IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 130-135
www.iosrjournals.org

Using Concept of Steganography and Visual Cryptography for Secured Data hiding

Mr. Deepak S. Bhiogade, Prof. Milind Tote
Dept. of Computer Technology Nuva College of Engineering & Technology, Nagpur, India
Dept. of Computer Technology Gurunanak Institute of Engineering & Technology,Nagpur, India

Abstract: *The most advanced and updated Shamir Encryption algorithm is efficient enough to prevent and stop unauthorized and illegal access to the secured encoded data. It is best to solution to ensure reliability and security of the data with the help of Steganography and Visual Cryptography. On the ground of the failure of the previous extensive research by expert to ensure security of the data.*

Index Terms: *Data hiding, Efficient, Integrity, High performance, Reliable, Secured.*

I. INTRODUCTION

Steganography is the art, Science, or practice in which messages, images, or files are hidden inside other messages, images or files. The person sending the hidden data and the person meant to receive the data are the only once who know about it, but to everyone else, the object containing the hidden data just seem likes an everyday normal object. When it comes to the data transformation algorithms Steganography and Visual Cryptography take advantages of different methodology in order to protect their respective payload. 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 concern 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”.

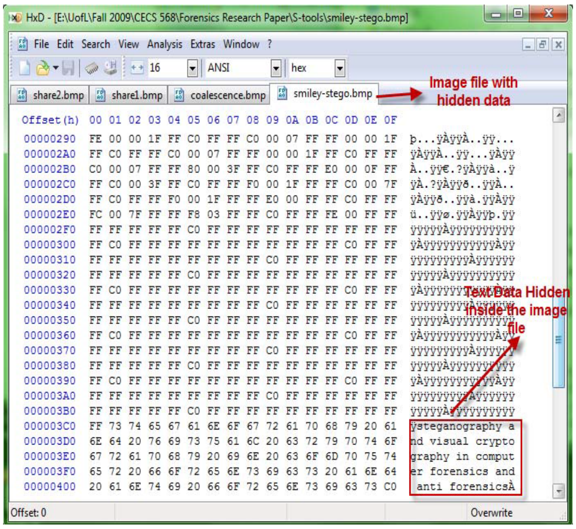
Cryptography is not concerned with hiding the existing of message, but rather its meaning by a process called Encryption. The word Cryptography derived from the Greek word Kryptos, meaning “Hidden”.

Seganography embed 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 technique called steganalysis, advances in steganalysis which makes it constantly evolving field. Since most steganography 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 eyes. 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. Steganography struggle to find more efficient method to embed a secret message in cover object, only to be defeated by techniques derived by steganalysts.

II. LITERATURE REVIEW

Steganography and visual cryptography had so far been dealt with as two separate entities as far as possibilities of use. A few algorithm touches on the concept of using Steganography and visual cryptography together, such as the JVW method mentioned above. JVW mentions the use of watermarking, embedding another image inside an image, and then using it secrete image. The secrete image would get split into shares which would need to be overlaid to reveal that secrete image. The use of Steganography alongside visual cryptography was a strong concept and adds a lot of challenges to detecting such hidden and encrypted data. For example, imagine an algorithm which uses one of the strong algorithms of Steganography to hide data inside an image, and they uses that image as a secrete image with a strong visual cryptography method. Basically we would then have a secrete image with hidden data which would be split up into shares. These shares can also be innocent images, not necessarily noise images. Then when these shares were reassembled or decoded to reconstruct in original image we would then have a revealed image which still contains the hidden data. So the receiver would be able to extract the hidden data from the revealed image. This algorithm cannot exist without having a perfect reconstruction property in the visual cryptography method. The reason for that was that if our reconstruction process or even the encryption process alters the image data, then it would consequently alter our hidden data which would make it impossible to extract the hidden data from the revealed image.

A few experiments were conducted using hex editor (HxD) and visual cryptography software called 'visual cryptography share encryptor'. Some plaintext was hiding using HxD in 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

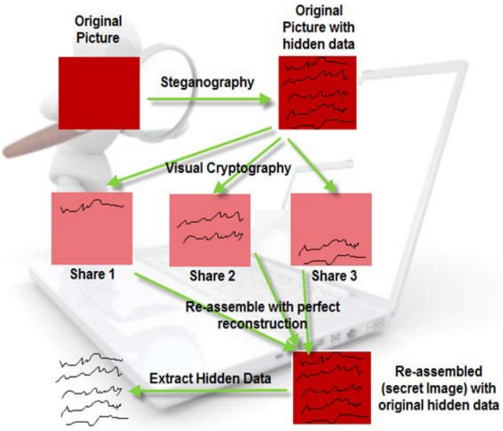
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

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 plaintext 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.

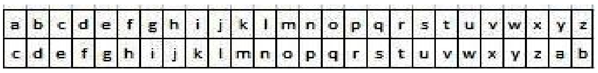
III. RESEARCH METHODOLOGY

The proposed work 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 secrete message in LSB (Least significant bit) of the cover image, the pixel value of the steg-image are modified by the visual cryptography to keep should prove the proposed algorithm's effectiveness in resistance to stganalysis with better visual quality. The user can select the targeted information in terms of plaintext for embedding the secrete message in LSB of the cover image. The implication of the visual cryptography will enable the pixel value of the steg-image to keep their statistic character. LSB steganography has low computation complexity and high embedding capacity, in which a secrete 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

3.1. 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 substitution cipher is the Caesar cipher.

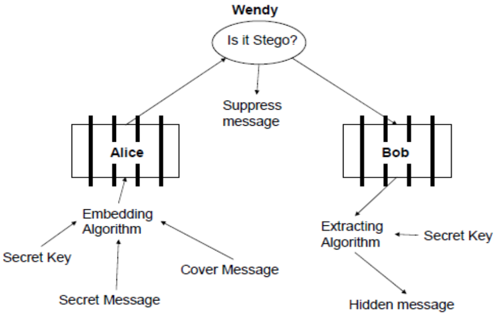


a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b

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

3.2. Symmetric-key vs. Public key cryptography

Codes are broken into 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 interceptor (Eve) from the decrypting and intelligently altering the message.



A commonly used Public-key encryption system is RSA uses modular arithmetic to encrypt and decrypt message.

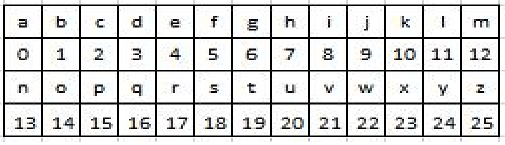
To set up RSA:
P and Q are prime number, usually over 20 digits.
M=PQ.
N=(P-1)(Q-1)
E has no common factor with N.
D is the inverse of E in modulo N.
Which means ED=(1mod N)
Bob publicizes M and E,
The encryption step is:
Alice encoded her message(X) by:
C=XE (mod M)
Then to decrypt:
Bob decoded by:
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 want to send the message "Hi".
H=7 and I=8 according to figure so
Hi=26(7)+260(8)=190
1905=73(mod 221)
Alice send 73 to Bob
Bob calculates:
7377=190(mod 221)
190=26(7)+260(8)
7=H,8=I
Hi.

3.3. Modular Arithmetic

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

The proposed project work consists of mainly two algorithms which are (1) Steganography using Genetic algorithm and (2) Visual cryptography with pseudorandom number. The application initiates with steganography modules where the cover image will be encrypted to generate Stego image. The steganography image generated in this module will act an input for visual cryptographic module.

3.3.1. Algorithm: Steganography

```
Input: Cover Image
Output: Stego Image
1.  read input image (Cover Image)
2.  read the Plain text message
3.  authentication using password
4.  switch (encoded_alg)
5.  case-1: Implement Battlesteg;
6.  break;
7.  case-2: Implement BlindHide;
8.  break;
9.  case-3: Implement Filterfirst;
10. break;
11. case-4: Implement Hideseek;
12. break;
13. convert image to double precision
14. embed the message in the cover image based on the percentage
15. generate random message
16. apply uniformly distributed pseudorandom integers
17. msg=rand([0 round ( 255* per/100)], size(I)); //perc= Embeds the message in the cover image based on
    the percentage.
18. I=I+msg;
19. divide Image into 8x8 blocks
20. apply the non-positive flipping F-
21. generate random 0 and 1s
22. change LSB as per flipping
23. apply non–negative flipping F+
24. generate random -1 and 0s
25. change LSB as per flipping
26. calculate correlation
27. Initialize maximum chromosome
28. flip second lowest bit randomly for number of time
29. PSNR=snr(chrom-Cn) // Cn= Correlation of non-negative flipping
30. fitness=alpha*(e1+e2)+PSNR
31. if fitness >max fitness // maxfitness=0 is initialized
32. maxfitness = fitness;
```

```
33. chrommax =Cp;
34. crossover = crossover+1; //crossover=0 is initializes
35. end
36. replace chromosome with new one.
```

3.3.2. Algorithm: Embedding process

```
1. for i=1….,l(c) do
2. si← ci
3. end for
4. generate random sequence ki using seed k
5. n ←k1
6. for i=1….l(m) do
7. sn←cn↔mi
8. n←n+ki
9. end for
```

3.3.3. Algorithm : Extraction process

```
1. generate random sequence ki using seed ki
2. n ← k1
3. for i=1….l(m) do
4. mi ← LSB(cn)
5. n←n+ki
6. end for
```

3.3.4. Algorithm : Visual Cryptography

Input: Stego-Image
Output: Encrypted Shares

1. Read Stego-image generated
2. The Stego-image is breaked into three layers namely split-1, split-2, split-3 these three files are containing the hidden data these three files have to be reconstructed perfectly.
3. The re-assembled picture and the extracted data will be gained again.

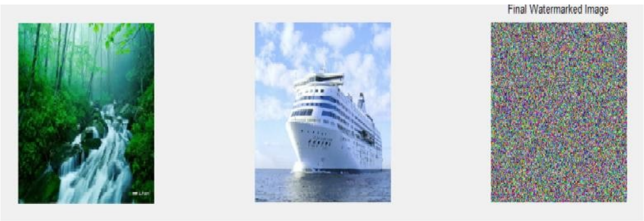


Figure 3.1 Final Watermark Image after embedding the Normal Image and Cover Image.

IV. CONCLUSION

The proposed system has discussed implementation of securely using steganography technique with singular value decomposition and Visual cryptography using Shamir encryption 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 secrete message. The security features of the steganography are highly optimized using singular value decomposition. The proposed system is highly resilient against RS attack and optimally used for both grayscale and colored output in visual secretes shares making it highly compatible for real-time application. The future work could be towards the enhancing the algorithm using neural network for the visual cryptography, so that the system can generate highly undetectable secrete shares using certain set of training data which might be automatically generated and is disposed after the task has been performed. Such type of approach might render the most secure staganographic and visual cryptographic scheme.

REFERENCES

[1] O.Kurtuldu and N. Arica, “A new Steganography method using image layers,” in Computer and Information Sciences, 2008 ’08. 23rd International Symposium on, 2008 , pp. 1-4.

[2] j. Mielikainen, “LSB matching revisited,” Signal processing Letters, IEEE, vol. 13, pp. 285-287, 2006.

[3] L. Xiangyan, l. Bin, L. Fenlin. “A Dynamic Compensation LSB Steganography Resisting RS Steganalysis.” In SoutheastCon, 2006. Proceedings of the IEEE, 2006, pp. 244-249.

[4] Hsien-chu Wu; Chwei-shyong Tsai; Shu-Chuan Huang; Colored digital watermarking technology based on visual cryptography, Nonlinear Signal and Image Processing, IEEE-Euarasip, 2005.

[5] 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.

[6] Katzenbeisser, S. and petitcolas F. A. P. information hiding techniques for steganography and digital watermarking. Artech House, Norwood, MA 02062, USA. 1999.

[7] N. Johnson and S. Jajodia, Steganalysis of image created using current steganography software workshop on information hiding, 1998.

[8] Jithesh K. Dr A. V. Senthil kumar, Multi Layer Information Hiding-A Blend of Steganography and Visual Cryptography, Journal of Theoritical and Applied Information Technology, 2010.