مجلة

كلية التـــراث الجامعة

مجلة علمية محكمة

متعددة التخصصات نصف سنوية

العدد السابع والثلاثون

15 حزيران 2023

ISSN 2074-5621

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم (ب 3059/4) والمؤرخ في (2014/ 4/7)

A method to protect information sent over network using the concept of book cipher

Hind Jumaa Serteep

Computer since department, Al-Mustansiriyah University, Ministry of Higher Education and Scientific Research , Iraq.

الخلاصة

في عصر يعتبر فيه تبادل المستندات الإلكترونية ومراقبة الأرصدة المصرفية والتداول الإلكتروني ودفع الفواتير أمرًا بالغ الأهمية للإنسانية ، إلى جانب مشاركة المعلومات والتواصل مع بعضنا البعض ، للتغلب على هذه الصعوبة ، يجب نقل البيانات عبر شبكات الاتصال بطريقة آمنة وسريعة مع حصانة من الاختراقات التقنية ، مع التوسع في استخدام الويب والوسائط المتعددة ، يزداد الطلب على مناهج الأمان التي تهدف إلى حماية البيانات والمعلومات الرقمية. إخفاء المعلومات هو علم يستخدم العديد من الوسائط المتعددة ، بما في ذلك الصوت والنص والصورة والفيديو ، بالإضافة إلى بروتوكول TCP / IP ، كناقل لنقل المعلومات الآمنة عبر الويب ، وفي هذا البحث تم اقتراح تقنية لإخفاء المعلومات بالاعتماد على (book cipher) يتضمن صورًا كمفاتيح تشفير بدلاً من الكتاب أو جزء من نص مرتبط بتقنية تعيين ACSII ، وستكون النتيجة جدولًا مشفرًا تم إنشاؤه عن طريق فصل النص ومطابقة البتات مع تلك الخاصة بمفتاح التشفير (الصورة) ، والطريقة المقترحة تحافظ على جودة الصورة دون تغيير وتظهر النتائج قوتها ونفقاتها الحسابية المنخفضة

Abstract

In an age where exchanging electronic documents, monitoring bank balances, electronic trading and paying bills are crucial to humanity, beside of sharing information and communication with each other, To overcome this difficulty, data must be transmitted across communication networks in a safe and quick manner with immunity to technical breakthroughs, With the expansion in the utilization of the Web and multimedia , so does the demand for security approaches that aim to protect data and digital information. Steganography is a science that uses various multimedia, including audio, text, image, and video, as well as the TCP/IP protocol, as a transporter for secure information move through the web , In the paper a technique was proposed for steganography relying upon the book cipher involving pictures as encryption keys rather than a book or piece of text joined with ACSII mapping technology , the outcome will be an encoded table made by parting text and matching bits with that of the encryption key (the image), The suggested method keeps the picture quality unaltered and the outcomes show its solidarity and low computational expense

Key words;- Image steganography , book cipher , last significant Bit , Matching pixels, pixel coordinates.

1. Introduction

The technology of both communications and multimedia are in development rapidly that make the majority of users of this technology now prefer to use the Internet as their primary means of data transfer between them. Additionally, everyone now has access to a range of communication methods, such as e-mails, chats, social media, etc. Despite the fact that data is shared through these techniques in a straightforward, quick, and accurate manner, where these services are not a significant issue in transmission but form security threat to confidentiality of

this information through the theft of personal or sensitive information in a variety of ways[1] . Steganography is a more effective method than cryptography for protecting data, according to Enhancements in computer security. Because cryptography's output is distorted, it can draw the consideration of an outsider to encoded messages While steganography involves the capacity to incorporate data into computerized cover that prevents the secret message from being perceived where the result isn't noticeable [2] The art of steganography involves concealing data in a way That prevents messages stored away from being found. Steganography literally translates to "covered writing" and it is got form Greek. It uses a wide variety of covert communication techniques to hide the message's presence. In spite of the fact that steganography is an old art, the development of computers has given it new life. where the Steganography work on the Digital covers that are altered by computer-based steganographic techniques to embed information different from the native covers [3].

Steganography has its situation in security. It isn't purposeful to trade cryptography, yet achieve it, camouflages a message with steganography will reduce the likelihood that a message will be found. furthermore, if the message is encrypted, an additional layer of security is provided, because it is more difficult for an attacker to detect embedded cipher text in a cover, that will generate many different stenographic methodologies join conventional cryptography with steganography where the sender encrypts the secret message before applying Steganography [4]. Cryptography is the craftsmanship and the knowledge branch of changing the information to a nonsense structure that looks irregular and unimportant to a hacker. All in all, secret message in cryptography is change to such an extent that it can't be perceived, then the secret message is sent to intended recipient who can only read it after eliminate the nonsense from the secret message. Figure 1 below shown the general mode of steganography.

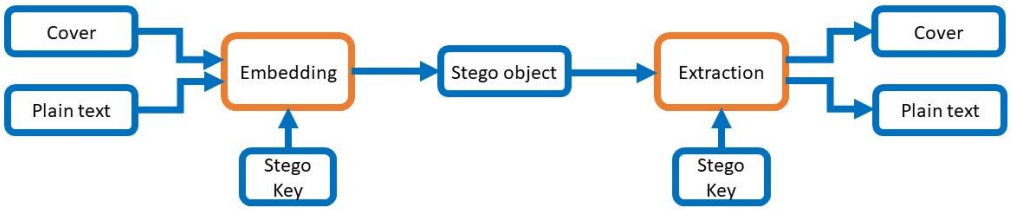

Figure 1: general mode of steganography

plain text is the name called of the secret information before it scrambled by the encryption approach and after encryption is called cipher text, the process of encoding content of the secret message in order to safeguard it from unauthorized person is called encryption, while the recovering process of the secret message is called decryption, so both of encryption and decryption rely upon the key and the encrypting technique [5]. Figure 2 below shown the general mode of encryption.

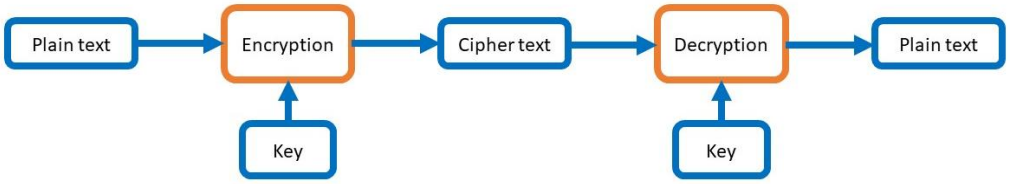

Figure 2 : general mode of encryption

The classification of cryptography system depending on the no of keys that use in the encryption, the cryptography approach who use single shared key for encryption and

decryption is called symmetric encryption, while the cryptography approach who use two keys one for encryption and the other for decryption is called asymmetric approach [6].

1.1 Digital steganography

Steganography is the act of encoding secret data in a way such the actual presence of the data is hidden, since forever ago, numerous steganographic strategies have been reported, including the utilization of cunningly picked words, imperceptible ink composed between lines, regulation of line or word dispersing and microdots [7].

Contingent upon the kind of the cover object there are numerous reasonable steganographic methods which are continued to get security. It tends to be displayed in Figure (3). In actuality, the cover object's structure substantially influences the message embedding strategy [8]

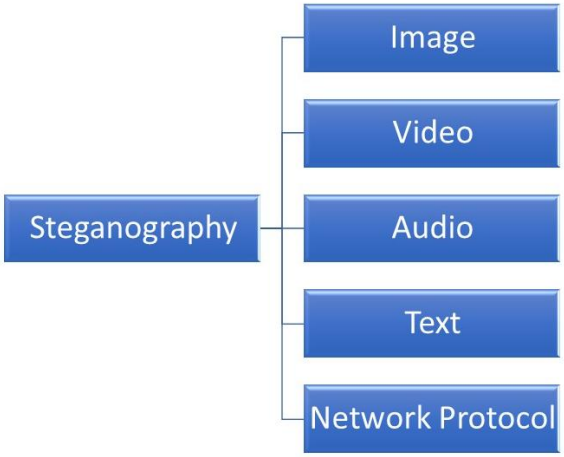

Figure 3. Digital Medium to Achieve Steganography

1.1.1 Image Steganography: Image steganography is the practice of using the cover item as the image in a steganography.in this procedure pixel intensities are utilized to conceal the data, which falls into one of three categories: Transform methods, perceptual masking approaches, and least-significant bit embedding (or simple embedding) [8]

1.1.2. Network Steganography: Network protocol steganography refers to the process of using a network protocol as a carrier, such as TCP, UDP, ICMP, IP, etc. There are covert channels in the OSI network layer model where unused header bits of TCP/IP fields can be exploited for steganography [9].

1.1.3. Video Steganography: Video Steganography is a method to conceal any sort of documents or data into computerized video format. Video (a collection of images) is employed as transporter for buried data. Choosing video as cover medium is liked because it has the natural potential to store a significant amount of secret information while maintaining perceptual transparency. Due to its potential to overcome the obstacles of other approaches like capacity and enormous processing, video steganography currently dominates the study sector [10].

1.1.4 Audio steganography :- Due to the widespread use of voice over IP, the audio file formats WAV, AVI, MIDI, and MPEG are used as the cover object in this technique (VOIP)[11]

1.2 Steganography Measures

1- Robustness:- Robustness is the capability of embedded data to survive changes to the stego-image, such as scaling, random noise addition, linear and non-linear filtering, sharpening, and blurring [12].
2- Tamper Resistance:- In addition to robustness against destruction, tamper-resistance describes how difficult it is for an attacker to change or counterfeit a message once it has been implanted in a stego-image, such as when a pirate substitutes a copyright mark with one that claims legal ownership [7].
- Hiding Capacity :- The term "hiding capacity" actually relates to how much data a cover object can conceal. High payload capacity can be indicated by a large amount of buried stego-object data [11].
4- Computer complexity:- How difficult and time-consuming it is to insert and retrieve a concealed message [13].
5- Perceptual Transparency: - In order to conceal the message within the cover, some noise modulation or cover image distortion is required, the embedding process actually should happen without critical corruption or loss of perceptual nature of the cover. Even if an attacker in a secret communications application is unable to extract the message but discovers some deformation that raises suspicion of the presence of concealed data in a stego-object, the stenographic encoding has failed [14].
2. Infrastructure: -
2.1 digital image: - this section will talk about binary, grayscale, and color digital images
A- Binary Image: - The most fundamental image kinds are binary images, which only have two distinct qualities: black and white. Black is represented by the number "0," and white by the value "1." Typically, a binary image is constructed from a gray-scale image. When the broad form or shape of the image is needed for computer vision applications, a binary image is helpful. They are also referred to as one-bit / pixel images [15].
B- Gray scale image:- Grayscale picture: They lack any color information and only indicate the brightness of the image. due to the image's 8-bit data depth and 256 different gray level ranges (0-255) [16].
C- Color Image: - Since a color image contains three matrices to represent each pixel's red (R), green (G), and blue (B) values, it is sometimes referred to as an RGB image. Consequently, there are three matching values for each pixel. The range of values for each R, G, and B component is from 0 to 255, making a total of 24 bits (or bits/pixel) required for each of the three-color components [4].
2.2 Book Cipher
the secret information is encrypted using the book cipher by employing a specific key, which is then used to decrypt the secret information. Any book or other text may serve as the specific key. The basis being that the words present in the secret information to be encoded is replaced by the location of the similar words present in the key but it's crucial that both the sender and the receiver have the exact same key [17]. the word cannot be encoded that the case when a word shows up in the plain text yet not in the book (the key) A different strategy to solve this issue is to substitute individual letters rather than whole words[18].
2.2.1 Week point
Book cipher has some week point
1- The code book must be digitalized and organized in a form of data for both the encryption and decryption sites, which takes a tremendous amount of time [19]

2- The number of code books available would be significantly reduced if Assuming that the enemy knew the language of the plain text e.g English or Chinese [18].
3- There are several restrictions associated to plain text, such as the addressing of the space and the repetition of words if the word is absent from the key.

2.3 ASCII Mapping Technique (AMT)

The steganography ACSII mapping technique is used to create an encoded table by mapping the text message and match some bit with that of the cover image [20]
In order to use the AMT approach, the secret message must first be changed into binary format before being dispersing and spreading throughout all channels of an RGB or grayscale image via a matching procedure. The locations of the matching bits will be kept in a table that result from matching procedure where each individual bit from the secret message matches with individual bits from the channels of the RGB image or gray image. The positions of the secret message on the RGB image or gray image are saved in this table. This method will make it very tough for stego analysis to decipher the hidden information [21].

3- The Proposed Technique:-

The proposed method is created by consolidating the book cipher with the ASCII mapping technique. Computerized touch to book code will eliminate the requirements it out of date, The traditional book cipher used a book or a piece of text as the reference key, in our proposed technique the reference key is an image (which can be one image or a group of images). Because there are an infinite number of images available on the web, choosing a reference key is simple, and the redundancy will lessen the impact of brute-force attacks
Assume two individuals (person1 and person2) well send and get information to one another in a safe way, person1 has reference key which it nth series of pictures while Person 2 has a different nth series of pictures. Both individual 1 and person2 realize the reference picture key (the pictures and their order) of the opposite side
Person1 will perform the follow steps
1- divide the secret massage into separate words, and then separate the words into separate litters.
2- transfer each litter to number according to ASCII table
3- transfer number to binary number
4- By adding a certain amount of zeros to the left of the last binary number digit, each letter's binary number is converted to an 8-bit string.
5- hashing every 8-bit string into its own string containing one bit, two bits, or four bits
6- person1 convert the pixel values of the reference image key (Red , bule & green) to binary , this conversion is done for all reference key image (the nth image)
7- person1 start matching the first individual part of the secret message and compare it with the LSB of the red channel of the first image of the reference key image , the second part of the secret message will compare with the LSB of the red channel of the second image of the reference key image , and the third part compare with the red channel of the third image of reference key image , and so on to the last image of the reference , then the comparation transfer with the LSB of the green channels of the images of the reference , then the comparation transfer with LSB of the blue channel of the images of the reference , Each time matching found record the location of the match pixel from the images of the reference image key , after the matching procedure finish by the last part of the secret message , the matching pixels location send only to the other side.

Note , if the matching procedure arrived to the blue channel of the last image key of the reference image key the matching procedure will go back and start the match from the last matching location of the red channel of the first image

Person 2 will carry out the following steps at the receiving site to obtain the secret message.

1- after the matching pixel location are successfully received at the receiver side , person2 collecting the binary stream depending on the matching pixel location with reference image key of person 1

2- the binary stream divides in to 8-bit group (bytes)

3- transfer the byte value to decimal value

4- Using the ASCII table, convert the decimal value to letters to get the hidden message.

4- Result and Discussion

The proposed method was put into practice using and evaluated Visual Basic 2013 as the programming language on a 64-bit operating system-equipped personal computer (Microsoft Window 8.1)

there are some issue associated with traditional book ciphers like space addressing to and non-alphabetic letters (@, #, %, &, *, +, -,/… .) and a word does not exist in the reference book , these issue has been overcame by our proposed technique because it match bits instead of word or sub- word or litters , all of these charterers are recorded in the ACSII table

4.1 Case study

The following case study has been provided to simplify the suggested technique and make it clear. Assuming that person 1 wants to communicate a secret message (cat) to person 2, Table (1) beneath outline how to break the secret message's characters into individual bits

Table 1:- the individual bits of a secret message

character	ASCII value	binery value	individual bits							
c	99	01100011	0	1	1	1	0	0	1	1
a	97	01100001	0	1	1	0	0	0	0	1
t	116	01110100	0	1	1	1	0	1	0	0

Both person1 and person2 will consent to follow a similar grouping for find the matched pixels, in other word they settle on the succession of pictures of the reference picture key and settle on start match on the red channels of the reference key pictures then the green channels of the reference key pictures then the blue channel of the reference key pictures, after that they begin once again on the red channels, etc

Person1 pick five deferent pictures as it's reference picture key and he named it as (image1, image2, image3, image4, image5) , After the matching process for the secret message (cat) was finished and the individual bits location table is made , Person 1 will just send the coordinates (x,y) to person2 without the reference image key because there is no change on reference key images done by the proposed method, since person 2 (the receiver) already have them he will map the pixels coordinate over the reference image key to obtain the secret message, table (2) show the matching pixel coordinates

Table 2:- the result matching pixel coordinates

character	individual bits	reference image key	X	Y
c	0	Image1 , red channel	0	2
	1	Image2 , red channel	0	1
	1	Image3 , red channel	0	4
	0	Image4 , red channel	0	2
	0	Image5 , red channel	0	4
	0	Image1 , green channel	0	1
	1	Image2 , green channel	0	3
	1	Image3 , green channel	0	4
a	0	Image4 , green channel	0	0
	1	Image5 , green channel	0	1
	1	Image1 , blue channel	0	2
	0	Image2 , blue channel	0	4
	0	Image3 , blue channel	0	3
	0	Image4 , blue channel	0	2
	0	Image5 , blue channel	0	1
	1	Image1 , red channel	0	4
t	0	Image2 , red channel	0	5
	1	Image3 , red channel	0	7
	1	Image4 , red channel	0	5
	1	Image5 , red channel	0	8
	0	Image1 , green channel	0	3
	1	Image2 , green channel	0	5
	0	Image3 , green channel	0	7
	0	Image4 , green channel	0	3

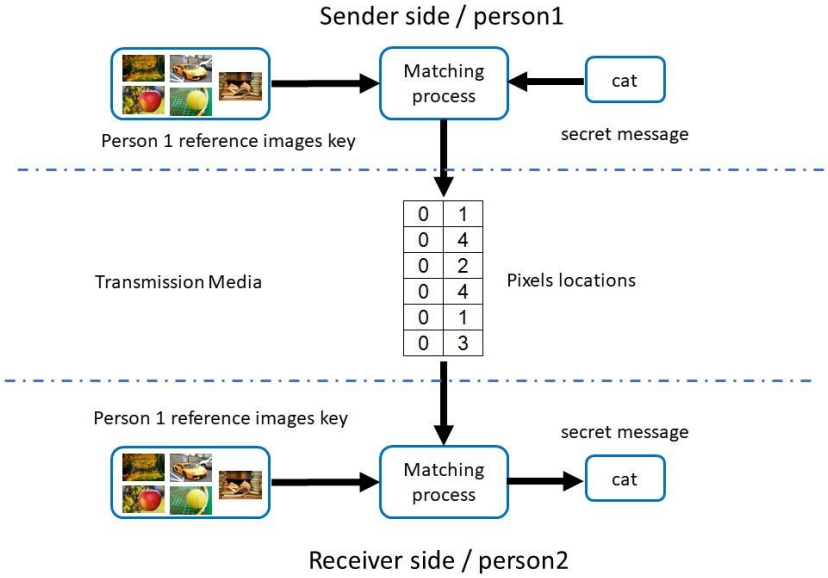

Figure 4:- The Proposed Method

The proposed method steps explain in the above figure (4), where only the pixels coordinates sent from person1 to person 2, and in accordance with the agreement made between the sender and the receiver, person 2 knows to map the pixel coordinate over the reference image key of person 1. He (person 2) realizes that the first pixel coordinates is in the red channel of image #1, the second coordinate is in the red channel of image #2, the third coordinate is in the red channel of image #3, and so on until the last red channel, at that point the process is repeated,

but now he looks in the green channels of the reference key image form image #1 to image #5 then the blue channels of the reference key image form image #1 to image #5.
If the recipient or the assailant utilize different reference picture key set or he change the succession of the reference picture key set he will receive wrong secret message, See figure (5) below.

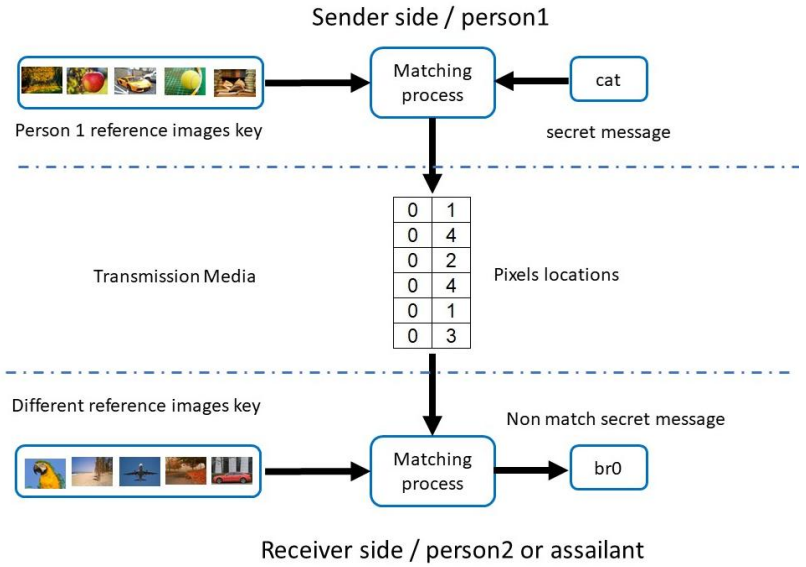

Figure (5) :- The effect of different reference image key

5- Conclusion

The author's approach of massage steganography, which increases the security of data transit over networks, relies on a book cipher concept with images serving as reference keys, It is accomplished by comparing each segment of the secret message bit stream to the LSB of the reference key pictures. Along with this, there are other factors (such as security, capacity, and flexibility) that should be considered while analyzing the results

1- Capacity: - The suggested solution works with a variety of picture file types, including JPEG, PNG, and BMP, and as the quantity of reference images grows, so does its capacity to conceal additional text. Additionally, this approach can be used to other languages

2- flexibility: - the proposed technique based on match the secret message bits with the LSB of the key ordered reference images The secret message can be divided into segments of one or two bits and even 4 bits segment. for example, If the matching process uses segments of two bits, it stacks a bigger information than if it uses segments of one bit

3- Security: - As there is a boundless inventory of picture accessible on the web it become the significant justification for picking this proposed method, the sender can change the reference key picture at a specific period of time or change the succession of the reference key picture.

4- Computation complexity: - it is referred as the cost of embedding and extracting of a secret message.

Disadvantage: - less robust if the attacker changes the values of the matching pixel location., the secret message may be lost.

REFERENCES

1- Khalid Kadhim Jabbar, Hussin Abd Hilal, Rana Saad Mohammed ,(2018), 'Text Cryptography Using Multiple Encryption Algorithms Based On Circular Queue Via Cloud

Computing Environment ', University of Mustansiriya , *Journal of Theoretical and Applied Information Technology* , Vol.96. No 12 , 30th June.
2- Sarab M. Hameed, Zuhair Hussein Ali, Ghadah K. AL-Khafaji, Safa Ahmed, (2021) , 'Chaos-based Color Image Steganography Method Using 3 D Cat Map' , *Iraqi Journal of Science*, Vol. 62, No. 9, pp: 3220-3227
3- Asst. Prof. Dr.Refat Talib Hussein , M.Sc. Awatf A. Jafar ,(2010), 'Novel security Image Steganography Based on DWT and Pseudorandom Sequences ', *Journal of Engineering and Development*, Vol. 14, No. 1, March
4- Zahraa Salah Dhaief1, Raniah Ali Mustafa2 and Amal Abdulbaqi Maryoosh , (2020), Mustansiriyah University , 'Hiding Encrypted Text in Image using Least Significant Bit image Steganography Technique ', *International Journal of Engineering Research and Advanced Technology (IJERAT)* , Volume.6, Issue 8 , August
5- Sura Fahmy Yousif (2014) , 'Wavelet Based Image Steganographic System Using Chaotic Signals' , A Thesis Submitted to the Electrical Engineering Department College of Engineering AL-Mustansiriya University.
6- Ehklas Abbas Albahrani , amal abdulbagi maryooh , Sadeq H. Lafta, (2020) , AL-Mustansiriya University , 'Block Image Encryption Based On Modified Playfair And Chaotic System ', *Journal of information security and application* , Volume 51, April .
7-Eugene T. Lin and Edward J. Delp , 'A Review Of Data Hiding In Digital Images' , School of Electrical and computer Engineering , Purdue University , IS &T'S 1999 PICS Conference.
8- Mehdi Hussain and Mureed Hussain, (2013) , 'A Survey of Image Steganography Techniques' , *International Journal of Advanced Science and Technology* Vol. 54, May.
9- Handel, T. & Sandford, M. , (1996), 'Hiding data in the OSI network model', Proceedings of the 1st International Workshop on Information Hiding, June.
10- Dr. Manjula G R, Sushma R B , 'Video Steganography: A Survey of techniques and methodologies' , International Conference on Smart Data Intelligence (ICSMDI 2021)
11- Mohit ,(2016) ,' An Enhanced Least Significant Bit Steganography Technique' , *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* ,Volume 5 , issue 6 , June .
12- M. Swanson, M. Kobayashi, and A. Tewfik, (1998), 'Multimedia data embedding and watermarking technologies' , Proceedings of the IEEE, Vol. 86, No. 6, pp. 1064-1087, June.
13- B.Deekshitha, Gnanamanjari.S, Chaithanya.S , (2017) ,' Survey On Different Methods Of Image Steganography' , *International Journal of Advance Research and Innovative Ideas in Education, IJARIIE* , Vol-2 Issue-5.
14- R. Wolfgang, C. Podilchuk and E. Delp, (1999) , ' Perceptual watermarks for images and video' , Proceedings of the IEEE, Volume: 87, Issue: 7, July.
15- Rana Riad K. Al-Taie , Basma Jumaa Saleh , Hiba A. Abu-Alsaad , (2021), Al-Mustansiriyah University , ; A Review Paper: Digital Image Filtering Processing; , Technium Vol. 3, Issue 9 pp.1-11 , ISSN 2668-778X
16- Heba Kh. Abbas, Anwar H. Al-Saleh, Ali A. Al-Zuky, (2019) , Al-Mustansiriyah University , 'Optical Images Fusion Based on Linear Interpolation Methods' , *Iraqi Journal of Science*, Vol. 60, No.4, pp: 924-936
17- R. Lele , R. Jainani , V Mikhelkar , A. Nada, Mrs . V. Meshram , (2014) , ' The Book Cipher Optimized Method To Implement Encryption And Decryption ', *International journal of scientific & technology research* , volune 3 , issue 1 , Jan.

18- C. Wang , S. Ju ,(2010) , ' A Novel Method to Implement Book Cipher' , *School of Computer Science and Telecommunication Engineering*, Jiangsu University, Zhenjiang, China , journal of computers, VOL. 5, NO. 11, November.
19- C. Wang , S. Ju ,(2008) 'Book cipher with infinite key space ', *School of Computer Science and Telecommunication Engineering* , Zhenjing , China , *International Symposium Of Information Science And Engineering* .
20- Huwaida T. Elshoush , Ibtihal A. Ali ,(2021) ' A Novel Approach to Information Hiding Technique using ASCII Mapping Based Image Steganography' , Faculty of Mathematical Sciences University of Khartoum, Sudan , *Journal of Information Hiding and Multimedia Signal Processing* , Volume 12, Number 2, June.
21- Ahmed Abdulrudah Abbass, Salam Al-Augby, Hussein L. Hussein, Jasim Hussein and Robert Tornai ,(2021) , ' ASCII Mapping Technique for Text Hiding in the RGB and Gray Images' , *Journal of Engineering and Applied Sciences* , Volume: 16, Issue 4, Page No.: 161-165