Scientific Journal Impact Factor (SJIF) : 3.518

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

ENHANCING DATA SECURITY FEATURES BY IMPROVISING CRYPTOGRAPHIC,STEGANOGRAPHIC AND HOMOMORPHISM TECHNIQUES

Harilekshmy R[1]

[1]Department of Computer Science, College of Engineering,Kallooppara

Abstract- Now digital communication has essentially become a part of infrastructure, a lot of applications are Internet-based and it is important that communications are to be made secret. As a result, the security of information passed over an open channel has become a main issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. Here we propose a new idea to secure information in digital media by combining cryptographic, steganographic and homomorphism techniques. If these three methods could be combined, it would provide a high degree of security to information being communicated over a network

Keywords- Cryptography, Steganography, homomorphism, dynamic encryption, color pixel, cipher image, intermediate text, byte array.

I. INTRODUCTION

In modern world, internet is the main source for communication. Informations are exchanged through these highly networked electronic medias and through internet is not as much secure and there are many risk factors. The confidential information which are transmitted through internet might be intercepted or distorted by unintended receivers or hackers. So we have to give great importance to secure those information which are in transit. For secure transmission of data many algorithms have been developed. In this paper we uses cryptography, steganography and homomorphism algorithms for data security and confidentiality.

A. Cryptography

Cryptography converts the information by transforming it into an unreadable form, so that person with the knowledge of algorithm and key can access the data. This process of transforming the data is termed as encryption. In encryption, using the encryption algorithm and the key, an information content which is called as the plaintext is transformed into a non-readable form. The information content in this form is termed as the cipher text. The encryption key specifies how the message is to be encoded. The process of converting cipher text back to its original form is termed as decryption. One with the knowledge of the corresponding decryption algorithm and the key only can retrieve and read the information. Based on the keys used, the encryption process can be classified as symmetric and asymmetric encryption. In symmetric encryption, for both encryption and decryption process same key is used. The sender and receiver have to agree this common key, which is used for encryption and decryption process. In the asymmetric encryption, the encryption key of the receiver is made public for anyone to use and encrypt messages. This key is known as the public key. But, only the receiving side know the decryption key and is capable to read the encrypted messages. The key which is private to the receiving party is known as the private key.

B. Steganography

Steganography hides the information to prevent hackers from detecting the presence of the secret. It is a process of hiding the message within a media without leaving a remarkable trace. It masks the presence of secret information, making the true message undetectable to the observer. The information that is hidden within the media can be either plain text, cipher text or images.

Steganography is used where encryption is not permitted or is used to supplement encryption. An encrypted file may still hide the information using steganography, so that even if the encrypted file is decrypted, the hidden message is not visible.

Today steganography, allows a user to hide large amount of informations within image, audio or video files. These forms of steganography often are used in conjunction with cryptography so that the information is two-time protected; first it is encrypted and then hides so that an hacker has to first find the information and then decrypt it. One of the most widely used applications of steganography is called digital watermarking.

C. Homomorphism

Homomorphism is a method of sharing images between two parties by using homomorphic property with public key cryptosystem[1]. In homomorphism first multiply two encrypted images, and to decrypt the resulted image to extract and recover the original image if the second original image is available. The extraction and reconstruction of original image at the receiving end is done with the help of a carrier image. Homomorphic systems are special type of cryptosystems which maintain the operations performed on ciphertexts. A homomorphic system has the property that when any algebraic operation is performed on the input data before encryption, the resulting encryption is same as if that algebraic operation is performed on the data input after encryption. Here we uses this homomorphic property for sharing secret images using a carrier image as cover image for both transfer and extraction of original image. In homomorphism, same key is used for both encryption and decryption process, the key needs to be secure and must be shared between sending and receiving side. The purpose of homomorphism is to securely transfer and to share a secret image between two persons.

Even if an intruder or a third party gets a copy of the protected transmitted image he cannot be able to extract the original image. In homomorphism, extreme care must be taken for calculating the value of the keys because the size and the value of the public key depends the security of the encrypted image.

II . RELATED WORKS

Several papers had proposed to secure information in digital media. Most of papers presents a generalized model by combining cryptographic and steganographic technique. All the existing methods are combination of encryption and steganography to enhance the security of the data to be sent[2]. First the message is encrypted using any algorithm and the resultant cipher message is then embedded into a cover image using LSB algorithm[3]. But all the encryption algorithm has several weakness.There are various attacks possible on cryptographic techniques. Like brute force key search can be done on every possible key in order to recover the plaintext. Also cryptanalysis techniques are possible on different cipher text to find the keys. So if the existence of the message is detected, then it will not be difficult for a cryptanalyst to retrieve the message. Cryptography and steganography techniques of digital images are widely used to prevent opponents attacks from unauthorized access. Steganalysis techniques are also possible for the detection of hidden messages. Seperate steganalysis algorithms are available for the three commonly used cover medias: image, audio and video[4]. Most of these cryptographic and steganographic methods are based on single methodology system may be crash in highly complicated network environment. Also based on simple algorithms, which can be broken by careful analysis and can be easily decoded by an attacker. However no method exists which combines the above mentioned cryptography, steganography and homomorphism techniques. The proposed system is based on both of the technologies cryptography and steganography and uses both the concept in advance manner to produce an unbreakable encryption. This system is based on very powerful algorithms for steganography and cryptography so that an attacker cannot able to decode these algorithm so data will be more secured in large network environment. This methodology can be useful in many confidential areas as it provide high degree of security.

III . PROPOSED WORK

A. SENDER SIDE

We propose a more secure message transmission scheme using double encryption, steganography and homomorphism. We can represent an image in the form of a set of pixels[5]. The method applied here uses a key pixel along with angular encryption for the encryption process. The ASCII value of each of the characters in the message is taken to perform operations to produce the cipher image. The cipher image is then concealed using steganographic technique with a cover image and is converted into an intermediate text, an unreadable format. This intermediate text is once again encrypted using the encryption method as proposed above to obtain another image which is the final cipher image. A Homomorphic method of encryption for sharing secret images is applied to this cipher image, which results a byte array. This byte array is sent to the receiver through the network.

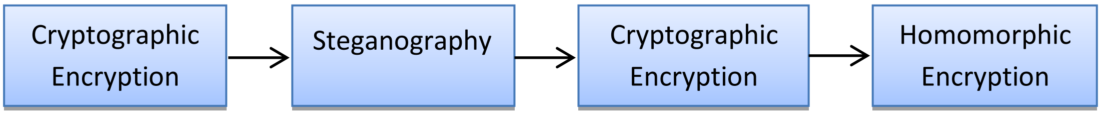


Fig. 1. Block diagram for sender side

Cryptographic Encryption

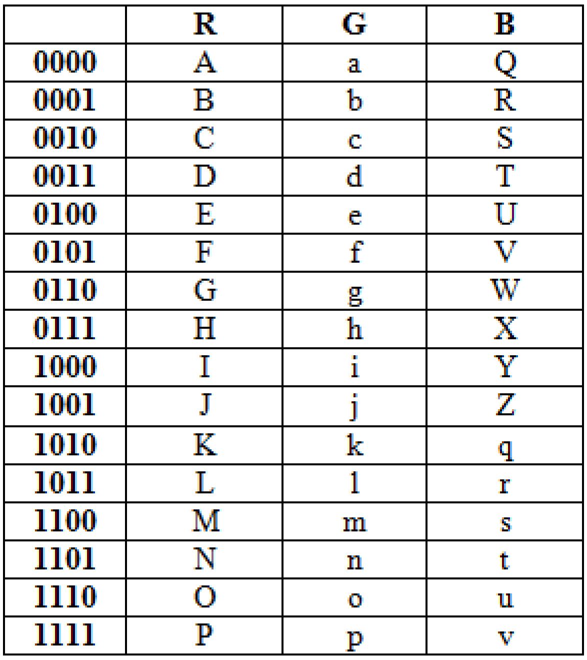
The original text message is resolved into individual characters. A specific point P(x, y) is selected on the input image. The number of pixels (n) from the point P(x, y) to the first pixel in the image is calculated. If the value of n is greater than 255, modulo operation is performed to limit the value of n to 255. This value of n is Exclusively-ORed with the ASCII value of the character to be encrypted. The angle between the point P(x, y) on the image and the first pixel of the image is calculated by taking an imaginary line joining the point P(x, y) to the first pixel by assuming as a triangle. The angle is taken as the value to perform shifting operation[6]. The resulting value obtained as the result of the Exclusive-OR operation between the ASCII value of character and n is converted into 8-bit binary format and is shifted angle times to the left. As the value of the angle and n keep changing for every pixel in the image, as a result a dynamic encryption[7] is obtained. These elements are taken as the R,G,B value of pixel to be set. Each encrypted character of the message (color pixel) is placed in the cipher image, starting from the first pixel onto subsequent pixel co-ordinates. This process is explained in CRYPTOGRAPHIC ENCRYPTION, which is carried out for the entire length of the message to obtain an image which is the cipher image.

```
CRYPTOGRAPHIC ENCRYPTION
Input: Message, Image, Point P(x, y).
Output: Cipher image.
1: Take first character in the message
2: Take first pixel in the input image.
3: Calculate $\theta$ = angle between first pixel and P(x, y).
4: Calculate n = number of pixels between the first pixel and P(x, y).
5: XOR the ASCII value of character and n.
6: Shift the 8-bit binary value $\theta$ times to the left.
7: Resolve into R,G,B values.
8: Set the pixels in the image to obtain the cipher image.
```

Steganography

The steganographic process is applied to the cipher image obtained from cryptographic encryption by selecting a cover image. The process is done by selecting each pixel of the cipher image and Exclusively-ORing it with the corresponding pixel of the cover image. This can be done by splitting each pixel in the cipher image into its R,G,B values and represent each value in its 8 bit binary format. Similarly the corresponding pixel of the cover image is converted into its respective R,G,B values and represent each value in binary format of 8 bits. In cipher image, each of the 8 bits of the R,G,B is Exclusively-ORed with the corresponding R,G,B component of the cover image to obtain resulting value of 8 bits for Red (R), 8 bits for Green (G), 8 bits for Blue (B). The resulting 8 bit binary format is split into two parts of two 4 bits for each of the elements. The first part contains the four most significant bits and the second part contains four least significant bits. We then use characters to represent the 4 bit binary values as given in Table.1.

Table. 1. Character Encoding



	R	G	B
0000	A	a	Q
0001	B	b	R
0010	C	c	S
0011	D	d	T
0100	E	e	U
0101	F	f	V
0110	G	g	W
0111	H	h	X
1000	I	i	Y
1001	J	j	Z
1010	K	k	q
1011	L	l	r
1100	M	m	s
1101	N	n	t
1110	O	o	u
1111	P	p	v

This method is explained in STEGANOGRAPHY and is carried out for the entire pixels in the cipher image to obtain a character code for every pixel in the cipher image. All the character codes are then combined to obtain the intermediate text.

```
STEGANOGRAPHY
Input: Cover image, Cipher image.
Output: Intermediate text.
1: Every pixels in the cipher image is split into its R,G,B values.
2: Every pixels in the cover image is split into its R,G,B values.
3: Apply Exclusive-OR operation of the respective R,G,B values of the cipher image and cover image.
4: Split the resulting R,G,B values of the pixel value into two 4-bit binary values.
5: Assign the respective character coding for the 4-bit binary values.
6: Combine all the characters to obtain the intermediate text.
```

The intermediate text is again encrypted using the procedure CRYPTOGRAPHIC ENCRYPTION to obtain the final cipher image. As this technique uses cryptography and steganography, image is doubly encrypted, a high level of security is obtained.

Homomorphic Encryption

The homomorphism is used to securely transfer and to share the secret cipher image. If an intruder gets a copy of the protected transmitted cipher image he cannot be able to extract the original image. In homomorphic encryption, we take the final cipher image and a cover image. These two images have been encrypted using homomorphic property, the same key is used for encrypting both images separately. Then any of the algebraic operation is performed on these encrypted images. A homomorphic cryptosystem has the property that when any specific algebraic operation is performed on the input data before encryption, the resulting encryption is same as if that algebraic operation is performed on the data input after encryption. Thus the homomorphic encryption results a byte array. This byte array is sent to the receiver through the network.

Key Management

The cover image, a point on the cover image and a secret key are the keys used to encrypt and embed the confidential message within the cover image. The point p(x,y), cover image and the homomorphic key is transmitted to the receiver through e-mail. Since the secret key and the point is shared by both sender and receiver, so the original message can be decrypted only by the intended receiver. The point p(x, y), cover image and the homomorphic key can be used for extracting the confidential message. In homomorphism, extreme care must be taken while calculating the value of the keys because the security of encrypted cipher image depends on the size and the value of the public key.

B. RECEIVER SIDE

The receiver obtains the byte array through the network. Then homomorphic decryption is applied to the byte array with the help of cover image and the key, results the final cipher image. The receiver obtains the image, decrypts the cipher image to obtain the intermediate text and analyses this text with the cover image to reconstruct the cipher image. Finally this cipher image is once again decrypted to obtain the original message.

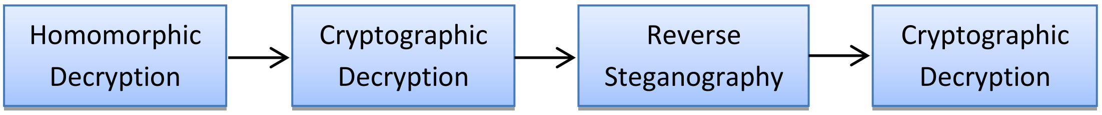


Fig.2. Block diagram for receiver side

The homomorphic decryption is applied to the received byte array with the help of cover image and the key. To decrypt the resulted image and to extract and reconstruct the original image if the second original image is available. The extraction and reconstruction of original cipher image at the receiving end is done with the help of cover image and the key as used by the sender. Thus the receiver obtains cipher image as a result of homomorphic decryption. The receiver decrypts this cipher image by using the specified point P(x, y) used by the sender. Every pixel in the received image is represented into its R,G,B values of the pixel. The specified point P(x, y) is used to obtain the angle and the number of pixels (n) between the current pixel to be decrypted and P(x, y). The value obtained is represented as a 8-bit binary form and the value is shifted angle times to the right. The result of the shifting operation is Exclusively-ORed with n to obtain the ASCII value for every character of the intermediate text. The ASCII value for every character in the text obtained using the above process, is converted into its character equivalent and combined to obtain the intermediate text. This is explained in CRYPTOGRAPHIC DECRYPTION.

CRYPTOGRAPHIC DECRYPTION
Input: Cipher image, Point P(x,y).
Output: Intermediate text.

1: For each pixel in the final cipher image
2: Calculate θ = angle between first pixel and P(x, y)
3: Calculate n = number of pixels between the first pixel and P(x, y).
4: Calculate Value = Shift the output θ times to the right
5: XOR Value and n to obtain the ASCII value.
6: Convert ASCII to its character equivalent.
7: Combine all the characters to obtain the intermediate text.

The every two characters in the intermediate text corresponds to the values of each of the components (R,G,B) of a pixel. Each character in the intermediate text has a 4-bit binary code associated with it. This code is assigned to every text by making use of reverse of the mapping process as used during encryption with the help of Table.1. The resulting values are then grouped into groups of two 4-bit binary values to obtain an 8-bit binary value. This 8-bit binary value corresponds to R or G or B component of the pixel in the cipher image. These binary values are then grouped into groups of three 8-bits (3x8=24 bits) to obtain the R,G,B values for a single pixel which is reconstructed from the intermediate text. The copy of the cover image used by the sender is resolved into its individual pixels and the R,G,B values of each pixel is Exclusively-ORed with the respective R,G,B values reconstructed from the intermediate text. The resulting values obtained are converted into the R,G,B values of each pixel of the secret image (or) cipher image. This procedure REVERSE STEGANOGRAPHY is done for the entire length of the intermediate text. The cipher image is constructed by plotting the corresponding pixel values into the image.

REVERSE STEGANOGRAPHY
Input: Cover image, Intermediate text.
Output: Cipher image.
1: For every character in the intermediate text assign the respective character codes.
2: Combine two successive 4-bit binary character codes to obtain an 8-bit binary value.
3: Split the cover image into pixels and resolve the R,G,B values for each pixel.
4: Perform Exclusive-OR operation of 8-bit character codes and the respective R,G,B values for the corresponding pixels.
5: Set the corresponding pixel in the image to obtain the cipher image.

The cipher image is again decrypted using the procedure CRYPTOGRAPHIC DECRYPTION as described above to obtain the original message. Thus original message is obtained at the receiver end.

IV. IMPLEMENTATION AND RESULTS

The proposed system was implemented in java using NetBeans IDE. The users can transmit messages securely and efficiently through the system with cryptography, steganography and homomorphism techniques. Since the message is dual encrypted, which converts the message to image then to cipher text and then to byte array an unreadable form. There is no chance of retrieving the message from the cipher. The encryption technique is also efficient since each step of the process is fully dependent on the key.
The encryption method stated above was applied to a message shown below. The input image and cover image used for the process is shown in Fig.3. and Fig.4. The encrypted results obtained were shown in Fig.5 and the intermediate text and the bytearray shown below.

Message to be encrypted : **For more details please meet me tomorrow at 9.30 am.**

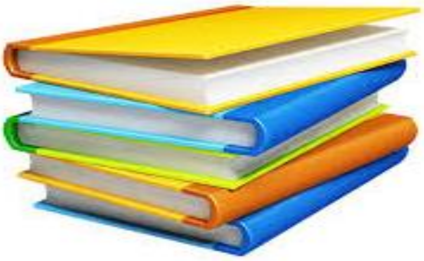


Fig. 3. Input image

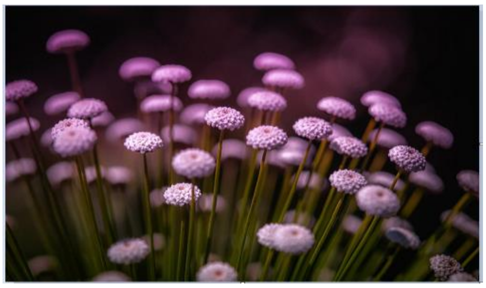


Fig. 4. Cover image

Intermediate text

```
AGaaQWAAagQWDHeeWXGEfbVQGHeoTXHBhfUtDLdlTrDLdlTrDJdlTrFMdbXZHCgf
UTFChoTQDLdlTrDIdiTYFPfcTsEJfcTsDGhfUZHDhpSqDIdiTYDIdiTYFHgaWTHA
eoWUDDdmXTCKcoTTDIdiTYDIdiTYEDdmWTHMdmTSEOegWtHDgkUqDIdiTYGCdiQV
DEfdTWHAhcXWHDheVtEEdiTYDIdiTYABdbUu
```

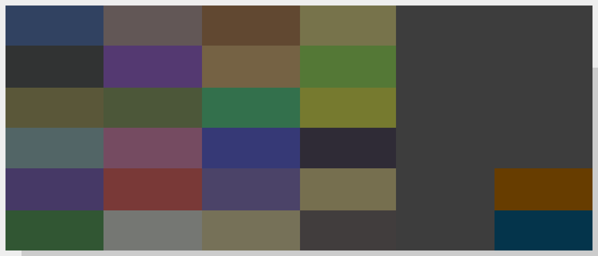


Fig.5. Cipher image

Bytearray

```
¬í |sr ¶java.math.BigIntegerŒüŸ©;û└ –I ◘bitCountI      bitLengthI ‼
firstNonzeroByteNumI ♀lowestSetBitI –signum[ magnitudet ┐[Bxr ┼java.
lang.Number†¬•♫”à‹┐  xpÿÿÿÿÿÿÿÿÿÿÿÿþÿÿÿþ ur ┐[B¬ó┤ø–◘Tà┐  xp →┐.Y#`^
ùxsq ~ ÿÿÿÿÿÿÿÿÿÿÿÿþÿÿÿþ uq ~ ┘→┐.Y#`_Fxsq ~ ÿÿÿÿÿÿÿÿÿÿÿÿþÿÿÿþ uq ~ ┘
→┘ \²Ne/lxsq ~ ÿÿÿÿÿÿÿÿÿÿÿÿþÿÿÿþ  uq ~ ┘ →┘ \²Te2‹xsq ~
```

The Bytearray was decrypted using the decryption paradox techniques to obtain the decrypted outputs as shown in Fig.6 and the text shown below.

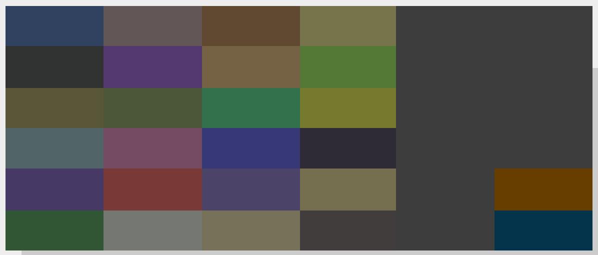
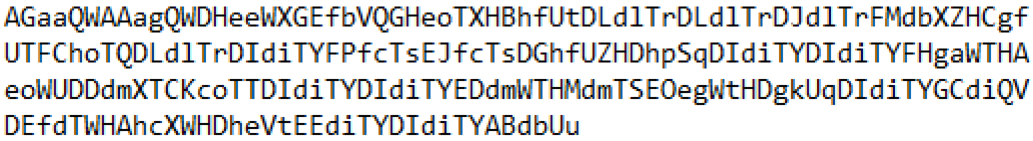


Fig. 6. Cipher image after decryption

Intermediate text after decryption



```
AGaaQWAAagQWDHeeWXGEfbVQGHeoTXHBhfUtDLdlTrDLdlTrDJdlTrFMdbXZHCgf
UTFChoTQDLdlTrDIdiTYFPfcTsEJfcTsDGhfUZHDhpSqDIdiTYDIdiTYFHgaWTHA
eoWUDDdmXTCKcoTTDIdiTYDIdiTYEDdmWTHMdmTSEOegWtHDgkUqDIdiTYGCdiQV
DEfdTWHAhcXWHDheVtEEdiTYDIdiTYABdbUu
```

Decrypted original message : **For more details please meet me tomorrow at 9.30 am.**

V . CONCLUSION AND FUTURE SCOPE

An almost unbreakable encryption is developed by combining cryptography, steganography and homomorphism. Thus a secure and efficient encoding system was proposed which include dual encryption and steganography. The dual encryption provides better security since each step of the encryption process fully depends on the key. The resultant cipher is embedded within the key image which prevents the detection of the secret. This methodology can be very much useful in confidential areas as it provide 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 confidential areas like National security organizations, Anti-terrorist departments etc.

REFERENCES

I. Naveed Islam, William Puech, Robert Brouzet. A Homomorphic Method for Sharing Secret Images. Springer. IWDW'09: 8th International Workshop on Digital Watermarking, Springer, pp.121-135, 2009, LNCS, <10.1007/978-3-642-03688-0 13>. <lirmm-00416025>

II. Khalil Challita and Hikmat Farhat(2011) ,"Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208,The Society of Digital Information and Wireless Communications, (ISSN2220-9085).

III. Shouchao Song, Jie Zhangb, Xin Liao, Jiao Du Qiaoyan Wen(2011), "A Novel Secure Communication Protocol Combining Steganography and Cryptography", 2011 Published by Elsevier Ltd. Selection and/or peerunder responsibility of [CEIS] In Advanced in Control Engineering and Information Science.

IV. Natarajan Meghanathan1 and Lopamudra Nayak," Steganalysis algorithms for detecting the Hidden information in image, audio and Video cover media", 2Jackson State University, 1400 Lynch St, Jackson, MS, USA

V. Dhawal Seth, L. Ramanathan(2010),"Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 8887) Volume 9 No.11, November.

VI. Sujay Narayana, Gaurav Prasad (December2010) "Two new approaches for secured image Steganography using Cryptographic Techniques and Type Conversions", Signal and Image Processing:An International Journal(SIPIJ)Vol.1,No.2,DOI: 10.5121/sipij.2010.1206 60

VII. A Aswathy Nair, Deepu Job(Jul 2014), "A Secure Dual Encryption Scheme CombinedWith Steganography" International Journal of Engineering Trends and Technology (IJETT) Volume 13 Number 5.