International Journal of Research in Advent Technology, Vol.2, No.7, July 2014
E-ISSN: 2321-9637

A Survey on Metamorphic Cryptography Techniques

Shraddha Subhedar
Department of Information Technology, Mumbai University
Email: shraddhasubhedar23@gmail.com

Abstract- With the huge growth of computer networks and advancement in technology, a huge amount of information is being exchanged. A large part of this information is confidential or private which increases the demand for stronger encryption techniques. Security has become a critical feature for thriving networks. Metamorphic Cryptography is the fusion of steganography and cryptography. Using Cryptography one can secure information by making sure that the secret can only understood by right person. Steganography is the process of sharing information in undetectable way making sure that nobody else can even detect the presence of secret.If these two methods could be combined, it would provide a fool-proof security to information being communicated over a network. This paper provides a survey on Metamorphic Cryptography, mainly covering the fundamental concepts, some commonly used strategies for improving steganographic as well as cryptographic security and development of two corresponding metamorphic schemes.One of the methods shows how to secure message using static parsing by multiple cover objects. Another method shows a new way of hiding an image in another image directly by S-DES algorithm using key image and the data obtained is concealed in another image.

Index Terms- Metamorphic Cryptography; Static parsing steganography; ISC Embedding;Discrete Cosine Transform.

1. INTRODUCTION

Information security is of utmost importance in today's fast developing era. Information or messages are being exchanged over various types of networks.

In present world of communication, one of the necessary requirements to prevent data theft is securing information. A large part of this information is confidential or private which increases the demand for stronger encryption techniques. Security has become a critical feature for thriving networks. Cryptography is derived from the Greek words "kryptos"(meaning "hidden") and "graphein" (meaning "to write"). Cryptography is the study of means of converting information from its normal comprehensible form into an incomprehensible format, rendering it unreadable without the secret knowledge. The process of converting information by transforming it into unreadable format is known as encryption. Encryption techniques can be sometimes broken by cryptanalysis, also called as code breaking, although modern cryptographic techniques are virtually unbreakable. Cryptography encrypts the actual message that is being sent.

This mechanism employs mathematical schemes and algorithms to scramble data into unreadable text. It can only be decoded or decrypted by the party that possesses the associated key. Using Cryptography one can secure information by making sure that the secret can only understood by right person.

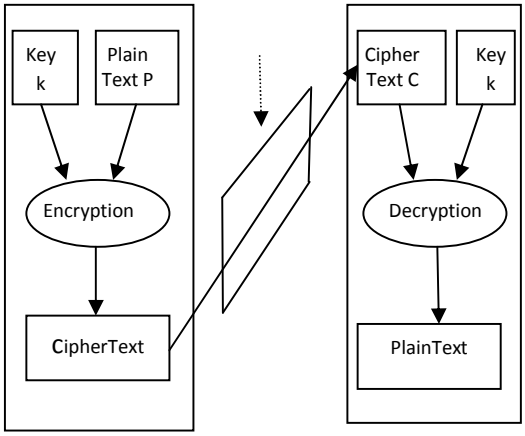
Steganography is derived from the Greek word "stegnos" (meaning "covered/secret") and "graphein" (meaning "to write/draw"). Steganography the study of means of concealing the information in order to prevent hackers from detecting the presence of the secret information. The process of concealing the message in a cover without leaving the remarkable trace is known as Steganography. is the process of sharing information in undetectable way making sure that nobody else can even detect the presence of secret. Steganography is the form of convert communication in which a secret message is camouflaged with a carrier data.

2. LITERATURE SURVEY

2.1. Review of cryptography

Until modern times cryptography referred almost exclusively to encryption, which is the process of converting ordinary information called plaintext into unintelligible gibberish called cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext.
A cipher or cipher is a pair of algorithms that create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a "key". This is a secret

parameter (ideally known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cipher texts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys are important, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.



2.2. Cryptographic methodologies

1. Methodology for transforming plain text to cipher text.
All encryption algorithms are based on two general principles: substitution and transposition, in which elements in the plaintext are rearranged.

2. Methodology for number of keys used.
There are some standards methods [Li *et al*.(2011)] which are used with cryptography such as secret key, public key, digital signature and hash function.

Secret Key (Symmetric) With secret key cryptography, a single key is used for both encryption and decryption. Public Key : two-key crypto system in which two parties could engage in a secure communication over a insecure communications channel without having to share a secret key.

Digital Signature The digital signature is more like stamp or signature of the sender which is embedded together with the data and encrypts it with the private key in order to send it to the other party.

Hash Function The hash function is a one way encryption, the hash function is a well defined procedure or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes.

3. Methodology for processing plain text.

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

2.3. Review of Steganography

Stegnography refers to the technique of hiding information in digital media in order to conceal the existence of the information.[Raphael and sundaram (2011)]

Steganographic Methodologies

Least Significant Bit (LSB) Based Steganography

It works by replacing the LSBs of randomly selected pixels in the cover image with the secret message bits. The selection of pixels may be determined by a secret key.

Multiple Bit-planes Based Steganography

The methodology of LSB embedding can be easily extended to hiding data in multiple bit-planes.

Noise-adding Based Steganography

Instead of replacing the LSBs of the cover image pixels, LSB matching adds or subtracts them by 1 if they does not match the message bits.

Prediction Error Based Steganography

Data can be hidden into the prediction errors. Using a pixel's neighboring pixel is a simple way to predict the current pixel value and thus their difference can be considered as a kind of prediction error.

Quantization Based Steganography

Quantization index modulation (QIM) is a commonly used data embedding technique in digital watermarking and it can be employed for steganography.

3. WHY NOT NON-METAMORPHIC SYSTEM?

- Based on only single Methodology

Existing technology for data security is base on single methodology i.e. steganography or cryptography. Achieving goal in both technologies is same and it is restricted in today's information security system. Achieving high degree for information security multiple methods must be implemented to secure data. Based on single methodology system may be crash in high complicated network environment.

- Simple techniques for data hiding

In steganography and cryptography techniques used for information hiding are based on simple algorithm which can be easily decoded by attacker.

- Less secure in case of attack over network by attacker:

Simple encoding algorithm can decode by attacker and he can make change or he can make use of this secure data for his own selfish purpose easily.

4. EXAMPLES OF DISCUSSION FOR METAMORPHIC APPROACH

4.1. Static parsing steganography approach

In this approach, both the sender and the recipient agree on a cover image to send a secret message. [Khalil *et al*. (2010)] The protocol does not modify the cover image, rather it determines the bits of the secret message that match the ones in the cover image and stores their different locations (i.e. in the cover image) in a vector. This vector is then sent encrypted using classical cryptography to the recipient.

A steganalyst in this case may intercept a vector of bits that is possibly encrypted, without knowing to which cover image it corresponds. So to defeat our scheme, a steganalyst has to intercept the secret message sent to the recipient and must know which cover image it corresponds to.

SPS consists of 2 main steps.

1. A cover image (that both the sender and receiver share), and the secret message to be sent are converted into bits. Let us denote the output files by Image1 and secret1, respectively.

2. In this step, we encode the secret message Secret1 based on Image1. The idea is based on the problem of finding the longest common substring of two strings using a generalized suffix tree, which can be done in linear time . The algorithm uses a divide-and-conquer

strategy and works as follows. It starts with the whole bits of Secret1 and tries to find a match of all the bits of Secret1 in Image1. If this is the case, it stores the indexes of the start and end bits of Secret1 that occur within Image1 in an output file Output1. If not, the algorithm recursively tries to find a match of the first and second halves of Secret1 in Image1. It keeps repeating the process until all the bits of Secret1 have been matched with some bits of Image1. We next give a pseudo-code on how the algorithm works. Denote by LCS(S1, S2) the algorithm that finds the longest common subsequence of S1 that appears in S2, and returns true if the whole of S1 occurs in S2. We allow this modification of the algorithm (i.e. LCS) in order to simplify the implementation of SPS next described.

SPS (s e c r e tMe s s a g e , cove r Image) ;

i f LCS(s e c r e tMe s s a g e , cove r Image) i s t r u e ,

t h e n

s t o r e t h e p o s i t i o n s of t h e i n d e x e s

of t h e s t a r t and end b i t s of S e c r e t

t h a t o c c u r wi t h i n Image t h e o u t p u t

f i l e Output ,

e l s e

SPS (Le f t P a r t ¡s e c r e tMe s s a g e , cove r Image)

SPS (Ri g h t P a r t ¡s e c r e tMe s s a g e , cove r Image)

r e t u r n Output ,

4.2. A technique combining AES and DCT methods

The design for the combining two different techniques is purely based on the idea – distort the message and hide the existence of the distorted message and for getting back the original message – retrieve the distorted message and regain the actual message by reversal of the distortion process. [Dipti *et al.* (2010)]
Here system can be designed with three modules

Hiding the Text

- **Crypto Module**

For Crypto Module the following steps are considered for encrypting the data:

- Insert text for encryption.
- Apply AES algorithm using 128 bit key
- Generate Cipher Text in hexadecimal form.

- **Security Module**

This is an intermediate module which provides an extra security features to our newly developed system. This module is used to modify the cipher text and to generate two extra keys. In the reverse process it regenerates the original cipher text**.** Before the hiding process this module works as follows-

- Separate the alphabets and digits from the cipher text.
- Keep track of the original position of the alphabet and the digits in the form of a secret key (Key 3).
- Separate first seven alphabets retrieved from first step and add the remaining alphabets at the end of the separated digits as in the first step. This generates the second key (Key 4).

- **Stego Module**

For Stego Module the following steps are considered for hiding the above generated Cipher text.

- Take seven alphabets from the above discussed Security Module.
- Scramble the alphabets using a 64 bit key (Key 2).
- Take a Gray Scale Image.
- Find the DCT of the Image.
- Hide the Cipher by altering DCTs.
- Apply Inverse DCT.
- Find the Stego Image.

Retrieving Text

- **Stego Module(Reverse Process)**

For Stego Module the following steps are considered for retrieving the cipher text

- Take DCT of the Original Image.
- Take DCT of the Stego Image.
- Take difference of DCT coefficients.
- Retrieve bits of the hidden seven alphabets from LSB of the DCT.
- Construct the distorted seven alphabets.
- Unscrambled the distorted seven alphabets using Key 2.
- Retrieve the original seven alphabets

- **Security Module (Reverse Process)**

For Security Module the following steps are considered for retrieving the cipher text:

- Club the seven characters with the alphabets of Key 4.
- Using Key 3 and Key 4 reconstruct the cipher text from alphabets and digits.

- **Crypto Module(Reverse Process)**

For Crypto Module the following steps are considered for retrieving the original text:

- Get the above retrieved cipher text.
- Reverse AES algorithm by using Key 1.
- Get the original message.

4.3. ISC Embedding

We could unify cryptographic and steganographic system in order to devise a new model holding the features that are peculiar both to the steganographic and to the cryptographic model. [Domenico and Luca(2012)]The unifying model results as a steganographic one with the addition of a new element: the *key image K*. The output of the embedding process is a JPEG image, the inputs are: the secret message bit sequence, an image *C*, and an image *K*.
C and *K* can be either uncompressed images or compressed ones (e.g., JPEG), in addition they can be either distinct images or the same image. The embedding process will be a modification of the JPEG encoding scheme.
First of all, we subdivide *C* in a set of 8 x 8 pixel blocks and compute the Discrete Cosine Transform (DCT) on each block obtaining a set of DCT coefficients; then they are quantized.

After quantization, DC coefficients and AC zero coefficients are discarded. The remaining AC nonzero coefficients are stored in a vector called coverAC[ ], that is a signed integer array.

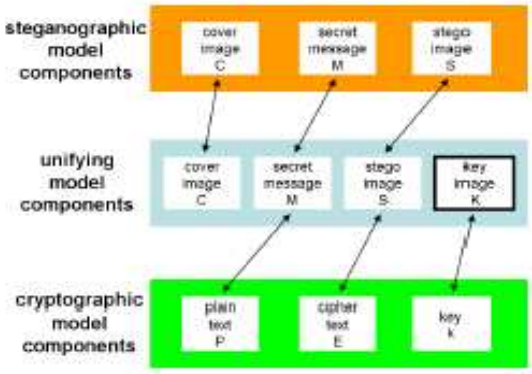


Fig. 1. ISC Embedding

We have to repeat the previous list of operations for the key image *K* obtaining keyAC[ ], a signed integer array as coverAC[ ].In order to yield the stego image *S*, we are able to modify coverAC[ ]

```
Embedding Algorithm Em1.
Input: coverAC[], keyACmessage bit array M
Output: stegoAC[]

for every bit M[i] of the message array M
if (M[i] == 1) // we want to codify a 1
if (coverAC[i] and keyAC[i] are both even or
both odd numbers)
if(coverAC[i] == 1) stegoAC[i] = 2
else if(coverAC[i] == -1) stegoAC[i] = -2
else
if(random() < 0.5)
stegoaAC[i] = coverAC[i] - 1;
else
stegoaAC[i] = coverAC[i] + 1;
end if
else // M[i] = 0, we want to codify a 0
if (coverAC[i] and keyAC[i] are one equal
and one uneven)
if(coverAC[i] == 1) stegoAC[i] = 2
else if(coverAC[i] == -1) stegoAC[i] = -2
else
if(random() < 0.5)
stegoaAC[i] = coverAC[i] - 1;
else
stegoaAC[i] = coverAC[i] + 1;
end if
end if
end for
```

Once the embedding algorithm terminates, we can proceed with stegoAC[ ] Huffman coding and eventually we obtain a JPEG image *S* as similar as possible to *C*. ISC extracting process is very simple and consists in a comparison between *S* nonzero AC coefficients (stegoAC[ ]) and *K* nonzero AC coefficients keyAC[ ]). In order to obtain these two sets of coefficients we perform a Huffman decoding step followed by the quantized AC coefficients extraction.
Once the extraction is finished we compute the following Ex1 extracting algorithm

```
Extracting Algorithm Ex1.
Input: stegoAC[], keyAC[ ]
Output: message bit array M
for every coefficient stegoAC[i]
if (stegoAC[i] and keyAC[i] are both even or both
odd)
M[i] = 0;
else
M[i] = 1;
end if
end for
```

5. WHY METAMORPHIC APPROACH?

- Provides double security for secure data transfer

Metamorphic cryptography is based on two methodologies i.e. Steganography and cryptography. Both the technologies are used for information hiding for individual purpose. And both are based on same result of information hiding. As our proposed system is based on both of the technologies and uses both the concept in advance manner our system provides double security in case of information hiding.

- Provides high degree of security while transferring data over the network

Metamorphic cryptography provides very high degree of security while transferring data over highly complicated network. As in large network environment many systems are transferring data to each other so data losses will be there as concern. Attacker may attack particular data by hacking sender or receiver system. As our proposed system is based on very powerful algorithms for steganography and cryptography attacker cannot decode these algorithm so data will be more secured in large network environment.

- System can be helpful in high confidential sectors.

This methodology can be very useful in much confidential area as it proved high degree of security. System can be use in every department of government area as it contains many confidential document that need

to be transfer to particular system or department. Proposed system can be very useful in area like National security organizations, Anti terrorist departments etc.

6. CONCLUSION

In this paper, review of the fundamental concepts of Metamorphic Approach. Discussion started with review of different cryptographic and steganographic methods.

Some examples of developing trends of Metamorphic Cryptography are sketched as follows.

Static parsing steganography. New steganographic protocols to hide secret messages. It does not modify the cover object and consists in sending a (possibly encrypted) vector that contains the different positions of the cover object that allow us to reconstruct the secret message from it. In this case, both the sender and the recipient should share a secret algorithm (or a key) on how to retrieve the secret message, given the cover object and the (secretly sent) vector.

A technique combining AES and DCT Methods. A new system using four keys which could be proven a highly secured method for data communication in near future. This method provides acceptable image quality with very little distortion in the image.

*ISC Embedding.*ISC algorithm is both an effective steganographic method as well as a theoretically unbreakable cryptographic one (ISC is an image based one-time pad). The strength of system resides in the new concept of key image. Involving two images (the cover and the key) in place of only one (the cover) we are able to change the cover coefficients randomly.

REFERENCES

[1] Bin Li; Junhui He; Jiwu Huang. (2011) : A Survey on Image Steganography and Steganalysis, Journal of Information Hiding and Multimedia Signal Processing, ISSN 2073-4212

[2] A. Joseph Raphael ; Dr.V. sundaram (2011): Cryptography and Steganography – A Survey, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630

[3] Khalil Challita; Hikmat Farhat; Roger Farley; Craig Lombardo (2010): Combining Steganography and Cryptography: New Directions, International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208

[4] Dipti Kapoor ; Sarmah; Neha Bajpai(2010): Proposed System for data hiding using Cryptography and Steganography, Journal of computer Sciences 10(15): 1650-1655

[5] Domenico Bloisi ; Luca Iocchi(2012): Image based steganography and cryptography, International Journal of Computer Science and Engineering (IJCSE) Vol.1, Issue 1 Aug 2012 105-115