Combining a Hill Encryption Algorithm and LSB Technique With Dispersed Way for Securing Arabic and English Text Messages Hidden in Cover Image

Enas Whab Abood
Dept. of Mathematical/ Collage of Science / University of Basrah

Received in :5/ April /2017 , Accepted in : 4 /June/ 2017

Abstract

In this paper a hybrid system was designed for securing transformed or stored text messages(Arabic and english) by embedding the message in a colored image as a cover file depending on LSB (Least Significant Bit) algorithm in a dispersed way and employing Hill data encryption algorithm for encrypt message before being hidden, A key of 3x3 was used for encryption with inverse for decryption, The system scores a good result for PSNR rate (75-86) that differentiates according to length of message and image resolution.

Key words: Steganography and Cryptography , Hill algorithm , Text hiding

Introduction

The internet is the new environment for dealing with information transferring, publishing and connecting people, so the security of the internet became more significant to protect the data and users from unauthorized access , uncover secret information or distortion it [1]. Data security concepts and systems was shown and developed by many researchers for electronic information protection like cryptography and steganography [2][3]. The cryptography is the art of transforming data from its original shape to another unreadable or corrupted with cryptography techniques in the side of sender and being decrypted by receiver to retrieve the original message [4].The cryptosystem components are plaintext which is the original message or data , encryption algorithm that converting plaintext to cipher text by applying key , decryption algorithm is invested to get back original text, Cipher text and Key for encryption [5]. Although the using of cryptography is successful in distortion of information or delusion that made the attacker helpless in retrieving information who still trying to find a way to break the codes even with creation of new methods in cryptography because the presence of a distortion information is a clue to presence of important information and could be broken or sabotaged ,so another way was deployed nowadays to protect critical information that is Steganography to hide the information from site at all which leads to be pass without interception [2].

Steganography which is denoted as the art or science of embedding data in an incent file like image, audio, video and text ,Steganography systems are categorized into two main types according to the techniques used for embedding that are spatial domain and transform domain .In spatial domain the hidden message is put directly in Least Significant Bits (LSBs), while transform domain embedding is done by editing the cover file frequency coefficients like the Fourier transform and wavelet [5][6][7].Steganosystem is consisted of secret data needed to be hidden , cover file that look incent image ,text or any other media ,algorithms for embedding and retrieving and some time a key needed. Steganography hitch is that once the existence of hidden information is exposed or yet assumed, the message is could be retrieved.

In this paper a hybrid technique is used to secure data transform consist of encryption of a text message using a Hill algorithm with some modification to encrypt a text of Arabic as well as English letters and characters, then embedding the cipher text in an RGB image with LSB technique in a dispersed way to strengthen the security of hiding against malicious attackers.

Related work

The Steganography was well known from long period by Greek as “covered writing” that means hiding information within another information[8]and its away to support the cryptosystem for hiding the encrypted information from unauthorized access these two kinds of security system were studied and developed by many researchers .In cryptography, a studies in an encryption algorithms and enhancing its power and the power of used key were presented and tested with new methods of testing . Saeed M.CH (2009) presented a new way to generate encryption key used in stream cipher that generate it randomly then submit it to conditions of authentic randomization , if it passes then used, elsewhere a genetic algorithm is applied to invent a new random key with length equal to message length and a new structure to hide cipher key within the message in addition to deception function to increase key safity [9].

A model for finding hash value to overcome the dictionary attack was suggested by Tahbob R. and Abu Taha M. (2011) with comparative between suggested system and MD5,SHA1,SHA512[10] .

A hybrid technique of cryptography and Steganography to provide two levels of security were proposed and being widely used and developed by researchers like R.Nivedhitha(2012) introduces two methods for securing image by DES algorithm encryption with the key image. then hide in another image by using LSB techniques ,The decryption can be done by the same key image using DES algorithm[4]. Saleh Marwa E. et.al.(2016) proposed a merged technique for data using Standard (AES) algorithm has been modified and used for encryption then the encrypted message has been hidden in Image by using method that is combining PVD-MPKmethod [11] with MSLDIP-MPK method with high embedding capacity [5] .

Cryptography

Cryptography algorithms was presented and developed for securing data and could be classified into two major types according to the type of key used in encryption: Symmetric and Asymmetric,In Symmetric cipher the key used in encryption is the same used in decryption like Digital Encryption Standard (DES), Triple-DES (3DES) and Hill algorithm.While in Asymmetric cipher different keys but mathematically related are used for encrypting and decrypting[12][13] .

Hill algorithm is most popular symmetric key encryption technique that uses a matrix as a key for encryption and its inverse for decryption and it represents an excellent technique that depends on the algebraic estimation with high speed and productivity[10] .

The Hill algorithm depend on a key that is could be any n×n matrix of integer value (2×2 , 3×3 , 4×4,…) that have an inverse with integer value to be used for decryption (Hint: The matrix of integer inverse almost have determinative equal to 1) .The text transformed to a matrix with n row equal to the key dimension then multiplies the key with the text matrix to get Ascii cipher text.To retrieve the original text from the Cipher text the encryption operations is reversed but the multiplication take place with the inverse of the key matrix[14].

Another type of classification is Block cipher and Stream cipher that depends on the amount of data encrypted, In Block cipher the plain text is encrypted as blocks of bits each of time and the size of the block either 32bits or 64 bits... etc. Like DES .Stream Ciphers techniques encrypt the data continuously bit by bit by integrate a key with original data a mostly using XOR , It considered a block cipher with bit length of each block like RC4 algorithm[13][15].

Steganography

Steganography trends are to hide messages in cover files and either the message or cover files could be any type of media like text, image and sound. Usually in images the hiding is being in LSB that caused a minor change cannot be realized by bare eyes [16].there are three main types of covered writing (Steganography) used in stegosystem:

➢ Pure Steganography:

Pure Steganography is a system with no information for hiding within a cover file, like key interchanging or any descriptive manner of hiding.

➢ Secret Key Steganography:

It depends on using a keyword for each side (sender and receiver), the sender picks up a cover file C for hiding his message M by secret key K . On the receiver side the same key is used with reversal operations to retrieve secret message M.

➢ Public Key Steganography:

This method needs two keys private and public ,The public is declared in a general database and used for hiding while the private key is used for secret message retrieval[17].

Many of cover writing techniques were shown [18] like:

○ Substitution System: Its work is to substitute the unimportant part of cover file by hiding message bits in a consecutive or dispersed way like Least Signification Bit (LSB) that uses for image and sound cover files .

○ Transform Domain Techniques : The frequency spectrum of image cover file is used to hide messages and this technique produced immunity against segmentation and image processing attacks comparing with LSB. A Discrete Cosine Transform(DCT) and Wavelet Transform represent a kind of transforms used for hiding purposes.

○ Spread Spectrum Techniques: In spectrum techniques the signal with some wave exceed low limit for sending information and the hiding message data are being spread with independent signal ,while the receiver is retrieving the hiding data using a special code used for sending, Generally two shapes of spread spectrum is invested: Direct sequence and Frequency Hopping.

○ Statistical Methods: This method works on changing statistical properties of the cover file (i.e. The cover file changes when sending bit 1 while stay the same with bit 0) so the receiver should be able to recognize the modified cover from the other.

Proposed System

The suggested method of hiding is depending on hiding an encrypted text message (Arabic and English) in LSB of colored image in dispersed way.

1. Text encryption

The first step is to encrypt the text consisting of Arabic and English letters and characters using Hill algorithm 3×3 matrix key as follows:

➢ Chose a key as matrix n×n for encryption with the inverse of integer number for decryption :

We are free to chose any key with any dimension with condition of having an integer value inverse matrix ,like:

$$key1 = \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}, key1^{-1} = \begin{bmatrix} 3 & -5 \\ -1 & 2 \end{bmatrix}$$

$$key2 = \begin{bmatrix} 2 & 10 & 6 \\ 2 & 11 & 8 \\ 4 & 24 & 21 \end{bmatrix}, key2^{-1} = \begin{bmatrix} 19 & -33 & 7 \\ -5 & 9 & -2 \\ 2 & -4 & 1 \end{bmatrix} \ldots\text{etc}$$

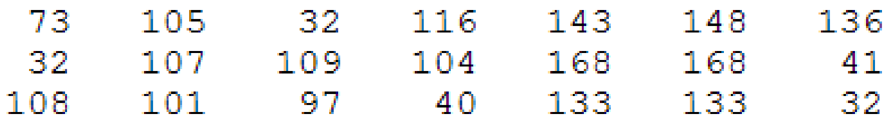
In this paper the key is:

$$\text{Key=} \begin{bmatrix} 1 & 5 & 3 \\ 2 & 11 & 8 \\ 4 & 24 & 21 \end{bmatrix} \textit{with inverse} \begin{bmatrix} 39 & -33 & 7 \\ -10 & 9 & -2 \\ 4 & -4 & 1 \end{bmatrix}$$

➢ Transform the text to Ascii code , Actually the Ascii code for English characters are started from 32 to 126 and Arabic characters Ascii started from 1569 to 1618 so we subtract 1442 from Arabic Ascii to get a new enhanced Ascii for any sentence or words consists of various characters in range (32-176):

'I like math(رياضيات) ' → 73 32 108 105 107 101 32 109 97 116
104 40 143 168 133 148 168 133 136 41 32

➢ Reshape the one dimensional ASCII code to a two dimensional array with row number equals to key dimension , If the Chosen Key is 3×3 then the text ASCII matrix became as 3×m:

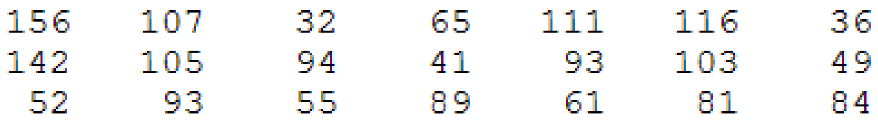


```
    73   105    32   116   143   148   136
    32   107   109   104   168   168    41
   108   101    97    40   133   133    32
```

Acsii_text=

➢ Multiply the Ascii_text with Key after subtracting 32 and taking the modulo of 145 that the number of characters to get numbers between 0-176 then add 32 again :

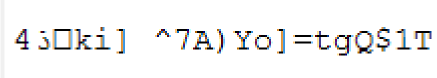
ASCII_mul =



```
   156   107    32    65   111   116    36
   142   105    94    41    93   103    49
    52    93    55    89    61    81    84
```

➢ Convert the ASCII_mul to character to get encrypted with consideration to the ASCII code of Arabic character that started from 1569 instead of 127 as in enhanced ASCII of the program :

Encryp_text=



```
4ز□ki] ^7A)Yo]=tgQ$1T
```

➢ End

2. Text Hiding :

Text Hiding is done with the LSB in color image that has value between 0 and 1 so any change in this bit gives a minor alternation in color that measured at 1/255 of color rate, which pays no attention from attackers and to strengthen the hiding power in addition to encrypt the text is using another key to represent the seed for random function that produces a random location for spreading the text bits in cover image ,the algorithm of hiding is below:

(1) Convert the encrypt_text to ASCII with binary code with length 8 bits.

(2) Convert image color value to binary code with 8 bits(0-255).

(3) Generate the list of random locations for encrypt_text bits using Rand () function available by MATLAB with seed number represents the key for hiding with default value equal to length of encrypt_text bits and could be changed by the system user.

(4) The length of encrypt_text bits stored at the end of image bits

(5) Substitute the bits of Encrypt_Text by image 8th bit (LSB) according to the generated locations.

(6) Reconstruct the cover image by transforming to decimal codes, Then reshape it to 3 dimensional matrix.

(7) Saving new image and send it to the receiver

(8) End

The system provides a simple GUI to the sender to enter necessary information like Plain_Text, Encryption_Key (matrix), Cover_Image and Hiding_Key (random seed) to process the encryption and hiding smoothly, Then saving Cover_Image as a new file to be sent, Figure(1)(2).

3. Message Revealing (Uncovering)

On the receiver side after getting the image the step of retrieving hidden message started by reversing the algorithm of hiding by generating location list using the same Hiding_key (random seed) and take the 8th bit from each location to form the character of Cipher_text .

4. Text Decryption

The Cipher_text is being decrypted by repeating all steps of encryption with exception that Decryption_key is equal to the inverse matrix of Encryption_key .The process is done with these steps:

➢ Translate the Encrypted_Test to ASCII codes and reshaping with row numbers equal to Key columns.

➢ Adjusting the values of the matrix of ASCII values by subtracting 32 from each element.

➢ Multiplying the ASCII matrix with Decryption_Key (inverse of Encryption_Key).

➢ Taking the value of remainder modulo 145 to reduce each matrix element.

➢ Adding 32 to each element of the resulting matrix.

➢ Reshaping the Matrix to a one dimensional Matrix and translate each ASCII value to opposite character with consideration to the value of the element over than 126 is added to 1442 then get opposite character which belongs to the Arabic character group.

The GUI of receiver is shown in Figure(3)(4).

Results and Discussion

The system was applied to many messages differentiate in length and images with various resolutions. The system produced a clear image with a good rate of hiding ever with bare eye or noise measurement using Peak Signal to Noise ratio (PSNR) according to equations[19]:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{i=1}^{N}(I_{ij} - IC_{ij})^2 \; , \; PSNR = 10Log_{10}\frac{L^2}{MSE}$$

M,N : Cover_Image resolution.
I : Cover_Image before hiding.
IC: Cover_Image after hiding.
L : The highest value of IC matrix which is in image case is 255.

In table (1) and Figure(5) the results of calculating the PSNR rate for different length of Encrypted_Text hidden in different resolution images .

Obviously from Figure(5) the text length effects in PSNR that the increasing in text length caused reducing in PSNR but it still good in hiding and unable to detection any text in images,Also increasing the resolution of image produces a better way to reduce PSNR that fortify the hidden process .The dispersed way in distribution bits of text in image enhancing hiding process and strengthen the proposed algorithm.

Conclution

Using Cryptography for secret message before being hidden gives an extra level of protection against attackers with ability to encrypt Arabic and English characters in the same time.

The dispersed way in hiding text bit in cover file strengthen the power of hiding specially if happens with key defined by the users.

Although the numbers of PSNR say about presence of distortion or noise in images after hiding ,but still the test of human eyes is important and it shows no noisy in any image or difference after from before hiding.

References

1. Tacticus, A. (1990), "*How to survive under siege / Aineias the Tac- tician*", pp. 84{90, 183{193. Clarendon ancient history series, Oxford, England: Clarendon Press.

2. Awadh,W. A. (2012),"*Text Message Hiding in Text Documents*",M.SC thesis,Collage of Science,Basrah university.

3. Abdulzahra, H. ; Ahmad, R. and Norliza, M. N.,"*Combining Cryptography And Steganography For Data Hiding In Images*", Applied Computational Science,pp:128-134

5.Nivedhitha, R. and Dr. Meyyappan, T. (2012),"*Image Security Using Steganography And Cryptographic Techniques*", International Journal of Engineering Trends and Technology.

6. Saleh, M. E.; Aly ,A. A. and Omara,F. A., 2016, "*Data Security Using Cryptography and Steganography Techniques*", (IJACSA) International Journal of Advanced Computer Science and Applications ..

7. Sharda, S. and Budhiraja, S. (2013) ,"*Image Steganography: A Review*," International Journal of Emerging Technology and Advanced Engineering (IJETAE), PP. 707–710, January.

8. Al_Dobooni, M. M. ;Sulaiman, A. H. and Bader Sadkhan, S. ,(1989), "*The Symbols , Codes and Computers –Introduction to Information Security*",Aldar Alarabia .

Stallings W.,(1999)," *Cryptography and Network Security", Prentice Hall* ", New Jersey,.

9. Saeed, M. J. (2009) ,"*Stream Encryption using Genetic Algorithm* ",Al-Rafedain Journal for Computers and mathematical Science.

10. Abo-Taha, Mohammed and Tahboob, Radhwan ,(2011),"*Practical one way hash algorithm using non-invertible matrix based on hill cipher technique*", Communications of the Arab Computer Society.

11. Saleh M. E.; Aly, A. A. and Omara, F. A. (2015), "*Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding,* " International Journal of Computer Science and Security (IJCSS), pp. 397 - 397.

12. Stallings, W. (2006) ,"*Cryptography and Network Security Principles and Practices*", Prentice Hall.

13."*Cryptography just for Beginnar*", http://www.tutorialspoint.com. (2015)

14.Yi-Shiung. Y, (2008) , "*A New Cryptosystem Using Matrix Transformation* ". Proceedings of IEEE International Canahan Conference on Security Technology, Taipei, Taiwan pp: 131-138.

15. Lars, R. Knudsen and Matthew, J. B. Robshaw, (2011),"*The Block Cipher Companion*",Information Security and Cryptography ,Springer-Verlag ,Berlin Heidelberg.

16. Hill, S. L, (1929): " *Cryptography in an algebraic alphabet* ". American Math. Monthly, pp: 306-312.

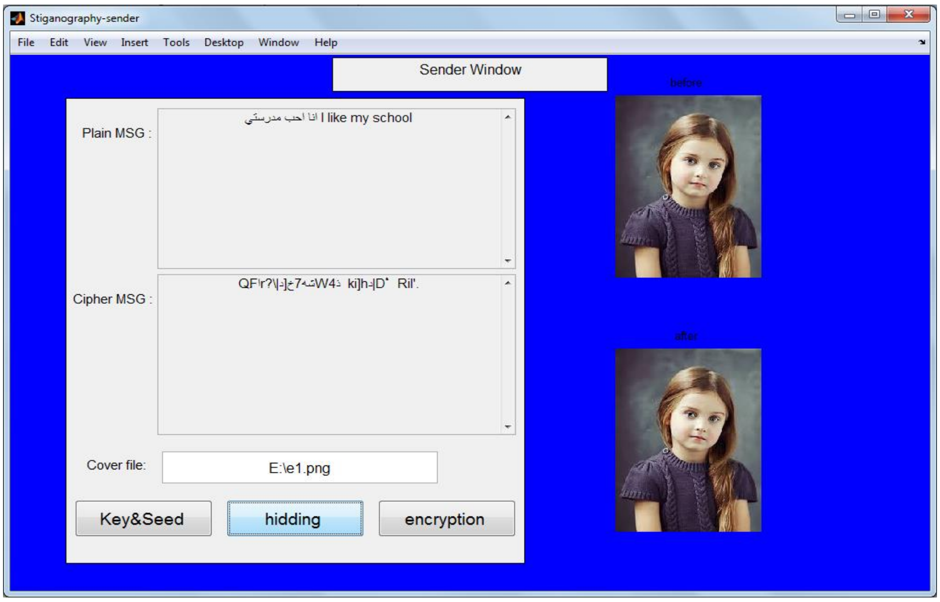
17. Sellars , Duncan, (1999),"*An Introduction to Steganography* " Computer Science Department ,University of Cape town South Africa.

18. Katzenbeisser, S. and Petitcolas F.A.P. ,(2000), "*Information hiding techniques for Steganography and digital watermarking*",Arttech House.

19. Qi,Hairong ; Snyder, Wesley E.&Sander, William A., (2002);"*Blind Consistency-Based Steganography for Information Hiding in Digital Media*".Multimedia and Expo,2002.ICME '02.Proceedings IEEE International Conference on Vol.1,pp:585-588.

Table (1): shows the PSNR rate values for different text length and different images resolution .

Image resolution	Text size	PSNR
444 X 444	360	75.8453
194 X 265	32	78.5776
1024 X 728	500	79.4432
	50	85.4241
	100	83.2974
	250	81.5445



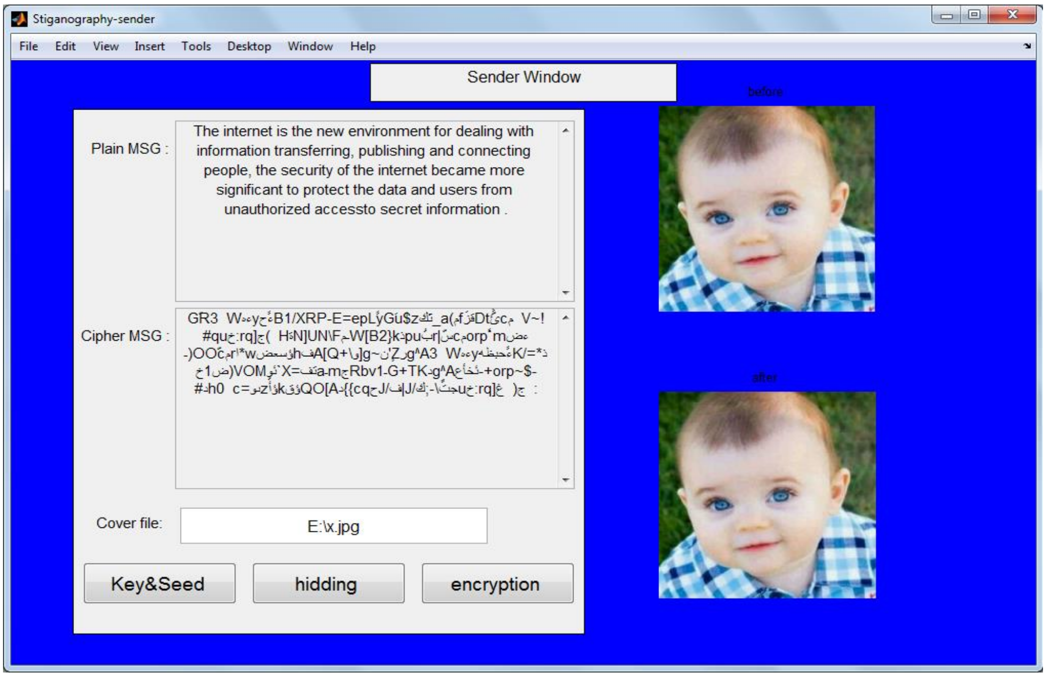
Plain MSG : انا احب مدرستي I like my school

Cipher MSG :

```
QF!r?\|-]خ7شهW4ذ  ki]hد|D˙  Ril'.
```

Cover file: E:\e1.png

Figure (1): Sender GUI for encrypting a secret message and hide it in cover_image



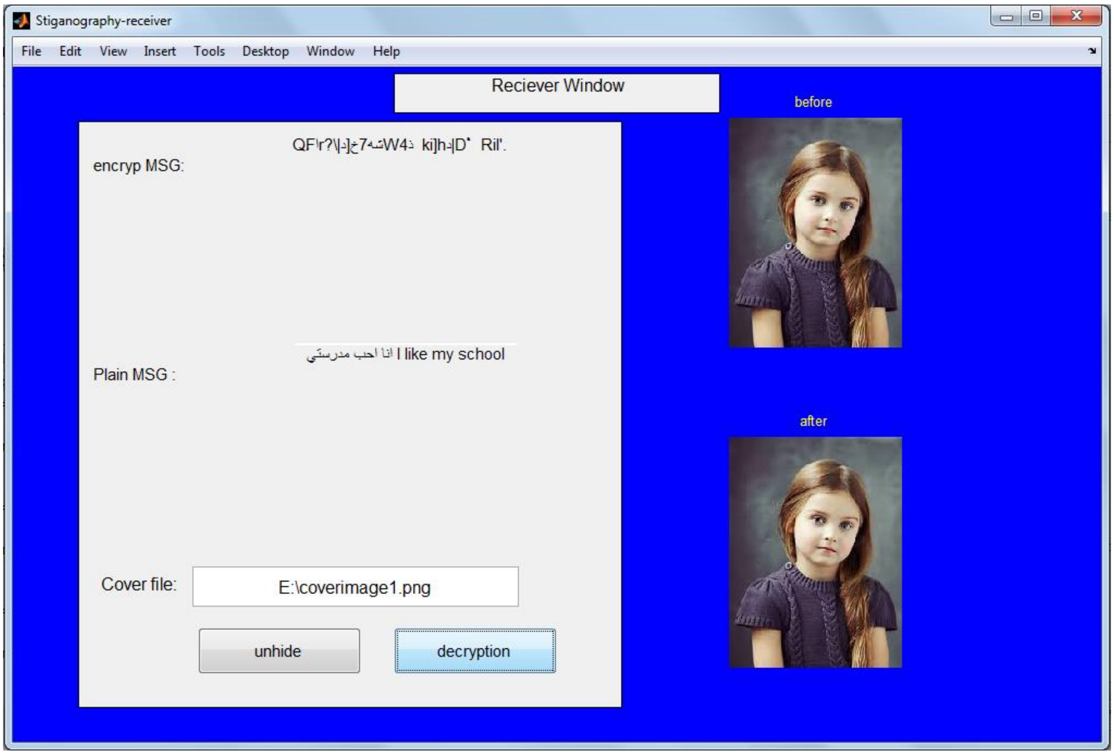
Plain MSG : The internet is the new environment for dealing with information transferring, publishing and connecting people, the security of the internet became more significant to protect the data and users from unauthorized accessto secret information .

Cipher MSG :

```
GR3  WدءyخَؤB1/XRP-E=epLỳGú$zتك_a(مfقزDtئٌc م  V~!
#quخ:rq]ج(  HةN]UN\Fمـ W[B2}kذpuبُـr|سَcمorp˚mعض
-)OOčمr!*wسعضؤhفـA[Q+\ى]g~ن'Zرg^A3  Wدءyحبطهءُ K/=*ذ
خ1ض)VOMثو`X=تقفa-mجRbv1-G+TKدg^Aعأخئ-+orp~$-
#دh0  c=ىوzأؤkزقQO[Aد{{cqحJ/فا|J/كِ;-\جتٌuخ:rq]غ  )ج  :
```

Cover file: E:\x.jpg

Figure (2) :Sender GUI for encrypting a secret message and hide it in cover_image

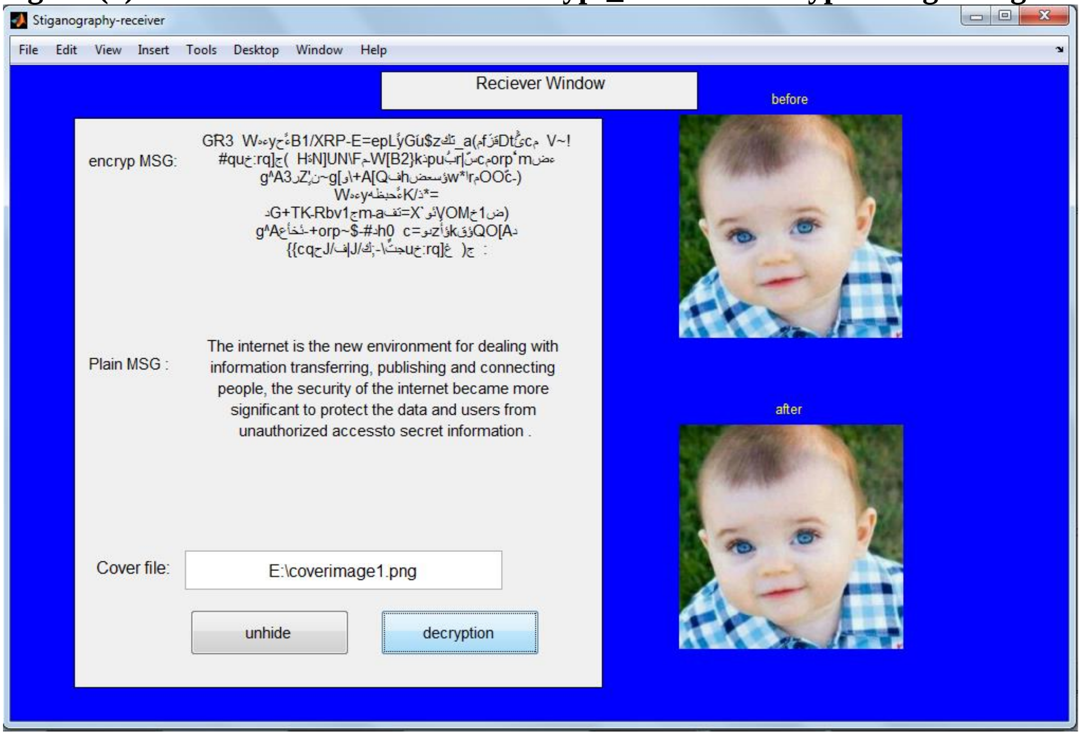


encryp MSG: QF'r?\|-]خ7تهW4ذ ki]h-|D' Ril'.

Plain MSG : انا احب مدرستي I like my school

Cover file: E:\coverimage1.png

Figure (3): Receiver GUI to uncover encrypt_text and Decrypt it to get original message

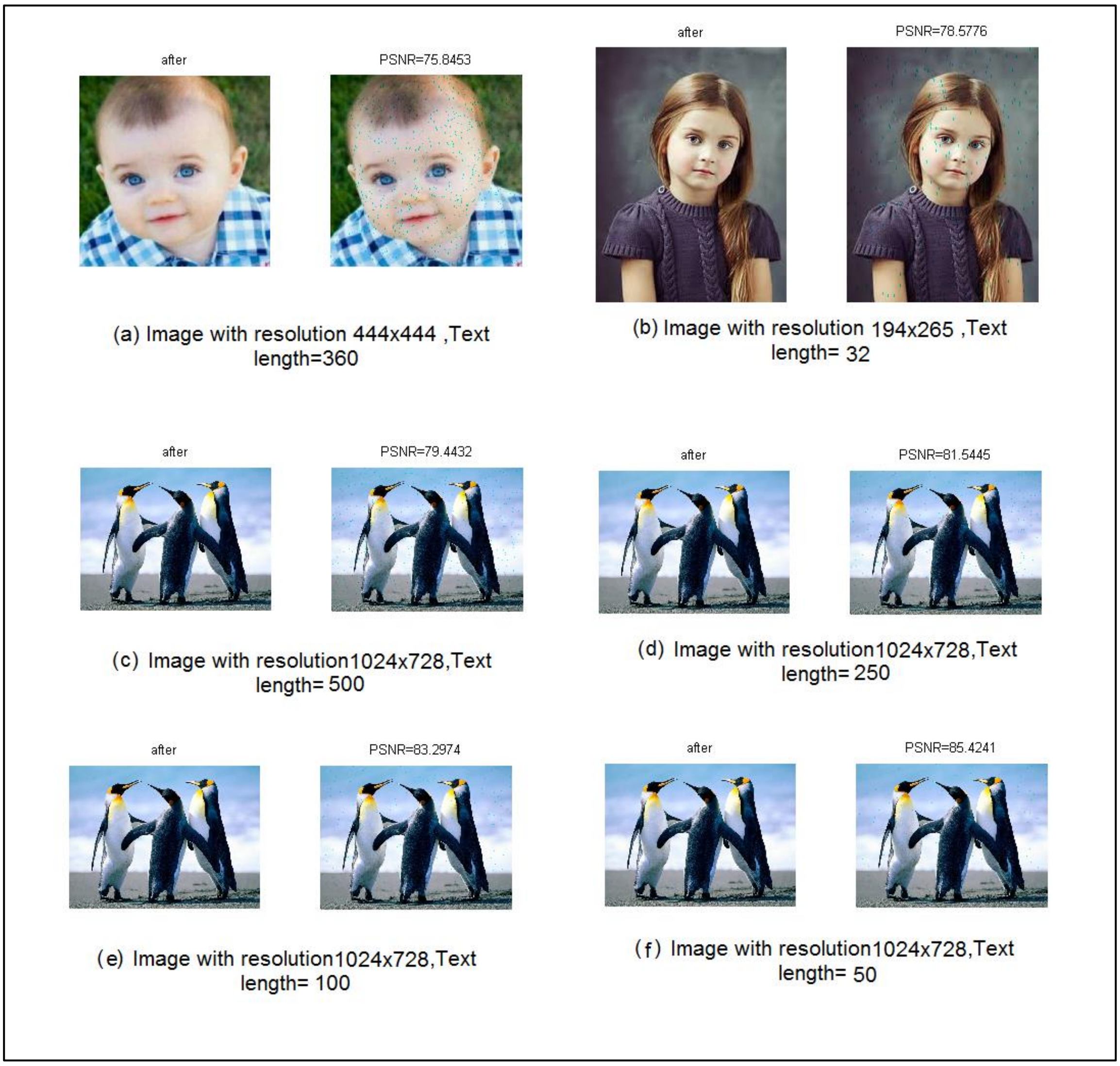


encryp MSG:
GR3 W••yحB1/XRP-E=epLýGù$zتك_a(مfقزDtىcم V~!
#quخ:rq]ج(H:N]UN\Fم-W[B2}kذpuبr|سc,orp'mضع
g^A3رZ'ن~g[و\+A[Qفhوسعضw*'rمOOc-)
W••yحبطهK/ذ*=
دG+TK-Rbv1جm-aتقف=X'ئوVOMخ1ض)
g^Aعأخئ-+orp~$-#ذh0 c=سوzأؤkؤقQO[Aد
{{cqجJ/فا|J/ك;-\جتuخ:rq]غ)ج :

Plain MSG : The internet is the new environment for dealing with information transferring, publishing and connecting people, the security of the internet became more significant to protect the data and users from unauthorized accessto secret information .

Cover file: E:\coverimage1.png

Figure (4) Receiver GUI to uncover encrypt_text and Decrypt it to get original message



(a) Image with resolution 444x444 ,Text length=360

(b) Image with resolution 194x265 ,Text length= 32

(c) Image with resolution1024x728,Text length= 500

(d) Image with resolution1024x728,Text length= 250

(e) Image with resolution1024x728,Text length= 100

(f) Image with resolution1024x728,Text length= 50

Figure (5): Shows the differences between the PSNR rate in different text lengths, and image resolutions,the right image from each group shows the distribution of text bits in cover_image bits.