Development of Binary Image Steganographic Model

By
Ziyad Tariq Al-Ta’i, Abd-Al Basset Kadhim, and Burhan Molan S.
(Diyala University\College of Sciences\ Computer Science Dep.)

Abstract

An increasingly large number of digital binary images have been used in everyday life, such as handwriting signatures captured by electronic signing pads. To prevent unauthorized used of these signatures, this paper presents a simple model for binary image steganography. But, for binary images in which the pixel take on only a limited number of values, hiding data without causing visible artifacts becomes more difficult. However, this model hides secret (signature) message data inside binary cover signature image, 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. Robustness tests have been applied to the proposed model according to test methodology.

الخلاصة

لقد أصبح عدد الصور الرقمية الثنائية يتزايد في استعمالات الحياة اليومية كالتواقيع المكتوبة يدويا والموقعة الكترونيا. ولكي نمنع الاستخدام المزيف لهذه التواقيع فان هذا البحث يقدم نموذج بسيط للإخفاء للصورة الثنائية. ولكن أخفاء البيانات داخل الصور الثنائية التي تأخذ عناصرها قيم محددة يصبح صعبا بدون ظهور عيوب. لذا يقدم هذا البحث نموذج يقوم بإخفاء بيانات التوقيع السري داخل الصورة الثنائية لتوقيع الغطاء بالاعتماد على تقنية التعامل مع بتات الحدود. وقد تم بنجاح تقييم النموذج المقترح من خلال المحاكاة بالحاسوب وتم تقديم النتائج كما ونوعا. وتم تطبيق اختبارات قوة البقاء على النموذج المقترح وفقا لمنهجية اختبار

Key words:

Electronic Signature, Binary Image, Binary Image Steganography, Boundary Bits Manipulation Technique.

1. Introduction

As digital media are getting wider popularity, their security related issues are becoming a greater concern; one central issue is confidentiality, which is typically achieved by encryption. However, as an encrypted message usually flags the importance of the message, it also attracts cryptanalysts interests [1].

Steganography is the art and science of communication in a way which hides the existence of the communication. Steganography has a different flavor from encryption, its purpose is to embed a piece of critical information in a non–critical host message (e.g., WebPages, advertisements, etc.) to distract opponent's attention. One less confusing name for Steganography would be data hiding. It should be understood that steganography is orthogonal to encryption, and it may be combined with encryption to achieve a higher level of security [1].

The goal of a secure steganographic method is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data. The two necessary conditions of secure steganography are [2]:

1- Key remains unknown to attacker.
2- The attacker does not know the actual cover.

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].

An increasingly large number of digital binary images have been used in everyday life. Handwriting signatures captured by electronic signing pads are digitally stored and are being used as the records for credit card payment by many department stores. Word processing software like Microsoft Word allows a user to store his/her signature in a binary image file for inclusion at specified locations of a document. The documents signed in such a way can be sending directly to a fax machine or be distributed across a network [4].

The unauthorized used of a signature, such as copying it onto an unauthorized payment, is becoming a big concern. In addition a variety of important documents, such as social security records, insurance information, and financial documents, have also been digitized and stored. Because it is easy to copy and edit digital images via software tools, the annotation and authentication of binary images as well as the detection of tempering are very important.

Most prior works on image data hiding are for color or grayscale images in which the pixels may take on a wide range of values. For those images, changing pixel values by a small a mount is generally unnoticeable under normal viewing conditions. This property of human visual system plays a key role in watermarking of perceptual media data [5]. For images in which the pixel take on only a limited number of values hiding data without causing visible artifacts becomes more difficult.

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].

2. Proposed Model: Simple Model for Binary Image Steganography

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

2.1 Hiding (Embedding) Side

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

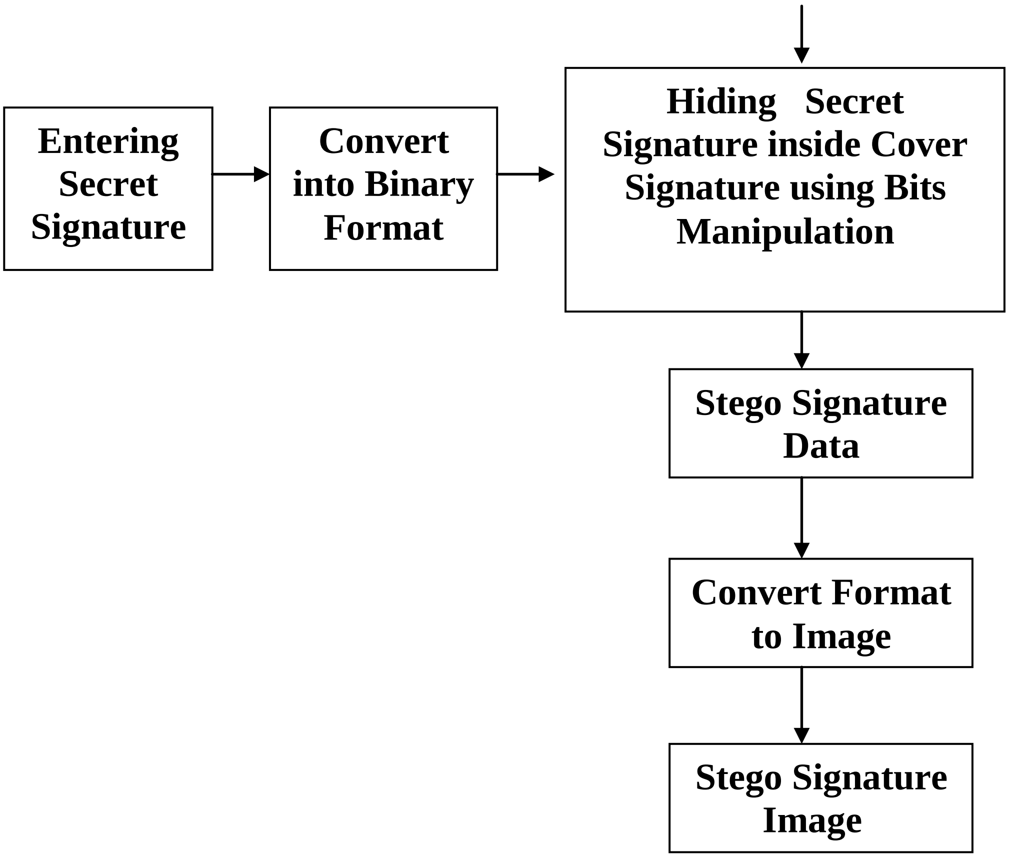

Entering Secret Signature
Convert into Binary Format
Hiding Secret Signature inside Cover Signature using Bits Manipulation
Stego Signature Data
Convert Format to Image
Stego Signature Image

Figure (1) Block Diagram of Hiding Side for Simple Binary Image Steganography Model

2.1.1 Entering and Converting Secret Signature into Binary Form

The secret signature is a group of characters and decimal numbers. At this process secret signature is entered to the model with size not more than the cover signature size. The secret signature can be converted to binary form file by considering each character consists of eight bits. Then taking the ASCII value for this character. After that, divide the ASCII value by two with neglecting the fractions after decimal point. If the result before neglecting the fractions equals the result after it, then the binary value is zero, otherwise the binary value is one. This procedure can be better clarified in algorithm (1).

Algorithm (1) Converting Secret Signature into Binary Form File

```
Input: Secret signature (group of letters and decimal numbers)
Output : Binary form file
   while not end of secret signature
   {
    1- Read a character
   for ( 1→8 ) Do
   {
   2- Gets ASCII value of character
   3- Divide ASCII  value by 2
   4- Take the integer value of step 3
   5- If (result of step 3 = result of step 4)
```

Algorithm (1) Continued

```
         Binary value = 0
       else
         Binary value  = 1
   6- Put ASCII  value = result of  step 4
   7-  Put binary value at output file
   } end for
   } end while
```

2.1.2 Hiding (Embedding) Secret Signature inside Cover Signature Image using Boundary Bits Manipulation

The idea of this technique is bits manipulation. A window (block of 3-bits) is taken from hiding cover signature file, with each bit of secret signature. The process of hiding is shown in figure (2), in which all probabilities ($2^3 = 8$) are covered.

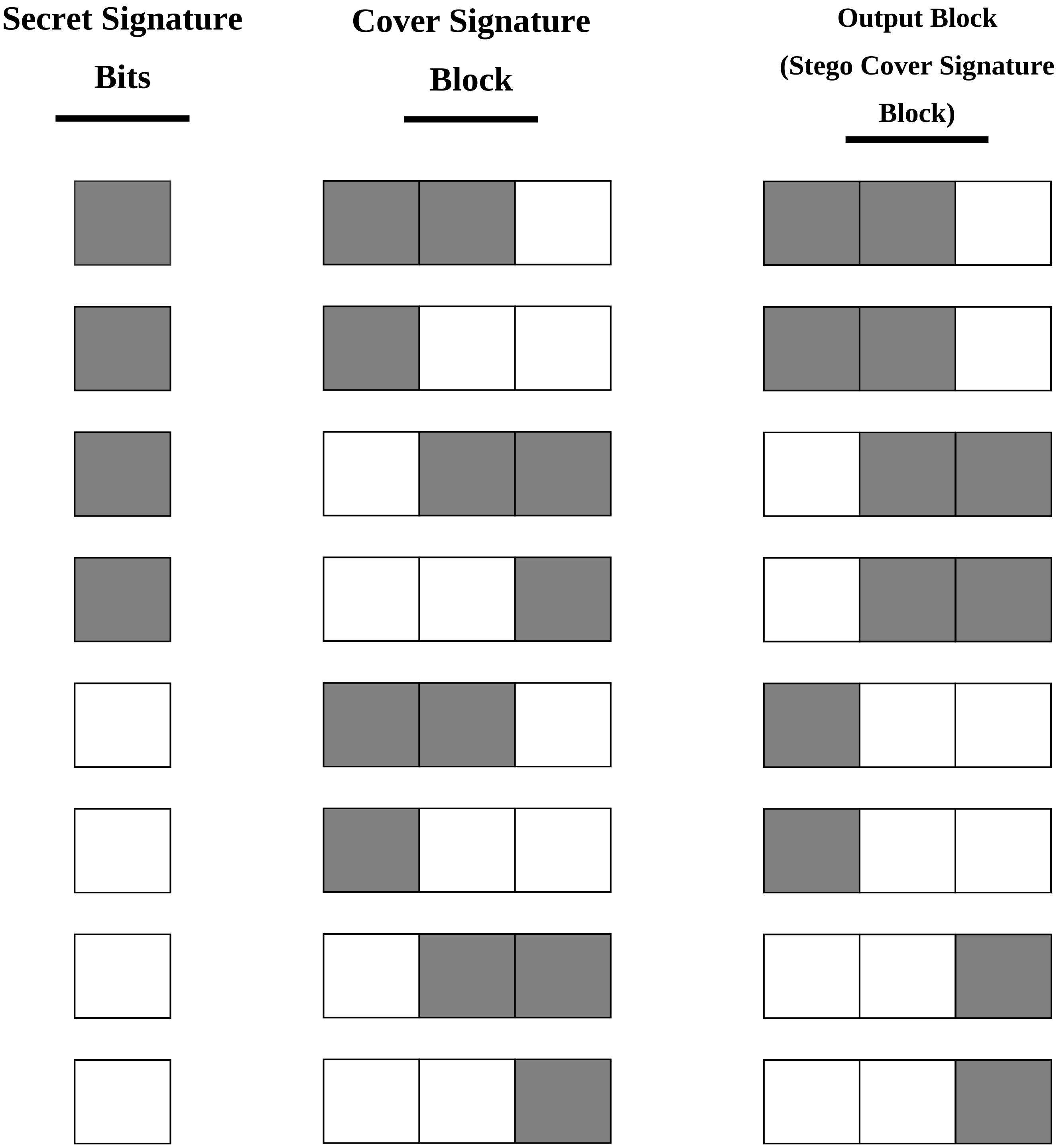


Figure (2) The Idea of Hiding (Embedding) Technique Using 3-Boundary Bits Manipulation. Black Represent 0 and White Represent 1

The secret signature bits and cover signature block are compared, new blocks are inserted at stego cover file depending on idea of figure (2).The secret signature bits and the blocks of cover signature blocks are remained with no change. This technique can be clarified at algorithm (2).

Algorithm (2) Hiding (Embedding) Secret Signature Inside Cover Signature Image using Boundary Bits Manipulation

```
Input  : 1- Binary cover image file
            2- Binary secret signature file
Output : Stego signature data file
  While not end of (input file (1))
  {
   While not end of (input file (2))
  {
  1- Read  block from input file  (1)
  2- While (block = 000   or    010   or   101   or   111)
    {
    Read another block  from input file (1)
     }
    1-  Read bit from input file (2)
    2-  If  bit = 0  and block=001
         Put block = 001   at output file
         If  bit = 0 and block = 011
```

Algorithm (2) Continued

```
      Put block = 001 at output file
      If bit = 0  and block = 100
      Put block = 100 at output file
      If bit = 0 and block = 110
      Put block = 100 at out put file
      If bit = 1 and block = 001
      Put block = 011 at output file
      If bit = 1 and block  = 011
      Put block = 011 at output file
      If  bit = 1  and  block = 100
      Put  block = 110   at output file
      If  bit = 1  and  block = 110
      Put block = 110   at output file
  } end while
 3-  Read block from input file (1)
 4-  Put block at output file
 } end while
```

2.1.3 Convert Stego Cover Data into Image Format

It is technique of concatenating image header with (stego image data after conversion into characters). This process can be shown in algorithm (3).

Algorithm (3) Convert Stego Signature Data into Image Format

```
Input : Stego signature image data file
 Output : Stego signature image
     1-  Concatenate header bytes at beginning of output file
     while not end of input file
      {
     2- Read a datum from input file.
     3-Convert a datum into a characters
     6- Put the character at output file
      } end while
```

2.2 Extracting side

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

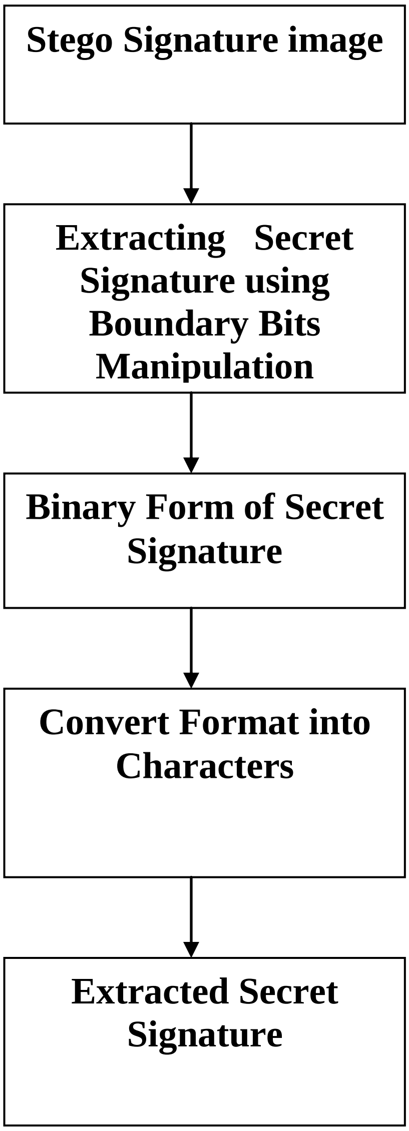

Stego Signature image
Extracting Secret Signature using Boundary Bits Manipulation
Binary Form of Secret Signature
Convert Format into Characters
Extracted Secret Signature

Figure (3) Block Diagram of Extracting Side for Simple Binary Image Steganography Model

2.2.1 Extracting Secret Signature using Boundary Bits Manipulation

The idea of this technique depends on number of zeros and number of ones in each block. A window (block of 3–bits) is taken from stego cover signature file. If the number of contiguous zeros in block is even, then put zero in output file (secret signature data file). If the number of contiguous ones in block is even then put one in output file. The process of extracting is show in figure (4).

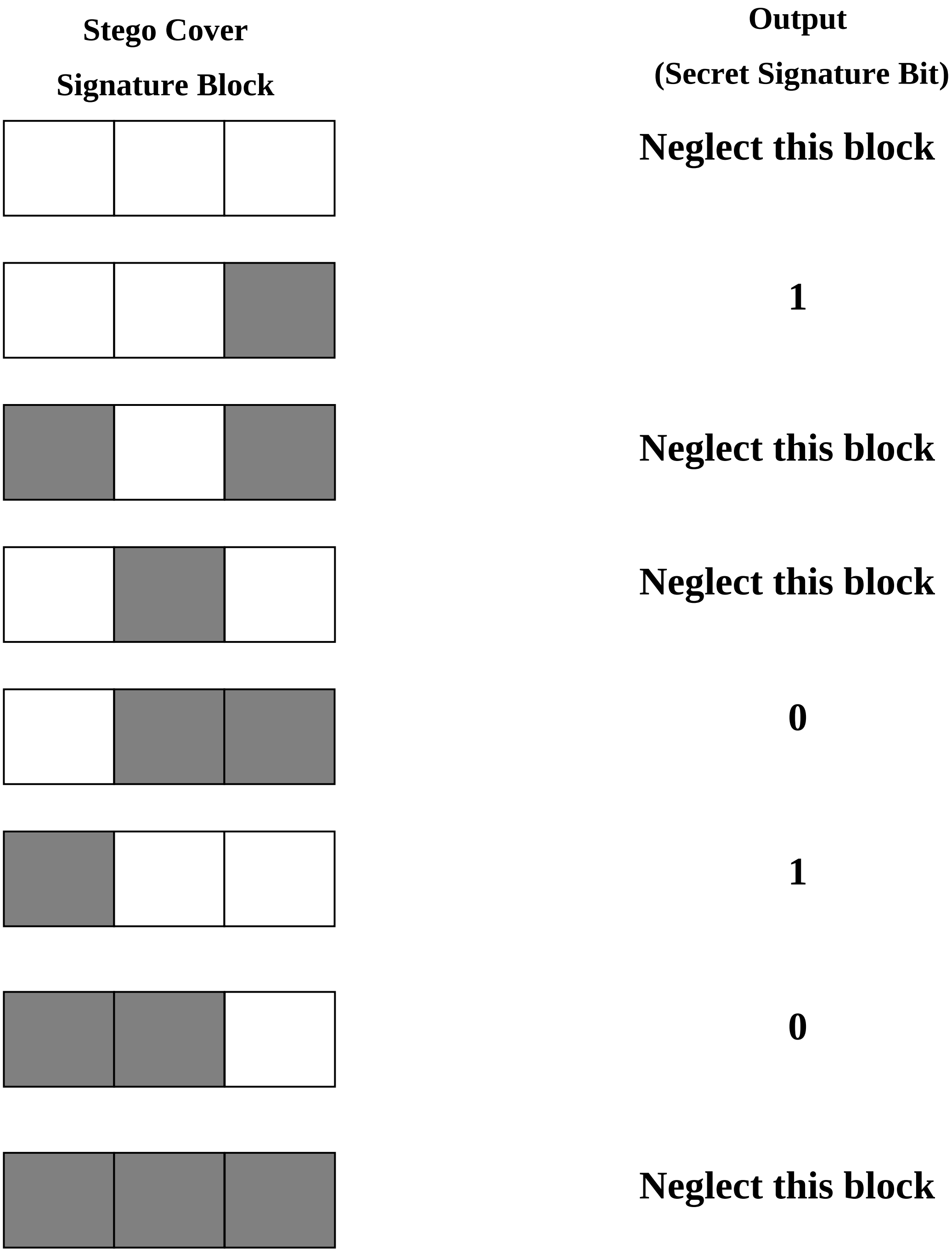


Figure (4) The Idea of Extracting Technique Using 3-Bit Manipulation. Black Represents 0 and White Represents 1.

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

Algorithm (4) Extracting Secret Signature Data Using Boundary Bit Manipulation

```
Input : Stego cover signature in binary form
Output : Secret  Signature data (bits)
 While not end of input file
  {
   1-  Read  block from input file
   2-  While ( block = 000   or  010   or    101   or  111)
       {
       Read  another block from input file
        }
   3- While ( block  = 001  or  100  or   011  or  110 )
        {
          count  number of 0 and 1's
        }
   4-If  number of  zeros in block is even
                   put    0  in output file
   5-If  number of   ones in block is even
                    put   1  in output file
    } end while
```

2.2.2 Convert Binary Secret Signature into Secret Signature Characters

At this technique every eight bits of binary secret signature are converted into a character. These characters are the original secret signature. This process can be clarified in detail by algorithm (5).

Algorithm (5) Converting Binary Secret Signature Into Secret Signature Characters

```
Input : Binary secret signature file
Output: Secret signature characters (Original secret signature)
 While not of input file
   {
   1- Read ( 8 ) bits  of input file
    2- Value = $\text{first bit} \times 128 + \text{second bit} \times 64 + \text{third bit} \times 32 + \text{fourth bit} \times 16 + \text{fifth bit} \times 8 + \text{sixth bit} \times 4 + \text{seventh bit} \times 2 + \text{eighth bit}$

    3- Signature character = ASCII of ( value in step2 )
    4- Put  signature character at secret signature output file
    } end while
```

3- Results:

The test samples of cover signature images are shown in table (1):

Table (1) Test Samples of Cover Signature Images

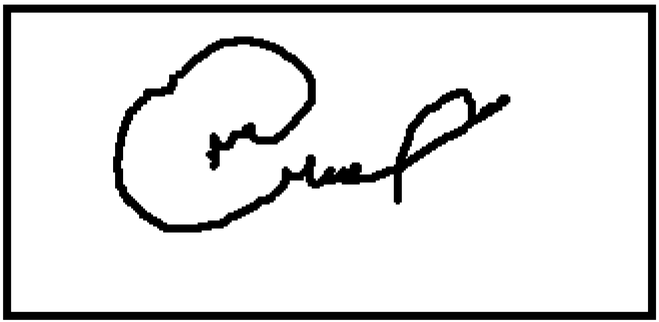
Sample Name	Size (KB)	Dimension	Attributes
Sample5.bmp	5.95	316×150	1-bit Binary
Sample7.bmp	139.8	316×151	1-bit Binary

The test secret signature samples are shown in table (2):

Table (2) Test Secret Signature Sample

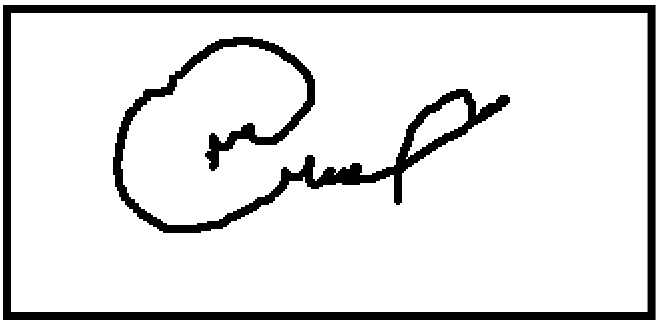
Sample Name	Signature
Secret5	(50!10H)
Secret6	(ac90/bmn33)

The comparison between original signature image stego signature image with embedded and extracted secret signature of the proposed model is shown in figure (5). At figure (5) the sample of cover signature image is (sample5.bmp) (described at table (1)), and the embedded secret signature is secret5 (described at table (2)).



(a)

Original Signature Image (Sample5.bmp)



(b)

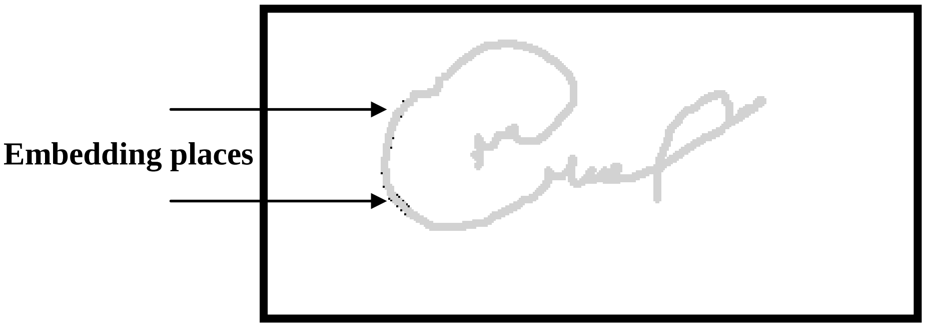
Stego Signature Image

50!10H

(c)

Embedded and Extract Secret Signature (Secret5)

Figure (5) Continued



(d)

Embedding positions

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

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

Table (3) Calculated Results of the Proposed Model

Model Type	$e$rms %	SNR$_{ms(dB)}$	Time (sec) Required for Embedding	Time (sec) Required for Extracting
Simple Model for Binary Image Steganography	0.0034	47.107	0.54	0.45

4. Tests

Johnson et al. [7] revealed that for each steganography and watermarking tool, a series of test were conducted to determine weather the hidden information could be detected and recovered.

The following tests are done in order to measure the survivability of this work.

4.1 Conversion Test

Using the proposed model with 1-bit test sample (described at table (1) and different secret signatures (described at table (2)), the stegocover signature is converted from 1-bit to 8-bit or 24-bit image. The embedded secret signature has not been detected, and it could be recovered.

4.2 Processing Test

Using the proposed model with different secret signature (described at table (2)), the stego cover is compressed using (ACDsee software) and then decompressed. The embedded secret signature has not been detected, but it could not be recovered.

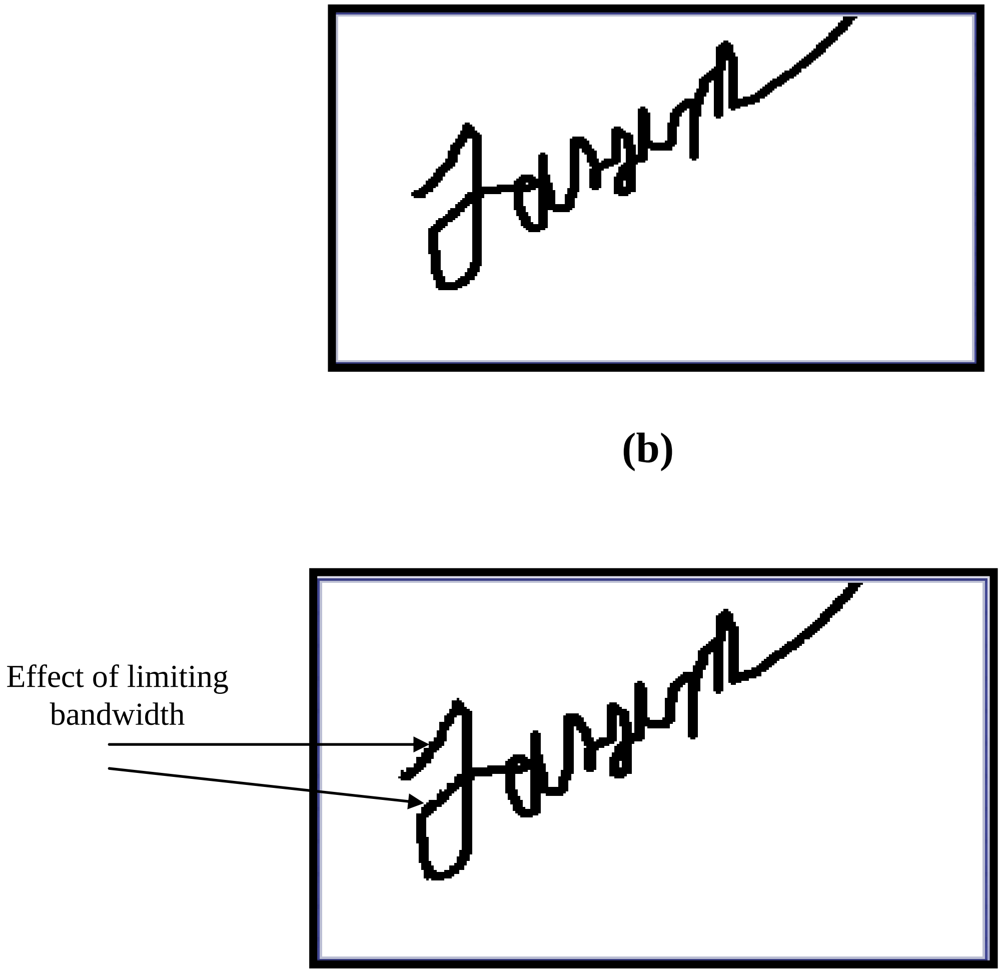
5. Conclusions

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

1- The hiding bandwidth is limited in the proposed model, as shown in figure (6).

ac90/bmn33

(a)



(b)

(c)

Figure (6) the effect of Hiding Bandwidth (a) Secret Signature (b)Original Cover Signature Sample (7) (c) Stego Cover with the Proposed Model

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

3- The idea of algorithms (2 and 4) 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.

4- The tests have been revealed that the survivability of secret signature is poor.

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

   a. Type of cover signature image.
   b. Size of secret signature.
   c. Block (window) size.
   d. The position of changing black pixel.

References

1. **Yu–Chee Tseng and Hsiang-Kuang Pan,"Secure and Invisible Data Hidingin 2–Color Image", Internet survey, http://citeseer.ist.psu.edu/chen00secure.html, 2000.**
2. **Fabien A. Petitcolas, R.J. Anderson , and M.G. Kuhn ," Information Hiding–a survey", proc. IEEE, vol.87, pp.1062–1078, July 1999.**
3. **Katzenbeisser S. and Petitcolas F. "Information Hiding Techniques For Steganography and Digital Watermarking", Artech House, USA, 2000.**

4. **Min wu, " Multimedia data hiding ", Thesis for the Degree of Doctor of philosophy, Dep. Of Electrical Engineering, University of Princeton, 2001.**
5. **C. Podilchuk, W. Zeng: "Image Adaptive Watermarking Using**

   Visual Models", IEEE Journal Selected Areas of Communications (JSAC), vol.16, no.4, May,1998.
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.**
7. **Johnson F. Neil, Zoran Duric, and Sushil Jajodia, "Information Hiding: Steganography and Watermarking–Attacks and Countermeasures", Book from Kluwer Academic Publishers 2001.**