An Efficient and Secure DIT Technique for Image Encoding and Compression

Sambangi Jithendra Kumar[1]**, Dr Ch. Ramesh**[2]**, D.Prakasa Rao**[3]
[1]M.tech Scholar, [2]Professor.[3]Assistant Professor
[1,2,3]Department of CSE, Aditya Institute of Tech. & Management (AITAM) Tekkali, Srikakulam District, Andhra Pradesh, India.

Abstract: **In addition to provide the security for data through image, we are using the concepts of cryptography and image processing. In this paper we are using both functionality for security of data and image. Before transferring data we can encrypt it by using cryptographic technique. In this paper we are using triple DES algorithm for data encryption and decryption. After encryption of data the cipher data can be stored into image using LSB technique. After storing data the image can be encrypt by using DIT (Data Inverse technique). The completion of encryption of image the image can be compressed by using Arithmetic compression and decompression technique. The above architecture provides data confidentiality and improves the performance. Now days transferring data and image through 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. In this paper we are using an efficient technique for provide more security.**

I. INTRODUCTION

Encryption is the method to convert the formal information to informal information. It prevents the data attacks to corrupt the information. Decryption is the process that converting the encrypted data to formal data. In this process compression plays 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 information storing in data and the end goal to spare less space and transmission time. Using the compression we can reduce the storage space at the time transferring the data in the network. The compression 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 the most 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 over unique picture to another picture that is difficult to comprehend; to keep the picture classified between clients, in other 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 over the image into a 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 who utilize pixel area models utilize very non-stationary indicators. For instance, JPEG-LS (lossless) pack every pixel taking into account 4 of the nearby pixels. Since this information is inaccessible when the image is encoded, application is not direct. Rather, 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 network in form of plain format. So that transferring data and image in form of plain is will loss 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 unknown format we can encrypt image by using any technique.

In late studies the digital signaling is empowered in much number of uses. 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 stego 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 is some other process that is encryption ten compression systems. 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, 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 gray scale 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 a day's transmission of information through picture over 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 give more security.

In Cryptographic Module, it is utilized for proselyte information into 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 recondite configuration that figure content will be put away into picture and sent to 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 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 recondite configuration that figure content will put away into picture and sent to 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.

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

Store data into image:
After completion of 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 image by using LSB technique. Before storing data into image the sender will retrieve each pixel from the image and convert into binary format after we can store data into image. After completion of storing data into image the sender will generate data hide image.

Image encryption and decryption:
After storing data into 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 two dimensional array named as P
(iii) Firstly row wise XOR all the bits of pixel from top to bottom like as like every image have rows or column wise pixels. Firstly XOR first and second row and then store first row as XOR Resultant second rows as it is than XOR second and third rows and store as according to previous operation and then apply to all the rows.
(iv) A square grid of required size constructed by taking binary data from the x 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 pixel from right to left like as Image file.
(v) Then stored all the pixels value of I in two dimensional array named as P firstly XOR last and lase second column until completion of reverse process encryption. After column xor again perform the row wise from right to left.

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 using arithmetic technique for image compression and decompression. After performing of encryption of image the sender will compress the image using Arithmetic

compression technique and sent to receiver. After sending the receiver will retrieve the compressed image and decompress by using the arithmetic decompression technique.

IV. 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 triple des cryptographic algorithm and data can be embedded into image and it can be compressed with compression mechanism and reverse process can be done at receiver end.

REFERENCES

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

[2] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

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

[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] 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.

[6] 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.

[7] Olivier Egger and Wei Li, Nov-1994, "*Very Low Bit Rate Image Coding Using Morphological Operators And Adaptive Decompositions*" IEEE International Conference on Image Processing Vol-3, PP No.326-330.

[8] Sreelekha G and P.S.Sathidevi, June 2007, "An Improved JPEG Compression Scheme Using Human Visual System Model" IEEE, PP No: 98-101.

[9] 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.

[10] 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.

[11] 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.

[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.

[13] Ken cabeen and peter gent," Image compression and the discrete cosine transform", Math 45 college of redwoods.

[14] Andrew B.Watson "Image Compression using the discrete cosine transform" Mathematica Journal 4(1),1994, p-81-88.

[15] K. Kantapanit and W. Wiriyasuttiwong. "Face Recognition by Edge Detection of JPEG Compressed Images and Backpropagation Neural Network" The Engineering Journal of Siam University. Volume 3, Year 2 , July-December, 2000.

[16] R.C.Gonzalez and R.E.Woods "Digital Image Processing", 2nd Edition Addison Wesley, USA ISBN: 0-201-60078, 1993sz.

BIOGRAPHIES

Sambangi Jithendra Kumar Holds a B.Tech certificate in Information Technology from Thandra Paparaya Institute Of Science And Technology the University of Jntu Kakinada. He is presently Pursuing M.Tech in Computer Science Engineering Department of computer science engineering from Aditya Institute of Technology and Management (AITAM), Tekkali, Srikakulam, AP, India.

Dr. Ch. Ramesh received the B. Tech degree from Nagarjuna University, M. Tech degree in Remote Sensing from Andhra University, another M. Tech degree in Computer Science & Engineering from JNTUH and Ph.D degree in Computer Science & Engineering from JNTUH. He is a professor & Associate Dean in the department of Computer Science & Engineering, Aditya Institute of Technology and Management, Tekkali, India. His research interests include Image Processing, Pattern Recognition, Formal Languages and Automata Theory and Unix Programming.

D.prakasa Rao received the B.Tech degree from AITAM College, Tekkali from JNTU University, M. Tech degree in Computer Science in Aitam ,Tekkali from JNTUK University. He is an Assistant professor in the department of Computer Science & Engineering, Aditya Institute of Technology and Management, Tekkali, India. His research interests include Image Processing and Networking Concepts.