# Digital Image Steganogrpahy Using Universal Distortion In Encrypted Images

[1]M.Shanmugapriya, [2]Mrs.M.Beemajan Saheen
*[1]Pg Scolar , [2]AP/CSE*
*S.Veerasamy Chettiar College Of Engg & Tech,Puliangudi*

***Abstract***

*Digital image steganography using universal distortion in Encrypted Images is paidan attention to achieve a better capability. It divides the embedding procedure intothree rounds to hide the messages. It includes the content owner, the data hider, andthe recipient. The content owner encrypts the original image using a stream cipheralgorithm and uploads cipher text to the server. The data-hider on the server divides the encrypted image into three channels and respectively embeds different amountof bits into each one to generate a marked encrypted image. On the recipient side,additional message can be extracted from the marked encrypted image, and theoriginal image can be recovered without any errors. While most of the traditionalmethods use one criterion to recover the whole image, we propose to do therecovery by a progressive mechanism. Rate-distortion of the proposed methodoutperforms state-of-the-art RDH-EI methods.***

## I. INTRODUCTION

Digital image steganography using universal distortion in Encrypted Images Using Embedding Strategy has been originated from reversible data hiding (RDH) in plaintext images. It is feasible in the applications like cloud storage and medical systems. In cloud storage, a content owner can encryptan image to preserve user privacy, and upload the encrypted data onto cloud side. On the cloud side, when managing huge amount of encrypted images, an administrator can embed messages into the cipher text. This embedding not only saves the storage overhead, but also provides convenient way of searching encrypted images. On the recipient side, when a user downloads the encrypted data containing additional messages from the server, user can loss-lessly recover the original images after decryption. Some attempts on RDH-EI have been made. In a content owner encrypts the original image using stream encrypting, and a data-hider embeds additional bits into cipher text blocks by flipping three least significant bits (LSB) of half the pixels in each block. On recipient side, the cipher text image is decrypted and two candidates for each block are generated by flipping again. As the original block is smoother than the interfered embedded bits can be extracted and original image can be loss-lessly recovered. This method was improved in by exploiting spatial correlation between neighboring blocks to achieve a better embedding rate, which was further improved in a full embedding strategy to achieve larger embedding rate. Secure RDH-EI can be ensured by public key modulation. RDH-EI can also be realized in encrypted JPEG bit streams by slightly modifying the encrypted data. One problemis that data extraction can only be done after image decryption. Separable RDH-EI was proposed to resolve this problem, allowing one to extract hidden data directly from the encrypted image. In the data-hider permutes and divides the encrypted pixels into segments, and compresses some layers of each segment to fewer bits using a predefined matrix. The recipient extracts additional message from the marked encrypted image. After decryption, the original LSBs are recovered by comparing the estimated bits with the compressed. If higher biplanes are used, better embedding rate can be achieved.

Some RDH-EI methods were also proposed to enlarge embedding rates by vacating embedding room before encryption. Rate-distortion is important in RDH-EI. Rate stands for the embedding rate while Distortion the difference between the original image and the decrypted marked image. Users with only the decryption key always need to view the image content by decrypting the marked encrypted image directly. We limit the distortion to three LBS-layers in encrypted images, to preserve the decrypted image with good quality. Subjecting to this condition, we propose a progressive recovery based separable RDH-EI to achieve a better capability, which is an extension. We divide the embedding procedure into three rounds to hide additional messages. Different from the traditional recovery using only one criterion, the progressively recovery uses three criterions. Guaranteed by the progressive mechanism, larger payloads can be achieved.

## II. SUREVEY

**ZhenxingQian et al** propose to do the recovery by a progressive mechanism. Rate-distortion of the proposed method outperforms state-of-threat RDH-EI methods. **Bin Li et al** proposed cost function is designed by using a high-pass filter to locate the less predictable parts in an image and the new cost function is applicable for this approach.
**Somali S.Ekhande et al** proposes; a universal approach for Steganalysis for detecting presence of hidden messages embedded within digital images. This paper describes wavelet like decomposition to build higher order statistical model of natural images.

## III. PROPOSED SYSTEM

A method of reversible data hiding in encrypted images (RDH-EI) based on progressive recovery has been proposed.
• It including three parties: the content owner, the data-hider and the recipient.
• The content owner encrypts the original image and uploads the encrypted image onto a remote server.
• The data-hider divides the encrypted image into three sets and embeds
message into each set to generate a marked encrypted image.
• The recipient extracts message using an extraction key. Approximate image with good quality can be obtained by decryption if the receiver has decryption key.
• When both keys are available, the original image can be loss-lessly recovered by progressive recovery.

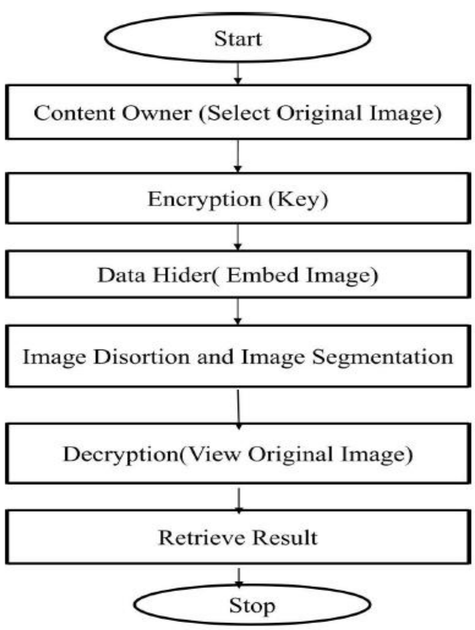



**Figure proposed system flow**

## IV. MODULE SPECIFICATION

• Data Embedding System by Content Owner

• Image Degrade by Data-Hider

• Image Segmentation

• Decryption/Decode

• Performance analysis

## V. DATA EMBEDDING SYSTEM BY CONTENT OWNER

STEGANOGRAPHY aims to hide secret messages into innocuous digital media without drawing suspicion. It faces challenges posed by modern stegno-analysis. This intends to detect the traces of data hiding. We select steganography image and Then Read hidden Data from the Source. The Embedding System has activated after Start the Image and data read from source. In this module we have Embed the data's inside of image pixel. The data will be hidden, then the embedded image has stored in server.

## VI. IMAGE DEGRADE BY DATA-HIDER

While completing the embedding process, next start the image Degrade Process. Here, we retrieve the embedded image from server then apply decomposing function to the selective image.

## VII. IMAGE SEGMENTATION

An image is decomposed into several sub-lattices, where pixels within the same sub-lattice are separated by a distance larger than the support width of the potential function and apply the CMD function Cost assignment and data embedding are performed in each sub-lattice sequentially. The distortion function quantifies the effect of modifying an input cover object to the corresponding output steno object. A distortion function is considered additive when it is expressed as a sum of embedding costs for individual pixels which element-wisely evaluate the effect of respective embedding modification.

## VIII. DECRYPTION/DECODE

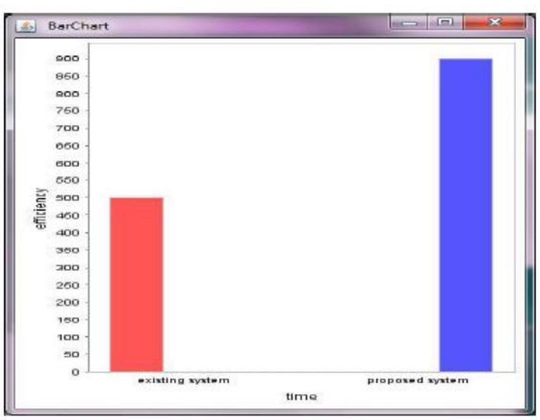
At end of the steganography process, we decode the message using steganography image. After embedding for a sub-lattice, the costs of pixels in the remaining sub-lattices are updated. And find the performance analysis in cost and secure level.

## IX. PERFORMANCE ANALYSIS

Finally we retrieve our results from the end of the process. The Final result can be in Graphical representation format.

## X. IMPLEMENTATION RESULTS






## XI. CONCLUSION

Finally, new RDH-EI protocol for three parties have been proposed. Main improvement is extending the traditional recovery to the progressive based recovery. The progressive recovery based RDH-EI provides a better prediction way for estimating the LSB-layers of the original image using three rounds, which outperforms state-of-the-art RDH-EI methods. Since RDH-EI is equivalent to a rate-distortion problem, capability of the method should be evaluated by both the distortion and the embedding rate. For affair comparison, this paper limits the distortion to threes-layers, and accordingly improves the embedding rate.

## XII. FUTURE ENHANCEMENT

Experimental analysis confirm the effectiveness of our schemes and design. Since, RDH-EI is equivalent to a rate-distortion problem; capability of the method should be evaluated by both the distortion and the embedding rate. We continued the same process with the usage of different algorithm.

## REFERENCES

**[1].** J. Fredric, Reversible Data Hiding in Encrypted Images Using Progressive Recovery, IEEE SIGNAL PROCESSING LETTERS, VOL. 23, NO. 11, NOVEMBER 2016.

**[2].** L. Chen, Y. Q. Shi, P. Sutthiwan, and X.Niu, “Non-uniform quantization in breaking HUGO,” in Proc. 12th Int. Workshop Digit-ForensicsWatermarking, Auckland, New Zealand, Jul. 2014, pp. 48–62.

**[3].** W. Tang, H. Li, W. Leo, and J. Huang, “Adaptive stegno-analysis againstWOW embedding algorithm,” inProc. 2nd ACM Workshop Inf. HidingMultimedia Secure, Salzburg, Austria, Jun. 2014, pp. 91–96.

**[4].** T. Denmark, V. Sleigh, V. Holub, R. Cogranne, and J. Fridrich,“Selection-channel-aware rich model f or stegno-analysis of digital images,”in Proc. IEEE Int. Workshop Inf. Forensic Secure., Atlanta, GA, USA,Dec. 2014, pp. 48–53.

[5]. A.D.Ker et al., “Moving steganography and stegno-analysis fromthe laboratory into the real world,” in Proc. 1st ACM Workshop Inf.Hiding Multimedia Secure., Montpellier, France, Jun. 2013, pp. 45–58.

[6]. J. Fridrich and J. Kodovský, “Multivariate Gaussian model for designingadditive distortion for steganography,” in Proc. IEEE Int. Conf.Accost., Speech, Signal Process., Vancouver, BC, Canada, May 2013,pp. 2949–2953.

[7]. V. Holub and J. Fridrich, “Digital image steganography using universaldistortion,” in Proc. 1st ACM Workshop Inf. Hiding Multimedia Secure.,Montpellier, France, Jun. 2013, pp. 59–68.

[8]. J. Fredric and J. Kodovský, “Rich models for Steganalysis of digitalimages,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882,Jun. 2012.

[9]. Y.Shi, P.Sutthiwan, andL.Chen,“Textural features for Steganalysis,”in Proc. 14th Int. Conf. Inf. Hiding , vol. 7692. Berkeley, CA, USA,May 2012, pp. 63–77. 47

[10] V. Holub and J. Fridrich, "Designing stenographic distortion usingdirectional filters," in Proc. IEEE Int. Workshop Inf. Forensic Secure., Tenerife, Spain, Dec. 2012, pp. 234–239.
[11] G. Liu, W. Liu, Y. Dai, and S. Lie n, "Adaptive steganography bason syndrome-trellis codes and local complexity," in Proc. 4th IEEEInt. Conf.
Multimedia Inf. Newt. Secure. , Nanjing, China, Nov. 2012, pp. 323–327.