International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2020.3604

E-ISSN : 2454-6135

Volume.6, Issue 3
March -2020

New Data Transmission Method Based On Book Cipher Enhanced With ASCII Mapping

Hind Jumma Serteep

Assistant Teacher, Department of computer science,

Collage of Education, Al-Mustansiriyah University, Iraq

ABSTRACT

There are several ways to achieve protection of information follow between user and client from attack, misuse or unauthorized access straightly, one of these ways is steganography, steganography is a science of secretly data transfer using different multimedia like audio, text, video or image as a carrier. In the current paper, the author proposes another steganography procedure that it is easy to find and hard to break by an outsider . It based on combine between ASCII Mapping Technology (AMT) with book cipher encryption method using the image as an encryption key for the book cipher. The (AMT) technique is used to create an encoded table by mapping the text message and match some bits with that of the image, The proposed procedure was tried and the outcome shows its robustness and low computational cost beside it maintain image quality.

Key Words: *Steganography, ACSII mapping technology, Book cipher, Image, Pixels.*

1. INTRODUCTION

In the present world the fundamental worry of the data transmission over a communication network is the assurance of information from unapproved client. To manage this issue a few data concealing instrument exists like, steganography, Cryptography, Digital watermarking and so on. The initial two systems gives assurance on information though the third one gives the confirmation over the information utilizing some tag or marking on certain items like text , audio , video , image [1].

Steganography is fundamentally made out of the accompanying two words: Stegno and Graphy. "Stegno" is a Greek word which really signifies "covering" whereas "Graphy" is a Greek word signifies "composing". On the whole, steganography signifies "covered writing" which connotes the rationale to cover or hide whatever written [2]. The basis of Cryptography involves receiving some data that is readily readable and to encrypt this data into a new format

Encryption transforms original information, called plaintext or clear text, into transformed information, called cipher text, code text or simply cipher, which usually has the appearance of random, unintelligible data [3].

Essentially information hiding is the mean task of Steganography it is a significant system since it doesn't allow the assailant to distinguish if there is any message. This strategy fundamentally accentuation on hiding as opposed to secure data. Data in which mystery information is covered up is called transporter or cover object while information which is covered up is called stegno object [4].

1.1 Overview of Steganography

Steganography can be applied on various multimedia types like image, audio, video and text , see Figure 1. The carrier known as the signal, Steam or data file into which the hidden data is hidden by making modification. In our research we will focus on image steganography.

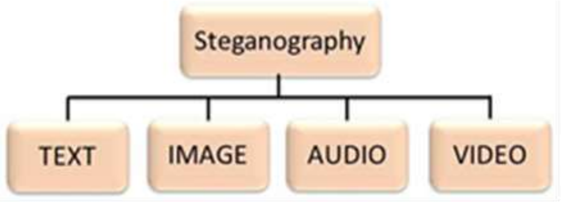


Figure 1: Steganography Categories According Carrier Types

Text Steganography: In this technique, basics of text are used to hide data based on format based and random method such as capital letter, tabs and spaces [5].

Image Steganography: Image intensity and pixels are used as covered object in which text as stego object is used. Some commonly used carrier objects in image steganography are GIFF, JPEG and BMP etc. In this technique, pixel values and intensities are changed based upon stego values in such a way that changes in covered objects remains approximately unnoticeable [6].

Audio Steganography: In this technique, audio in various formats like .WAV, .MIDI, .AVI, .MPEG as covered object is used. This technique is very popular due to high popularity of voice over IP (VOIP). Various methods are applied in audio based upon its characteristics like low bit coding, phase coding and spread spectrum [6].

Video Steganography: Video, basically combination of pictures in particular sequence is used as covered object in various formats like .MP4, .MPEG, .AVI etc. In this technique, discrete cosine transform (DCT) alters pixel value of image which is impossible to interpret by human eye due to Negligible change in the picture[5].

1.2 Steganography Goals And Challenges.

The goal of Steganography is to hide the important information of communication by embedding the secrete data to transmit into digital media file such as image or text file.

The challenge associated with Steganography techniques are influenced by the following factors.

1-Invisiblity: implies that the stego-image looks very similar to the original image [8].

2-Payload / Capacity: defines the amount of secret data which can be hided in the image [7][9].

3- Robustness against statistical attacks: Peak signal- to – Noise Ratio (PSNR) and Mean Square Error (MSE) are two most fidelity parameters which are used to measure the robustness against statistical attacks [10].

4- Computation Complexity: It is a computation of the expensiveness of the embedding and extraction process of a hidden message [11].

2. INFRASTRUCTURE

2.1 Book Cipher

Book cipher is an old encryption method, It was used by George Scovell for the Duke of Wellington's army in some campaigns of the Peninsular War (A.D. 1807-1814). Even in Cold War. The Book Cipher encryption is done by using a particular key to encrypt and then later decrypt a particular piece of information. This particular key can be a book, or any other piece of text. In other word [3] . In a book cipher, a message is translated into numbers using a specific book, dictionary or other text. The numbering system can vary, but typically it is based on page numbers, line numbers, word numbers or character numbers. The plaintext is translated letter by letter, or word by word, into numbers that represent each letter or word. The book or text therefore acts as an encryption key. The strength of the Book Cipher lies in it being homophonic in nature, which allows a single word to be replaced by the locations of an infinite number of the same word used in another book. [3]

There are reasons for the decline of usage of the book cipher , These reasons can by summarized by the following points
1. The reference books had to be digitalized, uploaded and stored in a database on the computer, which seemed redundant at the time.
2. If the hacker knew the language of the reference book, then it became easier to find the book in question.
3. Some constraint related to the plan text like, if the word doesn't exist in the key, the addressing of the spaces and the repetition of words.

2.2 ASCII Mapping Technique (AMT)

This technique is used to create an encoded table by mapping the text massage and matching some bits with that of the cover image [12], this done by convert each character of the secret message to ASCII code then convert it to binary number (8- bit) . Also the pixels value of the cover image convert to binary number (8-bit), then each binary value of the secret message spilt to (1-bit, 2- bit or 4-bit) and take the first part of the first character and compare it with the LSB of the binary value of the cover image , when matching found store the location of the matching pixels , this process repeat for all character of the secret message.

DOI : 10.31695/IJERAT.2020.3604

3. THE PROPOSED TECHNIQUE

The main idea of the proposed technique is combining between the (AMT) ASCII mapping technique with the book cipher, this technique presents a different way of implement age old encryption technique. This technique used cipher book with image as reference key, As there is an infinite supply of images available on the web easily this will reduce the effect of the brute-force attacks , these reference keys (Images) will play important role in the encryption and decryption of plain text.

Suppose two users (User A and User B) want to exchange data securely. Note that User A reference key (Image) not same as User B reference key (Image), But each users know the reference key of the other end user.

User A will follow the following steps to encryption the secret massage. See Figure 2

1- Spilt each word in the secret massage in the individual litters then get the ASCII code for each litter.

2- Convert the ASCII code to binary number (byte).

3- These binary number (bytes) spilt to (1-bit, 2-bit or 4 bit)

4- User A convert the pixel value of the (Red or blue or green) channel of the reference key (Image) to binary number

5- User A take the first splitting part (for example 1 bit) of the first litter of the secret massage and compare it with the LSB (1 bit) of each pixel of the reference key , when matching found store the location of the matching pixel, this proses will repeat for the separation parts of secret massage . (See table 2)

6- User A will send only the locations of the matching pixels to user B without the reference key. (See Fig 2)

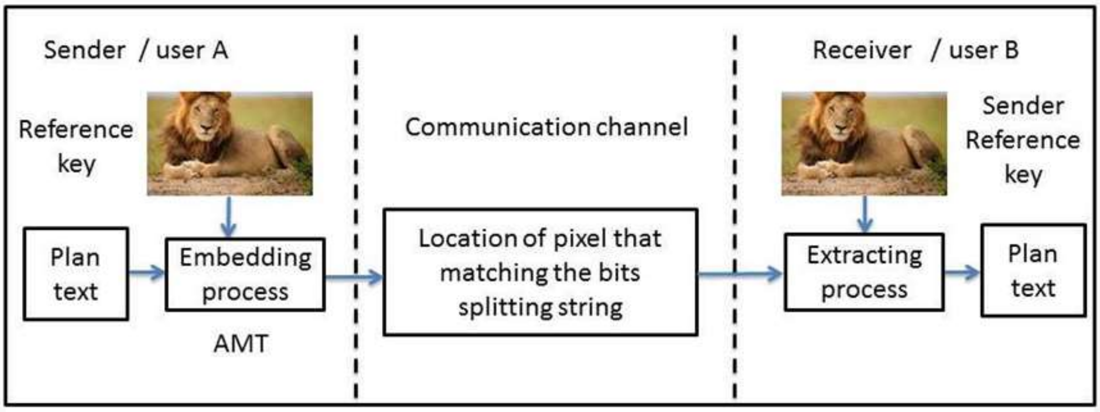


Figure 2: diagram illustrate the proposed technique

At the other side the recipient will follow the steps below to decryption process

1-After the matching pixels locations has been successfully transferred to the receiver's side , firstly user B obtain the binary values form the reference key depending the received matching pixels locations.

2- Grouping the binary value to obtain a byte.

3- Convert the byte value to decimal value

4- Convert these decimal values depending on the ACSII table to obtain the original secret massage.

4. RESULT AND DISCUSSION

The proposed technique has been designed by using Visual Basic 2013 as programming language , the program was building in personal computer has 64-bit operation system (Microsoft Window 8.1)

the proposed technique take into consideration the constrains of the book cipher and overcome then, for example when used the traditional book cipher and have a word in plain text and this word does not exist in the reference key , this issue can by overcome in the propose technique by splitting all the words in to character and convert in to ACSII then convert to binary value and this binary value spilt in to bits, in other word the traditional book cipher compare word and in the propose technique compare bits.

DOI : 10.31695/IJERAT.2020.3604

Also the addressing of space can be easily overcome by the propose technique simply the space ACSII value (space = 32) in the ASCII table and this value can be easily treated as treat the characters of the words. and the propose technique can by apply on other different characters like (@ , ! , #, % , ... etc). Beside the purpose technique keeps the reference key (image) unchanged because the image plays the role of the key to encode the secret massage.

4.1 Case Study

Let's suppose User A want to send this secret massage (high) to User B , Table #1 show the characters of the secret massage and how it splitting in to 2-bit binary value.

Table 1: character ACSII and binary value and splitting (2-bit) string

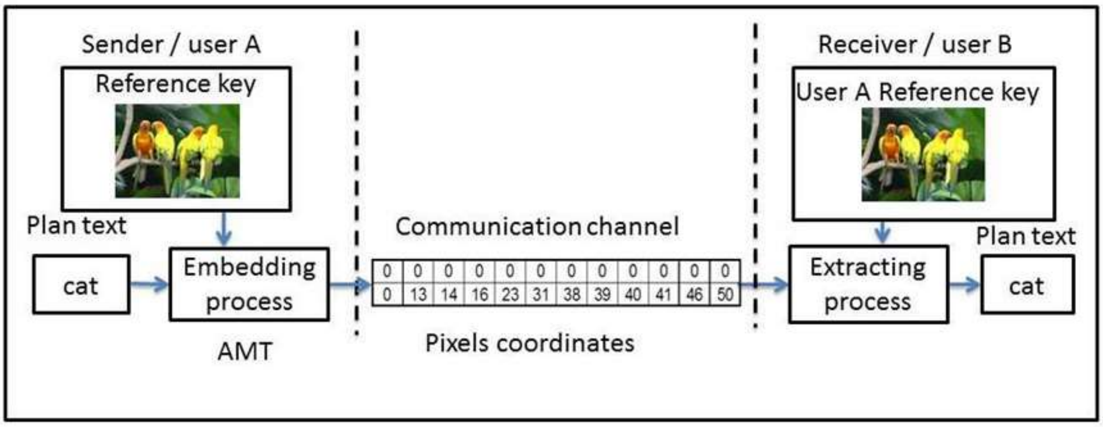
character	h				i				g				h			
ACSII	104				105				103				104			
Binary	1101000				1101001				1100111				1101000			
split binary	01	10	10	00	01	10	10	01	01	10	01	11	01	10	10	00

Table#2 shows the matching pixels locations for the 2-bit splitting binary value.

Table 2: splitting (2-bit) string with pixels coordinates

split binary		01	10	10	00	01	10	10	01	01	10	01	11	01	10	10	00
Pixel coordinate	X	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Y	4	5	12	16	18	19	26	29	34	37	38	53	56	67	68	73

Figure 3 show applicable example of the proposed method, in this example a short message used (cat) to send form (user A) to (user B). As seen the word (cat) is too short and it contain three litters and by splitting these litters in to (2-bit) binary string we get a 12 sets of 2-bit string.



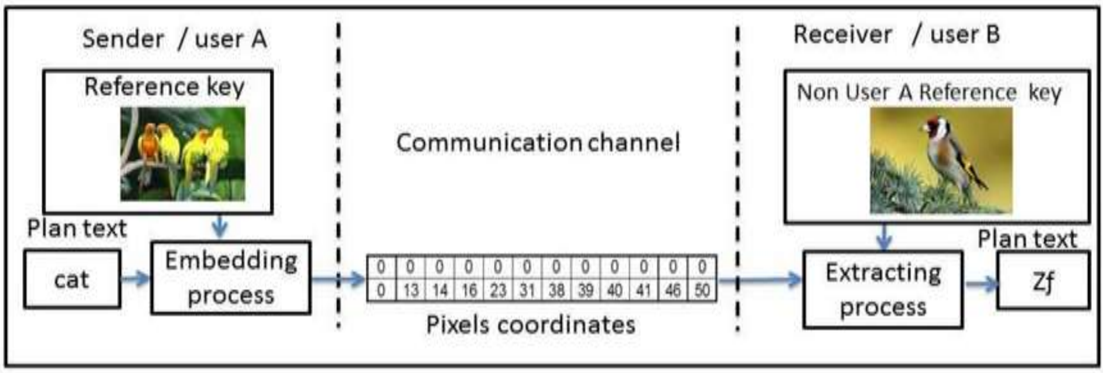
0	0	0	0	0	0	0	0	0	0	0	0
0	13	14	16	23	31	38	39	40	41	46	50

Figure 3: The Receiver use the correct reference key

After applying the AMT to generate the pixels coordinates we see that all x-coordinate are (0) that mean this word 2-bit location all listed in the 1st row of the image, as message light increase the x-coordinate will jump to 2nd row.

Fig4 show applicable example of the proposed method where the receiver used incorrect reference key (not same as user A reference key) and the receiver get incorrect message (Zf) while user A send the message (cat).

DOI : 10.31695/IJERAT.2020.3604



0	0	0	0	0	0	0	0	0	0	0	0
0	13	14	16	23	31	38	39	40	41	46	50

Figure 4: The Receiver use incorrect reference key

5. CONCLUSION

There are many aspects that consider during the conclusion; some of them are security, capacity, flexibility and robustness

Security: - the most important reason for choosing this encryption method is that it has infinite key space.

Flexibility: - the propose technique can divide the binary sequence of the secret massage in to (1-bit , 2-bit and 4-bit) segment that ably on the book cipher (as high the segment light it get more difficult to decrypt the massage by the hacker.

robustness: -in the decryption phase the receiver must use the same reference key that the sender use to generate the location list (X,Y) if the receiver use different reference key or the location list interrupted by the man in the meddle attack and they do not use the correct reference key for decrypt the secret message , they will not obtain the original secret message.

Capacity:- this new technique can apply in all mainly JPEG , PNG , BMP image file format an as much the image size increase more text can be encrypt without go back to the beginning of the image if the matching process reach the end of the image and the binary string not finished . Also this method can be extended to any other language also.

REFERENCES

1. S. Bhattacharyya, P.Indu and G. Sanyal "Hiding Data in Text using ASCII Mapping Technology (AMT)," International Journal of computer Applications, vol.70 -No.18 (0975-8887) May 2013.
2. Monit "An Enhanced Least Significant Bit Steganography Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 5, Issue 6, ISSN: 2278- 1323 June 2016.
3. Rasika Lele, Rohit Jainani, Vihang Mikhelkar, Aniket Nade, Mrs. V. Meshram "The Book Cipher Optimised Method To Implement Encryption And Decryption " , International Journal Of Scientific & Technology Research Volume 3, Issue 1, January 2014.
4. Ross J. Andreson and Fabien A.P. Petitcolas , " On the limits of steganography ," IEEE Journal on Selected Areas in Communications (Jsac), Special Issue on Copyright & Privacy Protection , Vol 16 no. 4 , pp 474-481, May 1998.
5. J. Kour and D. Vwema , " Steganography Technique-A Review Paper," International Journal of Emerging Research in Management & Technology , vol. 3 issue 5 , pp. 2278-9359, 2014.
6. M. Hussain and M. Hussain , " A survey of image steganography techniques," International Journal of Advanced Science and Technology vol.54 , 2013
7. V. R. Kukaplli , T. Rao and S.Reddy, " Image Steganography by Enhanced Pixel Indicator Method Using Most Significant Bit (MSB) Compare , International Journal of Computer Trends and Technology (IJCTT)-Vol 15 number 3 – Sep 2014.

8. Tuama , A. Y. , " Randomized Pixel Selection for Enhancing LSB Algorithm Security against Brite-Force Attack " , Journal of Mathematics and Statistics , 13 ((2)): 127-138.
9. Kumar, M. and M. Yadav , "Image steganography using frequency domain", International Journal of Scientific & Technology Research , 3(9): p 497-610 , 2014.
10. Goyal, M., Y. Lather, and V. Lather , " Analytical relation & comparison of PSNR and SSIM on babbon image and human eye perception using matlab" , International Journal of Advanced Research in Engineering and Applied Sciences 4(5) : p . 108-119, 2015.
11. Chen, P.-Y and H.-J. Lin , " ADWT based approach for image steganography ", International Journal of Applied Science and Engineering , 4(3): p. 275-290 , 2006.
12. H. L. Hussein , A. A. Abbass , S.A. Naji , S.AL-augby and J. H. Lafta , " Hiding text in gray image using mapping technique" ,IOP conf. Series: Journal of Physics . 1003, 2018.

DOI : 10.31695/IJERAT.2020.3604