RESEARCH ARTICLE OPEN ACCESS

Steganography and Visual Cryptography for Secured Data Hiding

Mr. Deepak S. Bhiogade, Prof. Shaikh Phiroj Chhaware
(Department of Computer Technology, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
Email: deepak.bh1985@gmail.com)
(Department of Computer Technology, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur
Email: firoj466@yahoo.com)

ABSTRACT
Our major concern is to have a secured, reliable, robust and the most efficient steganography and visual cryptography with view to have no unauthorized access to the encoded with the help of various decoding methods. The previous extensive research by the expert in this field regarding the existing concern of security of data failed shot to achieve the desire results. On this ground the proposed method is the updated and the advanced version best on Shamir encryption algorithm.

Keywords : Efficient, Integrity, High performance, Secured, Reliable data hiding.

I. INTRODUCTION

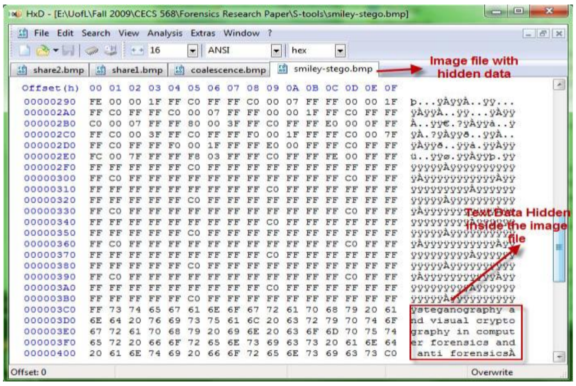
Steganography and visual cryptography are similar in concept. Ultimately they both are ways of hiding data from prying eyes and in many cases from forensic and security investigators. Some claim that visual cryptography is another type of steganography and some claim the inverse. Although in their basic purpose of hiding information they are indeed similar, when it comes to the data transformation algorithms steganography and visual cryptography take advantages of different methodologies in order to protect their respective pay load. In steganography, only the sender and receiver aware of the hidden data and typically if the loaded file thing that comes to their mind is the question of what is the encrypted and how they can decrypt the hidden message.

Steganography is concerned with sending a secret message while hiding its existence. The word steganography is derived from the Greek words steganos, meaning ‘covered’, and Graphein meaning ‘to write’.

Cryptography is not concerned with hiding the existence of message, but rather its meaning by a process called encryption. The word cryptography is derived from the Greek word kryptos, meaning ‘hidden’.Steganography embeds the secret message in a harmless looking cover, such as digital image file. The need for steganography is obvious but what is less obvious is the need for more research in the field. Simple techniques are easily detectable and there is a whole field of defeating steganographic techniques called steganalysis, advances in steganalysis which make it constantly evolving field. Since most steganographic system use digital image as cover, the whole field has borrowed methods and ideas from the closely related field of watermarking and finger printing which also manipulate digital audio and video, for the purpose of copyright. Even though, in principle, many aspect of image can be manipulated, in reality most stego system aim for the preservation of visual integrity of the image. Early stego system goals were to make changes not detectable by the human eye. This feature is not enough because statistical method can detect the changes in image even if it is not visible. Image compression also plays a role in steganography because it was found at on many occasion the result depend on the compression scheme used. Steganpgraphers struggle to find more efficient method to embed a secret message in a cover object, only to be defeated by techniques derived by steganalysts.

II. LITERATURE REVIEW

A few experiments were conducted using hex editor (HxD) and visual cryptography software called ‘ Visual Cryptography Share Encryptor’. Some plain text was hiding using HxD in to the image file.



HxD - [E:\UofL\Fall 2009\CECS 568\Forensics Research Paper\S-tools\smiley-stego.bmp]
File Edit Search View Analysis Extras Window ?
16
ANSI
hex
share2.bmp
share1.bmp
coalescence.bmp
smiley-stego.bmp
Image file with hidden data
Text Data Hidden inside the image file
Offset: 0
Overwrite

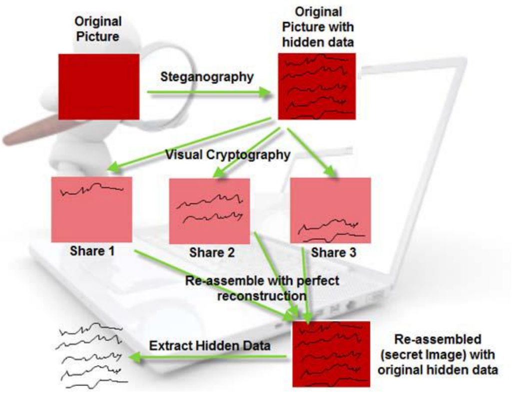
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000290  FE 00 00 1F FF C0 FF FF C0 00 07 FF FF 00 00 1F  þ...ÿÀÿÿÀ..ÿÿ...
000002A0  FF C0 FF FF C0 00 07 FF FF 00 00 1F FF C0 FF FF  ÿÀÿÿÀ..ÿÿ...ÿÀÿÿ
000002B0  C0 00 07 FF FF 80 00 3F FF C0 FF FF E0 00 0F FF  À..ÿÿ€.?ÿÀÿÿà..ÿ
000002C0  FF C0 00 3F FF C0 FF FF F0 00 1F FF FF C0 00 7F  ÿÀ.?ÿÀÿÿð..ÿÿÀ..
000002D0  FF C0 FF FF F0 00 1F FF FF E0 00 FF FF C0 FF FF  ÿÀÿÿð..ÿÿà.ÿÿÀÿÿ
000002E0  FC 00 7F FF FF F8 03 FF FF C0 FF FF FE 00 FF FF  ü..ÿÿø.ÿÿÀÿÿþ.ÿÿ
000002F0  FF FF FF FF FF C0 FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÀÿÿÿÿÿÿÿÿÿÿ
00000300  FF C0 FF FF FF FF FF FF FF FF FF FF FF C0 FF FF  ÿÀÿÿÿÿÿÿÿÿÿÿÿÀÿÿ
00000310  FF FF FF FF FF FF FF FF FF C0 FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÀÿÿÿÿÿÿ
00000320  FF FF FF FF FF C0 FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÀÿÿÿÿÿÿÿÿÿÿ
00000330  FF C0 FF FF FF FF FF FF FF FF FF FF FF C0 FF FF  ÿÀÿÿÿÿÿÿÿÿÿÿÿÀÿÿ
00000340  FF FF FF FF FF FF FF FF FF C0 FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÀÿÿÿÿÿÿ
00000350  FF FF FF FF FF C0 FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÀÿÿÿÿÿÿÿÿÿÿ
00000360  FF C0 FF FF FF FF FF FF FF FF FF FF FF C0 FF FF  ÿÀÿÿÿÿÿÿÿÿÿÿÿÀÿÿ
00000370  FF FF FF FF FF FF FF FF FF C0 FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÀÿÿÿÿÿÿ
00000380  FF FF FF FF FF C0 FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÀÿÿÿÿÿÿÿÿÿÿ
00000390  FF C0 FF FF FF FF FF FF FF FF FF FF FF C0 FF FF  ÿÀÿÿÿÿÿÿÿÿÿÿÿÀÿÿ
000003A0  FF FF FF FF FF FF FF FF FF C0 FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÀÿÿÿÿÿÿ
000003B0  FF FF FF FF FF C0 FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÀÿÿÿÿÿÿÿÿÿÿ
000003C0  FF 73 74 65 67 61 6E 6F 67 72 61 70 68 79 20 61  ÿsteganography a
000003D0  6E 64 20 76 69 73 75 61 6C 20 63 72 79 70 74 6F  nd visual crypto
000003E0  67 72 61 70 68 79 20 69 6E 20 63 6F 6D 70 75 74  graphy in comput
000003F0  65 72 20 66 6F 72 65 6E 73 69 63 73 20 61 6E 64  er forensics and
00000400  20 61 6E 74 69 20 66 6F 72 65 6E 73 69 63 73 C0   anti forensicsÀ
```

Then the image with the hidden text was split into shares, each time using various schemes, resulting in image shares that look like noise. Notice the plain text could not be spotted anywhere in the image data shown via the hex editor. This indicates that the algorithm use in that software lack the perfect any construction property since they did alter the data either in processor obtaining the shares, or in the process or reconstructing the hidden image.

III. RESEARCH METHODOLOGY

The proposed work is basically a framework designed in java swing with two modules e.g. Steganography using Shamir encryption Algorithm and visual cryptography. An input image is accepted as cover image for the input message in plain text format. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the steg-image are modified by the visual cryptography to keep should prove the proposed algorithm's effectiveness in resistance to steganalysis with better visual quality. The user can select the targeted information in terms of plain text for embedding the secret message in LSB of the cover image. The implications of the visual cryptography will enable the pixels value of the steg-image to keep their statistic character. LSB steganography has low computation complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium. This is also one of the strong algorithms which keep the information proof from any intruder.



Original Picture
Original Picture with hidden data
Steganography
Visual Cryptography
Share 1
Share 2
Share 3
Re-assemble with perfect reconstruction
Extract Hidden Data
Re-assembled (secret Image) with original hidden data

.

A. THE MONO-ALPHABETIC SUBSTITUTION CIPHER

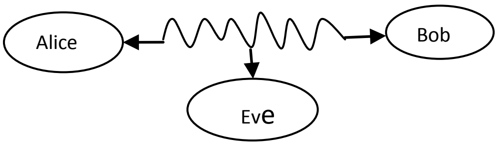
One of the simplest ciphers is the mono-alphabetic substitution cipher, which replace one character with another character. An example of simple mono-alphabetic substitutions ciphers is the Caesar cipher.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b

A normal sentence such as "Hello, my name is Caesar"is replaced with "fcjjm kw lykc gq aycqyp". Although the message now looks like complete gibberish.

B. SYMMETRIC-KEY VS. PUBLIC-KEY CRYPTOGRAPHY

Codes are broken into the two categories of Symmetric-key (SKC) and Public-key (PKC) cryptography. In SKC, both receiver (Bob) and sender (Alice) have to know the key to encode and decode the message. On the other hand, in PKC only Bob knows how to decode the message while Alice can only encode the message with information the receiver publicizes, stopping any interceptors (Eve) from the decrypting and intelligently altering the message.

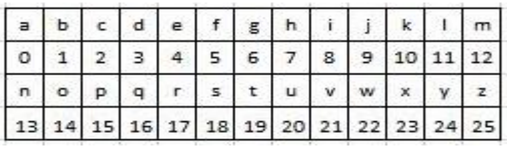


A commonly used Public-key ecryption system is RSA, RSA uses modular arithmetic to encrypt and decrypt messages.
To set up RSA:
P and Q are prime number, usually over 20 digits.
M=PQ.

N=(P-1)(Q-1).
E has no common factors with N.
D is the inverse of E in modulo N.
Which means ED=1(mod N)
Bob publicizes M and E.
The encryption step is:
Alice encodes her message(X) by:
C=XE (mod M)
Then to decrypt:
Bob decode by;
CD (mod M)
For example, if P=17, Q=13, M=221, N=192, E=5, D=77
Bob publicizes the number 221 and 5
Alice wants to send the message “Hi”.
H=7 and I=8 according to figure so
Hi=26(7) +260(8)=190
1905=73(mod221)
Alice sends 73 to Bob
Bob calculates:
7377=190(mod 221)
190=26(7)+260(8)
7=H,8=I
Hi.

C. MODULAR ARITHMETIC

The Caesar cipher can be made more difficult to break by using modular arithmetic; for example, Eve must make a larger number of guesses before reaching the correct message. Modular arithmetic just cycles number within a set range from zero to one less than the modulus. When considering the English alphabet, mod26 is used (number of letter).
Z=25, 25+2=27
However, the number must be less than 26 so



a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

27-26=1=B
Or we can say that
27=1 (mod 26)
For larger number:
53+14=19(mod 24)
In the case of a 24 hour clock.

IV. CONCLUSION

In this paper we have presented implementation of securely using steganography technique using Shamir algorithm. It can be concluded that when normal image security using steganography and visual cryptography technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganography are highly optimized using Shamir algorithm.

References

[1] Hsien-Chu Wu; Chwei-Shyong Tsai; Shu-Chuan Huang; Colored digital watermarking technology based on visual cryptography, Nonlinear Signal and Image Processing, *IEEE-Eurasip*, 2005.
[2] Chin-Chen Chang; Iuon-Chang lin;, A new (t,n) threshold image hiding scheme for sharing a secret color image, communication Technology Proceeding, *ICCT* 2003.
[3] Katzenbeisser, S. and Petitcolas F. A. P. information hiding techniques for steganography and digital watermarking. Artech House, Norwood, *MA 02062,USA*, 1999.
[4] N. Johnson and S. Jajodia. Steganalysis of image created using current steganography software workshop on information Hidding,1998.
[5] N. Johnson and S. jajodia steganalysis ; The investigation of hidden information. Proc Of the 1998 *IEEE Information Technology Conference*,1998.