Australian Journal of Basic and Applied Sciences, 7(9): 77-86, 2013
ISSN 1991-8178

New Approach For Data Hiding In Video

[1]Ghada thanoon, [2]Ruaa abdeljwad, [3]Bushra falah, [4]Hiba zeyad

[1]lecture, College of Computer & Mathematic Science-Mosul University, IRAQ.
[2]Ass.researcher, College of Computer & Mathematic Science-Mosul University, IRAQ.
[3]Ass.researcher, College of Computer & Mathematic Science-Mosul University, IRAQ.
[4]Ass.researcher, College of Computer & Mathematic Science-Mosul University, IRAQ.

Abstract: This research aims to accomplish the process of hiding text or image, or both of them, within the video file extension (avi). The process is done by splitting text or image information into data of even and odd sequence, and then concealed these data inside the frames that constitute the video file in a reverse manner, where the even data sequence are concealed in odd positions and vice versa. Note that the first video frame that will be concealment with will be determined by an agreed equation between the sender and the receiver, as well as the number of the line, which will be concealment with. If one frame is not sufficient for the text or image information then a new frame is used based on a previously agreed equation. The (least significant bit) method has been used in the covering-up process depending on the bits (7, 8 and 9), i.e., (the less important bits), and then calculating all the values of (PSNR, CR, MSE) for the image that has been hidden and retrieved. The results were good; also, Matlab 2009 language was used to accomplish this work.

Key words: Image Processing, Information Hiding, LSB, Digital Video AVI .

INTROUDUCTION

The art of concealment entered into a new age called the digital age and became abreast of developments and the increasing growth of multimedia applications on networks to increase the need to provide efficient methods of working to protect data and special property of the one, so it had to be the appearance of working on ways to provide security for these media to protect them from thieves and hackers from tampering or theft of distorted and dissemination of sensitive information.

Hence, the need to provide Data security methods, and this means Cryptography, which means providing protection for data storage and transfer by using the secret key, so it was still encryption successful way to protect stored data and sent over the network, but with the growing networks communication and global information network (Internet) has become difficult to maintain this data, especially that it will always be accessible to everyone via the Internet in the form of non-obvious cause for suspicion and interest among the spam and the thief to open this encryption or destruction information transmitted (Nori,A.,and,Aziz,S.,2011). We have imposed several restrictions to try to prevent the use of encryption across the network, one of these restrictions prevent the flow of any information to the source uses encryption in his correspondence as stated in the legislation issued by the Department of Justice U.S., which means the province informatics, so most governments started to impose control over the encryption and prevent institutions from dealing therefore it was necessary to develop data security and create new technolo-gies and this means the science of (Information hiding).

The purpose of concealing information not prevent others from knowing hidden information, but to remove the uncertainty already in the presence of hidden information, and special thing in the techniques of hiding information that they can use in modern technologies, can be used in multimedia computer such as (images, text, audio and video) (Donald, H., and, Baker, M., 1997).

The hiding of information meant to hide information in other information seemingly no reason to doubt and do not attention, and not be aware of hackers and attackers, so these information not accessible to network users, but remains content exclusive to the authorities, which are known how toextract This content(D.Yousef,2003).

The intent of this introduction, that with the development of science and methods used in the concealment there are methods evolve paralleling with it in the art of analyzing and breaking this data. Objective of hidden data is not to raise any point to doubt the concealment, and the goal of analyst concealment is uncertainty in all messages sent, and checked to make sure the existence of hidden data sent (F. Barzanchi ,2008).

The Art Of Hiding Information And Encryption:

Misses a lot of people when they consider encryption (Cryptography) and hide the data are the same thing , But with accurate look we see that encryption is the study of ways to send the message which could not decoded only the sender and the receiver. This is different from the art of hiding information and the

Corresponding Author: Ghada thanoon, lecture, College of Computer & Mathematic Science-Mosul University, IRAQ.
E-mail: ghadathanoon@yahoo.com

encryption, encryption will change the content of message but not presence it but hiding data will hide a message from foundation.(Donald,H.,and,Baker,M.,1997)(D.Yousef,2003).

In general, we can compare between the art of hiding the message and encryption through the table below:

Table 1: compression between encryption and hiding information

Encryption	Hiding information
works to hide the contents of the information.	Works to conceal the existence of information.
The connection is the guide.	Trying to hide the existence of a connection guide.
The final con-cealment outcome of the encryption is the cipher text.	The final outcome of steganography is an element of hiding.
The goal of the strong encryption methods to prevent spam from getting any information about the clear text of the cipher text that attacked.	Concealment methods target high-security prevent mediator observer from knowledge of the existence of confidential data originally.
depends on the well-known algorithms.	There is not a specific algorithm, but depends on the human nature of concealment.
for each encryption algorithm weaknesses allow an attacker to retrieve the secret message.	No finger print is found, but when you figure out a way to hide the secret message is covered.
possible to mix between two way encryption to get a doubly encryption.	Possible to mix between encryption and steganography to produce a high hide security.

3.(The Steganography) Coverage System:

The word (Steganography) is derived from the Greek language and is composed of two syllables (Steganos) and the mean covered or confidential and (Graphy) means writing or drawing , the two together mean the term (Covered writing) and we can define the (Steganography) as one approaches science of hiding, and art of communication in a way to hide presence of this connection i.e. data transfer through other data used as a Host or Carrier that harmless to the carrier to those data and manner that does not allow any enemy or observer that discover that there are confidential data. hiding cares about the confidentiality of the contents of the letter in addition to achieving a secret contact and when spam suspect the existence of hidden information it tries to undo or destroys or change the message, and then sends it to the recipient, who knows how to interpret it. (H.Shahad,and,O.Elaaf,2008)

4.Hiding methods:

focus idea of hiding in the message inside the cover for a hidden target configuration, And can be represented by this equation:

hiding Target = message to hide+ cover+key In general hiding methods can be divided into four basic methods: (A.,Muhalim,2003)

1. Script Concealment
2. audio Concealment
3. Video Concealment
4. Image Concealment

5.Files Movement:

There are many file formats for graphic images and movement of some of these versions of the files used to represent certain types of data.

The supported file to represent the movement of the image animation is a files with different formats carrying data in different ways, where separate these images to frames "Frame" each and every one of them represents a snapshot of the scene.

Types of motion files: - (Tane,W.,and,Alan,L.,1996)

1.AVI files (Audio video interleaved).

2.GIF files (Graphic interchange format).

3.MPEG files (Moving picture expert group).

4.ANM files.

6.AVI (Audio Video Interleaved):

Is a standard file format for audio and video has been supported by Microsoft Corp., which made this kind of a record for the integration of digital video under all Window environment through the creation of a new file extension(.avi)

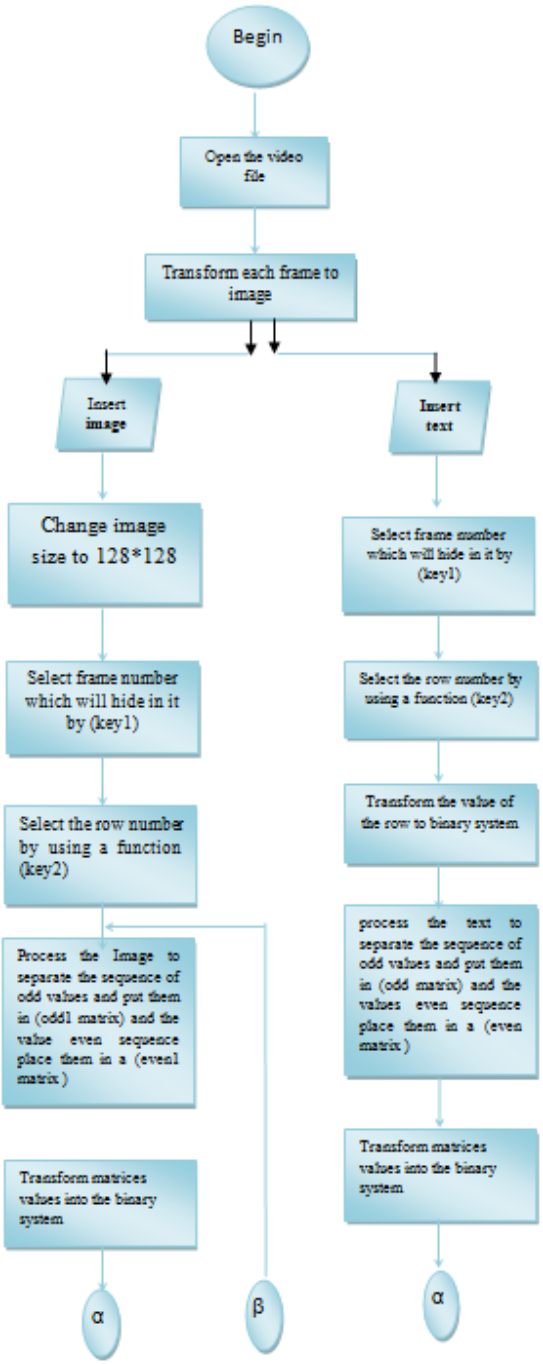
AVI format determine how video and audio are storage on the hard disk where the storage of the first frame of sound followed by the first frame of the video and the same thing for the second and so on. They called Audio Video Interleave because the overlap formula means that the storage of video and audio back-to-back in the AVI file (i.e.a section of audio data directly followed by a section of the video data) (Y.,Ghada,2003).

And as the overlap method uses AVI video and audio data, so we find that the audio remains in sync with the video, but this technique can not equipped with high-quality pictures with an integrated screen and give about 30 frames per second without the help of additives on the board.

The digital video files take sprawl AVI In the Windows environment containing a series of images "bmp" and the digital audio data. When handled such a file, the images should appear on the screen, one after the other and within the specific speed in order to be eye able to note punish frameworks "Frame" movement sequential and integrated, along with the note over the synchronization of digital picture with sound when it is turned this file.**(** M,H., 1996**)**

The Particle Part Of Research:

The flowchart one of the important ways in the analysis and design of software systems , it is very useful in the development of the system and easily understood for this reason will be explained flowchart for both the processes of hiding and retrieval (text and image).



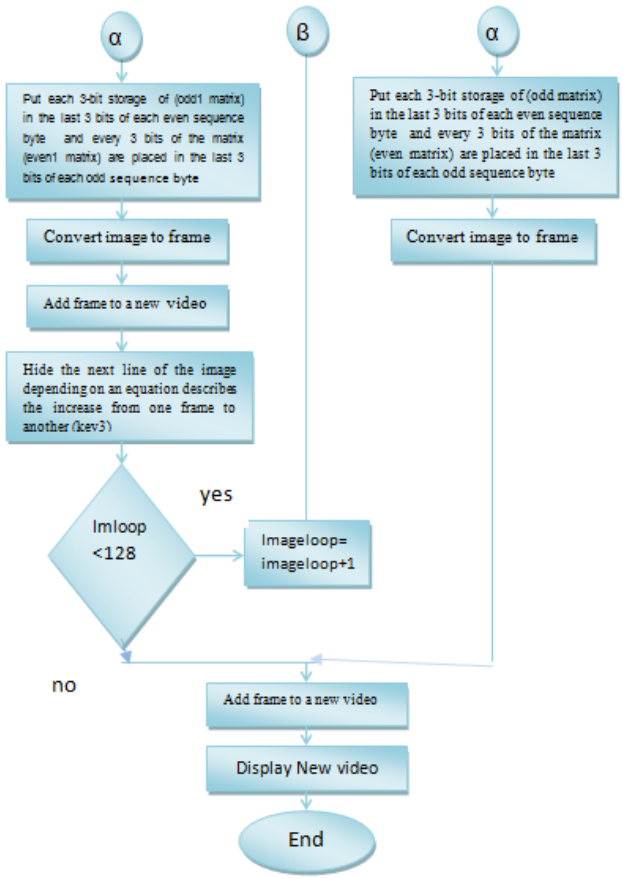


Fig. 1: process of hiding

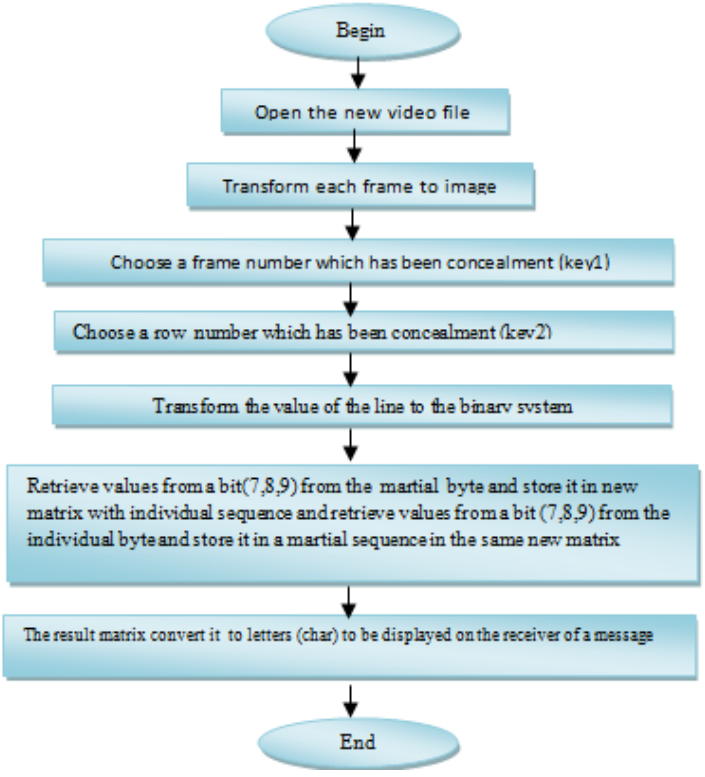


Fig. 2: process of retrieval text

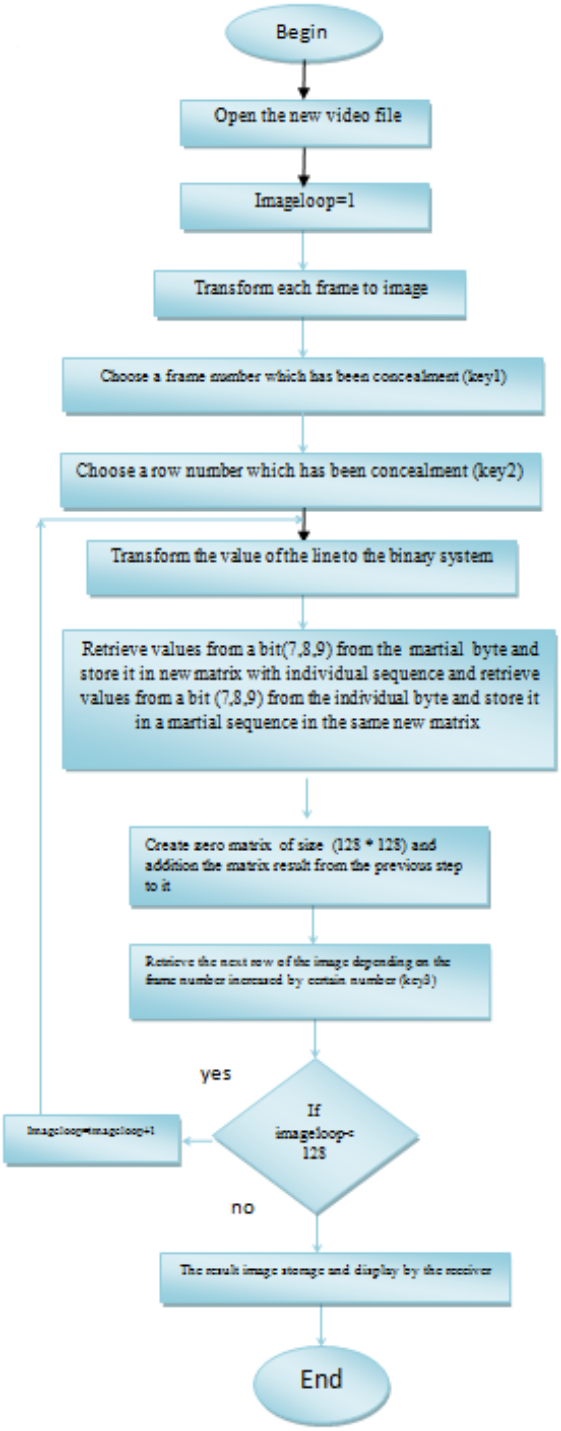


Fig. 3:process of retrieval image

Create The Cover And Massage:

1. Create the cover (video file):

This system will be used type of AVI video, a common quality of use.

2. Create the message (the text):

Initially the text is selected where the system gives the user the possibility to manually type the text or open any text file from the computer , that does not exceed the number of hidden characters in each frame of 128 characters for Video of size [512 * 512].

Action Steps System At The Sender:

The system reads the video file (AVI) and then extract each frame separately and deal with it as an image ,the no. of frame get from the formula agreed between the sender and receiver (key) to increase the difficulty of the discovery of frame number that has been concealment it.

The text is read and separate the sequence of individual character from the martial character sequence and put it in two matrices and then be transferred to the binary system with the size of (9 bit)
odd = dec2bin (text (1,1:2: no), 9);

even = dec2bin (text(1,2:2: no), 9);

After selecting the line number which will be concealment (line number which will be cover-ups will be the key agreed upon between the sender and receiver), the system will take each 3bit from (even) matrix and that marital contain the values stored in the deciding(7,8,9) individual with a byte sequence of the image, and took each 3bit of the matrix individual (odd) and stored in the bit (7,8,9) of the even with a byte sequence of the image.

After conducting these operations on the image ,then converted to a frame and add it to the new video created.

Action Steps System At The Receiver:

The system reads the file and convert video frames to images and then choose a frame number which has been concealment (considering that this number (key) Agreed between the sender and the receiver) and choose the number of the line that has been Concealment it (also as the key), and convert all values of this line to the binary system and the size of (9bit) and retrieve values from the bits (7,8,9) from the byte with martial sequence and stored in a new matrix sequence individually as well as in the case to decide (7,8,9) from a byte sequence Individual and stored in the same matrix sequence martially, the recovery process will continue until access to the dot (.) To signify that the message has ended.

Then the resulting matrix is converted to letters (char) to be displayed and read by the receiver. Create the message (image):

Prefers to be the image you want to hide it of type (jpg) and preferably be a quarter of the size of the (frame) size , it has been the adoption of image size (128 * 128) for Video of the size (512 * 512) in this research.

Action Steps System At The Sender:

The system reads the video file and extract every frame of it and convert each frame to image, and store each line of the image which to hide it in the frame of video.

To be agreed between the sender and the receiver of three keys (3 keys) first key specify the number of the first frame, which will be storing in it, and the second key is the line number to be concealment in it , while third key determines the amount of increase from one frame to another depending on the equation agreed upon it between the sender and receiver .

After the image is converted to Gray system by instruction grayimage = rgb2gray (image);

And resize it to 128 * 128.

After that values are separated sites (sequence) and placed in individual matrix (odd) the values of matrimonial sites and put them in matrix (even) of the image, then the system will convert both values to the binary system matrices odd=dec2bin(grayimage(1,1:2: no), 9);

even=dec2bin(grayimage(1,2:2:no), 9);

The system then converts the values of frame to the binary system too.

After selecting the first frame number which will be cover-ups, as well as the line number of the frame, which will be concealment process in which the system will take all the 3 bit of (even)matrix and put it in a (7,8,9) of byte odd sequence in the image and taking the values stored in (odd) matrix and put them in a(7,8,9) of byte even sequence in the image.

These operations will be conducted on each line of the image, where each line will hide in a frame and increase the number of frame depending on the formula agreed between the sender and receiver to store each line of the image.

Each image is added after conversion to the frame to a new video whose can been configured previously.

Action Steps System At The Receiver:

The receiver reads the video file and extract each frame of it.

All frames are converted to images and then select the first frame number which has been concealment (depending on the key Set between the sender and the receiver), and choose the number of the line which has been concealment. Then all values are converted this line to the binary system and the size of (9 bit) and retrieve values from deciding (7,8,9) of the byte with doubles sequence and stored it in a new matrix of sequence odd, as well as in the case to decide (7,8,9) of byte sequence individual and stored in the same matrix martial sequence.

Each line is recovered from the image of each frame of concealment which, depending on the formula agreed between the sender and the receiver , then the image is displayed (secret message) at the receiver.

8. An application Example:

Will be given a practical example to illustrate both concealment and retrieval processes of the type of text message:

The Steps Involved In The Process Of Concealment:

1.read the video file

2.Read the text you want to hide it

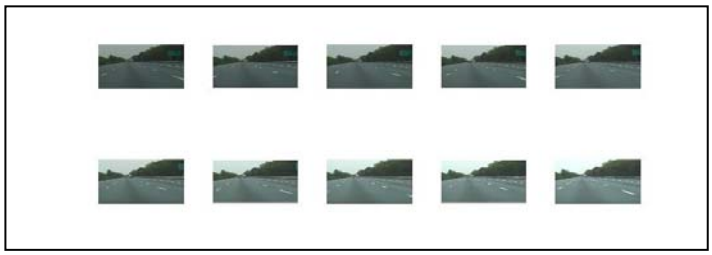


Fig. 4: Set of frames to compose motion file suppose the text is:text='steganography hides the very existence of a message so that if successful , it generally attracts no suspicion at all.';

3.separate characters of individual sequence from singles doubles

aa1od=seaorpy

aa2ev=tgngah

4. after implementation of instruction dec2bin to transform matrices values into binary system produces:

odd=0010100011 001100111 001100001 001101111 001110010 001110000 001111001

even=001110100 001100111 001101110 001100111 001100001 001101000

5.convert frame to image

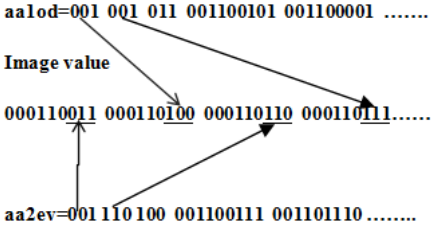
6.Choose a frame number which will be concealment based on the equation and suppose the output equation was number key1= 5

Fig. 5: Frame number 5

7.Choose the row number, depending on the equation was also the row No. key2= 1 and convert the value of this row to the binary system with size of (9 bit) to produce:

000110011 000110100 000110110 000110111 000111000 00011000 000111000 000111001 000111000……

8. Taking each 3bit of odd and stored in the bit (7,8,9) of the martial byte and take each 3bit of even matrix and stored in the bit (7,8,9) of the individual byte



The row values become:

000110**001** 000110**001** 000110**110** 000110**010** 000111**100** 000011**011** 000111**001** 000111**001** 000111**100** ….

9.Convert the image to the frame

Fig. 6: Convert the image to frame

10.Restore the frame to a new video as well as the frames that have not change.

The Steps Involved In The Process Of Retrieval:

1.Read the recipient video file:

2.convert the frames whose compose the video to the images.

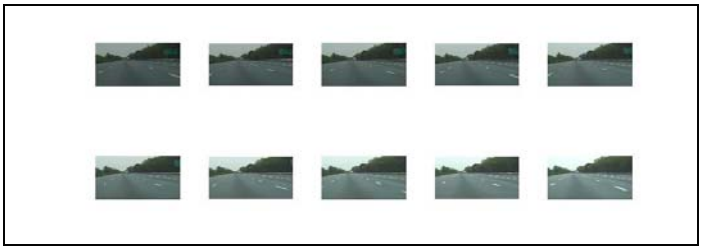


Fig. 7: Set of frames to compose motion file

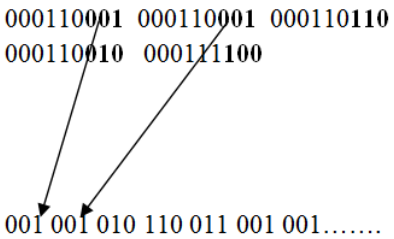
3.Choose a frame number (agreed upon is the number key1= 5)

Fig. 8: Frame number 5

4.Select the line number which has been concealment and agreed between the sender and receiver (key2=1) and convert it to a binary system and size of (9 bit)

000110001 000110001 000110110 000110010 000111100 000011011 000111001 000111001 000111100 …..

5.Retrieve values from bits (7,8,9) and put in a new matrix



6. Convert the resulting matrix to char to be retrieve the full text:message=steganography…….

Discussion of Results:

In this paper, a process of concealment for a range of different images within the type of video files (avi) has been calculated efficiency standards for images that have been concealed and then retrieval of video files which is :

1.PSNR (Peak Signal to Noise Ratio) :

PSNR=10log10[R^2/MSE] (1)

where:

R: represents the number of levels of gradation

2. MSE (Mean Square Error) square error rate picture:

MSE=$\sum_{m,n}$[I1(m,n)-I2(m,n)]^2/(m*n) (2)

where:

I1 (m, n) represents the original image before the process of concealment

I2(m, n) represents the recovered image.

3.Correlation ratio of the correlation coefficient:

CR=(COV(X,Y))/σXσY (3)

where:

X: represents the original image

Y: represents the recovered image

COV (X, Y): represents the variation

ΣXσY: represent the standard deviation (A.,Maysoon Khuder, 2003)

Table 2: shows the rates of efficiency standards for different images with different videos

Video file	Image	PSNR	MSE	CORRE L-ATION
		86.021	0.0117	0.9899
		72.227	0.2051	0.9985
		84.037	0.0103	0.9897

We note from the table above that the noise ratio in image (PSNR) is a high and this means that the picture is recovered from the process of concealment close to the original image and this achieves efficient of proposed algorithm , as well as for the value of square error (MSE) in image we note that the value of it is little and this means that the picture is the closest to the original image.

As for the correlation coefficient (CR) we note that the value is closer to one, and this means that the picture is very close to the original image.

Conclusions:

1. Dealing with video files very well be in terms of being a cover for the transfer of the message,whether (image or text or both) to being a relatively large size.

2.The process of text hiding are very sensitive to any change so when you hide text or retrieved must match 100% because any change to the location of bits will be change the text.

3.Distribution rows of image in frames of the video consider that the first frame starting to hide in it depand on equation not in sequentially order ,the same thing for the row whose hiding in it will deal to hash information of image in the video, which gives a high security for the proposed method of hiding.

4. Not hide image and text information sequentially, but took the image or text data with the even sequence was concealed in a odd sequence within the existing row in frame whose composed the video file and vice versa, which gave a high security in finding the text

5. by applying the proposed algorithm in hiding , has been retrieved text file completely and the matching rate was 100%, but for the image retrieved from the process of concealment has applied standards of efficiency and as shown in the table (2) and the results were good, which proves the efficiency of the proposed algorithm.

10.Recommendations:

1. You can use other types of video
2. The use of special methods to encrypt data before concealed.
3. be possible to compress the image and then concealed in a video file and use advantage of the properties of image to hide.
4. Possible application this algorithm audio files and section of video files.

REFRENCES

Barzanchi, F., 2008. hiding Data In Image, Sulaymania university, Iraq. www.boosla.com fowzibarazenji@yahoo.com

Donald, H., and M. Baker, 1997. Computer graphics C version, 2nd Edition، published: prentice.

Ghada Thanoon, Y., 2003. Tracking the flame in the digital color moving pictures , Master Research, Faculty of Computer Science and Mathematics, Department of Computer Science, University of Mosul, Iraq.

M, H.,1996. Overview of common multimedia file format, university of Miami information technology. http://www.miami.edu/it/as/classes/pdfs/av.formats.pdf

Maysoon Khuder, A., 2003. Image Compression Of Arabic text documents, Master Research, Faculty of Computer Science and Mathematics, University of Mosul, Iraq.

Muhalim, A., 2003. Information Hiding Using Steganography, University Technology Malaysia.

Nori, A. and S. Aziz, 2011. Investigation about concealment detection in color images, Journal of Mesopotamia for collage of computer science and mathematics, Folder (8), Issue No. (2).

Shahad, H. and O. Elaaf, 2008. Coverage was introduced color photo of the type of BMP, first Scientific Conference of Information Technology, University of Mosul, Iraq.

Tane,W. and, L. Alan, 1996. considerati-on for capture use and delivery, university of Bristol.

Yousef, D., 2003. Information Secu rity Steganography, King saud university College of computer& Information Sciences Information Systems Department.