International Research Journal of Computer Science (IRJCS)
Issue 2, Volume 2 (February 2015)
ISSN: 2393-9842
www.irjcs.com

The New Cryptography Algorithm with Dynamic Steganography

Gaurav Sawant, Kuldeep Jadeja, Kunal Bhat, Prof. Jignasha Dalal
Department of Computer Engineering,KJSIEIT
Ayurvihar Complex, Everard Nagar, Sion, Mumbai 400022
Maharashtra, India

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 text using a key, concealed into another image using Steganography. The proposed method thus achieves a high degree of security for information.
Keywords— ISB, BPP, PSNR

I. INTRODUCTION

In today's world there is an emphatic need of Security as we can certainly say nothing is secure. Talking with respect to Computers, various types of essential report files and folders are stored on it. Many Organizations, Schools, Colleges have their important data stored in file system. Only the authorized person is needed to have an access to that file System. Whenever an unauthorized person gets an access to those files, we don't have any idea what all things he can do with that data. 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 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. The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption. 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 the remarkable trace is known as Steganography. This 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.

II. BACKGROUND AND MOTIVATION

The project 'The New Cryptography Algorithm with Dynamic Steganography' aims at providing a strong, fortified application based on the new cryptography algorithm and Dynamic Steganography technique which can provide complete security to any kind of text that can be communicated over network. This security tool or application promises to provide a feature with which user can send his High confidential data in completely secure environment i.e. security cage. This project mainly aims at preventing any kind of unauthorized manipulation and threats in system.

III. PROBLEM STATEMENT

The most of the Security techniques are used independently in a stand-alone manner like Cryptography, Steganography. This application encompasses various Security techniques like Cryptographic Mechanism, Passing messages via Fake Image, Folder Locking, File Hiding, Preventing SQL injection, etc under One Roof.

IV. REVIEW OF LITERATURE

A. Metamorphic Cryptography – A paradox between Cryptography and Steganography

Cryptography encrypts the actual message that is being sent. This mechanism employs mathematical schemes and algorithms to scramble data in to unreadable text. It can only be decoded or decrypted by the party that possesses the associated key. To a computer, an image file is simply a file that shows different colours and intensities of light on different areas of the image. We can represent an image in the form of matrix of pixels. The method used in this paper is matrix multiplication using a colours 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.

1. Selection of P(x, y)

The colours key is taken and represented in a 3x3 matrix format by placing each digit of the R,G,B component of the colours in each of the three rows. This matrix forms the colours 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 (colours 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.

2. Angular Encryption

The angle 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 .Angle 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 times to the left. As the value of 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 colours 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 colours key.
3: Calculate the 3x3 colours 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 = 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 times to the left.
5.6: Form the 1x3 data matrix.
5.7: Perform matrix multiplication of the colours 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, Colours key, P(x, y).

Output: Cipher image.

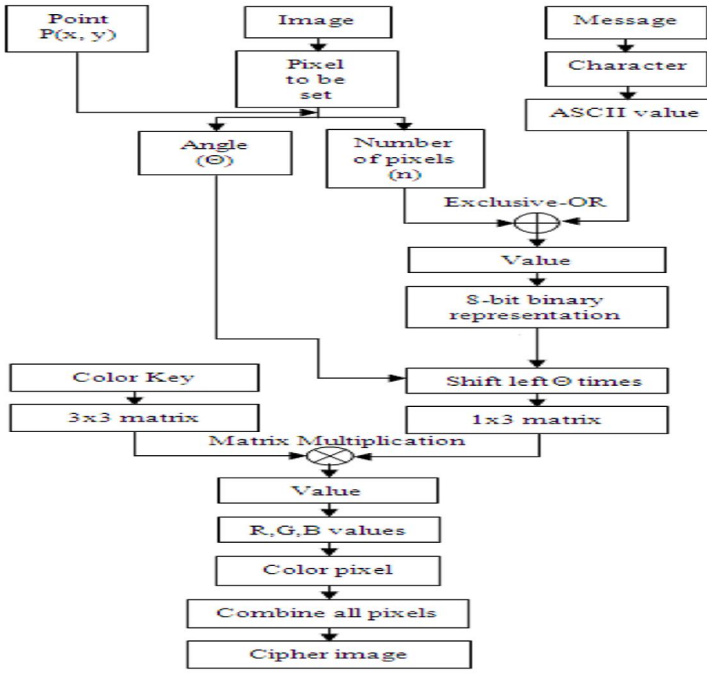

Fig.1. Block Diagram of Encryption

3. Steganography

A cover image is selected and it is used to perform 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.

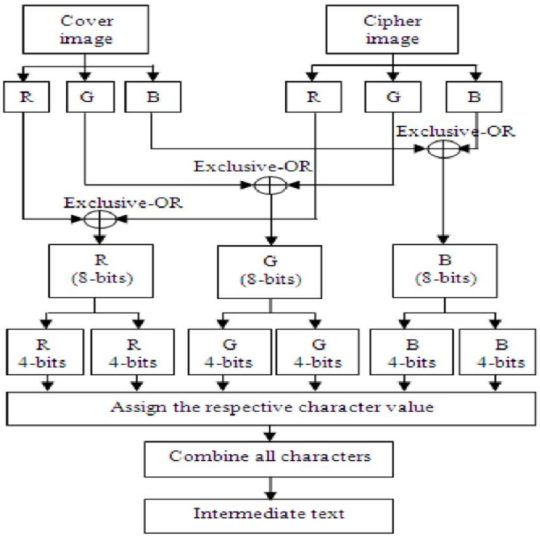

Fig.2. Block Diagram of Steganography

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.

B. Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganography Technique

The Cover image is prepared for data embedding by breaking it into its constituent bit planes. The technique used behind data embedding in the proposed system is, more significant the bit plane, lesser the amount of data embedded in it. The technique used in this paper ensures better perceptual qualities of the stego image. As such data to be embedded in the bit planes has been divided into three variable length data vectors of continuously decreasing lengths. The data vector with total length is divided into three variable length data vectors, viz: and of continuously decreasing magnitude. The data is embedded in the first three ISB planes under the control of a private key. In order to thwart the adversary data is not embedded sequentially. The key, which is generated using Pseudo Random Number Generator, ensures a highly randomized data embedding in the three given bit planes. The embedding process is carried out in data embedder, that outputs an image containing secret data and is generally termed as stego-image. The security of data embedded is a function of Key Length. Thus used pseudo random number generator is capable of addressing all the locations in first three Intermediate Significant Bit planes where data is to be embedded.

Embedding Strategy and relationship between length of data vector: The proposed data hiding system, breaks the data vector to be embedded, in smaller size vectors equal, in number to the number of ISB planes in which data is to be hidden. The lengths of data vectors can be related in several ways. In the implemented technique the data has been broken into three blocks with lengths L1, L2 and L3. This is because data is to be embedded in three ISBs. The relation between the lengths of data blocks is L1= L/2, L2= 3L/8 and L3=L/8; where L is the total length of data vector to be embedded in the cover medium. The data is embedded in the embedder under the control of a private key.

Extraction Strategy: The embedding algorithm uses private key to embed the data in the ISBs of cover image. The resultant image yielded by data embedder is called stego image. At the receiving end the extraction algorithm uses stego-image along with same key as that used at embedder to extract data from the stego-image. Since cover image is not needed for the retrieval of secret data the proposed system falls in the category of blind detection.

The requirements of a data hiding system when used for stegnographic purposes are of two fold viz, high hiding capacity and imperceptibility. The two parameters unfortunately are of opposing nature. This is because embedding more and more data in a cover image results in deterioration of the cover image quality, and as such an adversary could easily guess that some data has been embedded in the cover image. Keeping in view these conflicting features a reasonable amount of data has been taken to be embedded in the cover medium so as to keep degradation in the image quality minimum. For the testing the efficacy of the proposed scheme a set of nine standard grey scale test images (512 x512) were used. Table 1 shows all the used test images with their corresponding stego-image, besides showing hiding capacity (HC) also termed as payload and PSNR in decibels in each case.

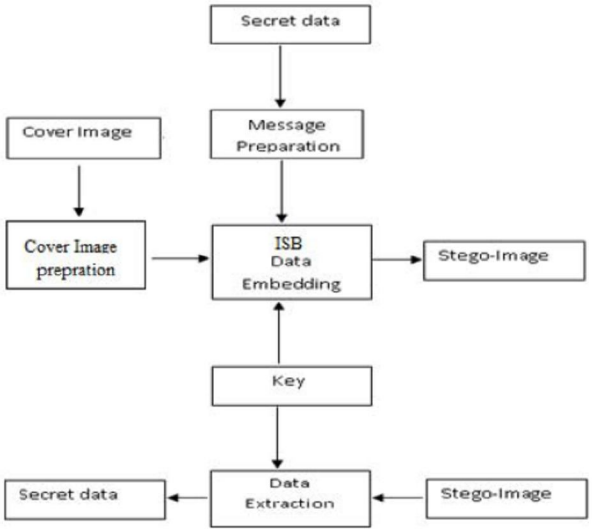

Fig. 1: Proposed high capacity data hiding and corresponding blind extraction system

In all cases the embedding capacity has been fixed as at 25% that comes out to be (262144x2 bits of payload) except test image 'lake' where the payload of 31.25% has been choosen. Further a comparison of the proposed data hiding scheme with that of Zeki et. al [16] can be seen in table 2. Table 3 shows graphical comparison between the proposed technique and that of Zeki et. al. The hiding Capacity (HC) and PSNR have been calculated as follows.

Hiding Capacity(HC): The amount of data that can be embedded in a cover image without deteriorating integrity of the cover image gives an idea about the hiding capacity. It is also referred to as payload. Hiding capacity is represented by bits per pixel (bpp). It is given by (total number message bits/total number of image bits)
multiplied by 100. If n and N respectively denote total message bits and image bits the hiding capacity is given by

Hiding Capacity (HC) = (n/N)*100

B. Peak Signal to Noise Ratio (PSNR): It is an important image, objective, quality index. It is actually a measure of quality of image when external data is embedded in it. It gives an idea about how much deterioration has embedding caused to the image.

It is represented as

$$PSNR = 10\log_{10}\frac{255^2}{mse}\,db$$

Where 'mse' is mean square error and is given by

$$mse = \left[\frac{1}{N*M}\right]^2 \sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} - \bar{X}_{ij})$$

Where N and M are image dimensions, X and $\overline{X}$ represent original and stego images respectively.
The data to be embedded in the cover medium has been divided into three variable length data vectors. The data vectors are subsequently embedded in first three ISB planes using a private key generated by Pseudo Random Number Generator (PNRG). The PRNG not only embeds data pseudo randomly in various bit planes but it also ensures pseudorandom embedding of data at various pixel locations, thus providing an adequate security to the data carried by the cover image.

C. The New Cryptography Algorithm with Dynamic Steganography

This paper uses New Cryptography Algorithm for Cryptography and Dynamic Steganography Technique for Steganography.

New Cryptography Algorithm:-

In this paper at first new cryptography (Encryption and Decryption) algorithm has been generated and new cryptography (Encryption and Decryption) algorithm has been compared by using some components like throughput of key generation, to generate Encryption text and to generate Decryption text. If any brute force attacks are applied on this algorithm, how much security is provided by this algorithm is included. In this algorithm some arithmetic and logical mathematical operations are performed.

IV. PROPOSED SYSTEM

We have surveyed and studied all the above methods and have decided to implement and do some more work on the method mentioned in the last paper that is, The new Cryptography algorithm with dynamic steganagraphy which is based on Arithmetic and Logical operation.
In this algorithm, the block size is 128 bits with 128 bits key size. Simple arithmetical and logical operations are used like logical XOR and Shifting. In this algorithm starting and ending 3-4 steps are executed only one time but among these few steps repeat n times. These steps are not fixed that how many times they are executed? So, if attackers know about the algorithm, they cannot assume that how many times steps are executed. So, security compare to other encryption algorithm is increased.

The new Cryptography algorithm:-

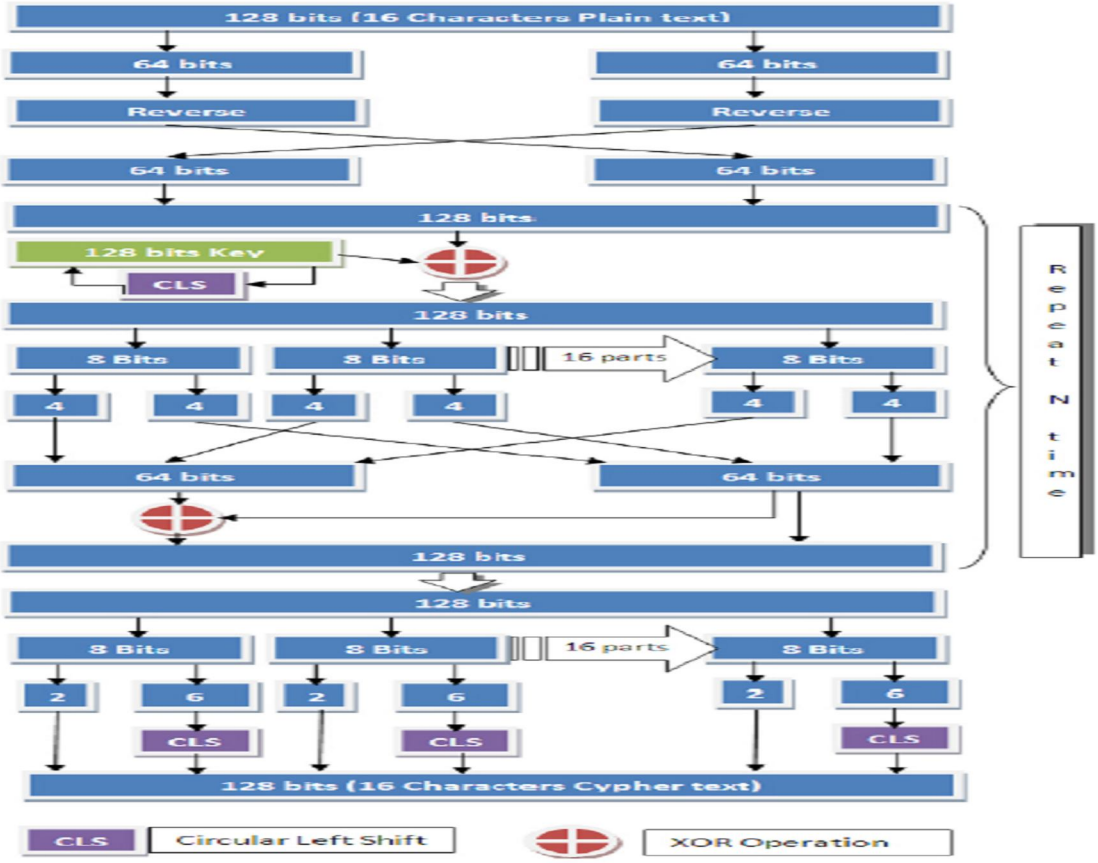

Figure 2. Encryption Algorithm

The steps of encryption and decryption algorithms are as following.

1) Steps of Encryption:

a) Convert 16 characters plain text in binary format (128 bits). Per character 8 bits.
b) Divide 128 bits plain text into two 64 bits separately.
c) Arrange both 64 bits in reverse order.
d) Merge both part and apply XOR operation with 128 bits of key (first convert key in binary form of 128 bits). And perform circular left shift operation on key for second round.
e) Divide 128 bits of result into 16 parts each of 8bits.
f) Divide each of the 8bits into two parts each of 4 bits.
g) Collect all the left 4 bits part and right 4 bits part in two 64-64 bits respectively.
h) Now apply XOR operation on left and right 64 bits and store the result in left 64 bits. And keep the right 64 bits as it is (no change in right 64 bits).
i) Combine both 64 bits into 128 bits format (Repeat N time from step no 4).
j) Now divide 128 bits into 16 parts each of 8bits.
k) Divide each of the 8bits into two parts of 2 bits and 6 bits respectively.
l) Perform circular left shift operation on all 6 bits.
m) Combine all parts - and get 128 bit (16 characters) of cipher text.

2) Steps of Decryption:

a) Convert 16 characters cipher text in binary format (128 bits).
b) Divide 128 bits into 16 parts each of 8bits.
c) Divide each of the 8 bits in two parts of 2 bits and 6 bits respectively.
d) Perform circular right shift operation on all 6 bits.
e) Combine all parts and get 128 bits.
f) Now apply XOR operation on left and right 64 bits and store result in left 64 bits. And keep the right 64 bits as it is (no change in right 64 bits).
g) Now divide 128 bits into 16 parts each of 8 bits.
h) Divide each of 8 bits into two parts each of 4 bits.
i) Collect all the left 4 bits part and right 4 bits part in two 64-64 bits respectively.
j) Combine both 64bits into 128 bits format
k) Merge both part and apply XOR operation with 128 bits of key (key convert at first in binary form). And perform circular rightshift operation on key for second round (Repeat N time from step no. 6)
l) Divided 128 bits plain text into two parts each of 64 bits.
m) Arrange reverse order of both 64 bits and combine both 64 bit parts, plain text in form of 16 characters and 128 bits is generated.

There are lots of encryption algorithms available in cryptography area. In which AES, DES, 3DES and Blowfish algorithms are very much popular. So, in my work, my algorithm is compared with all these algorithms. In these all algorithms different types of operations are performed like bitwise XOR, Substitution, Shifting and many more. Let's see the methods of other encryption algorithm.

AES (Advanced Encryption Standard): also called variant of Rijndael Algorithm, has 128 bits block size with 128(with 10 cycles of repeating), 192(with 12 cycles of repeating) or 256(with 14 cycles of repeating) bits of key size. Brute force attack can unlock the AES algorithm . In this attack algorithm attacker use dictionary of words in English and find out the words which is used as key.
DES (Data Encryption Standard): has 64 bits of block of plain text with 56 bits of key. The main problem is the small size of key. By using attack algorithm on DES, attacker can get plain text.
3DES (Triple Data Encryption Standard): is upgraded version of DES. The steps of 3DES algorithm are similar as in simple DES but encryption level is increased by 3 times. After increasing 3 times encryption level, 3DES is very much slower than other encryption method. There are so many issues found during study of all algorithms. Like…

1) The more complex structure of algorithm increases the time of execution. So the structure of algorithm should be simple to make algorithm faster.
2) The longer the length of key provides higher security as compare to shorter length of key and also increase the speed of execution of algorithm.

3) The overall performance of any algorithm depends upon selection of mathematical and/or logical operations applied on plain text, key and cipher text. In my algorithm, all this issues are considered to improve the performance of encryption algorithm.

Dynamic Steganography:-

The Cipher Text generated by New Cryptography algorithm is Embedded into cover image using Dynamic Steganography which is explained as follows:-

The Embedding Technique:-

The cover image is converted to binary. Each pixel becomes one byte. The length of cipher text is computed, say it is L. Some 3000 pixels at the beginning of the image are not disturbed as these pixels may carry the image characteristics. Then another 300 pixels are reserved for hiding L. Thus the embedding of cipher text bits starts from 3301th pixel. The embedding procedure is as discussed in the following steps.

Step1:Embed L in the reserved pixels (starting from 3001th pixel upto 3300th pixel) using two least significant bit locations. Embed the first two bits of cipher text at 7th and 8th bit locations of 3301th pixel. Take next two bits of cipher text. Set i= 3301. Set L= L -2.

Step2: Do any of the four sub steps (a) through (d) (a) If the two bits of cipher text embedded at the ith pixel of image are 00; then the next two bits of cipher text will be embedded in 7th and 8th bit locations of the (i+1)th pixel of the image. (b) If the two bits of cipher text embedded at the ith pixel of image are 01; then the next two bits of cipher text will be embedded in 8th and 7th bit locations of the (i+1)th pixel of the image (c) If the two bits of cipher text embedded at the ith pixel of image are 10; then the next two bits of cipher text will be embedded in 6th and 7th bit locations of the (i+1)th pixel of the image. (d) If the two bits of cipher text embedded at the ith pixel of image are 11; then the next two bits of cipher text will be embedded in 7th and 6th bit locations of the (i+1)th pixel of the image.

Step3: Set i= i+1 and L=L-2. If (L=0) goto step4, otherwise take the next two bits of cipher text and go to step2.

Step4: Stop.

The Retrieving Technique:-

Step1: Compute the length of the embedded message L by retrieving bits from the reserved pixels. Retrieve the first two cipher text bits from the 7th and 8th bit location of the 3301th pixel. Initialize the variable CIPHER with these two bits. Set L=L-2. Initialize i=3301.

Step2: Do any one of the four sub steps (a) through (d) (a) If the retrieved bits from the ith pixel are 11, then retrieve 7th and 6th bits from the (i+1)th pixel. (b) If the retrieved bits from the ith pixel are 10, then retrieve 6th and 7th bits from the (i+1)th pixel . (c) If the retrieved bits from the ith pixel are 01, then retrieve 8th and 7th bits from the (i+1)th pixel. (d) If the retrieved bits from the ith pixel are 00, then retrieve 7th and 8th bits from the (i+1)th pixel.

Step3: Append these two retrieved bits to the variable CIPHER. Set L=L-2.

Step4: if (L >0) go to step2, otherwise go to step5.

Step5:Stop

V. CONCLUSION

The Technique used in the system is unique and strong approach of doing Steganography with images. It provides two level of security one at the cryptography level and other at the steganography level. The cryptography is implemented with the help of new cryptography algorithm and steganography follows cipher text dependent embedding. After embedding cipher text into image the degradation in image quality is not noticeable by human visual system. Thus high level of security can be achieved.

VI. REFERENCES

[1] A Survey on Metamorphic Cryptography Techniques, International Journal of Research in Advent Technology, Vol.2, No.7, July 2014 E-ISSN: 2321-9637

[2] A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography, International Journal of Security and Its Applications, Vol. 6, No. 2, April, 2012

[3] A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique Anil Kumar *, Rohini Sharma

[4] Application Of a Large Key Cipher In a Image Steganography by Exploring The Darkest and The Brightest Pixels. Gandharba Swain1 and Saroj Kumar Lenka2

[5] Metamorphic Cryptography -A Paradox between Cryptography and Steganography Using Dynamic Encryption Thomas Leontin Philjon. J#1, Venkateshvara Rao. N#2

