this is largely bits of information .

There are many ways to hide information in digital images .The following approaches[2]:

- Least significant bit insertion .
- Masking and filtering .
- Algorithems and transformation.

2.2 LEAST SEGNIFICANT BIT INSERTION:

Many stego-tools make use of least significant bit (LSB).for example .11111111 is an 8-bit binary number .the rightmost bit is called the LSB because changing it has the least effect on the value of the number .The idea is that the LSB embedded in cover image produce little change to the overall file .the binary data of the secret message is broken up and then inserted into the LSB of each pixel in the image file.

Using the red ,green ,blue (RGB) model a stego-tool makes a copy of an image palette ,say , an 8-bit image. The LSB of each pixel is 8-bit binary number is replaced with one bit from the hidden message . a new RGB color in the pixel is changed to 8-bit binary number of the RGB color.

The cover image contents in each color 8-bits binary number of each pixel RGB color. The LSB of each pixel's 8-bit binary number is one bit or two which have no effect on the cover image of the hidden data .

2.3 ASIMPLIFIED EXAMPLE WITH A 24-BIT IMAGE:

1 pixel :

(00100111 11101001 11001000)

red green blue

LSB insertion works well with gray-scale images as well. It is possible to hide data in the least and second least significant bits and the human eye would still not be to discern it.

Unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression . for example ,converting a GIF or a BMP image ,which reconstructs the original message exactly (lossless compression), to a JPEG format, which does not (lossy compression), and then converting back , can destroy the data in the LSBs.

2.4 MASKING AND FILTERING:

Masking and filtering techniques hide information by marking an image and is usually restricted to 24-bit and more gray-scale image. digital watermarks include information such as copyright ,ownership ,or license.

2.5 ALGORITHMS AND TRANSFORMATIONS :

Another steganography techniques is to hide data in mathematical function that are in compression algorithms .

3 . THE PUBLIC-KEY CRYPTO-SYSTEM :

In the public key crypto system we use two keys:

One for implementing the ciphering procedure which keep public , and the other is the key for implementing the deciphering procedure it is called the deciphering key which kept secret it is easy.

There are two types mainly of the public-key :

1- RSA it is based on factoring the largest number .
2- Knapsack it is based on the knapsack problem .

3.1 CRYPTOGRAPHIC KNAPSACK SCHEM :

One of the earliest public-key cryptosystem is the knapsack cryptosystem , first described by Ralph & martin hellman in 1978 [3].

ENCIPHERING AND DECIPHERING :

Suppose Bob wants to send message to Alice, and Alices public-key is $a=(a_1, a_2,\ldots, a_n)$.to encipher message $x=(x_1, x_2,..., x_n)$ of n bits, Bob makes the sum[4]:

$$C = \sum_{i=1}^{n} x_i\, a_i \quad (1)$$

C is then sent to Alice . if the message is long it can be split up into blocks of n bits, padding the last block with zeros if necessary . If (*a*) is chosen to be a sequence of integers. The only way to find x is to try all 2^n possible value of *x* if equation 1 is satisfied ,which is unfeasible if n is say greater than 100 .

When Alice constructed her public enciphering key a , she first generated a super increasing sequence of natural numbers ($a'_1, a'_2,\ldots, a'_n$) .

The vector $a' = (a'_1, a'_2,\ldots, a'_n)$ is said to be a super increasing sequence if for each *i* , with $2\leq i\leq n$,

$$a_i \equiv a'_i\, w \ (mod\ m) \quad (2)$$

$$a'_i \ kept\ secret\ , a_i \ kept\ public$$

With condition that each element of a'_i greater than the sum of the preceding elements in equation as shown below:

$$a'_i \ > \sum_{j=1}^{i-1} a'_j \quad (3)$$

Alice choose *m* , *w* with condition for *m* , *w* as follows:

Hiding the "easy" super-increasing sequence from eavesdroppers involves performing several modulo transformations. The transformations are of the following type

$$\sum_{i=1}^{n} a_i' < m \quad (4)$$

$$\text{Ged}(w,m)=1 \quad (5)$$

Alice calculate : $w * w^{-1} = 1 \bmod m$ (6)

To decipher the encrypted message , Alice must calculate:

$$C' = C * w^{-1} \quad (7)$$

Now the compares technique between C' and a' to get x's which represent the binary of the message[5].

4. PROPOSED ALGORITHM:

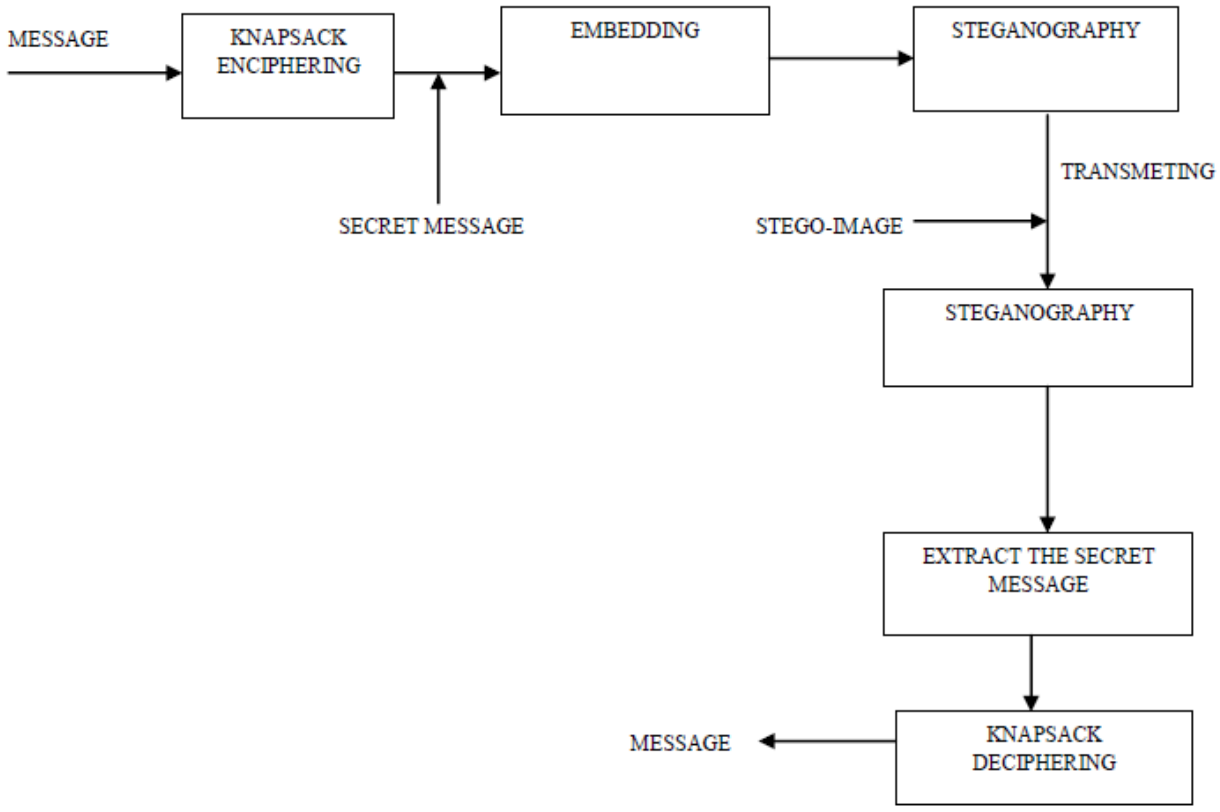
To implement this system :

First the message represented by binary string passing to the enciphering procedure of the knapsack public-key crypto-system.

The result from knapsack is cipher-text , then the cipher message embedded in a cover-image by using steganography Technique Least Significant Bit (LSB). We use the least two bits from the binary pixel to embed two bits of cipher message and then obtain the stego-image which is content the cover-image and the cipher message and then transmitted to the receiver via an unsecure channel.

At the receiver.First we extract the secret message from the stego-image by steganography technique , the output will be the bits of secret message , then we use knapsack deciphering algorithm to produce the original message .

Now we take a numerical example to explain the idea of this proposed algorithm.



Fig(4). THE PROPOSED SYSTEM

5. NUMERICAL EXAMPLE:

$a' = a'_1 , a'_2 , a'_3 , a'_4 , a'_5 , a'_6 , a'_7 , a'_8$ which kept secret at the receiver .

Here we use $n = 8$.

$a' = 2 , 7 , 11 , 21 , 42 , 89 , 180 , 345 .$

$$\sum a' = 706$$

$m = 881 \qquad w = 588$

And calculate w^{-1} via the relation:

$w * w' = 1 \bmod m \quad w^{-1} = 442$

Calculate a_i using the relation:

$a_i = a'_i * w \bmod m .$

This vector a_i is made public

$a_1 = 2 * 588 \bmod 881 = 295$

$a_2 = 592 \quad a_3 = 301 \quad a_4 = 14$

$a_5 = 28 \qquad a_6 = 353 \quad a_7 = 120$

$a_8 = 236$

$C = a_i * x$

Let x = 01100001

$C = a_1 * x_1 + a_2 * x_2 + a_3 * x_3 + a_4 * x_4 + a_5 * x_5 + a_6 * x_6 + a_7 * x_7 + a_8 * x_8$

$C = 592 + 301 + 236 = 1129 = \quad 010001101001$

This binary number is enter to steganography .

Let this represent two pixels as shown below:

00100101 01110001

10001111 01001001

10100011 01110110

Now embedded the cipher-text in cover-image:

00100101 01110001

10001100 01001010

10100001 01110110

These pixels of the stego-image the (LSB) will be very little change.

Now this stego-image will be transmitted to the receiver.

At the receiver:

Each one pixel from the cover-image can cover six bits of the encrypted message.

We use the least significant bit of steganography. we can embedded 960000 bits of the secret message if we cover image at least 400*400 pixels.

The receiver first calculate C' via the relation :

$C' = C * w^{-1} \bmod m$

When $w^{-1}$is the multiplicative inverse of w , now $w^{-1} = 442$

Then C' = 1129 * 442 mod 881 = 372

This number is compared with secret vector a' as follows:

The largest number of $a' = 354$ then :

$x_7 = 1$ then $372 - 354 = 18$

Then $x_6 , x_5 = 0$

$x_4 = 0$

$x_3 = 0$

$x_2 = 1$

$x_1 = 1$

$x_0 = 0$

The output is:

01100001

And so on complete for all message.

6. CONCLUSION:

Our proposed method is combination of the knapsack system public key with the steganography system (LSB) to produce the hybrid system. In this system we know that the knapsack has low security and the only solution of the knapsack system by a numeration technique. Here the security of the hybrid system will improve. Because this improvement will add to the knapsack system steganography system. Here we use the steganography to embed a cipher-text not the message, the cipher-text is the output of the knapsack system , hence we increase the security of the knapsack system. We gave a small numerical example to explain the idea.

REFRENCES:

1. Introduction to steganography , febreuary 11,2003.
2. Steganography techniques , file://H:\internet\Steganography Techniques.htm , 10/30/2005.
3. Desmedt , Y.G. , Skwizynski , J.K. ed, *what happened to the knapsack cryptographic schem ?* , Vol.142, Netherlands :Kluwer Academic

Publishers 1988 .

4. The Free Dictionary ,http://www.math.uu.nl/people/vdkallen/lllimplementations.html, Last Accessed : 6/8/2004.
5. The knapsack problem and the LLL algorithm , created by Jennifer Bakker ,spring 2004,math 187, professor : O'Bryant.