Hide Information Using Plain Drawing

Nadia F. Kasto
Department of Computer Science, College of Science, University of Baghdad. Baghdad-Iraq.

Abstract

This paper presented the development and implementation of a steganographic method, the secret message is hidden in plain drawing (AutoCAD drawing) with vector coordinate used as stego cover. This paper focuses on trading a few least significant bits of original floating-point values and replacing them with a secret text. A secret text is implemented by transform each character in the text into numbers (using RSA algorithm), then stores it as part of floating-point numbers embedded with plain drawing. The main goal of steganography was fulfilled since changing plain drawing did not drown any suspicion; the same drawing can be used by experimental person and does not alter the original data content.

الخلاصة

الهدف من هذا البحث بناء نظام لإخفاء المعلومات في أماكن مختلفة لمخطط رسمي, تمثيل المخطط باستخدام (AutoCAD) الذي سوف يتم استخدامه كغطاء للإخفاء. تم الإخفاء بالاعتماد على تحويل النص التي يتكون منها النص المراد إخفائه إلى قيم الرقمية للأحرف باستخدام خوارزمية RSA وخزنها كجزء من الأرقام الكسرية للمخطط الرسمي. تم تطبيقه على مخططات مختلفة وقد تم تنفيذ هدف الإخفاء بنجاح حيث بالا مكان استخدام الجداول للحسابات بدون أي أخطاء في جانب التنفيذ. أذا لايوجد اثر يذكر للتغيرات المضافة على الحسابات .

Introduction

The word steganography comes from the Greek roots stego-, or steganos, and -graphy, and means "covered writing." It is the technique of hiding secret messages within other media, so that to all eyes but those of the sender and intended receiver, no secret message appears to be present [1]. A general steganography system is shown in figure (1), in this system there are a number of knowing terminology which are illustrated as follows [5]:-

- **Embedded <Data type>.** Something to be hidden in some thing else.
- **Cover <Data type>.** An input with an "original" form of the stego message. In some application, such cover message is given from the outside, in others, it can be chosen during the hiding process.
- **Stego key or simply key.** Additional secret data that may be needed in the hiding process. In particular, the same key is usually needed to extract the embedded message again.
- **Stego <Data type>.** The output of hiding process. Something that has the embedded message hidden in it.
- **Embedding process.** The process of hidden the embedded message is called embedded process.
- **Extracting process.** Getting the embedded message out of the stego message again is called extracting process.

Stegoanalysis, or attacks on steganographic "carriers" can also be broadly split into two

categories: discovery of the message, or destruction of a message may be the most desirable outcome, it is also the most difficult [6].

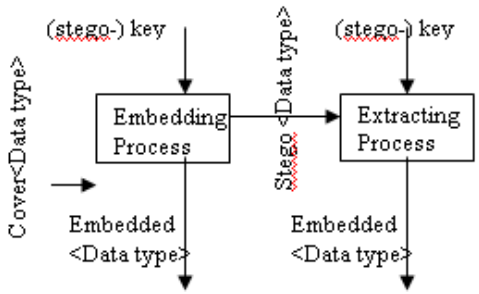
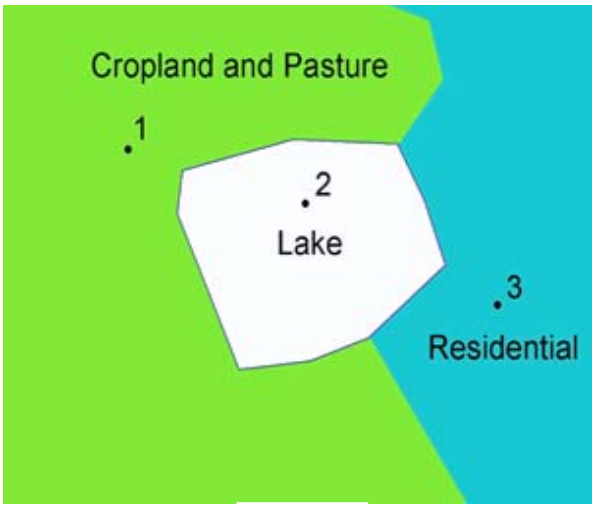


Figure (1):Steganography system (stego-system)

Steganography different from cryptography, Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message wills not [7]. There are plenty of ways to hide messages within images. This is relatively easy because an image arrays of colored dots [3]. Like BMP and JPEG, typically contains an enormous amount of redundant information's. This paper focuses on the more challenging problem of reliably hiding messages within vector data. Vector data use sequences of coordinates to represent points, lines, and regional boundaries on a plain [3, 9] used extensively by geographic information systems and AutoCAD drawing. Raster files can be manipulated quickly by the computer, but they are often less detailed and may be less visually appealing than vector data files, which can approximate the appearance of more traditional hand-drafted maps [9] (see figure 2A and 2B).

1	1	1	1	1	1	1	3	3	3
1	1	1	1	1	1	1	3	3	3
1	1	1	1	1	1	3	3	3	3
1	1	1	2	2	2	2	3	3	3
1	1	1	2	2	2	2	3	3	3
1	1	1	2	2	2	2	3	3	3
1	1	1	1	2	2	2	3	3	3
1	1	1	1	1	1	3	3	3	3
1	1	1	1	1	1	1	3	3	3
1	1	1	1	1	1	1	1	3	3

A



B

Figure (2): example of the structure of (A) raster file (B) vector data file

Therefore this paper combine cryptography with steganography, encrypted the secret message using of the RSA encryption method with public and private key, this is one of the most secure system which is known today, prior to the embedded process with plain drawing, such combination increases security of the overall communication process, as it is more difficult for an attracter to detect embedded cipher-text in a plain drawing.

The development method

The cover image used to hide the information in this research constructed on plain drawing using AutoCAD2002. AutoCAD is a computer aided design program (CAD) embedded with a

reach graphic environment created and supported by AutoDesk's company, AutoCAD provides native DWG compatibility primitives. Within its supporting embedded language the AutoLISP (programming languages that can be used to develop any compound or Meta design primitives). AutoCAD2002 software used to create a precision drawing of plain. This software allowed to create a dimensionally accurate scaled drawing with components, while AutoLISP routines quickly perform calculations and analysis of data used to generate drawing.

When using AutoCAD, the original data was always digitized to have only four decimal places; it is therefore natural to hide the message in the third and fourth floating point digits (**jittering**) without affecting the positional accuracy of the original data. So this paper deals with the problem of jittering, jittering means making tiny changes in vector coordinates of the plain drawing [3].

Assuming the message(viewed as a sequence of letters from an alphabet) we want to hide ,encoded it before send as a long string of digits (0 through 9), we would precede by biting off a two-digit chunk and simply sticking it into digits three and four of the fraction number. For example, if our message begins 30976... And the jitter number is 339.2784, then:

1. Bite off the beginning "30" of the message.
2. Take the fraction and wipe out the values in the third and fourth places: 339.27--.
3. Fill in the third and fourth places with "30": 339.2730.

In this example, jittering the value 339.2784 by "30" has changed it to 339.27830. To decode the message digits back from the jittered value is even easier: just inspect the third and fourth digits of the fraction: 339.27**30**. So by slicing the message into pieces and pack it into coordinates of points without effecting the positional accuracy of the original data at all.

RSA ALGORITHM

Cipher that uses two keys: one for encryption, the public key, and the other for decryption, the private key. As implied by the key names, the public key used to encode plaintext can be made available to anyone. However, the private key must remain secret, guaranteeing that only the person with the corresponding private key can decrypt the message [8]. The public key algorithm used in this paper is RSA algorithm. The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman,this is one of the most secure public key systems which is known today[4].

1- RSA Key Generation Algorithm

Bellow is a summary of the RSA [10]

1. n = pq where p and q are distinct primes.
2. phi = (p-1)(q-1)
3. e < n such that gcd(e, phi)=1
4. $d = e^{-1} \bmod phi$.
5. $c = m^{\wedge e} \bmod n$.
6. $m = c^{\wedge d} \bmod n$.

- m is positive integer m,n.(in this paper m is represent the ASCII of each characters)
- n is known as the modulus.
- e is known as the public exponent or encryption exponent,
- d is known as the private exponent or decryption exponent,
- Public key (n, e) Private Key (n, d).
- c is the ciphertext (see table1 RSA key generation and code) **.**

2- Encryption

Sender A does the following:-

1. Obtains the public key (n, e).
2. Represents the plaintext message as a positive integer m < n.
3. Computes the cipher text $c = m^{\wedge e} \bmod n$.
4. Sends the cipher text c to B.

3- Decryption

Recipient B does the following:-

1. Uses private key (n, d) to compute $m = c^{\wedge d} \bmod n$.
2. Extracts the plaintext from the integer representative m.
3. Convert integer m to characters

Table (1) : RSA key generation and code P=17 q=37 n=629 phi=576 e=5 d=461 **Note** Using block code for each character represented as three numbers,RSA algorithm is this paper work effenicieny with n>=99999.

character	ASCII number	RSA code
Space	32	427
"	34	238
$	36	406
.	46	**071**
A	65	114

Table (1): (Continued)

B	66	495
C	67	509
D	68	**068**
E	69	205
F	70	**049**
G	71	**090**
H	72	412
I	73	184
J	74	296
K	75	334
L	76	587
M	77	280
N	78	210
O	79	350
P	80	598
Q	81	268
R	82	**097**
S	83	478
T	84	322
U	85	323
V	86	562
W	87	627
X	88	362
Y	89	616
Z	90	218
a	97	156
b	98	557
c	99	437
d	100	121
e	101	492
f	102	595
g	103	273
h	104	287
i	105	549
j	106	242
k	107	456
l	108	534
m	109	079
n	110	332
o	111	518
p	112	482
q	113	180
r	114	428
s	115	506
t	116	165
u	117	376
v	118	305
w	119	578
x	120	256
y	121	100
z	122	175

Hiding the public key

The simplest form of hiding the public key, as proposed it in this paper is to use **embedding method**, embedding consists of using the distance between points to convey information. Usually it is accomplished by select any vertical or horizontal lines from drawing. Converted it to disconnection lines [3]. Convert the public key to sequence of bits (convert each number to 4 bits). Therefore disconnection lines will correspond to bits represent the public key, long length for a 1 , a short length for a 0, every message will be preceded by the reference length (encoding as 0), just get public key started. Decoding a hidden key allows for some slop in the relative length. Find the beginning of the message, t he first length is intercepted as a 0, subsequently, any large increase in the next line length is interpreted as a 1 and any large decrease in length is interpreted as a 0,by focusing on increase and decrease, the public key can decoded without depend on the exact preservation of relative length. This is what protects the key from changes by AutoCAD operations (see figure -4- public key (n=629, e=5), horizontal line from left to right represent e= $(0101)_2$, while vertical line from down to up represent n= $(011000101001)_2$).

Algorithm process

In this section I clarify in details the main processes used by the suggested method.

1- Embedding process

1. Prepare the input text (secret message).
2. Add $ to the end of secret message to determine the end of input text.
3. Transform each character of secret message into numbers, using RSA algorithm.
4. Select the cover plain drawing.
5. Hiding the public key.
6. Determine vertical lines or horizontal lines used to hide message.

6-1 If vertical line then

6-1-1 Select vertical line ((x, y1), (x, y2)), with point (minim(x), y1).

6-1-2 If more than minim (x) is found, then select the line ((x, y1), (x, y2)), with point (x, minim (y1)).

6-1-3 The line ((x,y1) to (x,y2)) is found, change the least two significant number y1 in points(x,y1) with two numbers selected from coded secret message .Also change the least two significant number y2 in points(x,y2) with two successor numbers selected from coded secret message.

6-1-4 Pick another unused vertical line (go to 5-1-1) until all numbers in table 3 used.

6-2 If horizontal line then

6-2-1 Select horizontal line ((x1, y), (x2, y)), with point(x1, minim (y)).

6-2-2 If more than minim (y) is found, then select the line ((x1, y), (x2, y)), with point (minim (x1), y).

6-2-3 The line ((x1, y) to (x2, y)) is found, change the least two significant number x1 in points(x1, y) with two numbers selected from coded secret message. Also change the least two significant

number x2 in points(x2,y) with two successor numbers selected from coded secret message.
6-2-4 Pick another unused horizontal line (go to 5-2-1) until all numbers of coded secret message are used.

2- Extracting Process

To brought the message from plain drawing reversed algorithm is used

1. Select plain drawing, embedded with secret.
2. Extract the public key
3. Extracting text is done by using information in step 6 in the embedding process (vertical lines or horizontal lines used to hide message).
4. Cut the least two significant number of each point by order until found the number represent the end of message.
5. Transform numbers to character by
6. Concatenate characters, so the output will be the input text (secret message).

Example

1. Secret message

> The goal of steganography is to hide message inside other message in away that does allow any "enemy" to even detect that there is a second message present.

2. Add $ to the end of secret message.
3. Transform secret message to numbers using RSA algorithm.

> 322**28**7492**42**7273**51**8156**53**4427**51**859**42**7506**16**5492**27**3156**33**2518**27**34281**56**482**28**7100**42**7549**50**6427**16**5518**427**287**549**121**492**427**079**492**506**506**156**273**492**427**459**332**506**549**121**492**42**7518**165**287**492**428**42**7079**492**506**506**156**180**492**549**332**427**156**578**156**100**427**16**528**7156**165**427**121**518**492**506**427**156**534**534**518**578**427**156**332**100**427**238**492**332**492**079**100**238**427**16**5518**427**121**492**165**492**437**16**5427**16**5287**156**165**42**7165**287**492**428**492**42**7549**506**427**156**427**506**492**437**518**332**121**427**079**492**506**506**156**273**492**427**482**428**492**506**492**332**1650**71**

4. Use plain drawing in figure (3) to store secret message.
5. Hide public key n=629, e=5 in part of plain drawing as horizontal and vertical disconnection lines.
6. Embedded secret message in plain drawing (see figure 5-A, 5-B).

Conclusions and Future Works

The conclusions of this paper are focused on

- AutoCAD operations include moving the plain around, rotating; changing their scale often this is done using CAD primitives. All these operations usually introduce huge changes in coordinates, thereby destroying any information contained in their least significant digit. But it meets two criteria important to steganography: it is hidden to the casual observer, and not alters the original data content.
- Using disconnection lines protects the public key from changes by AutoCAD operations and does not alter the positional accuracy of the real coordinates.

I suggest the following points for future works

- Architectural techniques deal with the problem of floating-point computation at 2D and 3D images, different points for drawing deals with floating point number can be used to store secure message.
- Development equation to determine the place where storing secret message.
- Distances between points can be used to convey information. Usually it is accomplished by adding extra lines to the description of a distance between points lie on the figure itself, they do not change how it looks; they only change its internal representation. The line distances can transmit messages in many ways.

Fig. (3): Plan drawing showing the cover image

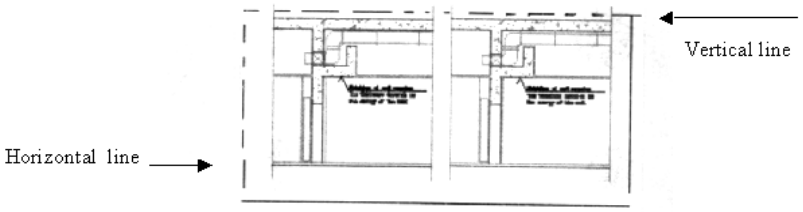


Fig. (4): Section plan drawing showing the public key

Fig. (5-A): Output of vertical line algorithm

Fig. (5-B): Output of horizontal line algorithm

References

1. Bill Thoen **Apr 09, 2002**,"*GIS & Steganography part 1: Hidden Secrets in the Digital Ether"*, Internet Survey, http:// www.directionsmag.com.
2. Bill Thoen **Apr 16, 2002**, "*GIS & Steganography part 2:As applied to MapInfo and ArcView* " Internet Survey, http://www.directionsmag.com.
3. Bill Hubber **Apr 18, 2002** "*GIS & Steganography part 3: Vector Steganography* " Internet Survey, http://www.directionsmag.com.
4. Brain Beckett, **1997** "*Introducrion to cryptology and PC security*",McGraw-Hill companies.
5. Brigit P., **1996** "*Information Hiding Terminology*", First International Workshop of lecture notes in computer, Vol. 1174, PP.347-350, and Springert.
6. James C Judge **November 30, 2001** "*Steganography: Past, Present, Future*", Internet Survey,http://www.new\stegography4.html.
7. Neil F. Johnson, **August 2002**, "*Steganography ; Art & Science of Hiding Communication*",office of Naval Research Navel-industry partnership conference, Washington DC,USA,13-14.
8. Gennaro R., Jarecki S., Krawczyk H, , rabin T., **1996** "*Robust and efficient sharing of RSA*", In Advances in cryptology-crypto.
9. "*Geographic Information Systems*", USGS,Science for a change world, Internet Survey ,http://www.Geographic Information Systems[GIS]poster.htm.