Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption

Thomas Leontin Philjon. J[#1], Venkateshvara Rao. N[#2]

[#]*Department of Information Technology, Kings Engineering College, Sriperumbudur, Chennai, India.*

[1]tom.lpj@gmail.com

[2]raosusi1969@yahoo.co.in

***Abstract*— Cryptography is the art of securing information by making sure that the secret can be understood only by the right person. Steganography is the process of sharing information in an undetectable way by making sure that nobody else can even detect the presence of a secret. If these two methods could be combined, it would provide a fool-proof security to information being communicated over a network. This paper fuses the two methods and a new technique – Metamorphic Cryptography is born. The message is transformed into a cipher image using a key, concealed into another image using Steganography by converting it into an intermediate text and finally transformed once again into an image. The proposed method thus achieves a high degree of security for information.**

***Keywords*— Metamorphic cryptography, Cryptography, Steganography, matrix multiplication, angular encryption, dynamic encryption, color key, cipher image, intermediate text, color key matrix, data matrix, paradox.**

I. INTRODUCTION

Information security is of utmost importance in today's fast developing era. Information or messages are being exchanged over various types of networks. 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. Communication is not secure due to the presence of hackers who wait for a chance to gain access to confidential data.

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 (plain text) by transforming it into unreadable format (cipher text) 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 [3].

Steganography is derived from the Greek word "stegnos" (meaning "covered/secret") and "graphein" (meaning "to write/draw") [1]. Steganography is 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 a remarkable trace is known as Steganography. Steganography is the form of convert communication in which a secret message is camouflaged with a carrier data. Steganography masks the very presence of communication, making the true message not discernable to the observer.

Cryptography and Steganography achieve the same goal using different means. Encryption encodes the data so that an unintended recipient cannot determine its intended meaning. Steganography in contrast attempts to prevent an unintended recipient from suspecting that the data is there [4]. The proposed method combines the two techniques (cryptography and steganography) to provide a very high degree of security for the data.

II. BACKGROUND

Besides cryptography, steganography can be employed to secure information in digital media. 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.

III. THE PROPOSED ENCRYPTION PARADOX TECHNIQUE

To a computer, an image file is simply a file that shows different colors and intensities of light on different areas of the image. We can represent an image in the form of matrix of pixels [2]. The method used in this paper is matrix multiplication using a color key along with angular encryption during the encryption process. 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 text. This intermediate text is once again encrypted using the encryption technique as proposed above to obtain another image which is the final image. This image is sent to the receiver through the network. The receiver obtains the image, decrypts it to obtain the intermediate text and analyses this text with the cover image to reconstruct the cipher image. This cipher image is once again decrypted to obtain the original message.

A. Selection of P(x, y)

The color key is taken and represented in a 3x3 matrix format by placing each digit of the R,G,B component of the color in each of the three rows. This matrix forms the color key matrix used during encryption. The original message (text) is resolved into individual characters. A specific point P(x, y) is selected on the image. Each encrypted character of the message (color pixel) is placed in the cipher image onto subsequent pixel co-ordinates starting from the first pixel. The number of the pixels (n) from the point P(x, y) to the current pixel to be set is calculated. If 'n' is greater than 255, modulo operation is performed to limit the value to 255. The value is Exclusively-ORed with the ASCII value of the character to be encrypted.

B. Angular Encryption

The angle (Θ) between the point P(x, y) on the image and the pixel to be set is found out by taking the angle between an imaginary line joining the end point of the image to the point P(x, y) and the imaginary line joining the point P(x, y) to the pixel to be set. Θ is taken as the value to perform shifting operation. The value obtained as the result of the Exclusive-OR operation between the ASCII value and 'n' is converted into 8-bit binary format and is shifted Θ times to the left. As the value of Θ and 'n' keep changing for every pixel in the image, dynamic encryption is obtained. The resulting value obtained is taken for matrix multiplication by representing it in a 1x3 matrix format. This matrix is the data matrix used for matrix multiplication. The color key matrix (3x3 matrix) is matrix multiplied with the data matrix (1x3 matrix) to obtain a 1x3 matrix. The elements corresponding to each row of this matrix is taken as the R,G,B value of pixel to be set.

The above process is repeated for the entire length of the message to obtain an image which is the cipher image (or) secret image. This process is depicted in Fig.1.

ALGORITHM ENCRYPTION

1: Input the message to be encrypted.
2: Input the color key.
3: Calculate the 3x3 color 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 character ⊕ n.
  5.5: Shift the 8-bit binary value Θ times to the left.
  5.6: Form the 1x3 data matrix.
  5.7: Perform matrix multiplication of the color key matrix and data matrix.
  5.8: Resolve into R,G,B values.
  5.9: Set the pixel in the image.
6: Obtain the full image.

END ENCRYPTION

Input: Message, Color key, P(x, y).
Output: Cipher image.

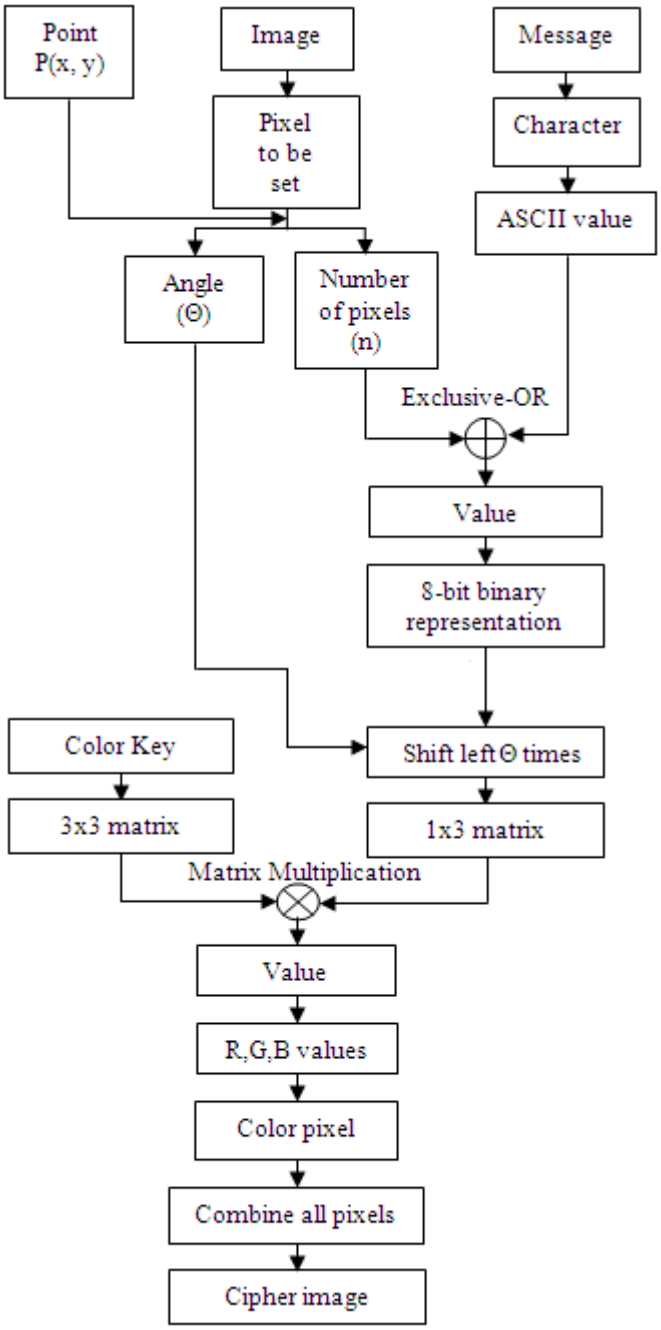

Fig.1. Block Diagram of Encryption

C. Steganography

A cover image is selected and it is used to perform steganographic process with the cipher image (or) secret image. This can be done by taking each pixel of the cipher image and Exclusively-ORing it with the corresponding pixel of the cover image. The process is done by splitting each pixel of the cipher image into R,G,B values and representing each value in its binary format of 8 bits. Similarly the corresponding pixel of the cover image is converted into its respective R,G,B values. Every component is represented in binary format of 8 bits. Each of the 8 bits of the R,G,B of the cipher image is Exclusively-ORed with the corresponding component of the cover image to obtain a resulting value of 8 bits for R (Red), 8 bits for G (Green), 8 bits for B (Blue). The 8 bit binary format is split into two parts thereby forming two 4 bits for each of the elements. The first part contains the first four most significant bits and the second part contains the remaining four least significant bits. We then use characters to represent the 4 bit binary values. If the binary value 0000 is denoted as 'A', 1111 as 'P' and intermediate values assigned with the respective letters of the alphabet, then the pixels can be converted into the form of text comprising of the letters from 'A' to 'P'. Letters 'A' to 'P' can be assigned to represent the values for the 'R' component of the pixel, 'a' to 'p' can be assigned to represent the binary values 0000 to 1111 for the 'G' component of the pixel and letters 'Q' to 'Z' can be used to represent binary values 0000 to 1001 while letters 'q', 'r', 's', 't', 'u', 'v' can be used to represent the remaining values 1010 to 1111 values of the 'B' component of the pixel. Thus every pixel of the cipher image is mapped to its cover image pixel and a character is obtained.

This method is done for the entire pixels in the cipher image to obtain a character for every pixel in the cipher image which is then combined to obtain the intermediate text. This process is depicted in Fig.2.

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 R,G,B values.
  3.2: Split the corresponding cover image pixels into their corresponding R,G,B values.
  3.3: Perform Exclusive-OR operation of the respective R,G,B values of the cipher image and cover image.
  3.4: Split the resulting value to 4-bit binary values for each R,G,B 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.

END STEGANOGRAPHY

Input: Cipher image, cover image.
Output: Intermediate text.

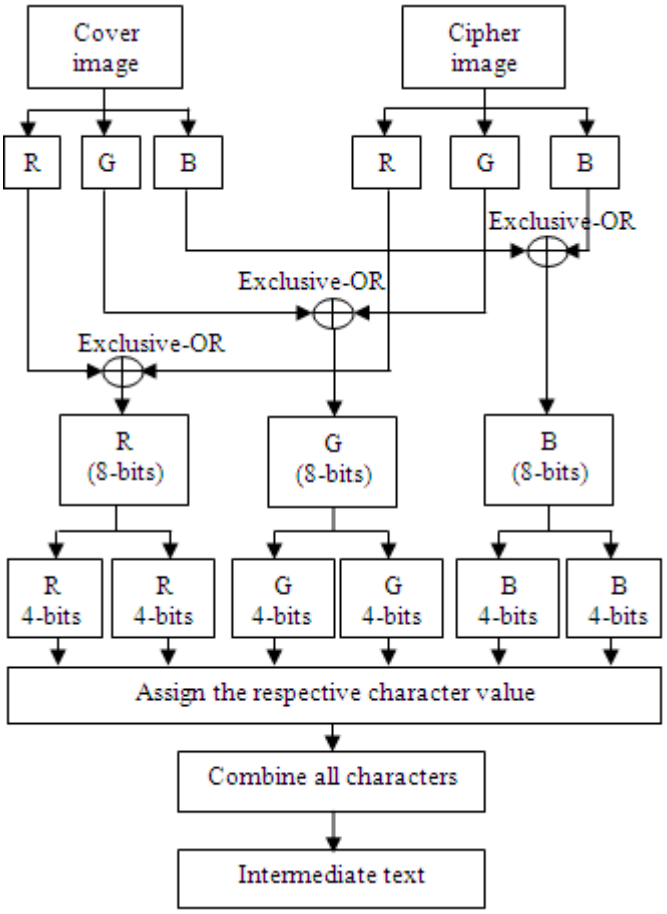

Fig.2. Block Diagram of Steganography

The intermediate text is once again encrypted using the procedure of ALGORITHM ENCRYPTION to obtain the final image. This image is sent to the receiver through the network. As this technique uses cryptography and steganography, this technique can also be called as a paradox between cryptography and steganography. As the image is doubly encrypted, a high level of security is obtained. This process is depicted in Fig.3.

ALGORITHM PARADOX_ENCRYPTION

1: Input the message to ALGORITHM ENCRYPTION.
2: Obtain the cipher image.
3: Input the cipher image to ALGORITHM STEGANOGRAPHY.
4: Obtain the intermediate text.
5: Load the intermediate text to ALGORITHM ENCRYPTION.
6: Obtain the final image to be transmitted.

END PARADOX_ENCRYPTION

Input: Message.
Output: Final image.

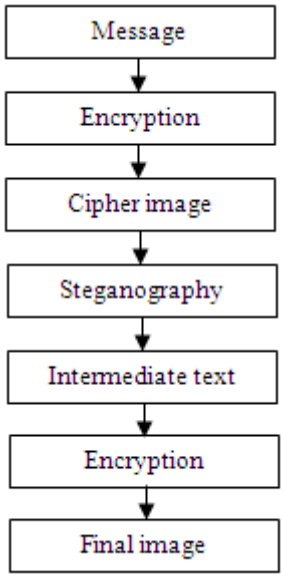

Fig.3. Block Diagram of the Paradox for Encryption

IV. THE PROPOSED DECRYPTION PARADOX TECHNIQUE

The receiver decrypts the image obtained by using its color key and specified point P(x, y). The color key is represented in the 3x3 matrix. It is then inverted to obtain the inverse of the color key matrix. Every pixel in the received image is represented as a 1x3 matrix by substituting each row element in the matrix with R,G,B values of the pixel. This 1x3 matrix is multiplied with the inverse of the color key matrix of size 3x3 to obtain a 1x3 matrix. The point P(x, y) is used as the reference to obtain the angle (Θ) and the number of pixels (n) between the current pixel to be decrypted and P(x, y). The value obtained as a result of matrix multiplication is represented in a 8-bit binary form and the value is shifted 'Θ' 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 process is depicted in Fig.4.

ALGORITHM DECRYPTION

1: Load the final image.
2: Input color key.
3: Calculate the 3x3 color key matrix.
4: Invert the color key matrix.
5: For every pixel in the final image
  5.1: Calculate the 1x3 data matrix from its R,G,B 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 color key matrix and the data matrix.
  5.5: Calculate Value = Shift the output of 5.4 'Θ' times to the right
  5.6: Calculate ASCII = Value⊕ n.
  5.7: Convert ASCII to its character equivalent.
6: Combine all the characters.
7: Obtain the intermediate text.

END DECRYPTION

Input: Final image, color key, P(x, y).
Output: Intermediate text.

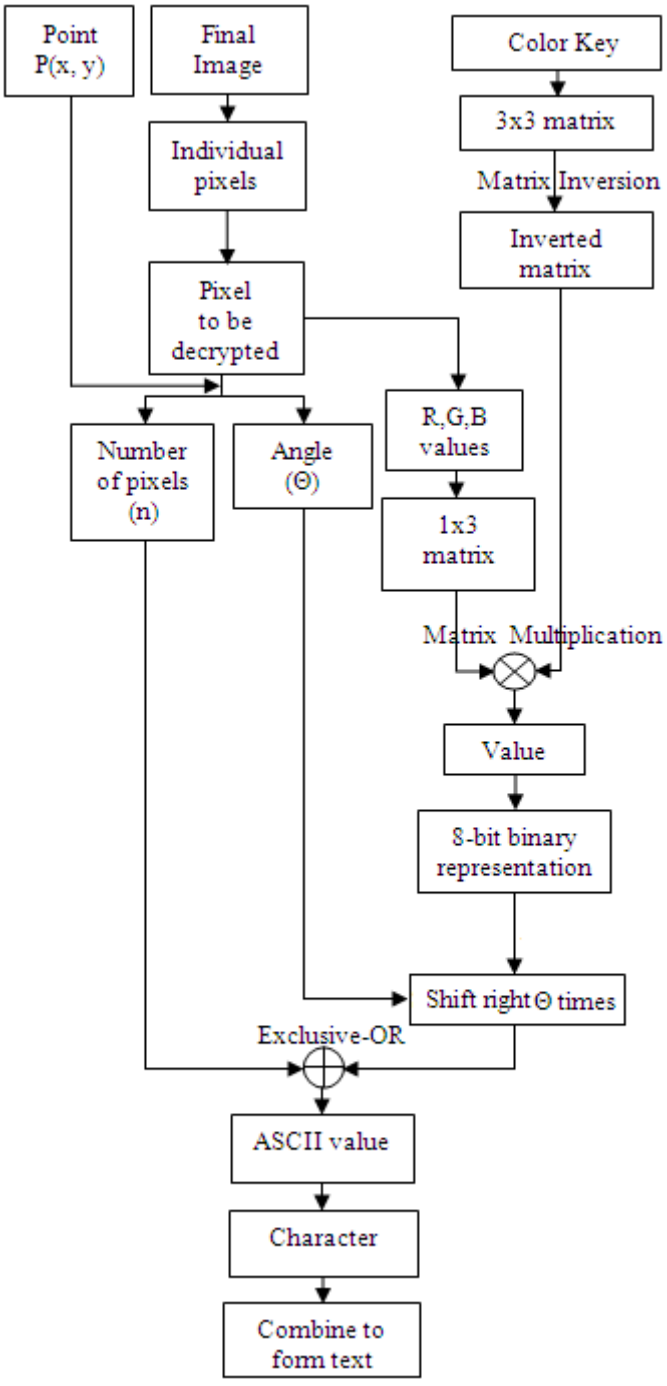

Fig.4. Block Diagram of Decryption

Every two characters of the intermediate text correspond to the values of each of the components (R,G,B) of a pixel. Each character has a 4-bit binary code which is associated with it. This code is assigned to the text by making use of reverse of the mapping process as used during encryption. The binary value 0000 is assigned to 'A', 1111 to 'P' and intermediate binary values are assigned to the respective letters of the alphabet. The text can thus be converted into the form of binary comprising of the values from 0000 to 1111 for every character in the text. Binary values 0000 to 1111 are assigned for characters 'A' to 'P' in the intermediate text to represent the values for the 'R' component of the pixel, binary values 0000 to 1111 are assigned for characters 'a' to 'p' in the intermediate text to represent the values for the 'G' component of the pixel and binary values 0000 to 1001 are assigned for characters 'Q' to 'Z' while the remaining values 1010 to 1111 are assigned for characters 'q', 'r', 's', 't', 'u', 'v' in the intermediate text to represent the values of the 'B' component of the pixel. The values are then grouped into groups of two 4-bit binary values to obtain an 8-bit binary value. An 8-bit binary value corresponds to a component (R or G or B) of the pixel in the cipher image. These binary values are grouped into groups of three 8-bits (3x8=24 bits) to represent the R,G,B values for a single pixel which is reconstructed from the intermediate text. The copy of the cover image present in the receiver end is resolved into 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 is done for the entire length of the intermediate text. The cipher image is constructed by plotting the corresponding pixel values in the image. This process is depicted in Fig.5.

ALGORITHM RETRIEVAL_CIPHERIMAGE

1: Input the cover image.
2: Input intermediate text.
3: For every character in the intermediate text
  3.1: Assign the respective character codes.
  3.2: Combine two successive 4-bit binary character codes to obtain an 8-bit binary value.
  3.3: Split the cover image into the respective pixels and resolve the R,G,B values for each pixel.
  3.4: Perform Exclusive-OR operation of 8-bit character codes and the respective R,G,B values for the corresponding pixels.
  3.5: Set the corresponding pixel in the image using the output obtained.
4: Obtain the cipher image.

END RETRIEVAL_CIPHERIMAGE

Input: Cover image, intermediate text.
Output: Cipher image.

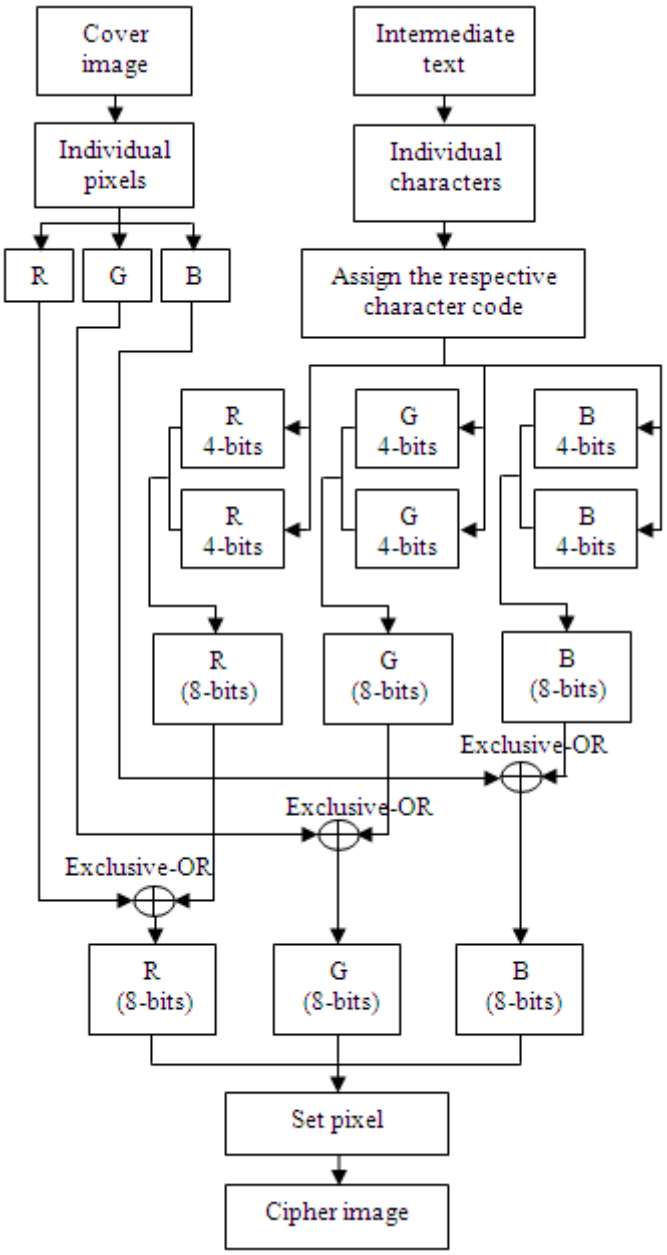

Fig.5. Block Diagram of Retrieval of cipher image

The cipher image is once again decrypted using the procedure of ALGORITHM DECRYPTION as described above to obtain the original message. As this technique uses cryptography and steganography, this technique can also be called as a paradox between cryptography and steganography. Thus a very high level of security is obtained.The decryption paradox process is depicted in Fig.6.

ALGORITHM PARADOX_DECRYPTION

1: Input the final image to ALGORITHM DECRYPTION.
2: Obtain the intermediate text.
3: Input the intermediate text to ALGORITHM RETRIEVAL_CIPHERIMAGE.
4: Obtain the cipher image.

5: Input the cipher image to ALGORITHM DECRYPTION.
6: Obtain the original message.

END PARADOX_DECRYPTION

Input: Final image.
Output: Original Message.

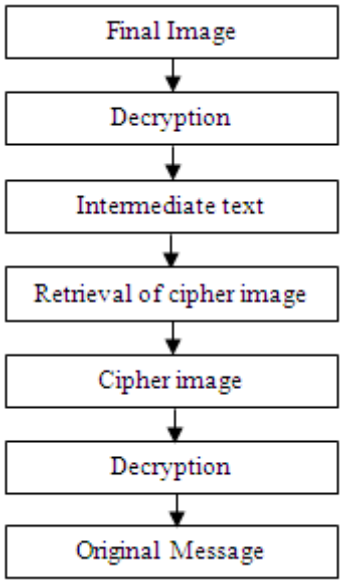

Fig.6. Block Diagram of the Paradox for Decryption

Thus the original message is obtained at the receiver end.

V. Experimental Results

The encryption paradox method stated above was applied to a message shown in Fig.7. The cover image used for the process is shown in Fig.8. The encrypted results were obtained as shown in Fig.9, Fig.10 and Fig.11.

The image in Fig.11 was decrypted using the decryption paradox technique to obtain the decrypted outputs as shown in Fig.12, Fig.13 and Fig.14.

Meet me tomorrow.
At 9.00 a.m.

Fig.7. Message to be encrypted.

Fig.8. Cover image.

Fig.9. Cipher image.

KOlpuqGPiitQJMkktXPGphvqOEohvRKOlmuVJDkgttIBjht
XIBjetQIBjhtXMJmpuVGGhpsrIBjitYGPihsuKOljtvGPihsuN
CnkvQNLocvUMAmjuX
OEojvXKOlktvKFlatZKFlfuSKFlfuTOEokvZOEohvSKOlpur
PGpivrKFlatZIBjhtXIKjotZPGpivt

Fig.10.Intermediate Text.

Fig.11. Final Image

KOlpuqGPiitQJMkktXPGphvqOEohvRKOlmuVJDkgttIBjht
XIBjetQIBjhtXMJmpuVGGhpsrIBjitYGPihsuKOljtvGPihsuN
CnkvQNLocvUMAmjuX
OEojvXKOlktvKFlatZKFlfuSKFlfuTOEokvZOEohvSKOlpur
PGpivrKFlatZIBjhtXIKjotZPGpivt

Fig.12. Intermediate Text after decryption

Fig.13.Cipher image after decryption

Meet me tomorrow.
At 9.00 a.m.

Fig.14. Decrypted Original Message.

VI. Conclusions

Unlike the existing cryptographic systems, where only the cryptographic or steganographic techniques are explored, the proposed paradoxical approach explores the techniques in both cryptography and steganography. Portable Network Graphics format is used to save the images as they consume little space even when the size of the image is drastically increased. This prevents the problem of traffic in the network which arises when the size of the data to be transmitted securely is 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.

Acknowledgment

We are thankful to our parents to whom we are greatly indebted for their support and encouragement.

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.2010.120660
[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.