Engineering Sciences International Research Journal
ISSN (Print) : 2330 – 4338 ; Volume 1 Issue 1 ǁ February. 2013 ǁ

Cryptography and Steganography Usingdynamic Encryption

K. Srividya[1], S.Vani Kumari[2], G. Neelima[3]

Abstract: 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. Steganography is the study of means of concealing the information in order to prevent hacker from detecting the presence of the secret information by camouflaging secret message with carrier data. These two methods are combined to provide a high security to information that is being communicated over a network hence the new technique Metamorphic Cryptography is born.

However the proposed idea is the inception of new technique that combines cryptography and steganography by transforming the message into a cipher image using a key and concealing it into another image using Steganography by converting it into an intermediate text and finally transforming it once again into an image which produces an almost unbreakable encryption. Hence the proposed method thus achieves a high degree of security for information.

Keywords: Cryptography, Steganography, matrix multiplication, E-OR function, cipher image, intermediate text.

1. INTRODUCTION

Cryptography and Steganography techniques of digital images are widely used to prevent and frustrate opponent's attacks from unauthorised access. There are many cryptographic and steganographic methods which have been proposed. Most of them are simple techniques which can be broken by careful analysis. However no method exists which combines the above mentioned techniques. The proposed idea is thus the inception of a new technique that combines cryptography and steganography to produce an almost unbreakable encryption.

A file is given as input by the sender. Then the process uses the ASCII value of each character of the message is taken into account to perform manipulations to produce the cipher image. The cipher image is then concealed using a cover image using steganographic technique and is converted into an intermediate image known as Steg image.

This intermediate image is finally encrypted into a final image using the same or any other key and then sent to the receiver side through the network. The receiver obtains the image, decrypts it to obtain the intermediate image using the shared key and then obtains the steg image from which the cover image is removed to reconstruct the cipher image. This cipher image is once again decrypted using the shared key to obtain the original message/file.

In the System analysis, the process for the sender side is as follows

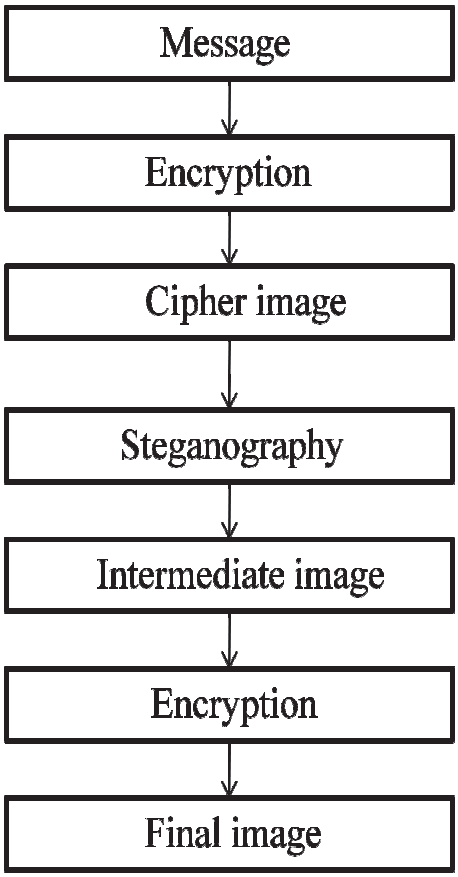


Fig. 1. Sender Side Process

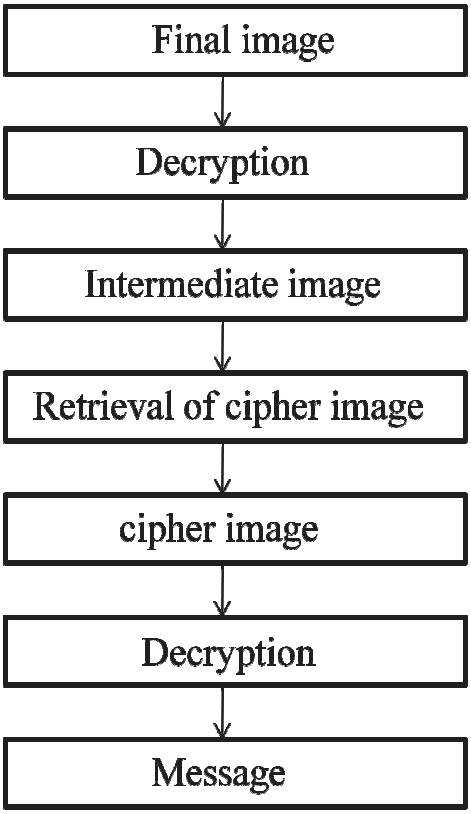


Fig. 2. Receiver Side Process

2. PROPOSED SYSTEM

The use of Cryptography technique is to make the file or message to be made into an incompatible format. The input for the encryption module can be a “file” or “message" which is first encrypted and a cipher image is generated. 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. Encryption techniques can be sometimes broken by cryptanalysis, also called as code breaking. In order to provide more security and to make it an unbreakable format, we are using the Steganographic technique along with Cryptography.

3. ALGORITHM ENCRYPTION

1: Input the message to be encrypted.

2: Input the shared key.

3: Calculate the 3x3 shared key matrix.

4: Input the point P(x, y).

5: For every character in the message

5.1: Find the pixel to be set in the cipher image.
5.2: Calculate Θ = angle between current pixel and P(x, y)
5.3: Calculate n = number of pixels between the current pixel and P(x, y).
5.4: Value = ASCII value of characterΘ n.
5.5: Shift the 8-bit binary value Θ times to the left.

4. ALGORITHM STEGANOGRAPHY

1: Input the cover image.

2: Input the cipher image.

3: For every pixel in the cipher image
3.1: Split the pixel into its grayscale values.
3.2: Split the corresponding cover image pixels into their corresponding grayscale values.
3.3: Perform Exclusive-OR operation of the respective gray values of the cipher image and cover image.
3.4: Split the resulting value to 4-bit binary values for each grayscale values of the pixel.
3.5: Assign the respective character equivalent for the 4-bit binary values.

4: Combine all the characters.

5: Obtain the intermediate text.

5. ALGORITHM DECRYPTION

1: Load the final image.

2: Input shared key.

3: Calculate the 3x3 shared key matrix.

4: Invert the shared key matrix.

5: For every pixel in the final image

5.1: Calculate the 1x3 data matrix from its grayscale values
5.2: Calculate Θ = angle between current pixel and P(x, y)
5.3: Calculate n = number of pixels between the current pixel and P(x, y).
5.4: Perform matrix multiplication of the inverted grayscale key matrix and the data matrix.
5.5: Calculate Value = Shift the output of 5.4 ‘Θ’ times to the right

6. CONCLUSION

Metamorphic Cryptography is the advanced technique which provides more security. In our technique, Graphics Interchangeable Format is used to save the images i.e. for the cover image as well as for the cipher image as they consume little space even when the size of the image is drastically increased. The technique can be further enhanced by making

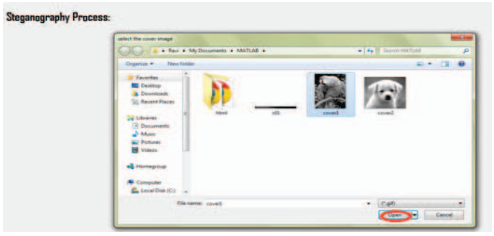
this method compatible to encrypt audio or video or any other data which has to be transmitted securely.

7. RESULTS

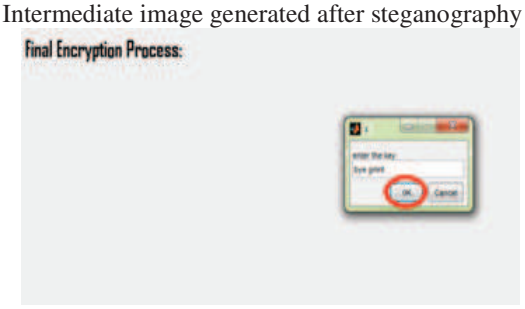
1. Input the Shared Key

2. Cipher Image is generated after Encryption Process

3. Browse the Cover Image



4. Intermediate image generated after steganography

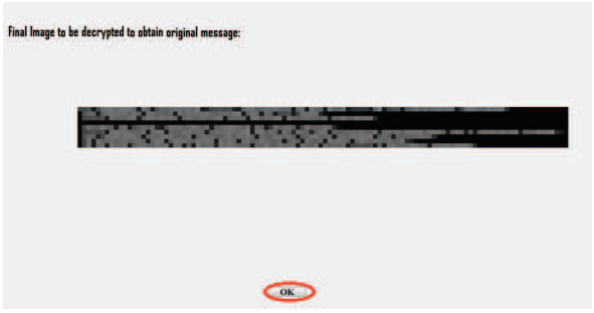


5. Key to be entered for Final Encryption

6. Final Image to be sent to the Receiver
7. Browse the final image

8 Enter the Shared Key

.9 Intermediate image is generated
10. Browse the Cover Image



11. Cipher Image is generated

12. To decrypt the message, enter the shared key

8. REFERENCES

[1] Clair, Bryan. "Steganography: How to Send a Secret Message." 8 Nov. 2001.

[2] Sujay Narayana, Gaurav Prasad "Two new approaches for secured image Steganography using Cryptographic Techniques and Type Conversions",Signal & Image Processing:An International Journal(SIPIJ)Vol.1,No.2,December2010DOI: 10.5121/sipij.2010.1206 60

[3] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson Education, Singapore, 2003.

[4] Westfeld, A., and G. Wolf, Steganography in a Video conferencing system, in proceedings of the second international workshop on information hiding, vol. 1525 of lecture notes in computer science,Springer,1998.pp. 32-47.IEEE-ICRTIT 2011

* * *

[1.]*K.SRIVIDYA, Assistant Professor*
Dept. of CSE, GMRIT
GMR NAGAR RAJAM, JNTU KAKINADA
srividya.kotagiri@gmail.com
[2]*S.VaniKumari, Sr.Assistant Professor*
Dept. of CSE, GMRIT, MR NAGAR RAJAMJNTU KAKINADA
vanikumari.s@gmail.com
[3]*G.Neelima , Assistant Professor*
Dept. Of CSE, MRIT, GMR NAGAR, RAJAM, JNTU KAKINADA
gullipalli.neelima@gmail.com