Signature Steganography

Thahir Abd-Alhadi, Ziyad Tariq Mustafa
College of Science, Diyala University, Diyala, Iraq.
(**Received:** 15 / 2 / 2010 ---- **Accepted:** 17 / 5 / 2010)

Abstract
Handwriting signatures captured electronic signing pads are getting wider popularity. The unauthorized used of a signature, such as copying it into an unauthorized payment, is becoming a big concern. Therefore, this paper presents data hiding model as an alternative to the cryptographic authentication approach. This model hides secret signature data inside monochrome cover signature image, depending on gray scale levels of pixel values. 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.
Key words: Electronic Signature, Gray scales Image Hiding, Steganography, and Watermarking.

Introduction
Every few years, computer security has to re-invent itself. New technologies and applications bring new threats, and force us to invent new protection mechanisms. Cryptography became important when started to build networked computer systems. At the same time, moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private message can be embedded in innocuous cover messages. One of the hot spots in security research is information hiding .

An increasingly large number of digital 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. And for parcel delivery by major courier services such as the United Parcel Service (UPS). Word processing software like Microsoft Word allows a user to store his/her signature in an 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 .

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 images as well as the detection of tempering are very important. While the embedded data expected to have some robustness against minor distortion and preferably to withstand printing and scanning, the robustness of embedded data intentional removal or other obliteration is not primary concern because there is little incentive to do, so in the targeted application of annotation and authentication .

Information hiding represents a class of processes used to embed data into various forms of media such as image, audio, or text. The embedded data should be invisible to a human observer . However, Provos reported that information hiding process extracts redundant bits from the cover medium. Redundant bits are those bits that can be modified without destroying the integrity of the cover medium. The embedding process then selects the bits that will be replaced with data from the hiding message.

Johnson et al. showed that there are many different methods for hiding information in images. These methods may include hiding information in unused space in file headers to hold extra information. Embedding techniques can range from the placement of information in imperceptible levels (noise), manipulation of compression algorithms, to the modification of carrier properties such as luminance, contrast, or colors(this is depend on type of image).

Proposed Model:
This model is divided into two stages: hiding side and extracting side signature in signature using monochrome images.

Hiding (Embedding) Side:
The block diagram of hiding side of this model is shown in figure (1).

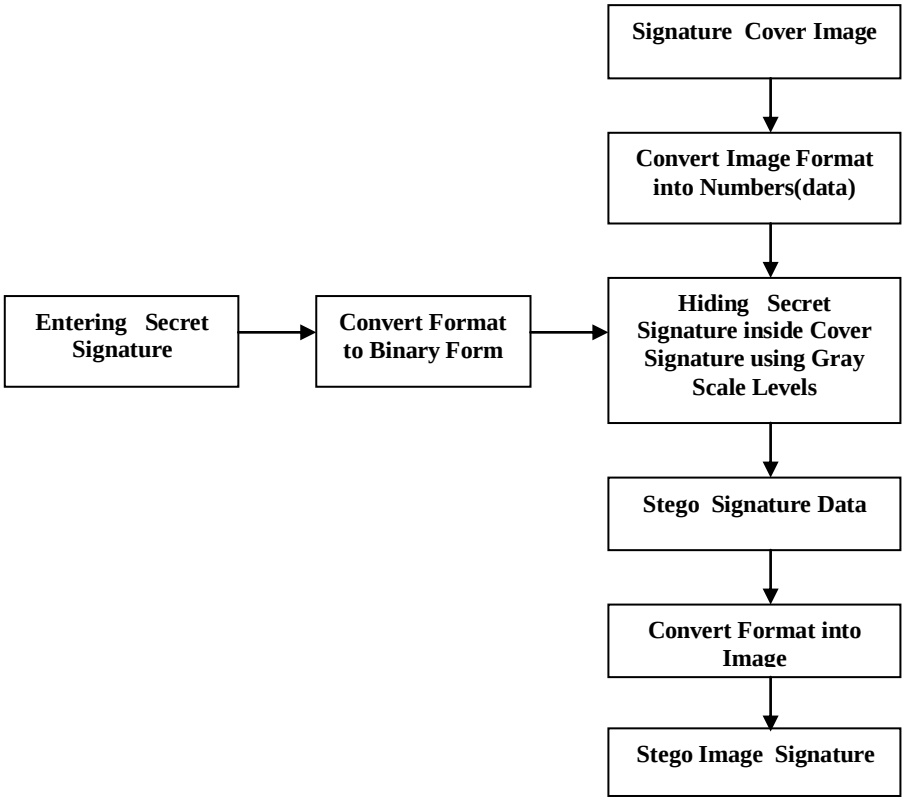


Figure (1) Block Diagram of Hiding Side for the Proposed Model

Convert Cover Signature Image Format into Numbers:

This is a first process in hiding side. The monochrome image consists of header and body (stream of characters). The values of these characters are (0–255 in decimal) according to (8–bit digital representation). A file of stream numbers can be obtained by separating the header and converting characters to decimal numbers. This file can easily be processed. This process can be described by algorithm (1).

Algorithm (1) Convert Cover Signature Image Format into Stream of Numbers
Input : Cover signature image file with BMP format
Output : Stream of numbers file
1- Skip header bytes
While not end of input file
{
2- Read a byte value
3- Convert byte value to decimal value
4- Put decimal value into output file
} End while

Entering and Converting Secret Signature into Binary Form:

This is a second process in hiding side. 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 the ASCII value for this character is taken. 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 (2).

Algorithm (2) 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)
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

Hiding (Embedding) Secret Signature inside Cover Signature Image using Gray Scale Levels:
This is a third process in hiding side of this model. The idea of hiding is depended on levels of colors between black (0) and white (255) with correspondence to 8–bit representation for each pixel. Specifically, hiding is done in black pixels depending on secret signature bits. The output of this process is stego signature data. This procedure can be better described at algorithm (3).

Algorithm (3) Hiding Secret Signature Inside Cover Signature Image depending on Gray Scale Levels
Input : 1- stream of numbers file for cover signature image
2- Binary form file for secret signature
Output : stego signature data file
While not end of input file (1)
{
While not end of input file (2)
{
1- Read a number from input file (1)
2- If number ≠ 0
{
3- Put the read number in output file
4- Read another number from input file (1)
} end if
else {
5- Read a bit from input file (2)
If bit = 0
{ Put number = 2 }
else { number = 3 }
6- Put number(2 or 3) in output file
}end else
} end while
7- Read number from input file (1)
8- Put the read number in output file
} end while

2.1.4 Convert Stego Signature Data into Image Format:
This is a last process in hiding side of this model. It is the reverse process of the technique (2.1.1). It is technique of concatenating image header with (stego image data after conversion into characters). This process can be shown in algorithm (4).

Algorithm (4) 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
4-Put the character at output file
} end while

Extracting side:

Extracting side of this model is shown in figure (2).

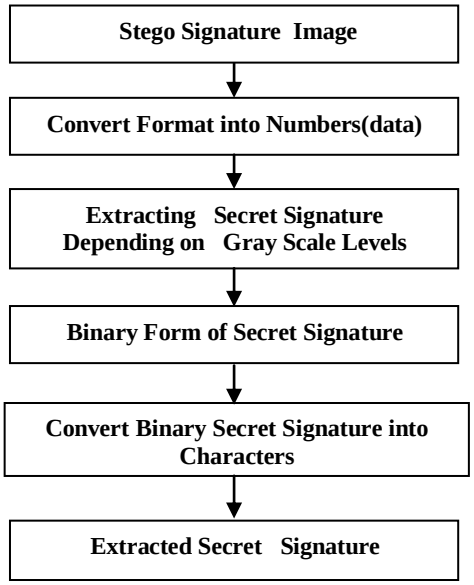


Figure (2) Block Diagram of Extracting Side for the Proposed Model

Convert Stego Signature Image into Numbers:
This is a first process in extracting side of this model. This technique is exactly similar to the process of technique (2.1.1).
Extracting Secret Signature Depending on Gray Scale Levels:
This is a second process in extracting side of this model. This technique is depending on values of stego signature numbers. The output of this process is a binary form file of secret signature. This technique can be described by algorithm (5).

Algorithm (5) Extracting Secret Signature Depending on Gray Scale Levels
Input : stego signature image numbers file
Output : Binary form of secret signature file
while not end of input file
{
1- Read number from input file
2- If number = 2
{
3- Put binary 0 at output file }
4- else If number = 3
{
5- Put binary 1 at out put file
}
} end while

Convert Binary Secret Signature into Secret Signature Characters:
This is a third process in extracting side of this model. 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 (6).

Algorithm (6) 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 = first bit × 128 + second bit × 64 + third bit × 32 + fourth bit × 16 + fifth bit × 8 + sixth bit × 4 + seventh bit × 2 + 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
Sample1.bmp	21.2	178×115	8-bit Monochrome
Sample2.bmp	152	596×260	8-bit Monochrome

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

Table (2) Test Secret Signature Sample

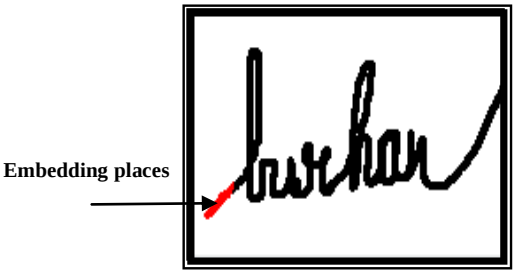
Sample Name	Signature
Secret1	(cbamoz)
Secret2	(ahmed)

The comparison between original signature image and stego signature image with embedded and extracted secret signature of proposed model is shown in figure (3) and figure (4). At figure (3) the sample of cover signature image is (sample1.bmp) described at table (1), and the embedded secret signature is secret1 (described at table (2)). At figure (4) the sample of cover signature image is (sample2.bmp) (described at table (1)) and the embedded secret signature is secret2 (described in table (2)).

(a) Original Signature Image (Sample1.bmp)

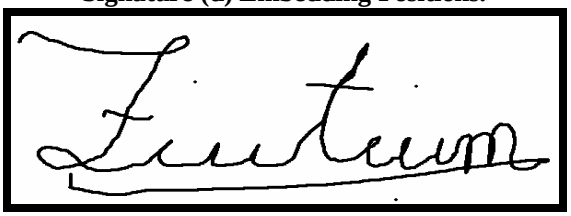
(b) Stego Signature Image

(c) Embedded and Extracted Secret Signature (Secret1)

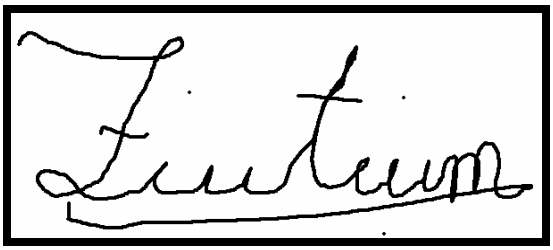


(d) Embedding Positions

Figure (3) Proposed Model Comparison between (a) Original Signature Image (b) Stego Signature Image (c) The Embedded and Extracted Secret Signature (d) Embedding Positions.



(a) Original Signature Image (Sample2.bmp)



(b) **Stego Signature Image**

(c) Embedded and Extracted Secret Signature (Secret2)

(d) Embedding Positions

Figure (4) Proposed Model Comparison between (a) Original Signature Image (b) Stego Signature Image (c)The Embedded and Extracted Secret Signature (d)Embedding Positions.

The results for proposed model are shown in table (3).

Table (3) Results for Proposed Model

erms %	$SNR_{ms(dB)}$	Time (sec) Required for Embedding	Time (sec) Required for Extracting
0.0061	41.968	2.94	0.55

Tests:

Johnson et al. [6] 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 the proposed model.

Conversion Test:

Using proposed model with 8-bit test samples and different secret signatures, the stegocover signature is converted from 8-bit to 24-bit image. The embedded secret signature has not been detected, but it could not be recovered.

Processing Test:

Using proposed model with 8-bit test samples and different secret signature, the stegocover is compressed using (ACDsee software) and then decompressed. The embedded secret signature has not been detected, but it could not be recovered.

5. Conclusions

This work are specified the following below:

1- The proposed model is able to successfully hide secret signature inside monochrome cover signature subjectively as shown in figures (3 and 4), and quantitively as shown in table (3).
2- The tests have been revealed that the survivability of secret signature is poor.
3- 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 pixel value in model.

References

1. Katzenbeisser S. and Petitcolas F. **"Information Hiding Techniques For Steganography and Digital Watermarking"**, Artech House, USA, 2000.
2. Min wu , Bede liu, **"Data Hiding in Binary Image for Authentication And Annotation"**, Proc. IEEE, Transaction on Multimedia, Vol. 6 August 2004.
3. Min wu, **" Multimedia data hiding "**, Thesis for the Degree of Doctor of philosophy, Dep. Of Electrical Engineering, University of Princeton, 2001.
4. Stefan Katzenbeisser and Fabien A.B. Petitcolas, **"Information Hiding Techniques for Steganography and Digital Watermarking "**, Book from Artech House Inc., 2000.
5- Niels Provos, **" Probabilistic Method for Improving Information Hiding"**, Technical Report (01–1) from Center for Information Technology Integration (CITI). University of Michigan, USA, January 31, 2001.
6- Johnson F. Neil, Zoran Duric, and Sushil Jajodia, **"Information Hiding: Steganography and Watermarking–Attacks and Countermeasures"**, Book from Kluwer Academic Publishers 2001.

اخفاء التوقيع

ظاهر عبد الهادي عبد الله ، زياد طارق مصطفى

كلية العلوم ، جامعة ديالى ، ديالى ، العراق

(تاريخ الاستلام: 15 / 2 / 2010 ---- **تاريخ القبول:** 17 / 5 / 2010)

الملخص:

لقد أصبحت التواقيع المكتوبة يدويا والموقعة الكترونيا شائعة بكثرة. ولقد أصبح الاستخدام المزيف للتوقيع مثل استنساخ التوقيع لتسديد الأجور زيفا من الاهتمامات الكبيرة. ولهذا فان هذا البحث يقدم نموذج إخفاء البيانات كبديل لاتجاه موثوقية التشفير.

يقدم هذا البحث نموذج يقوم بإخفاء بيانات التوقيع السري داخل الصورة المتدرجة الألوان بين الأسود والأبيض لتوقيع الغطاء بالاعتماد على قيم المستويات الرمادية لعناصر الصورة. وقد تم الإخفاء بنجاح من خلال المحاكاة بالحاسوب وتم تقديم النتائج كما ونوعا. وتم تطبيق اختبارات قوة البقاء على النموذج المقترح وفقا لمنهجية اختبار.

الكلمات المفتاحية : التوقيع الالكتروني ،اخفاء الصورة ذات التدرج الرمادي ،اخفاء ، العلامة المائية .