ISSN:2231-0711

Sambangi Sharmila et al | IJCSET(www.ijcset.net) | November 2016 | Vol 6, Issue 11, 370-374

# Inverse of Data Encoding Using Secure ETC Technique

**Sambangi Sharmila**
*Mtech Student,Dept of CSE,*
*Visakha Institution of Engineering and Technology,*
*Visakhapatnam*

**A.Hari Kumar**
*Assistant Professor, Dept of CSE,*
*Visakha Institution of Engineering and Technology*
*, Visakhapatnam*

**Abstract: By adopting the concepts of cryptography and image processing we will provide security for data through the image. This paper proposes a cryptographic technique by considering functionality for the security of data and image. By using triple DES algorithm data encryption and decryption is done .Later through LSB technique encryption of data, the cipher data can be stored into the image. After storing data the image can be encrypted by using DIT (Data Inverse technique).Once the encryption of image is completed the image compression is done using Arithmetic compression and decompression technique. The proposed architecture provides data confidentiality and improves the performance. These days transferring data and image through the network without losing data integrity are a complex task to provide security of data and image, we can use the cryptography techniques, image encryption, and decryption and compression techniques.**

**Keywords: LSB, DIT, ETC, Arithmetic Compression and decompression technique, image encryption and decryption.**

## I. INTRODUCTION

We can convert the electronic data into cipher text by using Encryption method. By this method data attacks to corrupt, the information can be prevented. Encrypted data is being converted to formal data by using decryption. In this process, compression plays a crucial role in encryption and decryption of the data by reducing the size of the data.[1,2]Compression is the reducing in size of the information storing in data and the end goal to spare less space and transmission time. To reduce the storage space at the time of transferring the data in the network we can use compression which depends on the number of the components in the encryption and the decryption process.

Mathematical coding is a type of entropy encoding utilized as a part of lossless information compression. Mathematical coding contrasts from different types of entropy encoding, for example, Huffman coding. Math coding is seemingly an ideal encryption coding strategy if the goal is the best compression apportion since it, as a rule, accomplishes preferable result over Huffman coding. This coding is an information compression method that encodes information by making a code string which notates a fractional data between the data of 0 and 1. In the compression of the multimedia data of lossless compression process have the capability to compress the data[8].

With the steadily expanding development of mixed media applications, security is an imperative issue in correspondence and capacity of images, and encryption is one the approaches to guarantee security. Picture encryption procedures attempt to change the unique picture to another picture that is difficult to comprehend; to keep the picture classified between clients, in another word, it is key that no one could become more acquainted with the substance without a key for decryption. Besides, extraordinary and dependable security in Storage and transmission of computerized images is required in numerous applications, for example, digital TV, online individual photo collection, therapeutic imaging frameworks, military picture interchanges and classified video gatherings, and so forth. Keeping in mind the end goal to satisfy such an assignment, numerous picture encryption techniques have been proposed.

Demonstrating images introduces a few new difficulties, however. Most existing image pressure calculations depend on changes, e.g.,[9] the DCT (Discrete Cosine Transform) in JPEG. Changes mean to change the image into space where it might be spoken to with just a couple of coefficients. Utilizing a bitwise stream figure, however, it gets to be difficult to consider changes since encryption is a non-straight process. Conversely, image coders which utilize pixel area models utilize very non-stationary indicators. For instance, JPEG-LS (lossless) packs every pixel taking into account 4 of the nearby pixels. Since this information is inaccessible when the image is encoded, the application is not direct. Rather, the pressure of scrambled dim scale image will require more noteworthy utilization of the doped bits and other learning strategies.This work naturally suggests an extension to gray-scale and other larger-alphabet images. A first approach is to break an image up into a series of bit-planes where each bit-plane represents all the bits of equal significance in the binary expansion of the pixel values. Image structure is typically highly concentrated in the most significant bit-planes though. As a result, little compression gain is available with this approach. Accurate image models are necessary to be able to achieve significant gains when compressing encrypted data.

## II. RELATED WORK

In previous days transfer the image and data through the network in form of plain format. So that transferring data and image in form of plain are will lose the security in a network. So that we can provide the security the transferring image and data can be sent in form of unknown format. So that by convert data and image into an unknown format we can encrypt image by using any technique.

In late studies, the digital signaling is empowered in many numbers of users. It is presented in media systems and these administrations are utilizing as a part of mystery correspondence. Present specialized arrangements are secure changes of the information utilizing cryptographic systems utilizing secure system layer methods. That is for securing information at the time of exchanging the information. This watches out for the cryptographic layer emphasizes by producing to ensure the unapproved access of the clients. It is for giving the approve get to in the system for information access. There are some disadvantages such as simple encryption over image does not maintain optimal security. Performance is always an important factor while transmission of secure data over stage images. Simple shared based key generation traditional approach in easy to break.

The encoding of the image has been increasing the usability of the data exchanging. In this the process of data that converts the image data to binary data using discrete cosine transform or lossless encoding using compressions. There are some other processes that are encryption ten compression system. It uses the key to encrypt and compression and to decryption process can be done by key only. Without it, the decryption process is not possible. This is mainly used by military operations. This process works on black and white pixels and convert the images and provides the authentication and the copyright protection[1]. The third stage is the distinguishing proof procedure which includes the numbering of the offers that are created from the mystery image. These shares also, the key are then exchanged to the beneficiary. The collector takes the assistance of the way to build the mystery image in the unscrambling process. The method proposed is a special one from the others in a way that the key is created with substantial data about the qualities utilized as a part of the encryption process. The majority of the encryption forms first produce the key and at that point do the encryption process. This strategy produces a connection between the encryption process and the key[2,3].

To accomplish higher pressure proportions, the lossy pressure of encoded information was likewise concentrated on . Zhang et. Al proposed a versatile lossy coding system of encoded images through a multi-determination development. In a compressive detecting (CS) system was used to pack scrambled images came about because of straight encryption.[4] An adjusted premise interest calculation can then be connected to gauge the first image from the compacted and scrambled information. Another CS-based methodology for encoding compacted images was accounted for. Moreover, Zhang outlined an image encryption plan by means of pixel-area change and exhibited that the encoded document can be effectively compacted by disposing of the exorbitantly unpleasant and fine data of coefficients in the change space.[5] As of late, Zhang et. al recommended another pressure approach for scrambled images through multi-layer disintegration. Augmentations to visually impaired pressure of encoded recordings were created. Compression- then-Encryption (CTE) meets the necessities in numerous protected transmission situations, the request of applying the pressure and encryption should be turned around in some different circumstances. As the substance proprietor, Alice is constantly intrigued by ensuring the protection of the picture information through encryption. In any case, Alice has no motivating force to pack her information, and henceforth, won't utilize[6] her constrained computational assets to run a pressure calculation before encoding the information. This is particularly genuine when Alice utilizes an asset denied cell phone. If not otherwise specified, 8-bit grayscale images are assumed .Both lossless and lossy compression of encrypted images will be considered. Specifically, we propose a permutation-based image encryption approach conducted over the prediction error domain.

## III. PROPOSED SYSTEM

***Presently Key Generation algorithm:***

Diffie-hellman is one of the key exchange algorithms and is used for Delta value generation.

*Global public elements:*

This algorithm considers the two public keys:
p(prime number)
q(primitive root)
q<p.

*User A key generation:*

A day's transmission of information through picture over the system without losing information uprightness is a mind boggling errand. To give security of information and picture, we can utilize the cryptography procedures, picture encryption and unscrambling system and pressure strategies. In this paper, we are utilizing a proficient strategy for giving more security.

In Cryptographic Module, it is utilized for proselyte information into the recondite organization. The transformation of information into recondite configuration is called encryption and changing over figure content into plain content is known as the unscrambling, before sending information through picture the sender will encode information utilizing Triple DES calculation. In the wake of changing over information into a recondite configuration, that figure content will be put away into the picture and sent to the recipient. The recipient will recover the figure content from the picture and unscramble utilizing triple des to recover the plain content.

***Data encryption and decryption****:*

In this module is utilized for believer information into the recondite organization. The change of information into recondite is called encryption and changing over figure content into plain content is known as the unscrambling. Before sending information through picture the sender will encode information utilizing Triple DES calculation. In the wake of changing over information into a recondite configuration, that figure content will put away into the picture and sent to the collector. The collector will recover the figure content from the picture and decode utilizing triple des. In the wake of unscrambling the figure message, the beneficiary will recover the plain content.

*User A selects a private key and calculates a public key.*
Select private key $X_A$ $X_A<p$
Generate public key $Y_A$
$Y_A=q^{XA} \bmod p$

*User B key generation:*
User B selects a private key and Calculates a public key.
Select private key $X_B$ $X_B<p$
Generate public key $Y_B$

$Y_B=q^{XB} \bmod p$

*Generation of secret key by User A:*
User A generates a secret key using his private key and User B public key.
$K=(Y_B)^{XA} \bmod p$
Generation of secret key by User B:
User B generates a secret key using his private key and User A public key.
$K=(Y_A)^{XB} \bmod p$

*Store data into image:*
After completion of the encryption process, the sender will get cipher text. The sender will take the cipher text and convert into binary format. After converting binary format, the sender will store into an image by using LSB technique. Before storing data into the image the sender will retrieve each pixel from the image and convert into binary format after we can store data into an image. After completion of storing data into the image, the sender will generate data hide the image.

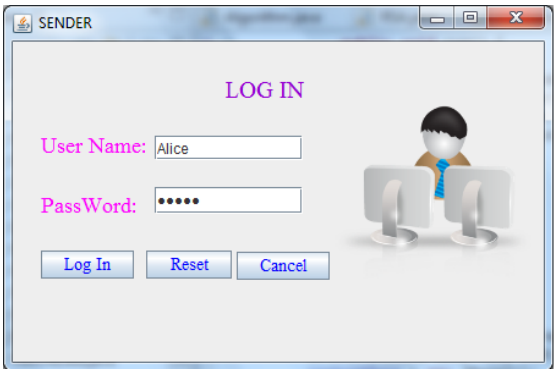
***Image encryption and decryption:***
After storing data into the image the sender will encrypt and decrypt the image. In this paper, the sender and receiver will use POT technique for image encryption and decryption. The procedure of POT technique as follows.

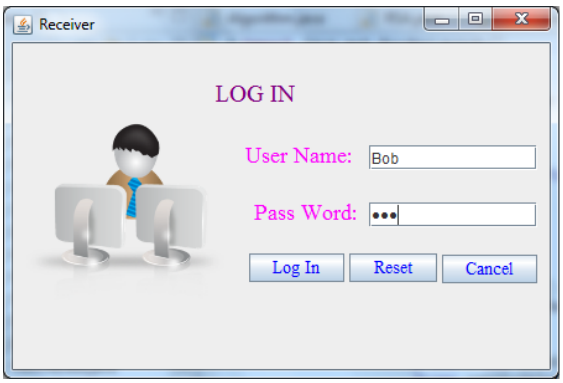
*1. Encryption process:*
(i) First of all select whole image and give named as I.
(ii) Then stored all the pixels value of I in a two-dimensional array named as P
(iii) Firstly row-wise XOR all the bits of the pixel from top to bottom like every image have rows or column wise pixels. Firstly XOR first and second row and then store first row as XOR Result and second rows as it is then XOR second and third rows and store according to the previous operation and then apply to all the rows.
(iv) A square grid of required size constructed by taking binary data from the or data.
(V) Now grid transposition applied by reading data diagonally and writing it down on row basis from left to right.
(Vi) A new grid generated after transposition.
(vii) The new grid is converted into ASCII sequence and written into Image file.

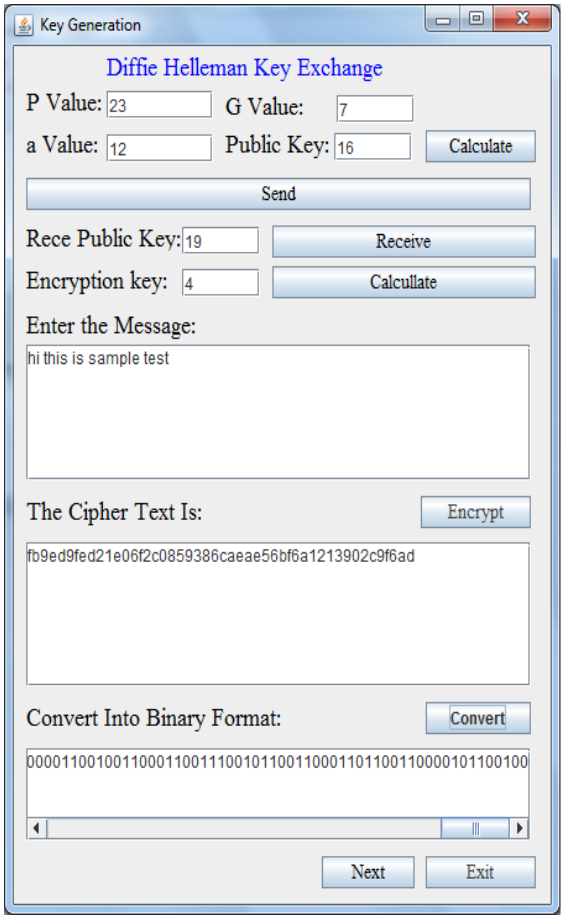
*2. Decryption process :*
After decompression of image, the image can be converted into pixel and perform the decryption process.
(i) A square grid of required size constructed by taking binary data from the
(ii) Now grid transposition applied by reading data diagonally and writing it down on row basis from left to right.
(iii) A new grid generated after transposition.
(iv) After column wise XOR all the bits of the pixel from right to left like asImage file.
(v) Then stored all the pixels value of I in a two-dimensional array named as PC firstly XOR last and lose the second column until completion of reverse process encryption. After column xor again perform the row-wise from right to left .

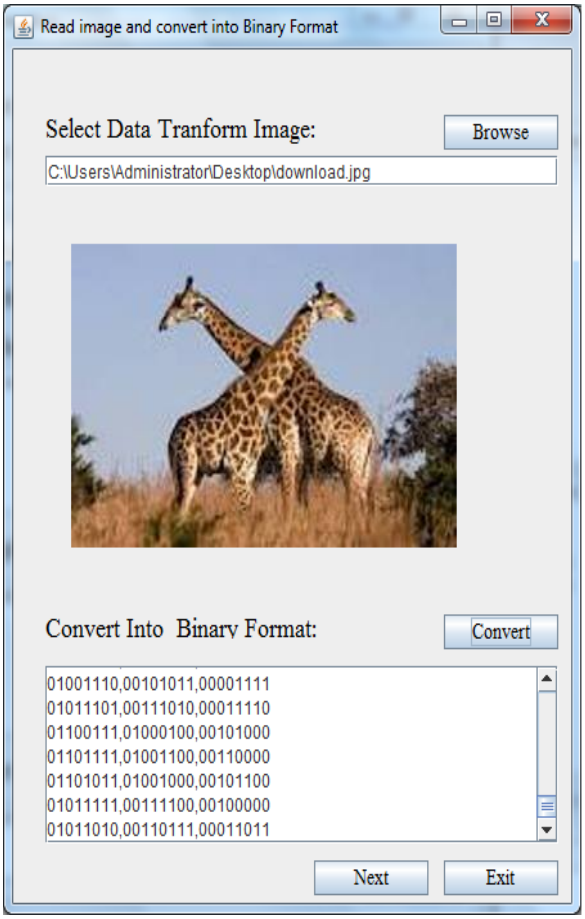
*3. And getting original image* Image compression and decompression:
In this module the sender will perform the compression technique for image compression and receiver will perform the decompression technique for image decompression. For performing compression and decompression, we are a using arithmetic technique for image compression and decompression. After performing encryption of image, the sender will compress the image using Arithmetic compression technique and sent to the receiver. After sending the receiver will retrieve the compressed image and decompress by using the arithmetic decompression technique.

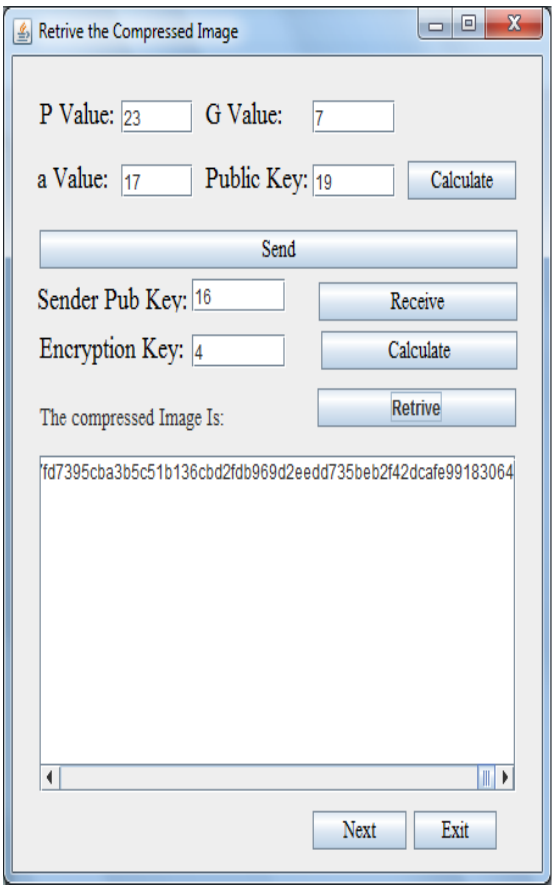
## IV. RESULTS

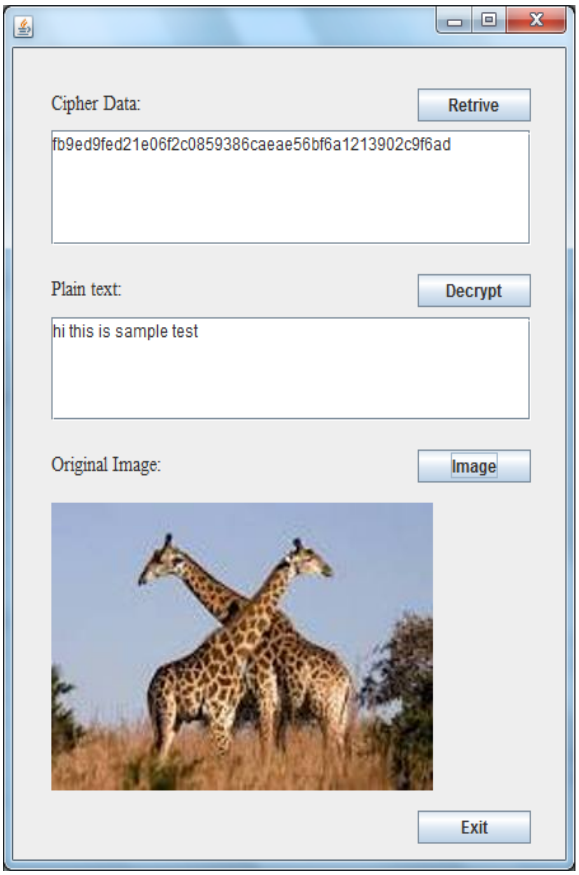



Key Generation
Diffie Helleman Key Exchange
P Value: 23
G Value: 7
a Value: 12
Public Key: 16
Calculate
Send
Rece Public Key: 19
Receive
Encryption key: 4
Calculate
Enter the Message:
hi this is sample test
The Cipher Text Is:
Encrypt
fb9ed9fed21e06f2c0859386caeae56bf6a1213902c9f6ad
Convert Into Binary Format:
Convert
0000110010011000110011100101100110001101100110000101100100
Next
Exit


Read image and convert into Binary Format
Select Data Tranform Image:
Browse
C:\Users\Administrator\Desktop\download.jpg
Convert Into Binary Format:
Convert
01001110,00101011,00001111
01011101,00111010,00011110
01100111,01000100,00101000
01101111,01001100,00110000
01101011,01001000,00101100
01011111,00111100,00100000
01011010,00110111,00011011
Next
Exit


Retrive the Compressed Image
P Value: 23
G Value: 7
a Value: 17
Public Key: 19
Calculate
Send
Sender Pub Key: 16
Receive
Encryption Key: 4
Calculate
The compressed Image Is:
Retrive
fd7395cba3b5c51b136cbd2fdb969d2eedd735beb2f42dcafe99183064
Next
Exit


Cipher Data:
Retrive
fb9ed9fed21e06f2c0859386caeae56bf6a1213902c9f6ad
Plain text:
Decrypt
hi this is sample test
Original Image:
Image
Exit

## CONCLUSION

We have been concluding our current research work with efficient with compression and encryption model. It efficiently creates a key between two end users with Diffie hellman key exchange protocol and data can be encoded with the triple des cryptographic algorithm and data can be embedded into an image and it can be compressed with compression mechanism and the reverse process can be done at the receiver end.

## REFERENCES


[1] T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357

[2] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053–1066, Jun. 2012

[3] A. Kumar and A. Makur, "Distributed source coding based encryption and lossless compression of gray scale and color images," in Proc. MMSP, 2008, pp. 760–764.

[4] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 180–187, Mar. 2010.

[5] J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryptionthen- compression system," in Proc. ICASSP, 2013, pp. 2872–2876.

[6] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.

[7] M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452–468, Jun. 2011.

[8] Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.

[9] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[10] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in Proc. 16th Eur. Signal Process. Conf., Aug. 2008, pp. 1–5.

[11] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.

[12] D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.