Animation Steganography using Binary Images

By

Burhan Mollan Salih.

(Diyala University\College of Sciences\ Computer Science Dep.)

Abstract

Steganography is the science of secret message delivery using cover media. The cover carriers can be image, video, animation, sound or text data. A digital image is a flexible medium used to carry a secret message because the slight modification of a cover image is hard to distinguish by human eye. Secret data hiding in binary images is more difficult than other formats since binary images require only one bit representation to indicate black and white. However, this model proposes technique to hide secret message using animations as cover-object. In the proposed model, animation sample frames are converted to binary images. Then, these binary images are used as a cover for hiding secret data depending on boundary bits manipulation technique.

The performance of the proposed model has been successfully tested by computer simulation and the results are presented both quantitavely and qualitatively.

Keywords: Animation Frame, Animation Steganography, Binary Image,

Binary Image Steganography, Boundary Bits Manipulation Technique.

اخفاء المعلومات في الصور المتحركة باستخدام الصور الثنائية

برهان مولان صالح

الخلاصة

اخفاء المعلومات(ستيكانوكرافي) هو علم ايصال الرسالة السرية باستخدام الوسائط(الغطاء). الغطاء قد يكون صورة , فيديو , صور متحركة, صوت او بيانات نصية. الصورة الرقمية هي وسيلة مرنة تستخدم لحمل الرسالة السرية لان التعديل الطفيف على صورة الغطاء من الصعب تميزها بواسطة العين البشرية. اخفاء البيانات السرية في الصور الرقمية هو اكثر صعوبة من غيرها حيث ان الصورة الرقمية تتطلب خانة واحدة (one bit) فقط لتمثيل اللون الابيض والاسود. هذا البحث يقترح تقنية لاخفاء رسالة سرية باستخدام الصور المتحركة كغطاء. في النموذج المقترح عينة اطارات الصور المتحركة حولت الى صور ثنائية ثم هذه الصور الثنائية استعملت كغطاء لاخفاء بيانات سرية بالاعتماد على تقنية التعامل مع بتات الحدود. وقد تم بنجاح تقييم النموذج المقترح من خلال المحاكاة بالحاسوب وتم تقديم النتائج كما ونوعا.

الكلمات المفتاحية: اطار الصور المتحركة , اخفاء المعلومات للصور المتحركة ,الصور الثنائية , اخفاء المعلومات للصور الثنائية , تقنية التعامل مع بتات الحدود.

Introduction

The security of digital media becomes of major concern due to its emergencies and wide spread. The security of the transformation of hidden data can be achieved by two ways: encryption and steganography. A combination of the two techniques can be used to further increase the security of data. In encryption, the message is changed so that no data can be disclosed if received by an attacker [1]. In the Steganography system scenario, before the hiding process, the sender must select the appropriate message carrier (i.e image, video, audio, text) and select the effective secret messages as well as the robust password (which suppose to be known by the receiver). The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email or chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used by the sender [2].

The motivation behind developing image Steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the Steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message[2].

Steganography is divided into three main types: pure steganography, secret key steganography, and public key steganography. A steganography system that does not require prior exchange of some secret information is a pure steganography. In a secret key steganography system the sender chooses a cover and embeds the secret message into it using secret key. Public key steganography systems require the use of two keys, one private and another public. Whereas the public key is used in the embedding process, the secret key is used to reconstruct the secret message [3].

Animation, when applied to images, is defined as moving diagrams that are made up

of a series of images that represent a distinct narrative unit. Each of the images should be usually connected either by unity of location or time. The individual image used in an animation is a frame. Every animation follows a set of rules or grammar that governs the way the sequence is arranged. These rules can be in the form of regular expressions or can be represented by Finite Automata. Let F represent the set consisting of the frames that can be used in this animation. i.e.{F1,F2,….,Fq}. Let 'A' represents the regular expression for the animation. 'A' can contain any number of frames and it represents the order in which the image frames are played. For example A = F1 (F3F2 F3)* F3F2 is a valid representation of animation. There is frame table called a frame id and corresponding picture image[4].

Binary images, such as signatures, drawings, and scanned documents, are increasingly common in our everyday life. Having the capability of hiding data in binary images can facilitate the authentication, annotation, and tracking of these documents in the digital

domain. However, data hiding in binary images is much more difficult than in images with a wide range of colors or brightness levels. In a conventional color picture, minor tuning the color of a small pixel is usually not perceivable by eyes, and coded messages can be conveyed through minor color changes on the pixels. On the other hand, black and white are the only two colors in a binary image and they are drastically different to our eyes[5].

In particular flipping white or black pixels that are not on the boundary is likely to introduce visible artifacts in binary images. Several methods for hiding data in specific types of binary images have been proposed in literature. These previously proposed approaches either can not be easily extended to other binary images, or can only embed a small amount of data [6].

This paper about hiding secret data inside binary images which are animation frames using (3*3) bit manipulation method.

Proposed Model: Animation Steganography using Binary Images

The proposed model is divided into two sides: Hiding side and extracting side.

Hiding (Embedding) Side

Hiding side of this model is shown in figure (1).

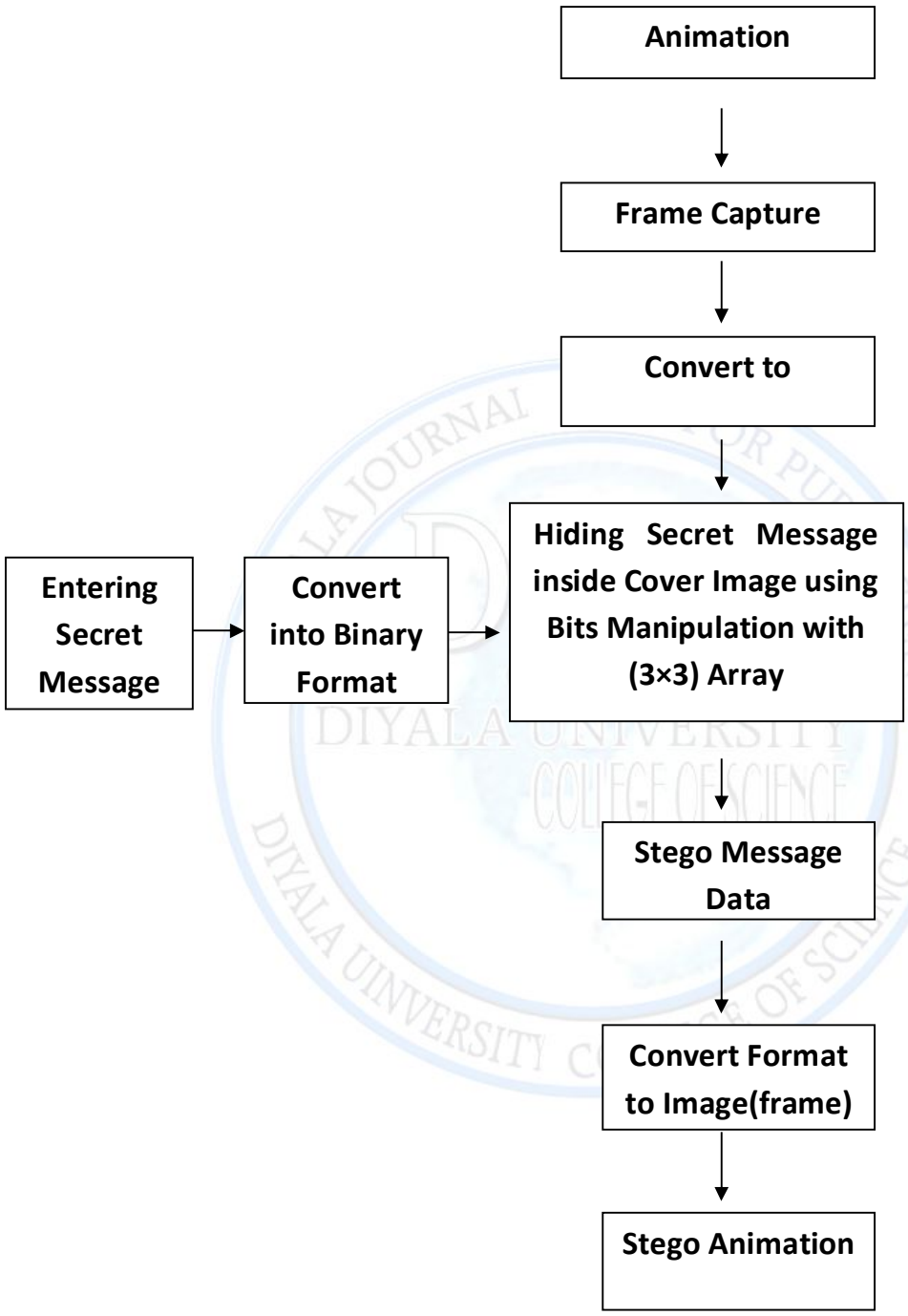


Figure (1) Block Diagram of embedding side of the proposed model

Conversion Captured Animation Frames into Binary Images.

First step in the proposed model is capturing animations frames. Then each frame is giving an ID number(as a key) in order to recognize it in extraction side, The capture frame is converted into binary image using threshold value (127).

Hiding (Embedding) Secret Message inside Cover Image using Boundary Bits Manipulation(3*3 array).

The idea of this technique is bits manipulation. A window (block of 3*3 bits) is taken from hiding cover message file, with each bit of secret message. The process of |hiding is shown in figure (2), in which all probabilities ($2^9 = 512$) are covered.

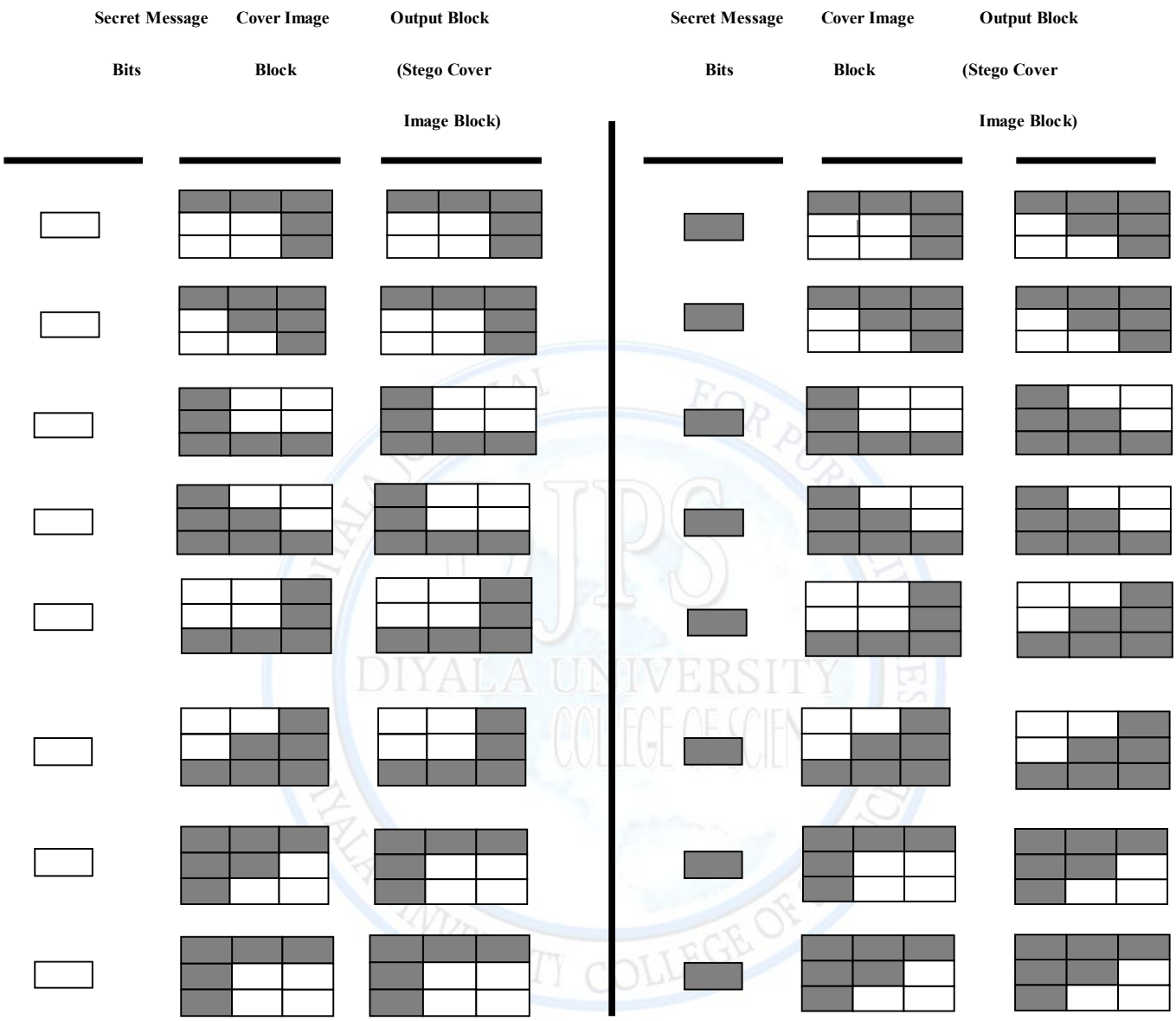


Figure (2) The Idea of Hiding (Embedding) Technique using Boundary Bits Manipulation(3*3 array). Black represent 0 and White represent 1

By comparison between secret message bits and cover image block, new blocks are inserted at stego cover file depending on idea of figure (2). After finishing the bits of secret message, the blocks of cover image are remained with no change. This technique can be clarified at algorithm (1).

Algorithm (1) Hiding (Embedding) Secret Message Inside Cover Image using Boundary Bits Manipulation(3*3 array)

Input :

1- Binary cover image file

2- Binary secret message file

Output : Stego message data file

While not end of (input file (1))

{

Read block from input file (1)

While not end of (input file (2))

{

1-Read bit from input file (2)

Flag=false

PP1:

If bit = 0 and block = $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ **Put block =** $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ **at output file , Flag=true ,and Goto pointer 1.**

If bit = 0 and block = $\begin{pmatrix}1&0&0\\1&1&0\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&0&0\\1&0&0\\1&1&1\end{pmatrix}$ at output file , Flag=true ,and Goto pointer 1.

If bit = 0 and block = $\begin{pmatrix}1&1&1\\0&0&1\\0&0&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\0&0&1\\0&0&1\end{pmatrix}$ at output file , Flag=true ,and Goto pointer 1.

If bit = 0 and block = $\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\0&0&1\\0&0&1\end{pmatrix}$ at output file , Flag=true , andGoto pointer 1.

If bit = 0 and block = $\begin{pmatrix}0&0&1\\0&0&1\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}0&0&1\\0&0&1\\1&1&1\end{pmatrix}$ at output file , Flag=true , and Goto pointer 1.

If bit = 0 and block = $\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}0&0&1\\0&0&1\\1&1&1\end{pmatrix}$ at output file , Flag=true ,Goto pointer 1.

If bit = 0 and block = $\begin{pmatrix}1&1&1\\1&0&0\\1&0&0\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\1&0&0\\1&0&0\end{pmatrix}$ at output file , Flag=true , and Goto pointer 1.

If bit = 0 and block = $\begin{pmatrix}1&1&1\\1&1&0\\1&0&0\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\1&0&0\\1&0&0\end{pmatrix}$ at output file , Flag=true , and Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}1&1&1\\0&0&1\\0&0&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$ at output file , Flag=true , and Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}1&0&0\\1&0&0\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&0&0\\1&1&0\\1&1&1\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}1&0&0\\1&1&0\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}1&0&0\\1&1&0\\1&1&1\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}0&0&1\\0&0&1\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$ Put block = $\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}1&1&1\\1&0&0\\1&0&0\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\1&1&0\\1&0&0\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

If bit = 1 and block = $\begin{pmatrix}1&1&1\\1&1&0\\1&0&0\end{pmatrix}$ Put block = $\begin{pmatrix}1&1&1\\1&1&0\\1&0&0\end{pmatrix}$ at output file , Flag=true , and

Goto pointer 1.

Pointer 1 :

If Flag = True

{

Put block at output file

```
Read another block from input file (1)
Goto Pointer 2
} End If
If  Flag = False
{
Put block at output file
Read block from input file (1)
 Goto PP1
} End If
 Pointer  2 :
} end while
Read block from input file (1)
Put block at output file
 } end while
```

Convert Stego Cover Data into Image Format

It is technique of concatenating image header with (stego image data after conversion into characters). After this process convert stego image data file to stego message image and will be repeat same steps with other binary image after finishing the embedded process will be calculate all images and convert it to animation and send the animation with ID key(which frame became in it secret messages) to receiver side.

Extracting side

Extracting side of this mode is shown in figure (3)

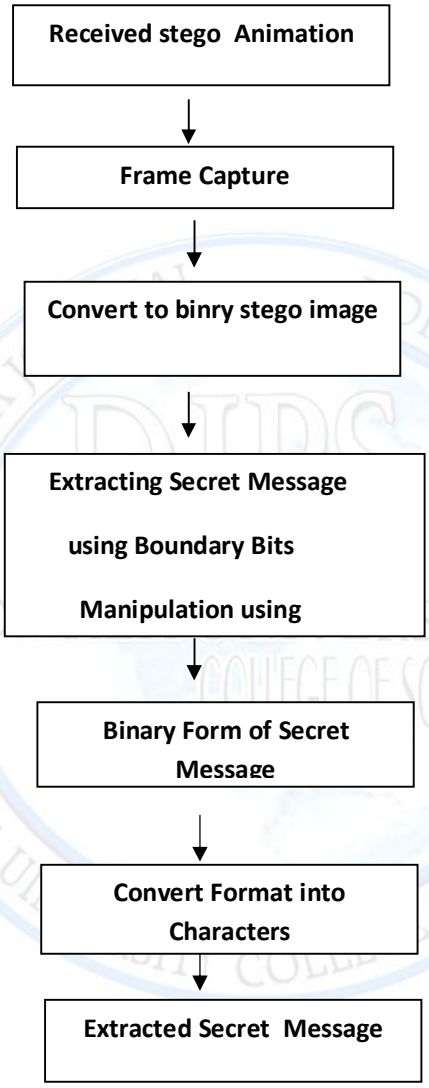


Figure (3) Block Diagram of Extracting Side of the proposed model

Receive Stego Animation

After received the animation with ID keys of frames same procedure will be convert the animation to binary image and he know where the secret messages embedded by using ID keys.

Extracting Secret Data using (3*3) Boundary Bits Manipulation

The idea of this technique depends on the value of second row and second column in each block. A window (block of 9–bits) is taken from stego cover image file. If the bit in block (3*3 array) in the location (2,2) is 0 put zero in output file otherwise put one in the output file. The process of extracting is shown in figure (4).

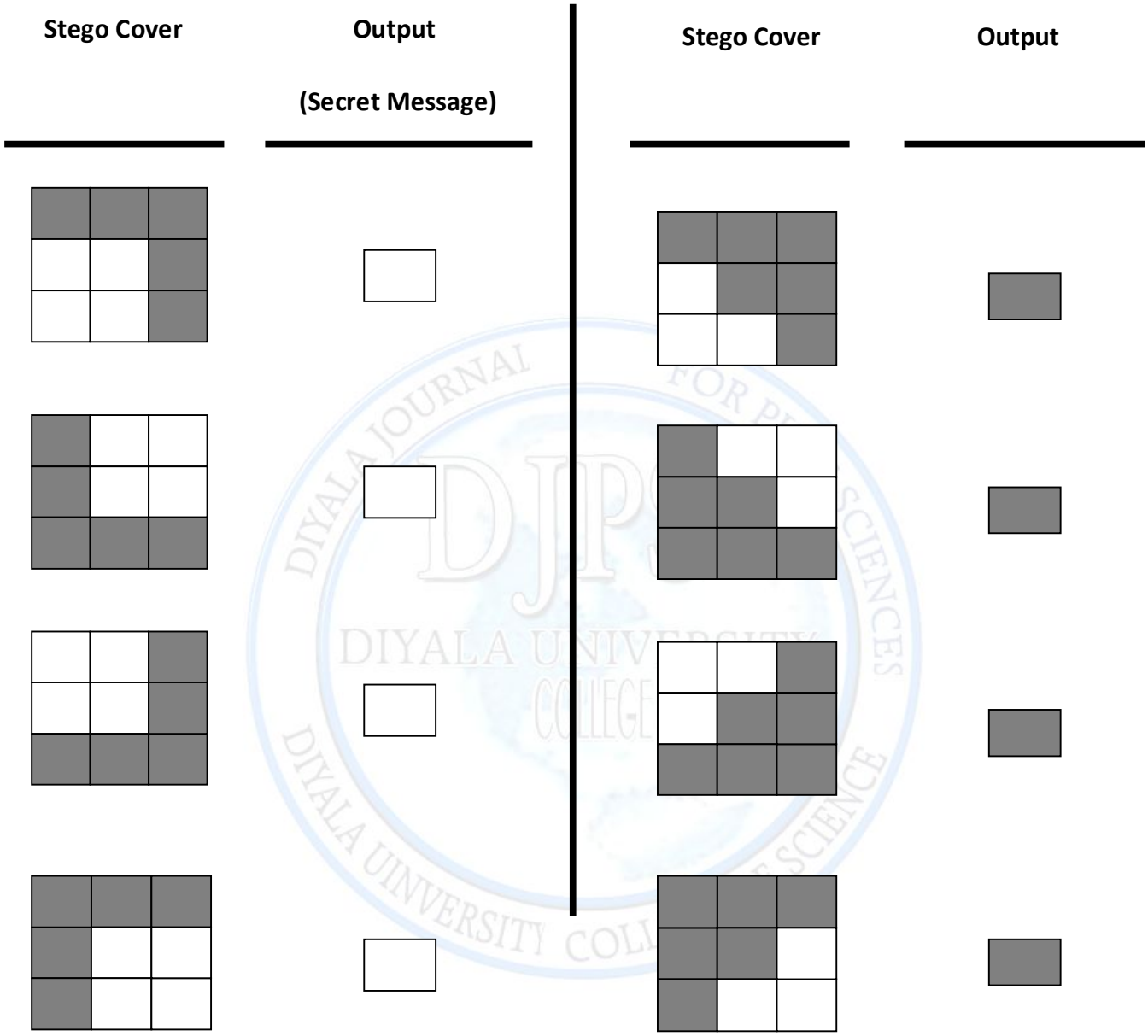


Figure (4) The Idea of Extracting Technique using Bit Manipulation(3*3 array). Black represents 0 and White represents 1.

The process which is described at figure (4), will be continued until last block of stego cover image file. This technique can be clarified at algorithm (2).

Algorithm (2) Extracting Secret Message Data using Boundary Bit Manipulation(3*3 array)

Input : Stego cover image in binary form

Output : Secret message data (bits)

While not end of input file

{

1- Read block from input file

2- If block = $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ **put 0 in output file**

Else if block = $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ **put 0 in output file**

Else if block = $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ **put 0 in output file**

Else if block = $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ **put 0 in output file**

Else if block = $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ **put 1 in output file**

Else if block = $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ **put 1 in output file**

Else if block = $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ **put 1 in output file**

Else if block = $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ **put 1 in output file**

Else

Read another block

} end while

Convert Binary Secret Message into Secret Message Characters

At this technique every eight bits of binary secret message are converted into a character. These characters are the original secret message and will be continue with anther images to extract the remaining secret message.

Results

Result are taken with animation for small movement. Therefore, only three sample frames are

considered. The proposed model is implemented using Visual Basic (Version 6.0) language compatible

with XP Windows operating system. The sample frames of animation are shown in table (1):

Table (1) Test Samples of Cover Images			
Sample Name	**Size (KB)**	**Dimension**	**Attributes**
Sample1.bmp	**5.95**	**316×150**	**1-bit Binary**
Sample2.bmp	**5.95**	**316×150**	**1-bit Binary**
Sample3.bmp	**5.95**	**316×150**	**1-bit Binary**

The test secret message samples are shown in table (2).

Table (2) Test Secret Message Sample	
Sample Name	**Secret Message**
Secret1	**(bur1$/8%)**
Secret2	**(@99BUR)**
Secret3	**(Bu8#)**

The comparison between original image stego image with embedded and extracted secret message of the proposed model is shown in figure (5). At figure (5) the sample of cover images are (sample1&sample2&sample3) (described at table (1)), and the embedded secret Messages are (secret1&secret2&secret3) (described at table (2)) respectively. In the figure (5)

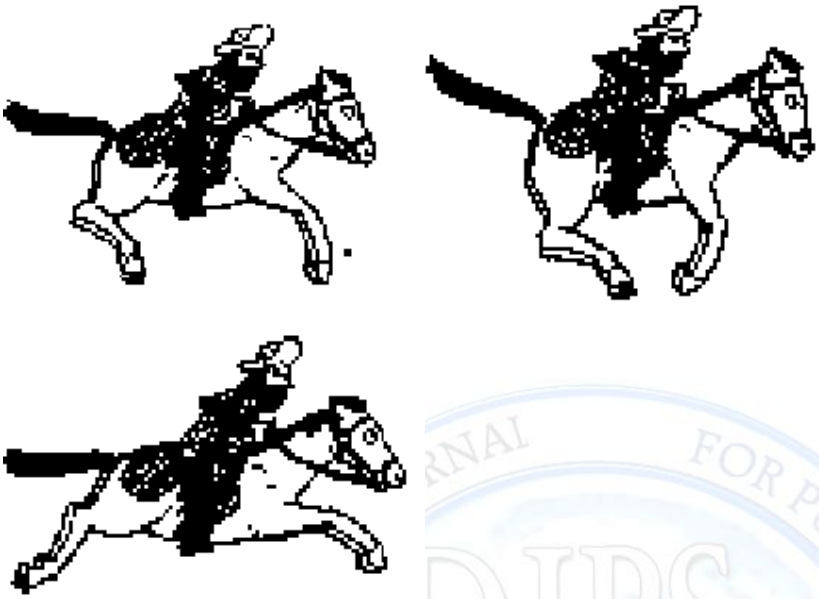
the process embedded of secret massage bits in the selected blocks of cover images blocks is in order (sequence) not spread spectrum. But in the figure (6) the embedding is not order (not sequence) spread spectrum depending on equation No(1).

(No. of blocks jump= no. of selected blocks / No. of secret massage bits) ……equation(1).

For example if you have binary image and after do process, there are 200 blocks selected from this image to hide data in it, and the number of secret massage bits is 21(three character) then by using equation No(1):the number of block jump =trunk (200/21)= 9.

(a)

Original Image (Sample1&Sample2&sample3)



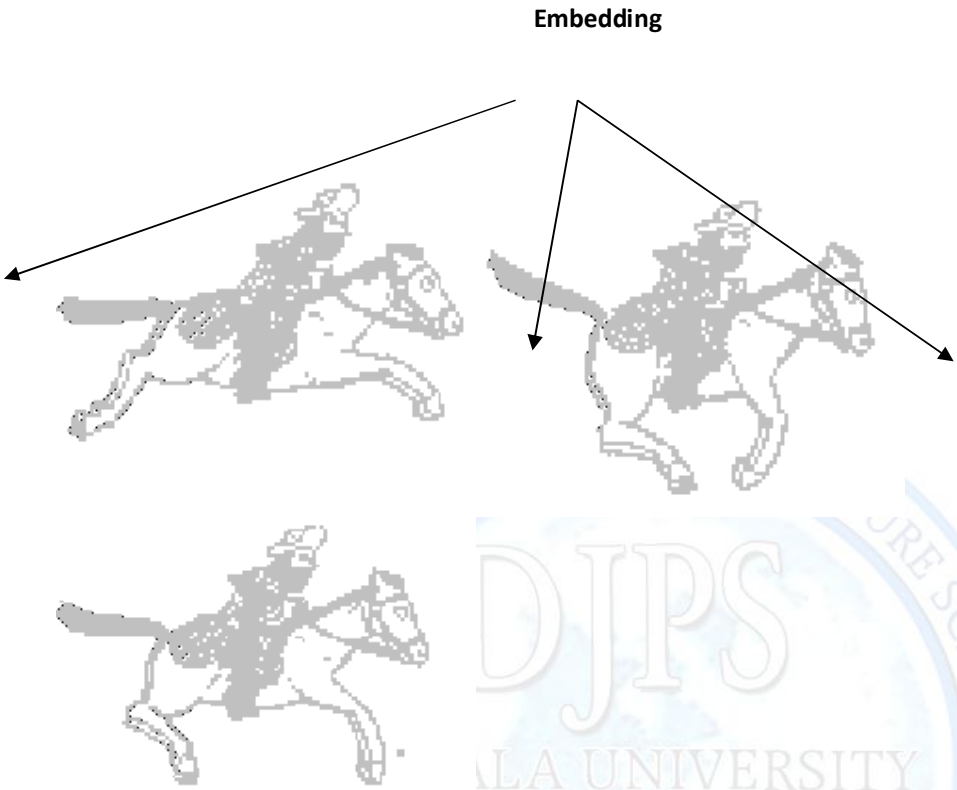
(b)

Stego Image of(Sample1&Sample2&sample3)

bur1$/8%	@99BUR	BU8#

(c)

Embedded and Extract Secret Message (Secret1&Secret2&Secret3)



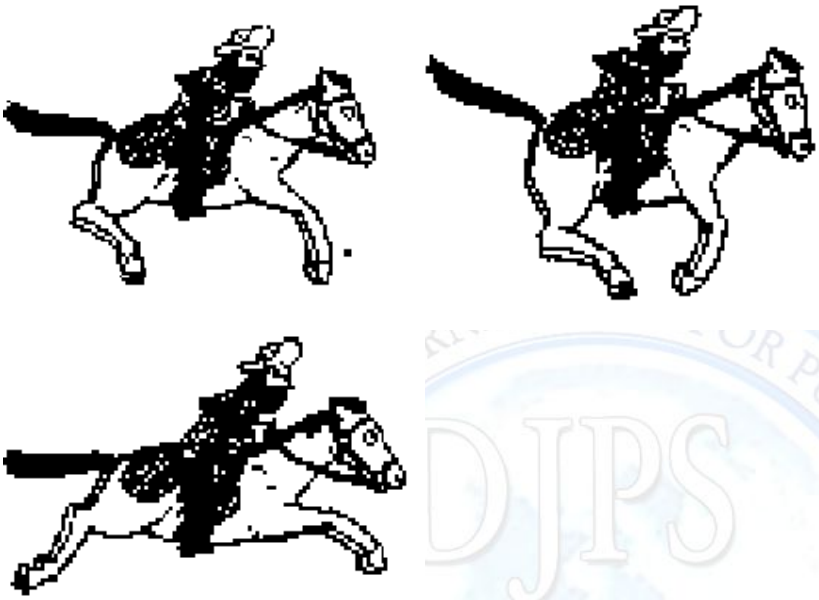
(d)

Embedding positions.

Figure (5) Proposed Model Comparison between (a) Original Image and (b) Stego Image with (c) The Embedding and Extracted Secret Message

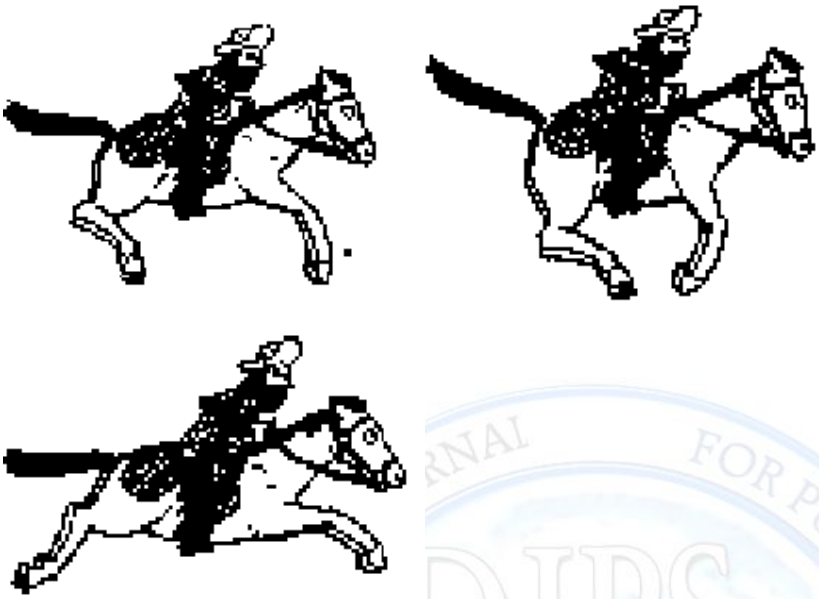
(d)Embedding Positions

Figure (6) shows the embedded the secret messages inside binary cover sample frames using equation No(1).



(a)

Original Image (Sample1&Sample2&sample3)



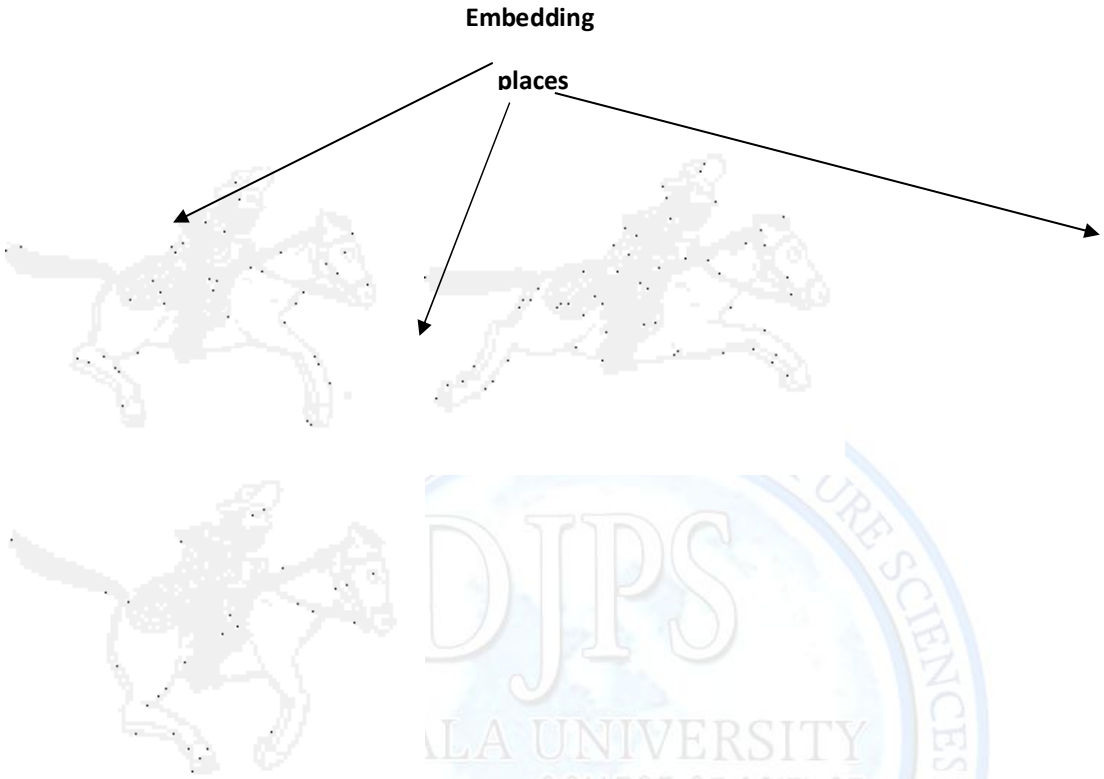
(b)

Stego Image of(Sample1&Sample2&sample3)

bur1$/8%	@99BUR	BU8#

(c)

Embedded and Extract Secret Message (Secret1&Secret2&Secret3)



(d)

Embedding positions

Figure (6) Proposed Model Comparison between (a) Original Image and (b) Stego Image with (c) The Embedding and Extracted Secret Message (d)Embedding Positions.

The calculated results of the proposed model are shown at table (3).

Samples	Secret Message	PSNR	MSE
Sample 1	Secret 1	31.75	43.02
Sample 2	Secret 2	32.27	38.18
Sample 3	Secret 3	34.23	24.30

Conclusions

The results have shown that the proposed model may successfully be used as a steganography system with following points to be discussed:

1- Animation can be used as a cover media for steganography.

2-Binary image are much harder than monochrome or color image in hiding techniques processing, because no much choices are allowed in binary image (the pixels 0 or 1).

3-The hiding bandwidth is limited in the proposed model.

4-The idea of hiding technique in proposed model depends on 3*3-bits block (window). The choice of 3*3-bits is used in order to reduce the number of probabilities in algorithms (1 and 2). These probabilities are shown in figures (2 and 4).

5-The idea of algorithms (1 and 2) and figures (2 and 4) is that adding boundary black pixel to group of black pixels has no effect, and deleting boundary black pixel from group of

black pixels has no effect on human visual system.

6-Using spread spectrum embedding as shown in figure(6) increases the security level.

7-The implementation of proposed model showed that there important factors must be taken in consideration such as:

a. Type of sample frame.

b. Size of secret data.

c. Block (window) size.

References

1. Ahmed Al-Jaber and Khair Eddin Sabri, "Data Hiding In A Binary Image", www.cas.mcmaster.ca/~sabrike/wp-content/uploads/2008/.../mcms2003.pdf, Department of Computer Science, King Abdullah II School for Information Technology (KASIT), University of Jordan.
2. Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Department of Information Systems, Al-albayt University , Mafraq, Jordan, march 2012.
3. Katzenbeisser S. and Petitcolas F. "Information Hiding Techniques For Steganography and Digital Watermarking", Artech House, USA, 2000.
4. Gopalakrishna Reddy Tadiparthi and Toshiyuki Sueyoshi, "StegAnim-A Novel Information Hiding Technique using Animations", Engineering Letters , November 2006
5. aMin Wu , bJessica Fridrich, bMiroslav Goljan, and aHongmei Gou "Handling Uneven Embedding Capacity in Binary Images",http://ws2.binghamton.edu / fridrich/ Research/ EI5681-20_WuFri.pdf, aECE Department, University of Maryland, College Park, USA, b ECE Department, SUNY Binghamton, Binghamton, USA,2005.
6. I. Cox, J. Kilian, T. Leighton, T. Shamoon: "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transaction on Image Processing, vol.6, no.12, pp. 1673–1687, 1997.