Design a New Robustness Technique for Image Stenography

Monika Gambhir[1], Amandeep kaur[2], Manpreet Kaur[3]
1Assistant Professor in Department of Electronics and Communication Engineering, N.C.C.E Panipat, India
2Student in Department of Electronics and Communication Engineering, N.C.C.E Panipat, India
3Student in Department of Electronics and Communication Engineering, N.I T Kuruksherta, India

ABSTRACT
We propose the secret and robust data transmission over the noisy channel. The secret data is encrypted and permutated using the permutation function, further encoded the data using the error detection and correction code. We show that the good quality of the stego-image and resistant against the various noise attacks (Like Salt and Pepper). Although we covered a number of security and capacity and robustness definitions, there has been no work successfully formulating the relationship between the two from the practical point of view. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. Robustness of steganography is one of the three main goals to be achieved. In this paper we increase the robustness by introducing some error detecting and correcting techniques.

Keywords
Steganography, Cryptography, Permutation function, and Error correction and detection code.

I. INTRODUCTION
Steganography provides digital way to keep the data secure. The Steganography consists of techniques to allow the communication between two persons. It hides not only the contents but also the existence of the communication in the eyes of any observer. These techniques use a second perceptible message, with meaning disjoined by the secret message. This second message works as a "Trojan horse", and is a container of the first one. The new technologies and, in special way, the information networks require more and more sophisticated strategies in order to prevent the message privacy. In this context, digital images and audio is excellent candidate to turn into containers of the messages, since the bits of a secret text message can be superimposed, as slight noise, to the bits employed for coding a digital image. Steganography refers to the science of invisible communication.Unlike cryptography, where the goal is to secure communications from an eaves-dropper, steganographic

steganographic techniques strive to hide the very

presence of the message itself from an observer techniques strive to hide the very presence of the message itself from an observer. There are two methods

Of performing steganography, one in spatial domain, and the other in frequency domain. Each technique has its own advantage and disadvantage. In the spatial domain , we can simply insert data into host image by changing the gray levels of some pixels in the host image, but the inserted information may be easily detected using computer analysis. In the frequency domain, we can insert data into the coefficients of a transformed image, for example using discrete Fourier transform (DFT), discrete cosine transform (DCT) and discrete wavelet transform (DWT). But we cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly.

The convolutional codes are the good error detection and correction code, which is using the concept of the interleaving. This Paper is organized as follows. In Section 2, we discuss about the Advanced Encryption Standard [AES] which is used for encryption of the secret data. In Section 3, we discuss about the proposed scheme. The Conclusion and discussion is in Section 4.

II.ADVANCED ENCRYPTION STANDARD (AES)
The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits

This is used to encrypt the secret data by the administrator. We fix the block size and key size to 128 bit.

We consider the 10 round versions. We use the following notations.

Let for all round index i = 0,…. ,10 and byte

index j = 0,…. ,15:

XJi: j th text byte of i-th round (in particular), Xi0 is the initial input plain text byte and is fixed

XJ.11: j th cipher text byte.

KJi.: j th expanded key byte of i-th round (in particular)

K0j is the user defined key:

K0j; :(ko, kl, k2 ...k15)

MKJi.: jth modified inverse expanded key byte of i-the round

W[i] = i-th key word of 32 bits.

kn: nth keybyte, n= {0,1,2,…. ,175}

Nk = (Key size)/32 = 128/32 = 4.

Nb = (Block size)/32 = 128/32 = 4. Nr = No. of cipher rounds = 10.

We use the standard convention of representing elements of F12 as polynomials of degree 7, over F2. We also adopt the standard practice of treating the elements of F28 as integers in the range 0, ..., 255.

We define four functions namely Rotbyte(.), Rc(.), and Rcon(.) and Indicating vector .

(i) Rotbyte(.) It rotates the bytes of key within the word, when word oriented structure is considered for key expansion mechanism. If ko kl, k2, k3 are four bytes of i-th key-word

W [i] arranged in big endian format. The byte substitution transformation of Rijndael uses an S-box, generated over F28 with□x □1□ □ □ □03base 16□ □ □as primitive element and g□x□ □ □ □x8 □ □x4 □□x3 □ □x □1□ □as the defining irreducible polynomial along with an affine transformation of □x6 □ □x5 □ □x □1□ □ □ 63base16 □ □. Thus, bs, using S-box, transforms the individual byte a(x) to bs(a(x)).

(ii) Rc(a(x)) is another round dependent byte oriented constant function defined over F28. POW(a(x)) contains

powers of a(x) in the field. Then

Rc (a (x)) = POW (a (x))(mod g (x))

In particular, for a(x)= {1, 2,….. ,10}

Rc (a (x)) = {1, 2, 4,8,16,32, 64,128, 27,54}

(iii) Rcon(a(x)) is a round dependent word oriented function such that Rcon(a(x)) = (Rc(a(x)),,o,,O). Here the commas define separation of each byte arranged in big endian format.

(iv). Indicator vector representing a byte, say

a (x) = x4 + x3 +1º 25,

is a 256x1 matrix with 1 only at 25th position and zeros elsewhere, i.e. the vector representing a(x) has 1 at the place corresponding to the numerical value of the byte and zero at all other positions in the matrix 0 to 255.

A. Brief description of Rijndael internals

Rijndael has an elegant algebraic structure over F28. The input plain text or the output cipher text of block size of 128- bits is viewed as a 4x4 matrix of 16 bytes arranged in a column major format. Rijndael consists of an initial round of key addition (ak) followed by 10 iterations of round transformations for the key size of 128-bits. Each (except the last) round transformation function is composed of the four sub transformation functions: Byte Substitution or bs, Row Shift or rs, Mix Column or mc and Add Round Key or ak.

The last round transformation does not include the mc function.

Byte substitution transformation: *bs:* This is the only

non-linear transformation in the entire Rijndael structure. It operates independently on each byte using a substitution table (S-box). The S-box, which is invertible in nature, is composed of two transformations

1. Taking multiplicative inverse of the desired byte in the finite field GF(28) with □x □1□ □ □ □03base16 □ □as primitive element and g□x□ □ □ □x8 □ □x4 □ □x3 □ □x1 □1□ □as

the defining irreducible polynomial. The element 16 00base is mapped to itself.

2. Applying an affine transformation of □x6 □ □x5 □ □x1 □1□ □equivalently 63 base16 .

Row shift transformation: *rs*: The 16 input bytes are

arranged in a column major format of a 4x4 matrix. To

achieve the desired confusion, a linear transformation rs

is applied. Here, the bytes in each row of the matrix are

given a cyclic left shift. For i = 1, 2, 3, 4 the bytes in the

i-th row are circularly left shifted by (i-1) bytes. The inverse of a row shift transformation is obtained by cyclically shifting the bytes in the reverse direction i.e. circularly right shifting 0, 1, 2, and 3 bytes in the first, second, third and fourth row of the 4x4 input matrix, respectively.

Mix column: *mc*: The linear transformation mix column

provides the diffusion by mixing the bits of each column. The

function □(z), given below, operates on the input column by

treating it as a degree three polynomial in F28□z□ □ This polynomial is multiplied by a rotated version of a standard polynomial m □z □ □F 8 □z □ □2□ □given by

m□z□_ □ □03z3 □ □01z2 □ □01z1 □ □02

and reduced modulo the polynomial □z4 1□□□□ □F2 8 □z□ □

□Here the coefficients denote elements of F2 8. It is known that the coefficients of m(z) are so chosen that the result □(z).m(z)is invertible modulo (z4 + 1) although this polynomial is reducible over F2.

Add Round Key: *ak*: In this function, the round key is added to the current byte as bit-wise exclusive OR. The XOR operation is the inverse of itself.

III. PROPOSED METHOD

In our proposed method, and we encrypt the secret data as EInitial which is encrypted using AES which is one of the most secure encryption method and using permutation function perme we permute the EInitial as E.The permutated data is encoded using the error detection and correction code.we hide the data inside the cover image X in the LSB.

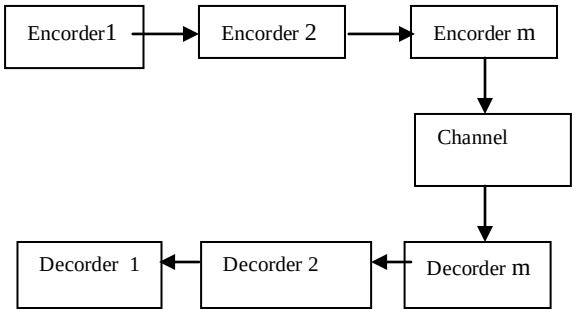

Fig. 1: Principle of Concatenated Codes

We are taking the digital grayscale image in which each pixel of 8-bits or 1-byte, representing the gray levels from black to white. Figure 2 shows the block diagram of a proposed system.

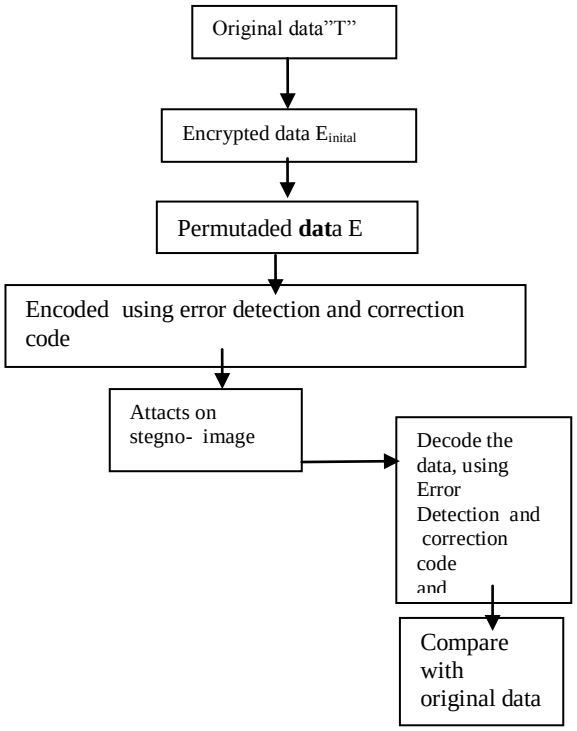

Figure2: Flow diagram of proposed system

We will analyze the effectiveness of the scheme, which is proposed by us. Even if the attackers know everything about the proposed scheme. Because the data is encrypted using the Advanced Encryption Standard (AES) with 128-bits. Robustness will increase when we use error detecting codes.Therefore we can say this proposed scheme is secure under this case.

IV. CONCLUSION

The main purpose of our proposed scheme is to make a full-proof method. And it should work in the noisy environment. For the robustness of the system we are using the AES and permutation function and for error correction we are using the Trellis and the interleaved code.

V. REFERENCES

[1] B.Gladman, "Implementation experience with the AES candidate algorithms," Proc. of 2nd AES candidate

conference, March 22-23, 1999, Rome, pp. 7-14.

(http://fp.gladman.plus.com/cryptography_technology/rijndae.

[2] Jiwu Huang, Yun Q. Shi, Yi Shi ," Embedding image watermarks in DC components," IEEE Trans. CSVT 10 (6) (2000) 974-979.

[3] N. Rajpal, A. Kumar and P. R. Jindal, "Demonstrating the Use of Error Coding Technique in the field of Steganography, along with Linear Feedback shift Register Technique," 2nd Workshop on Computer Vision, Graphics and Image Processing, pp. 22-27, Gwalior, India, February 2004.

[4] Y. K. Lee and L. H. Chen, "High Capacity Image

Steganographic Model," IEE Proceedings - Vision, Image, and signal processing, vol.147, No. 3, June 2000, pp. 288-294.

[5] Jiwu Huang, Yun Q. Shi, Yi Shi ," Embedding image watermarks in DC components," IEEE Trans. CSVT 10 (6) (2000) 974-979.

[6] J.Daemen and V.Rijmen. "The Design of Rijndael," AES - Advanced Encryption Standard}, ISBN 3-540-42580-2 Springer-Verlag Berlin Heidelberg, New York.

[7] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," IEEE computer, Vol. 31, No. 2, February 1998,pp. 26-34.

[8] N. Rajpal, A. Kumar, P. R. Jindal and A. Saroagi, "An Investigation into the use of Linear Feedback Shift Register for Data Encrypting and Data Hiding in the field of Steganography," Conference on e-security, Cyber Crime & Law, pp., Chandigarh, India, February 2004.

[9] Anil Kumar, Deepak Gambhir and Navin Rajpall "Robust and Secret Data Transmission Over the Noisy Channel" IEEE - ICSCN 2007, MIT Campus, Anna University, Chennai, India. Feb. 22-24, 2007. pp. 199-203.