A STATISTICS HIDING SCHEME BASED ON SCRAMBLING ENCRYPTION WITH REFERENCE PPM TECHNIQUE.

A.Ramya, S.Selvi, R.Vasanthi , B.Hema
1. Students, Department of ECE, Kalasalingam Institute of Technology, Krishnankoil
2. Ass-Proferror, Department of ECE, Kalasalingam Institute of Technology, Krishnankoil

ABSTRACT--*Steganography and Cryptography are two popular way of sending information in a secret way. The secret information to be transmitted is first encrypted into unreadable information using cryptography technique which is performed using chaotic algorithm.Next the encrypted information is covered with an image is known as stego-image.Finally the stego-image can be transmitted without revealing the secret information by the process called steganography which is performed by using APPM.Thus by using this two method we can achieve a secure communication.*

INDEX:Scrambling encryption, adaptive arithmetic coding, mapping, assembler, encrypting data, embedding, extraction and decryption.

I.INTRODUCTION:

In order to transmit the information securely two kinds of techniques are used such as cryptography and steganography. Cryptography is the science of using mathematics to encrypt and decrypt information. Steganography is used to hide the message under image is known as stego image . Algorithms used for cryptography are AES,RSA but they cannot be used for real time applications. Steganography takes place in spatial domain provide high payload and invisibility.LSB substitution and OPAP these algorithms modifies the cover pixel for data embedding. In EMD and DE a single bit data is embedded into a pair of pixels present in the cover image.PPM is one of the latest technique where a pair of pixel is hidden into a single bit.

By joining encryption and steganogaphy the security of data transmission is obtained. Here additional key is added to increase the strength of transmission . By using this technique the stages of security improved , provide high payload, well suited for real time application and high protection.

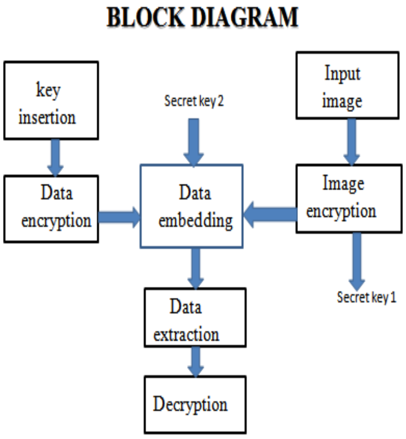
II.RELATED WORK:

Steganography with cryptography gives extra protection to the information. The steganographic technique afford stegoimage identical to the original image. The pixel value is adjusted in OPAP process.PVD method is used to calculate the difference between two pixel so that it is easy to find how many undisclosed bit can be inserted into cover pixel. Here the logistic map of 1-dimensional map is used in the interval [0 1].

$$\mathbf{X_i=\mu*X_{i-1}(1-X_{i-1}) \text{ where } 0\leq\mu\leq4 \text{ ......(1)}}$$

III.PROPOSED METHOD:

Some of the methodologies used in the proposed method are image encryption, data encryption, key evaluation, data emdebbing, data extraction and decryption.



ENCRYPTION:

In image encryption, the image is scrambled into unreadable format through three ways such as mapping, assembler and permutation. A map in computer terms is a relationship between one "value" and another "value". The Map is an advanced data type that allows you to assign a value with a "key”. The key is often a string, but could be any type of data. Permutation is stored in one dimensional array of size equal to the permutation size . The process involves three consecutive steps are initialize(),eliminate() and fill().In the first step ,ASCII code of element is obtained all the values are entered in the range 1 to N.In the second step the repeated value are replaced with zero. An assembler is a program that takes basic computer instructions and converts them into a pattern of bits that the computer's processor can use to perform its basic operations.

Both encryption and scrambling are based on chaotic sequence. Data Encryption is a widely-used method of data encryption using a private (secret) key .For each given message, the key is selected on random way from the massive number of keys. In the private key cryptographic methods, both the sender and the receiver must recognize and employ the similar key. In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text .The length of the key is a characteristic in considering how difficult it will be to decrypt the text in a given message. DES takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length.

EMBEDDING:

Image encryption and data encryption combined by data embedding, which is used by Adaptive Arithmetic coding. Arithmetic code is used to embed encrypted image with encrypted data with LSB. The reverse process of embedding and decryption is used to extract the data.

IV.PROCEDURE FOR THE PROPOSED SYSTEM:

In the proposed technique we hide the message in an image with the help of three secret keys.

1. The input image is given as input first.

2.Next the image encrypted while encrypting the pixels are mapped.

3.Random permutation process takes place it can be either row wise or column wise.

4.Assembler is a program that takes basic computer instructions and converts them into a pattern of bits that the computer's processor can use to perform its basic operations.

5.Then the encrypted image combined with encrypted data along with newly inserted key are embedded.

6. Finally, the original data is obtained after undergoing extraction and decryption process.

The receiver cannot get back the data until they know the algorithm applied for encryption and embedding. If any external person hack the data they can get only the embed key other two keys are unavailable . So that the secret data is transmitted securely .

V.RESULTS & ANALYSIS:

Here additional key is included for security purpose .Because of this MSE value is reduced which increase the quality of stegoimage.

Peak Signal to Noise Ratio (PSNR):-The PSNR is calculated using the equation,

$$PSNR = 10 \log_{10}\left(\frac{I_{\max}^{2}}{MSE}\right) dB$$

where I_{max} is the intensity value of each pixel which is equal to 255 for 8 bit gray scale images.

Mean Square Error (MSE):-

The MSE is calculated using the equation,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{i,j} - Y_{i,j}\right)^{2}$$

where M and N denote the pixels in the row wise and the column wise dimensions of the image Xi, j represents the pixels in the original image and Yi, j, represents the pixels of the stego image.

Type–image	**MSE**	**PSNR(db)**
Lena	0.0432	61
Boat	0.0435	62.5
Cameraman	0.044	62
Jet	0.010	68
Barbara	0.044	62
Elaine	0.0435	61.5

VI .CONCLUSION:

In this paper we have combined cryptography and steganography with extra key therefore that the data more safe also the MSE value is reduced.This technique is suited for real time application such as defence,banking,modern printer,government agencies and electronic money.It provides high payload and highly protected transmission.

REFERENCES:

[1] N. K.Pareek, Vinod Patidar ,K.K.Sud, (2006),"Image encryption using chaotic logistic map" ,IEEE Transactions on image and vision computing, vol. 24, no. 9, pp. 926-934.

[2] RakeshS,AjitkumarA,Kallar,Shadakshari B.C AnnappaB, (20 12) "Image encryption using block based uniform scrambling and chaotic logistic mapping "International Journal on Cryptography and Information Security (IJCIS),VoI.2, No.1.pp-49-57.

[3] C.K.Chan and L. M. Cheng, (2004), "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469-474, 2004.

[4] Xinpeng Zhang and Shuozhong Wang , (2006)"Efficient steganographic embedding by exploiting modification direction" IEEE Commun. Lett., vol. 10, no. 11,pp. 781-783, Nov.

[5] Andrew Ker, (2005) "steganalysis of LSB matching in grayscale images" IEEE signal processing letters , vol. 12, no. 6, pp. 441-444, Jun.

[6] R.M.Chao, H.C.Wu, C.C.Lee and Y.P.Chu (2009)" A novel image data hiding scheme with diamond encoding" EURASIPJ.Inf.Security,DOI.0.1155/2009/658047, Article I D 658047.

[7] Wien Hong and Tung-Shou ehen , (2012), "A noval data embedding method using adaptive pixel pair matching "IEEE
transactions on IEEE transactions on information forensics and security, vol. 7, NmblingO.l,February.