A Hybrid Image Encoding Technique with DCT and Mosaic based Segmentation

M. Varalakshmi
M. Tech Scholar
Department of CSE,AITAM,Tekkali,Srikakulam-532201,Andhrapradesh,India.
varalakshmi.modalavalasa@gmail.com

Dr. Ch. Ramesh
Professor
Department of CSE, AITAM,Tekkali,Srikakulam-532201,Andhrapradesh,India.
chappa_ramesh01@yahoo.co.in

Abstract:- Embedding the information in cover image is always an interesting research issue in the field of image steganography. In this paper, we are using a hybrid model with compression, data encoding and image mosiacing technique. Image (pixel values) can be compressed with efficient DCT technique, Data can be embedding in to cover image without losing the data integrity with LSB technique, because usage of significant bits of the image may damage the image and image can be parallel segmented without losing pixel integrity and combined at receiver end with improved noise free image mosaicking technique. Our experimental analysis gives more efficient results than traditional approaches.

Keywords: *DCT,Steganography,mosaicking technique,Authentication*

*****

I. INTRODUCTION

Steganography incorporates the camouflage of data inside PC documents. In computerized steganography, electronic correspondences may incorporate steganographic coding within a vehicle layer, for example, a report record, picture document, program or convention. Media records are perfect for steganographic transmission considering their substantial size. For instance, a sender may begin with a harmless picture document and alter the shade of each 100th pixel to relate to a letter in the letter set, a change so unobtrusive that somebody not particularly searching for it is probably not going to notice it[1][2].

All data concealing methods that might be utilized to trade steganograms in media transmission systems can be grouped under the general term of system steganography. This classification was initially presented by Krzysztof Szczypiorski in 2003[3]. In 2016, a first system steganography covering book was distributed by Mazurczyk et al.However, organize data stowing away was at that point connected in the late 1980s by Girling and Wolf. Contrary to normal steganography strategies that utilization computerized media (pictures, sound and video records) to shroud information, arrange steganography utilizes correspondence conventions' control components and their natural usefulness. Accordingly, such strategies can be harder to distinguish and dispose of[4][6].

Advanced steganography yield might be as printed reports. A message, the plaintext, might be first scrambled by customary means, creating a ciphertext. At that point, a harmless covertext is altered somehow to contain the ciphertext, bringing about the stegotext. For instance, the letter estimate, separating, typeface, or different qualities of a covertext can be controlled to convey the shrouded message. Just a beneficiary who knows the system utilized can recuperate the message and afterward decode it. Francis Bacon built up Bacon's figure in that capacity a strategy [5].

The ciphertext delivered by most advanced steganography strategies, be that as it may, is not printable. Conventional advanced techniques depend on annoying clamor in the channel document to conceal the message, thusly, the channel record must be transmitted to the beneficiary with no extra commotion from the transmission. Printing presents much commotion in the ciphertext, for the most part rendering the message unrecoverable. There are strategies that address this constraint, one striking illustration is ASCII Art Steganography [7].

II. RELATED WORK

Most steganographic frameworks today conceal messages by marginally adjusting a current cover question, for example, an advanced picture. The JPEG, being the most widely recognized picture arrange in utilize today, gotten by a wide margin the most consideration from the stego group. Useful stego frameworks were composed either utilizing heuristic standards or built secure with deference to a given model. One of the primary JPEG stego plans was JSteg1. It utilized the generally utilized installing worldview called Least Significant Bit (LSB) installing connected to quantized DCT coefficients. The message bits were just installed as LSBs in DCT coefficients not quite the same as 0 also, 1[8][11].

This rejection appeared to be essential because the qualities 0 and 1 constitute a LSB match (values that exclusive contrast in their LSBs) and by permitting changes in coefficients equivalent to 0 an expansive twisting would be presented. The inserting way through the picture was initially successive and in later usage stretched out to a pseudo-arbitrary way[9].The high perceptibility of JSteg is because of the way that it brings trademark ancient rarities into the principal arrange measurements (histogram) of DCT coefficients. The up and coming era of stego techniques subsequently centered around protecting measurable properties of cover pictures. Such techniques were later named as containing "factual rebuilding".

The thought is to isolate the cover protest into two disjoint parts, implant the message in one, and utilize the other part to perform "rectifications" in request to safeguard chose factual amounts, generally habitually the histogram of DCT coefficients. A related technique is the premise of Model Based Steganography, where a model of the DCT coefficients is safeguarded. This had the preferred standpoint that moderately high limit plans could be gotten that could protect not just the model of the worldwide histogram of DCT coefficients yet likewise each of the 64 histograms of individual DCT modes or even a chosen higher-arrange insight[10].

Another general course in steganography, that as of late gotten impressive consideration, can be inexactly named "negligible mutilation" implanting. Every coefficient is allocated a scalar esteem communicating the commitment of making an implanting change at that coefficient to general perceptibility. On the off chance that the crude, uncompressed cover picture is accessible to the sender as opposed to only its JPEG compacted shape, the sender can utilize the information of the unquantized DCT coefficients to together limit the general twisting because of quantization what's more, implanting. This sort of implanting is called Perturbed Quantization.

III. PROPOSED WORK

We propose an efficient compression based data embedding technique for efficient steganography, our model improves the compression rate for increasing the performance of data embedding in the pixel, our uniform based data embedding models initially compression the data which wants to embed and segment the image into equal number of parts with image mosaicing technique and embed in to pixels uniformly. Our proposed model efficiently embeds data into second least significant bit positions without losing the data integrity. Our proposed model gives more efficient results than traditional approaches

Even though various traditional approaches proposed by the various authors from years of research, every approach has it’s own advantages and disadvantages. Most of the models simply embed the information in the least significant bit positions of the image pixels so it is suitable to embed more information and embedding all the information in LSBs sequentially takes more time. The main objective the image steganography is efficient data embedding in to pixel with effective compression rate that should the achievable goal for the implementations.

Integrated Authentication and Keygeneration:
A paper certificate can be utilized as a client's confirmation calculate, yet an open key digital certificate can't be utilized as a verification consider organize applications. This is because a paper certificate can't be effectively manufactured or copied, yet an open key digital certificate can be effortlessly recorded and played back. In our plan, the proprietor of a GDC never needs to uncover the digital mark of the GDC in plaintext to the verifier. Rather, the proprietor demonstrates that he knows about the digital mark by reacting to the verifier's test. The learning of the digital mark on the GDC can give client validation. The proposed convention ought to fulfill the accompanying security prerequisites.
1) Unforgeability: A legitimate response must be produced by the certificate proprietor who knows the digital signature of the GDC.
2) One-wayness: No other individual can determine the digital signature of the certificate in the connection.
3) Non-transferability: A reaction to a verifier's test can't be moved into a reaction to another verifier's test, which would some way or another make pantomime of the client. Our proposed convention is based on the mix of the customary DL-based digital signature and the Diffie-Hellman Assumption (DHA).
Elgamal Algorithm:
This method contains three features such as key generation,encryption,decryption.
Consider two users A and B.
Key Generation:
In this the below steps as follows:

- A Generates an dcyclic group Gc of order q.
- A chooses a random number from x
- A computes Ha=Gc^x
- A shares Ha, Ga,q.

Encryption:
The encoding algorithm process as follows:
To encrypt a message m to A under her pubic key.

- B chooses a random number k from n to q-1 values such as n=1. Then calculates b1=g^k
- B calculates the shared secret s=g^k
- B sends the encoded text to A using shared secret.

Decryption:

The decoding algorithm works as follows to decode a encoded text.

- A calculates Shared secret S= $c1^x$
- Then calculates m=$c1^x$ .s

The ElGamal cryptosystem is generally utilized as a part of a half and half cryptosystem. I.e., the message itself is scrambled utilizing a symmetric cryptosystem and ElGamal is then used to encode the key utilized for the symmetric cryptosystem. This is because asymmetric cryptosystems like Elgamal are normally slower than symmetric ones for a similar level of security, so it is quicker to scramble the symmetric key (which more often than not is very little if contrasted with the span of the message) with Elgamal and the message (which can be discretionarily substantial) with a symmetric figure.

Triple DES algorithm

In this module,every client will encode and decode shared information. The encoded shred information will be put away into cloud benefit. If any client needs to recover that mutual information and decode by utilizing mystery key. The encryption and decoding of shared information we are utilizing triple TDES algorithm. By utilizing this algorithm, we can give greater security and adaptable of shared information.

Least significant bit technique:

In this module the sender will take parallel organized information of cipher information and image pixel esteems. The sender will take exchanging image and change over into double configuration. After change of paired the sender will take cipher arrange parallel information and put into double pixel estimation of minimum huge piece. The sender will take that put away double pixel esteems and again create information conceal image.

IV. CONCLUSION

We have been concluding our current research work with efficient hybrid model as secure authentication followed by key generation protocol for secure key generation.Data can be encoded and decoded at both ends and it can be embed in to image at least significant bits without pixel damage .Pixel value can be parallel compressed with efficient and novel model and cover image can be segmented in to equal parts after data embedding in to the image. Our proposed model gives more efficient results than traditional approaches

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] 11.. Uniform Embedding for Efficient JPEG Steganography byLinjie Guo, Student Member, IEEE, Jiangqun Ni, Member, IEEE, and Yun Qing Shi, Fellow, IEEE

[12] Ch. Ramesh, Dr. N.B. Venkateswarlu, Dr. J.V.R. Murthy "Fast DCT Algorithm using Winograd'sMehtod" (IJECT, vol.3, No.1, January-June, 2012, pp 98-110, ISSN 0976-6464(p), ISSN 0976-6472(o), I.R= 8.2691 in **2016.**

[13] Ch. Ramesh, Dr. N.B. Venkateswarlu, Dr. J.V.R. Murthy "A Novel K-Means Based JPEG Algorithm for Still Image Compression" , IJCET, vol.3, No.1, January-June, 2012, ISSN 0976-6367(p),ISSN 0976-6375(o),I.R=9.3590 in **2016**

[14] Ch. Ramesh, Dr. N.B. Venkateswarlu, Dr. J.V.R. Murthy "Filter Augmented JPEG Algorithms: A Critical Performance Study for Improving Bandwidth" IJCA, Vol. 60-No.17, ISSN: 0975-8887, December 2012, I.R=0.752in **2015**

[15] Ch. Ramesh, Dr. N.B. Venkateswarlu, Dr. J.V.R. Murthy "A New Classification Performance Aware Multisensor, Multi Resolution Satellite Image Compression Technique"

GJCST, 0975-4172 (O), 0975-4350 (P), Vol.13, No.7, Pp: 13-23, Aug. 2013.

[16] Ch. Ramesh, Dr. N.B. Venkateswarlu, Dr. J.V.R. Murthy "A Critical Performance Evaluation of Classification Methods with Modified JPEG Decompressed Multiband Images" GJRE, ISSN No. 2249-4596 (O), 0975-5861 (P), Vol. 13, No 16, pp: 41-55, Dec.2013.