Hiding Image within Video Clip

Nada Elya Tawfiq
College of Computer Science and Information Technology Nawroz University

Abstract: *Due to the huge development of computer science which was escorted by another vast development in the hiding techniques, which became of great possibilitiesin which it is difficult to break those techniques.Those techniques were classified depending on the method of embedding like inserting, replacing or exchange positions.*

In this research paper, a new hiding technique was developed to obtain high-quality results. The video image was segmented into frames, which is a three dimensional image of RGB (Red-Green-Blue) type. A part of the image is being embedded into first and last row of the three frames (i.e. into the external edges of the frame) in which a new algorithm to hide information has proposed in order to increase the complexity of retrieving that information and leads to add power to the algorithm.

The proposed algorithm followed in this research paper led to get a video segment which is difficult to expect finding embedded data within.

Finally MATLABR2010a was used implement the practical side of the hiding algorithm.

I. Introduction

Multimedia technologies are becoming more sophisticated, enabling the internet to accommodate a rapidly growing audience with a full range of services and efficient delivery methods. Although the internet now puts communication, education, commerce and socialization at our finger tips, its rapid growth has raised some weighty security concerns with respect to multimedia content. The owners of this content face enormous challenges in safeguarding their intellectual property, while still exploiting the internet as an important resource for commerce. Data Hiding Fundamentals and Applications focuses on the theory and state of the art applications of content security and data hiding in digital multimedia. One of the pillars of content security solutions is the imperceptible insertion of information into multimedia data for security purposes; the idea is that this inserted information will allow detection of unauthorized usage. [1]

Information hiding

The improving technology and the ubiquity of the internet have allowed more and more people to transmit data via the internet. The contents of the transmission can be in the form of words, voices, images, or even computer animation, some contents transmitted can be confidential data such as highly valued product design or war plans, so to product these contents from interceptor’s attention, the information hiding technology thus emerged.[2]

Hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change).[3]

Written another way, information hiding is the ability to prevent certain aspects of a class or software component from being accessible to its clients, through an explicit exporting policy and through reliance on the short form as the primary vehicle for class documentation.[4]

Steganography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek words steganos meaning "covered or protected", and graphei meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other covertext and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated.[5]

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.[1] Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.[5]

Data embedding security schemes

The choice of embedding algorithm in the most cases is driven by the results of the steganographic channel robustness analysis. One of the areas that improve steganographic robustness is usage of a key scheme for embedding messages. Various key steganographic schemes have various levels of protection. Key scheme term means a procedure of how to use key steganographic system based on the extent of its use. However, when the steganographic robustness is increased a bandwidth of the whole embedding system is decreased. Therefore the task of a scheme selection for achieving the optimal values of the steganographic system is not trivial.

Embedding messages in steganographic system can be carried out without use of a key or with use of a key. To improve steganographic robustness key can be used as a verification option. It can make an impact on the distribution of bits of a message within a container, as well as an impact on the procedure of forming a sequence of embedded bits of a message.

The first level of protection is determined only by the choice of embedding algorithm. This may be the least significant bits modification algorithm, or algorithms for modifying the frequency or spatial-temporal characteristics of the container. The first level of protection is presented in any steganographic channel. Steganographic system in this case can be represented as shown at The First Protection Level Scheme figure. There following notations are used: c - is a container file; F - steganographic channel space (frequency or/and amplitude container part that is available for steganographic modification and message signal transmission); SC - steganographic system; m - message to be embedded; E - embedding method; ĉ - modified container file.

The second protection level of the steganographic system, as well as all levels of protection of the higher orders, is characterized by the use of Key (password) via steganographic modification. An example of a simple key scheme, which provides a second level of protection, is to write the unmodified or modified password in the top or bottom of the message; or the distribution of the password sign on the entire length of the steganographic channel. Such key schemes do not affect the distribution of messages through the container and do not use a message preprocessing according to the defined key (see figure The Second Protection Level Scheme). This kind of steganographic systems are used in such tasks as, for instance, adding a digital signature for proof of copyright. Data embedding performance is not changed in comparison with the fastest approach of the first protection level usage.

Steganographic data channels that use key schemes based distribution of a message through the container and or preprocessing of an embedded message for data hiding are more secure. When the third protection level key scheme is used it affects the distribution of a message through the container (see figure The Third Protection Level Scheme, where F (P, L) – distribution function of a message within a container; P – minimum number of container samples that are needed to embed one message sample; L – step of a message distribution within a container). Accordingly, the performance of container processing will be lower than in the case of the first and the second key schemes. Taking into account that $P \geq L$, the simplest representation of the F(P, L) function could be as following:

$F(P, L) = cycle*L + step*P$ ……………..(1)

Where cycle is a number of the current L section and step is a number of the embedded message sample.

The difference between the fourth protection level scheme and the third one is that in steganographic system there are two distribution functions of a message within a container are used. The first is responsible for a message samples selection according to some function G (Q, N), and the second function F(P, L) is responsible for position selection in a container for message sample hiding. Here Q – the size of message block to be inserted; N – the size (in bits) of one sample of the message file (see figure The Fourth Protection Level Scheme).

II. Proposed Algorithm

In the proposed algorithm, a modified method of data hiding by LSB substitution method is developed to embed a secure image (for any extension) in the video clip, so that the interceptors will not notice about the existence of that image. The simple LSB substitution method is used to prevent illicit access of data and increase the system performance, so the effectiveness of the optimal LSB substitution in the worst case willbe proved. In the worst case, PSNR of the obtained stego-image can be computed by:

PSNR$_{\text{worst}}$$PSNR_{worst} = 10 \times \log_{10}\frac{255^2}{MSE}$ ……………………….. (2)

The proposed algorithm consists of two parts:

First part: Embedded the image

The first row of the image was taken in red color and put into the first row of the first dimension of the frame, and then the second row of the image was put into the last row of the frame. The same thing done to the rest of the colors (i.e. green and blue) whereas the first and second row of the image were taken and put into first and last row of the second dimension of the frame. Figure (2-1) shows the embedded of first and second row.

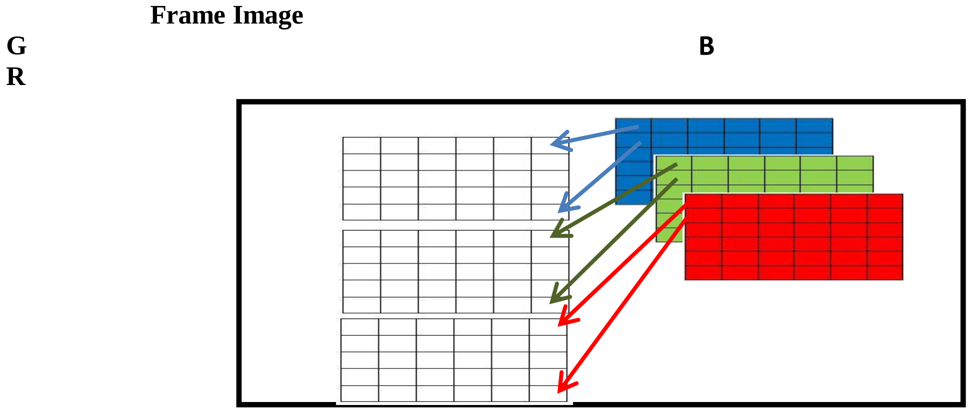


Figure (2-1) embed first and second row

- ***Second part: Extract the image***

The first and last row of the three dimensions of the frame were return to the first and second row of the RGB image, as shown figure below:

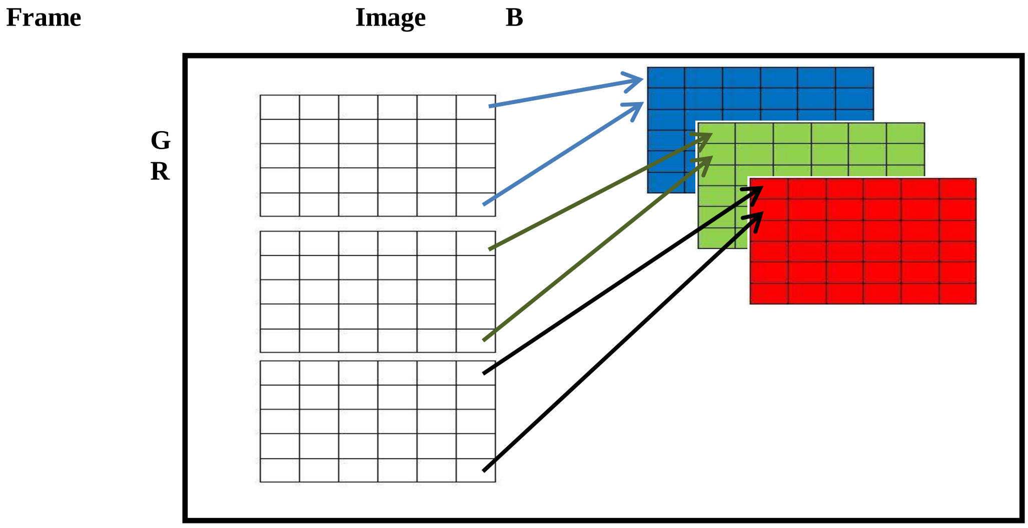


Figure (2-2) extract first and second row

The equations that applied for each frame are:

$$Frame\ no.k(1,:,1) = \sum_{i=1}^{m} img(i,:,1) \qquad \dots\dots\dots\dots\dots\dots\dots (3)$$

$$Frame\ no.k(1,:,2) = \sum_{i=1}^{m} img(i,:,2) \qquad \dots\dots\dots\dots\dots\dots\dots (4)$$

$$Frame\ no.k(1,:,3) = \sum_{i=1}^{m} img(i,:,3) \qquad \dots\dots\dots\dots\dots\dots\dots. (5)$$

$$Frame\ no.k(end,:,1) = \sum_{i=1}^{m} img(i,:,1) \qquad \dots\dots\dots\dots\dots\dots\dots. (6)$$

$$Frame\ no.k(end,:,1) = \sum_{i=1}^{m} img(i,:,2) \qquad \dots\dots\dots\dots\dots\dots\dots\dots (7)$$

$$Frame\ no.k(end,:,1) = \sum_{i=1}^{m} img(i,:,3) \qquad \dots\dots\dots\dots\dots\dots\dots\dots (8)$$

The steps of the proposed algorithm are shown as the following flowchart:

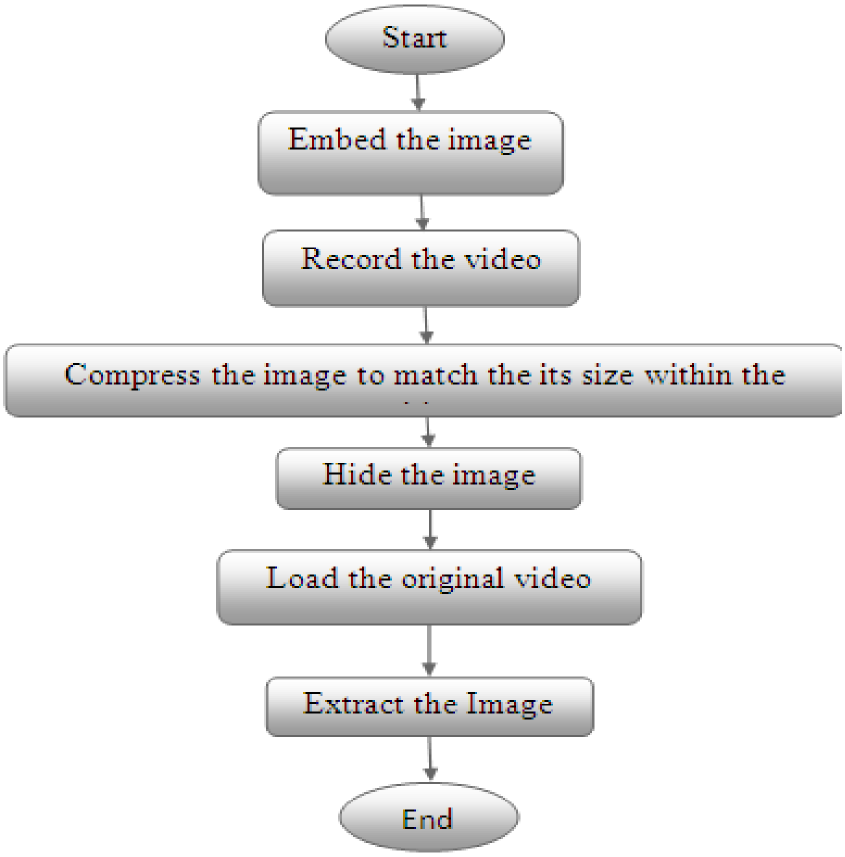


Figure (2-3) flowchart of proposed algorithm

III. The Applicative Side Of Proposed Algorithm

The algorithm was been programmed for the concealment the image within a video clip in the form of interfaces that represent the view of the Executive of the choices available in the algorithm proposed imitation between the user and program. The program consists of two main parts, the first part is for concealment, and the second part is for extract the image from the video, as shown in the Figure (3-1):

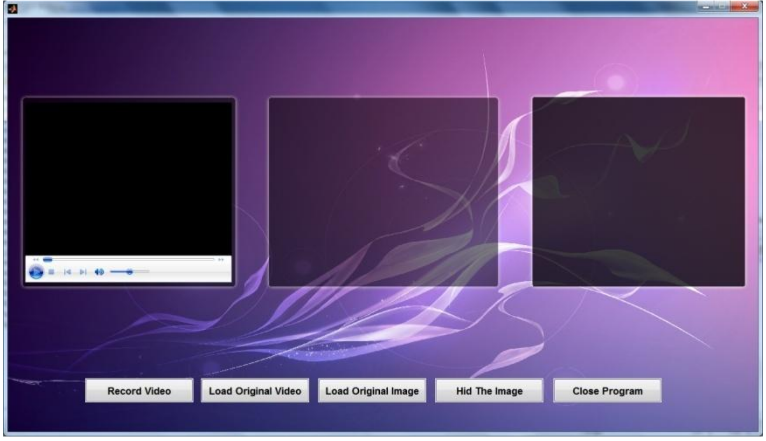


Figure (3-1) Interface of the program

When an embedded image was hidden within the video, it is compressed in order to match its size within the video as shown in Figure (3-2):

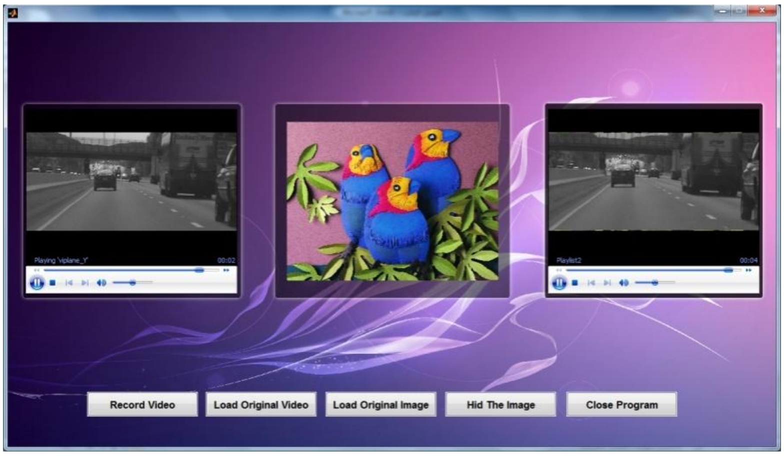
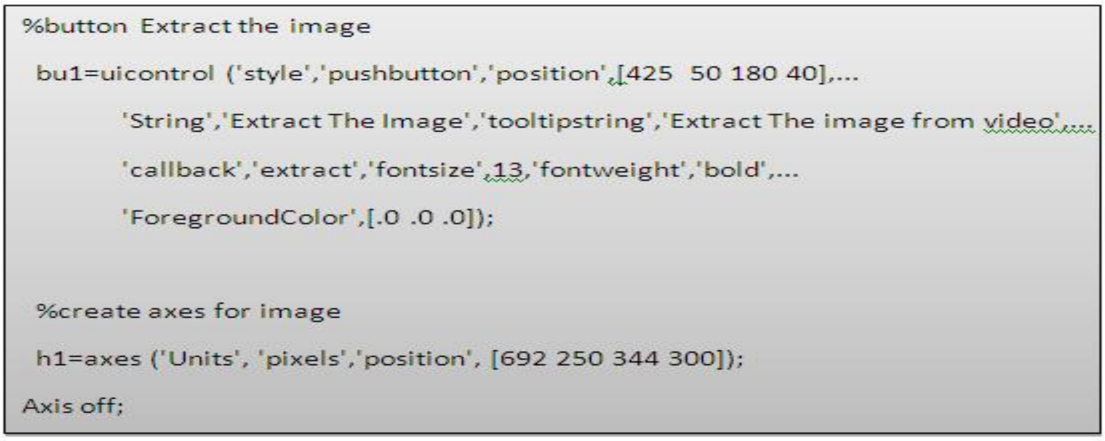


Figure (3-2) hides the image within the video

And the code used to hide the image within video is:



```
%button  Extract the image
  bu1=uicontrol ('style','pushbutton','position',[425  50 180 40],...
         'String','Extract The Image','tooltipstring','Extract The image from video',...
         'callback','extract','fontsize',13,'fontweight','bold',...
         'ForegroundColor',[.0 .0 .0]);


  %create axes for image
  h1=axes ('Units', 'pixels','position', [692 250 344 300]);
Axis off;
```

%button Hid video

Then load the videothat contains the hidden image to Extract that image and save it, as show in Figure (3-3).

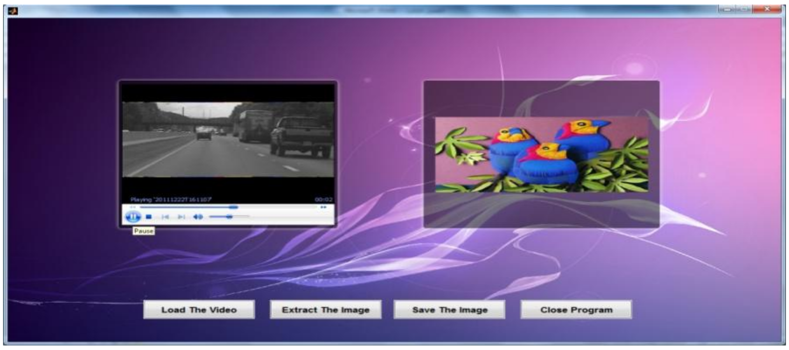
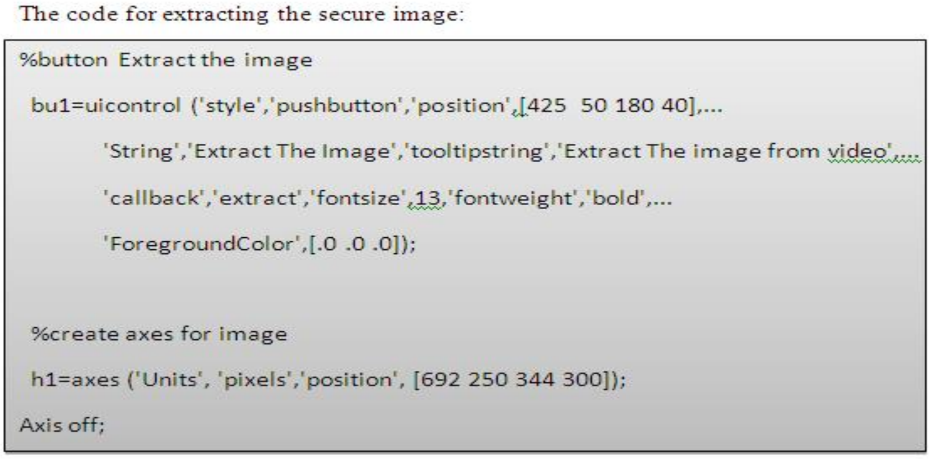


Figure (3-3) extracts the image.

The code for extracting the secure image:

%button Extract the image



The code for extracting the secure image:

```
%button  Extract the image
 bu1=uicontrol ('style','pushbutton','position',[425  50 180 40],...
         'String','Extract The Image','tooltipstring','Extract The image from video',...
         'callback','extract','fontsize',13,'fontweight','bold',...
         'ForegroundColor',[.0 .0 .0]);


 %create axes for image
 h1=axes ('Units', 'pixels','position', [692 250 344 300]);
Axis off;
```

IV. Conclusion

The Extensive experiments show the effectiveness of the proposed method. The experimental results show that the image is visually indistinguishable from the original video and that shows a dramatic improvement in the work with respect to image equality and computational efficiency.In the future it can embed many images may be contain noise within one video clip, then process thenoise by removing it before display the images. Table1 tabulates the PSNR for the proposed system.

Table 1: PSNR for the proposed algorithm

K	1	2	3
MSE	**61.7660**	**62.4659**	**60.5084**
PSNR	**30.2233**	**30.1744**	**30.3126**

References

[1]. Refrence: book: "DATA HIDING FUNDAMENTALS AND APPLICATRIONS" AUG-2004,HusrwSencar,

[2]. chin-Chen Chang, " International Journal of Pattern Recognition and Artifitial Intelligence", Volume 16, Issue 04, June 2002.

[3]. ab Grady Booch," Object-Oriented Analysis and Design with Applications", . Addison-Wesley, 2007, ISBN 0-201-89551-X, p. 51-52.

[4]. http://en,Wikipedia.org/wiki/Information_hiding.

[5]. Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet.Archived from the original on 2007-07-16.http://web.archive.org/web/20070716093719/http://www.alternet.org/story/11986/. Retrieved 2008-09-02.

[6]. Chvarkova, Iryna; Tsikhanenka, Siarhei; Sadau, Vasili (15 February 2008). "Steganographic Data Embedding Security Schemes Classification".*Steganography: Digital Data Embedding Techniques*. Intelligent Systems Scientific Community, Belarus.http://scientist.by/index.php?option=com_content&view=article&id=37%3Asteganography-digital-data-embedding-techniques&catid=9&Itemid=27&limitstart=5. Retrieved 25 March 2011.

[7]. Joshua R. Smith and Barrett O. Comisky, "Modulation and Information Hiding in Images", Cambridge, USA May 2009.