Sequential Recovery Based Lossless Data Hiding in RGB Images with Increased Embedding Capacity

Sruthy Raj
PG Scholar
Department of Electronics & Communication Engineering
MBC College of Engineering & Technology Peermade, Kerala, India- 685531

Annmary Thomas
Assistant Professor
Department of Electronics & Communication Engineering
MBC College of Engineering & Technology Peermade, Kerala, India- 685531

Abstract

While transmitting information over untrusted networks the security of the transmitted information is very vital.For this purpose a new approach for reversible data hiding in encrypted image (RDH-EI) with sequential recovery is proposed here. The overall framework consist of a content owner, a data hider and a remote recipient. The content owner encrypts an appropriate cover image for the secret data hiding and data hider embed a confidential data within this using a embedding key where the recipient can access the information only when the encryption and embedding key is obtained. While majority of the existing approaches utilize only direct decryption of the message, we propose to do the recovery by a sequential method where the quality of the recovered image is improved. This proposed technique is a novel approach to hide confidential data within RGB images for increased embedding capacity and increased recovered image quality.

Keywords: Image encryption, Peak Signal to Noise Ratio (PSNR), Reversible data hiding, RGB images, Steganography

I. INTRODUCTION

Our society has entered a period where the vast majority of the everyday administrations are directed and offered over open communication systems. This makes a dependably on accessibility to individuals in any edge of the world. With the progress of communication schemes and their extensive application security of the transmitted data is turning into a more substantial issue. Secure communication is a prime need in numerous applications, for example, to consolidate illustrative data with a picture (like specialist's notes going with a X-beam), inserting remedial sound or picture information on the off chance that deterioration happens from a poor association or transmission, distributed private interchanges, posting secret interchanges on the web to evade transmission, copyright assurance, keeping up secrecy and concealing information on the system in the event of a rupture.

Security in certifiable applications relies on upon numerous issues. Digital multimedia data can be utilised to transmit data over communication network. The information can be conveyed over PC systems with practically zero mistakes and regularly without impedance.

Cryptography and steganography are the widely used methods to improve the security. Both are firmly related yet steganography gives no knowledge of the presence of the secret information. There is a renowned quote in Bhagavad Gita "maunam caivasmi guhyanam" which says "of mystery things I am quiet which is sacred being the ace of all mystery",

II. EXISTING TECHNIQUES

X. Zhang [1] displayed a plan in which cover image is scrambled utilizing a stream cipher. The encoded image is isolated into different non-covering blocks and these each square again into two sets. The information hider inserts extra bits by flipping 3 LSB bits of these sets. The cover image is separated lossless at the recipient end by utilizing spatial correlation. These strategy had certain impediments, for example, each piece is installed just a single piece payload. Also, if the block size is little, the blunder bits of information extraction increment. This strategy did not consider the pixel correlations in the outskirt of neighboring blocks and did not completely abuse the pixels in ascertaining the smoothness of each piece.

A. Technique of side match

Later W. Hong, T. Chen, and H. Wu [2] reversibility property was enhanced utilizing the system of side match. This strategy utilizes spatial relationship between's neighbouring pixel pieces. The cover picture and secret data was recuperated by linking the outskirts of the recouped squares to the unrecovered pieces. This strategy accomplished better embedding rate by diminishing the error rate of extricated bits. In these the seperability property of RDH was not used.

B. Histogram shifting

Later Z. Ni, Y. Shi, N. Ansari, and S. Wei [3]in displayed a RDH method by utilizing the histogram moving. This straightforward technique utilized the extra space for embedding the secret data by moving the a portion of the pixel qualities and others are extended for lossless data embedding. Since the PSNR is around 48.13 dB the visual nature of checked scrambled picture itself is high. The significant restriction of this strategy is the time utilization than other traditional techniques.

C. Difference expansion method

J.Tian [4] has proposed difference expansion method for inserting information in cover pictures. For every pixel combine the whole number normal and difference is figured. The difference is extended keeping in mind the end goal to insert extra piece in the LSB of these pixel match. Quality degradation is similarly low since relationship between's two adjoining pixels is utilized. Compression and decompression causes no loss of information in this technique. The primary confinement of this strategy is blunders because of bit substitution which brings about visual quality degradation.

D. Prediction-error expansion

D.M. Thodi and J. J. Rodriguez [5] proposed a RDH procedure called prediction-error expansion which is a change of difference expansion technique .This strategy enhances the twisting execution at low implanting limits and eases the issue of limit control. This strategy uses the nearby relationship between's in the bigger neighborhood. Prediction error is acquired utilizing a reasonable calculation and this mistake is extended. The variance between forecast result and unique picture is utilized to implant extra information.

A hybrid method strategy was later presented with a calculation comprising three calculations adaptive embedding, Predictive–Error Expansion (PEE) and Pixel choice. Predictive Error extension insert the information and gives validation and uprightness to the client. The proposed framework separates the picture pixels into two sections. Later the required pixel is chosen and versatile installing is performed at the same time.

E. Distributed source coding

The work done by X. L. Li, B. Yang, and T. Y. Zeng [6]was a novel approach in which the cover information is first scrambled and after that compacting it. The compression is done utilizing conveyed source coding standards and is uninformed of encryption key. This paper additionally talked about a related issue of picture hashing. Under a few conditions the encoded information can be compacted to an indistinguishable rate from the first cover picture could have been compressed.

F. Public key modulation scheme

More secure RDH-EI strategy utilizing people in the public key modulation scheme was presented [7]. This strategy utilized a SVM classifier to recognize encoded and non-scrambled picture patches and mutually decoded the implanted message and the first picture flag which thus builds the installing limit. All the above techniques are actualized in PNG or TIF arrange. For JPEG pictures to implant information solid pressure is required which causes the loss of picture substance [8].
Z. Qian, X. Zhang, and S. Wang [9] actualized RDH-EI in JPEG pictures. In this first JPEG picture was acknowledged as a bit stream and scrambled this bit stream. Implanted extra information into the encoded pictures by altering the course of action of this bit stream. The real disadvantage of all these framework was information extraction should be possible simply after picture encryption as portrayed in fig 2.1.

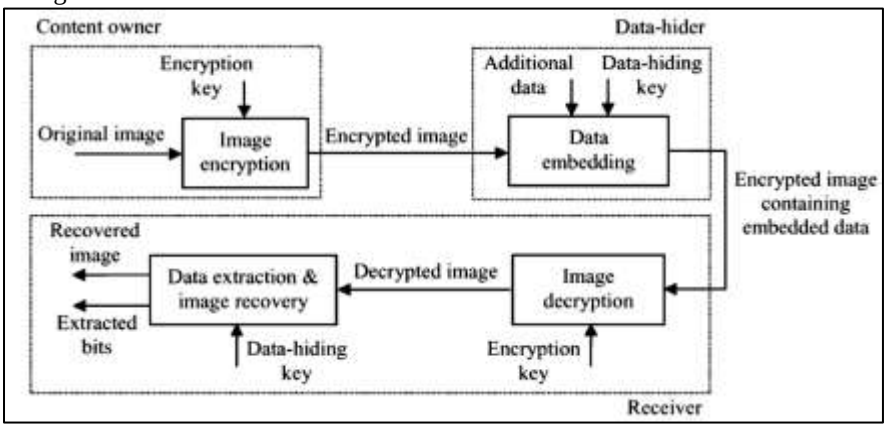

Fig. 2.1 Sketch of non-separable reversible data hiding in encrypted image.

G. Separable reversible data hiding

X. Zhang [10] introduced the idea of distinguishable reversible information covering up in scrambled pictures. In this strategy concealed information is separated straightforwardly from the encoded picture. The encoded picture is permuted and this is again

partitioned into sections. For each section the LSB layers are packed keeping in mind the end goal to install the mystery information. At beneficiary part the first LSBs are recuperated by contrasting the evaluated bits and the packed one. Three cases are presented at the collector side as in fig 2.2. Just with an encryption key or an installing key and the recuperation having them two.

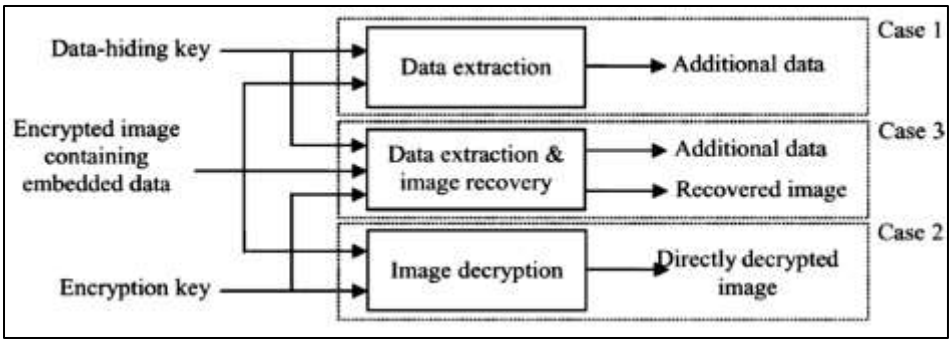

Fig. 2.2: Three cases at receiver side of the proposed separable scheme**.**

II. RDH with LDPC codes

In lossless compression of encrypted information utilizing LDPC codes a fourth LSB layer was utilized for extra information installing. An estimation mistake based information inserting plan was presented by W. Zhang, K. Mama, and N. Yu[11]. A few pixels are evaluated before encryption. A mistake free approach was presented by conjoining the idea of multi granularity encryption and extra mystery information is installed in a few smoother pieces. The primary impediment of this framework is the trouble in room get-away. Keeping in mind the end goal to beat this impediment room holding before encryption was presented. In this strategy extra space for inserting mystery information is purged out before encryption and in this way enhanced the implanting ability to more than ten times as expansive payloads. The weakness of these strategy is that the extra space purged out is constrained to at most 3 LSB –planes per pixel.

I. Sparse encoding

A cross breed approach consolidating benefits of RRBE and seperability property is utilizing patch level meager portrayal spoke to the cover picture as scanty coefficients by inadequate encoding utilizing an over total word reference. The direct inadequate portrayal discharge out a vast meager space for information installing and along these lines limit is moved forward.

The correlation on different information concealing systems was done on the premise of reaction of different strategy toward the parts of information stowing away. The parameter called PSNR is utilized for assessing the nature of the recouped picture.

III. PROPOSED METHOD

The proposed framework is a modification of separable reversible data hiding. The frame work consists of content owner, data hider, and recipient. 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 losslessly recovered by sequential recovery. The general framework for the data hiding is in fig 3.1

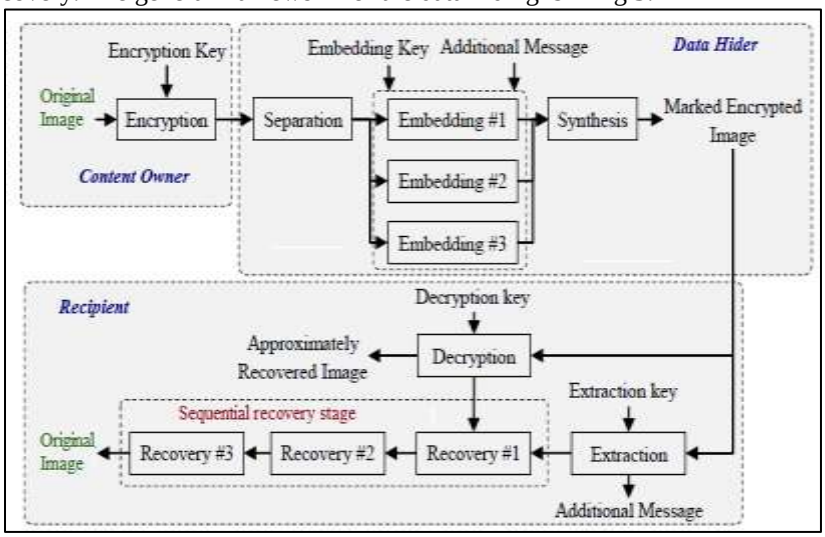

Fig. 3.1: general framework

An RGB image, sometimes referred to as a "true color" image, is stored in MATLAB as an m-by-n-by-3 data array that defines red, green, and blue color components for each individual pixel. RGB images do not use a palette. The color of each pixel is determined by the combination of the red, green, and blue intensities stored in each color plane at the pixel's location. Graphics file formats store RGB images as 24-bit images, where the red, green, and blue components are 8 bits each. This yields a potential of 16 million colors. The precision with which a real-life image can be replicated has led to the commonly used term "true color image". A pixel whose color components are (0, 0, 0) displays as black, and a pixel whose color components are (1, 1, 1) displays as white. The three color components for each pixel are stored along the third dimension of the data array. These properties of RGB image make it more useful in reversible data hiding.

A. Encryption and Embedding Secret Data

Consider an image A of size MxN the encrypted image can be generated by The 3 planes of the RGB image is encrypted using an encryption key K.

$$J = Enc(A, K) = A \oplus K \quad \text{.....(1)}$$

Later into each plane secret data is embedded separately. The data embedding in three planes include the following steps in each separate red, green and blue planes.

1) The pixels of the cipher text image are divided into three sets.
2) With an embedding key E the data-hider pseudo-randomly permutes the encrypted pixels within each set.
3) The data-hider divides each permuted set Si into segments with Li pixel such that $L_1 > L_2$ and $L_1 > L_3$.
4) Collect the bits of three LSB-layers in each segment
5) The data-hider generates three binary matricesG_1, G_2 and G_3 for compressing the groups in the sets S_1, S_2 and S_3
6) Each group $B_i(k_i)$ containing$3L_{i,}$ bits is compressed to $C_i(k_i)$ containing $3L_{i-P,}$ bits. A spare room of P bits in each group is vacated for hiding additional messages.
7) .After inversely permuting each set, the marked encrypted image is generated P bits can be embedded into each group ,an additional message not larger than $P \cdot (R1 + R2 + R3)$ bits can be hidden into the encrypted image
8) The coefficients $\{P, L_1, L_2, L_3\}$ can be embedded into the LSB-layers of some reserved pixels in the encrypted image, and include the original LSB bits into the additional message

On the recipient side, additional messages can be extracted if the receiver has the key E .The marked encrypted image is separated the set again. With the E the recipient permutes pixels in each set independently, and divides the permuted sets into segments each of which contains L_i pixels. Collect the bits of three LSB-layers in each segment and reconstruct the groups $B_i'(k_i)$From each group, the additional bits *are* extracted.

If the recipient has only the key K an approximate image is obtained .Since the distortion is limited to three LSB-layers, the directly decrypted image still preserves good quality

In case both K and E are available original image is obtained with high quality by the recipient identifies the best candidates from 2^Ppossible candidates and sequentially recovers each group through three rounds.

1) First round

Estimate pixel values within the Square set.

$$\tilde{p}_{i,j} = \frac{\left[p_{i-1,j}/8\right]+\left[p_{i,j-1}/8\right]+\left[p_{i+1,j}/8\right]+\left[p_{i,j+1}/8\right]}{4} \cdot 8 + 4$$

For each candidate vector , put these bits into the original 3LSB-layers

construct an enciphered pixel segments, and then decipher the pixel segments using E , finally we get the pixel values $t_{i,j}$.

Calculate the difference D. $t_{i,j}$ that makes D smallest is the original pixel.

$$D \quad \sum_{(i,j)\in G_i(k_i)} \left| t_{i,j} - \tilde{p}_{i,j} \right|$$

Update the reference image by substituting pixels in the square set with the original pixel $t_{i,j}$.

2) Second round

predicts the values within the Triangle set uisg the foloowing equation

$$\hat{p}_{i,j} = \left[\frac{\hat{p}_{i-1,j-1} + \hat{p}_{i+1,j-1} + \hat{p}_{i-1,j+1} + \hat{p}_{i+1,j+1} + 8 \cdot \left(\left[p_{i-1,j}/8\right]+\left[p_{i,j-1}/8\right]+\left[p_{i+1,j}/8\right]+\left[p_{i,j+1}/8\right]\right)+16}{8} \right]$$

3) Third round

predicts the values within the circle set using following equation

$$\tilde{p}_{i,j} = \left[\frac{\hat{p}_{i-1,j} + \hat{p}_{i,j-1} + \hat{p}_{i+1,j} + \hat{p}_{i,j+1}}{4} \right]$$

IV. WORK IMPLEMENTATION

Recovered image quality assessment was done on the basis of PSNR values. Higher the PSNR value higher is the quality of the recovered image. A group of experimental results are shown in table 1 in which different grey scale images where used to hide the secret message followed by the sequential recovery of cover image. The message embedded within the image was "hai dear...how are you...I am fine". The message was retrieved successfully and the recovered image PSNR values are listed in the table below.

Table - 4.1
PSNR values of different test samples (greyscale images)

Test sample	*PSNR*
boat	*59.7529*
barbara	*59.2309*
lena	*59.1658*
peppers	*58.9080*
baboon	*59.5911*
skull	*59.5012*

Later for the increased embedding capacity this sequential recovery based image recovery mechanism was extended to RGB image. In RGB 3 color planes make more space for the additional data without the degradation of the original image. Experimental Results for "Lena" is given below. Embedding capacity was found to be 39320 bits to embed the data "hai dear...how are you...I am fine" and the PSNR was found to be 63.6628 which was greater than the traditional methods

Fig. 4.1: Experimental Results for "Lena "shows the original image, the encrypted image, the marked encrypted image and the final recovered image through various stages

A group of experimental results are shown in table 4.2 in which different RGB images where used to hide the secret message followed by the sequential recovery of cover image. The message embedded within the image was "no secret"

Table - 4.2
PSNR values of different test samples(RGB)

Test sample	*PSNR*
lena	*64.0367*
butterfly	*64.0754*
tides	*64.0282*
mountain	*64.0152*

V. CONCLUSION

This novel method extended the traditional recovery method to the sequential recovery to improve the quality of the recovered image and also provide a better prediction way for estimating the LSB-layers of the original image using three rounds. Improve the embedding rate to a great extent by make use of RGB images. The embedded confidential information was extracted successfully and without any error. This technique can be used in many untrusted networks to communicate about confidential information. The proposed method acts as robust scheme that achieve better embedding capability and higher payloads with low computational complexity.

REFERENCES

[1] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett, vol. 18, no. 4, pp. 255258, Apr. 2011.
[2] W. Hong, T. Chen, and H. Wu, An improved reversible data hiding in encrypted images using side match, IEEE Signal Processing Lett vol. 19,no. 4, pp. 199–202, Apr. 2012.
[3] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans .Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354– 362, Mar.2006.
[4] J. Tian, "Reversible data embedding using a difference expansion" Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890 2003.
[5] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans .Image Process., vol. 16,no. 3, pp. 721–730, Mar. 2007.
[6] X. L. Li, B. Yang, and T. Y. Zeng, "on adaptive prediction-error expansion and pixel selection Image Process., vol. 20, no. 12, pp. 3524.
[7] M. Johnson, P. Ishwar, V.M. Prabhakaran, D. Schonberg and K. Ramachandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992-3006, Oct. 2004
[8] J. Zhou, W. Sun, L. Dong, et al. Secure reversible image data hiding over encrypted domain via key modulation, IEEE Transactions on Circuits and Systems for Video Technology, vol. 26,no. 3, pp. 441–452, Mar. 2016
[9] Z. Qian, X. Zhang, and S. Wang, Reversible data hiding in encrypted JPEG bit stream, IEEE Transactions on Multimedia vol. 16, no. 5, pp. 1486–1491, Aug. 2014.
[10] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Transactions Information Forensics and Security, vol. 7, no. 2, pp. 826–832, Apr. 2012
[11] X. Zhang, Z. Qian, G. Feng, and Y. Ren, "Efficient reversible data hiding in encrypted images," J. Vis. Commun. Image Represent. vol. 25, no. 2, pp. 322–328, Feb. 2014.
[12] W. Zhang, K. Ma, and N. Yu, "Reversibility improved data hiding in encrypted images," Signal Process., vol. 94, pp. 118–127, Jan. 2014.
[13] Z. Yin, B. Luo, and W. Hong, "Separable and error-free reversible data hiding in encrypted image with high payload," Sci. World J., vol. 2014, Mar. 2014, Art. ID 604876
[14] K. Ma, W. Zhang, et al. Reversible data hiding in encrypted images by reserving room before encryption, IEEE Transactions Information Forensics and Security, vol. 8, no. 3,pp. 553–562, Mar. 2013.
[15] X. Cao, L. Du, X. Wei, et al. High capacity reversible data hiding in encrypted images by patch-level sparse representation, IEEE Transactions on Cybernetics, 46(5): 1132-1143, 2016