REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES USING DISPERSED SPRING ENCRYPTING

V.V. Vinoth
Research Scholar
Department of ECE
Bharath University, Chennai
India
E-mail:vinothvv.velaian@gmail.com

Dr. B. Karthik
Associate Professor
Department of ECE
Bharath University, Chennai,
India
E-mail: karthik.ece@bharathuniv.ac.in

Abstract —**This paper presents a new method of reversible data hiding in encrypted images using distributed source coding.The data owner using stream cipher when the original image is encrypted. Then data hider selects some bit sequence and compress that bit sequence, using this bit sequence in the encrypted image and then reserved a room for the secret data. Slepian–Wolf encoded with low-density parity-check codes used in selected bit series. As well as the receiver has encryption key only, the receiver can recover the original image exactly with more feature using an image estimation algorithm. In that case, the receiver has both embedding and encryption key then using distributed source decoding receiver Extract secret data and absolutely recover the original image.**

Index Terms—I**Image recovery, reversible data hiding (RDH), Image encryption, data owner, data hider, receiver,distributed source coding**

I.INTRODUCTION

In day to day real life, many people‟ scan shared more information witheach other. Sometime this information is more secrete or in the form of images or so on. In a number of applications liked as delegated calculations, cloud computing the data owner needs for further processing transmits data to a remote server. In several cases, the data owner may not believe service provider so data owner needs before uploading encrypt the data. The service provider should capable to do processing in encrypted data. Several working or data processing is done on encrypted data. For example, adding a watermark to an encrypted image, compressing the encrypted image [1]-[3]. A common framework of redundancy compression [4], difference expansion [5], andhistogram shifting (HS) [6] approach. But using this approaches originalimage cannot be used directly after than image encryption.

As a new tendency allows the service provider to use RDH in encrypted images liked to embed additional messages, e.g., image metadata, labels, notations, or authentication information, without accessing the original contents into the encrypted images. The main aim is exactly recovering original image as well as at receiving side hidden msg properly extract. RDH in encrypted images is attractive. For example, in medical applications, a patient does not allow their medical images to be exposed to any outsiders, while the database administrator may needto embed medical records or the patient's information into the encrypted images. On the other hand, the original medical image for diagnosis must be recovered without error after decryption and retrieval of the hidden message.

This paper aims to increase embedding goods in encrypted images. We intend an autonomous RDH method using Slepian–Wolf source encoding for encrypted images [7].The design is motivated by the distributed sourcecoding(DSC) in which we encode the selected bits taken from the stream-ciphered image using low-density parity check(LDPC) codes [8] into pattern bits to make room to accommodate the secret data. With two different keys, theprojected method is separable. The unseen data can be totally extracted using the embedding key and the original image can be around reconstructed with high feature using the encryption key. With both keys available, the hidden data can be extremely extracted and the original image correctly recovered with the aid of some predictable side information. The projected method achieves a high embedding good and good image reconstruction feature and avoids the operations of room reserving by the data owner.

II.PREVIOUS WORKS

In this part, the modern RDH techniques of embedding the secret message in encrypted images are reviewed RDH for the encrypted image is generally considered for the applications in which the data-hiderand the image owner are not the same parties. The data-hider cannot access the image substance, and the secret message is seized by the data-hider. Thus, encryption is done by the dispatcher, hiding by the data-hider, and data extraction and/or image renovation by the receiver.

In VRAE, data owners encrypted straight the original image, and the data-hider embeds the extra bits by modifying several bits of the encrypted data.

The idea was first projected in, in which the owner encrypts the original image by higher Encryption Standard, and the data-hider embeds 1 bit in each block containing n pixels, meaning that the embedding rate is 1/n bpp. On the receiver side, data extraction and image recovery are realized by analyzing the restricted standard variation throughout decryption of the distinct encrypted image. This technique requires that image decryption and data extraction operations must be done in cooperation. In another language, extraction and decryption are indivisible.

In VRAE, data owners encrypted straight the original image, and the data-hider embeds the extra bits bymodifying several bits of the encrypted data. The idea was first projected in, in which the owner encrypts the original image by higher Encryption Standard, and the data- hider embeds 1 bit in each block containing n pixels, meaning that the embedding rate is 1/n bpp. On the receiver side, data extraction and image recovery are realized by analyzing the restricted standard variation throughout decryption of the distinct encrypted image. This technique requires that image decryption and data extraction operations must be done in cooperation. In another language, extraction and decryption are indivisible.

In the VRBE, the original images are processed by the owner before encryption to create spare space for data embedding, and the secret data are embedded into specified positions by the data-hider. For example, the method in creates embedding room in the plaintext image by embedding LSBs of certain pixels into other pixels using a traditional RDH method. The preprocessed image is then encrypted by the owner to generate an encrypted image. Thus, positions of these vacated LSBs in the encrypted image can be used by the data-hider, and a largepayload up to 0.5 bpp, can be achieved. With a similar idea, another method based on an estimation technique was proposed, in which a large portion of pixels are used to estimate the rest before encryption, and the final version of the encrypted image is formulated by concatenating the encrypted estimating errors and a large group of encrypted pixels. Additional bits can be embedded into the encrypted image by modifying the estimated errors. With this method, peak signal-to-noise ratio (PSNR) of the approximate image reconstructed by the receiver is higher than the previous methods.

In summary, methods in both VRAE and VRBE categories are effective for RDH in encrypted images. However, there are some limitations. VRAE RDH methods for encrypted images, estimation technique is necessary for the receiver, because no prior information of the original content is available except that he/she knows that the cover is a natural image. In traditional methods, LSB planes of the encrypted image are modified to accommodate theadditional message, and the image recovery is based on estimating the original LSB planes withan assessment criterion, such as the fluctuation function. Because these estimations are not accurate enough, the recovery is only suitable for the case when a small number of additional bits were embedded.

III.SYSTEM DESCRIPTION

The projected system is sketched in Fig. 1, which consists of three phases:

1) Image encryption
2) Data embedding and
3) Data extraction/image recovery.

In phase I, the data owner encrypts the original image into an encrypted image using a stream cipher and an encryption key. In phase II, the data-hider selects and compresses some MSB of the secret image to generate a spare space, and embeds additional bits into the encrypted image using an embedding key. In phase III, the receiver extracts the secret bits by using the embeddingkey. If he/she has the encryption key, the original image can be approximately reconstructed via image decryption and estimation. When both the encryption and embedding keys are available, the receiver can extract the compressed bits. Implement the source decoding using the estimated image as side information to perfectly recover the original image.

Encryption:

The Encryption is the procedure of encoding communication or information. In the encryption organization, the anticipated announcement gen or message, discussed to as ordinary text, is encrypted using an inscriptional algorithm.

Room Reserve:

Reserve the room (bandwidth) earlier the encryption of documents which is workingto be sent from sender to receiver through a network.

Decryption:

Decryption is the method of altering data that partakes been extracted scrawledcomplete encryption rear to its encrypted form. In decryption, the system extracts and exchanges the corrupted data transforms it into script and images that are effortlessly reasonable not only bythe bookworm then also by the system.

Encrypted Image Generation

In this module, to build the encrypted image, the rest stage can be divided into two steps:

- Image Partition
- Self-Reversible Embedding followed by image encryption.

At the establishment, image partition phase splits the inventive image into two fragments and then, the LSBs of are reversible with an ordinary RDH system so that LSBs of can be used for accepting communications; at last, encrypt the shuffled image to yield its final version.

Image Partition:

The operator here for reserving a room before encryption is a standard RDH technique, so the goal of image, partition.

Self Reversible Embedding:

The goal of self-reversible embedding is to embed is to embed the LSB-planes of into by employing traditional RDH algorithm. We simplify the method in to demonstrate the process of self-embedding.

Data Hiding In Encrypted Image:

In this module, Use standard cipher a content owner encrypts the original image with an encryption key. The content owner hands over it to a data hider and the data hider can embed some auxiliary data into the encrypted image by lossless some room according to a data hiding key.

Data Extraction and Image Recovery:

In this module, Extracting Data from Encrypted Images to succeed and modernize private information of images which are encrypted for guarding clients privacy, a substandard database administrator may only catch entrance to the data hiding key and have to influence data in the encrypted field. After the database manager gets the data hiding key, he can decrypt and extract the supplementary data by directly understanding the decrypted version. When requesting for modernizing information of encrypted images, the database manager, then, updates information concluded LSB additional and encrypts updated information according to the data hiding key all over again. As the whole process is entirely functioned on the encrypted domain, it sidesteps the outflow of original relaxed.

Data Extraction and Image Restoration

In this module, after producing the marked decrypted image, the content owner can advance extract the data and improve the original image.

IV.ALGORITHM

RDH:

Data hiding is a span including an extensive variety of applications for embedding messages in satisfied. Generally, hiding material rescinds the host image even, however, the alteration introduced by hiding is undetectable to the humanoid visual system. Conversely, around are certain delicate images aimed at which any embedding misrepresentation of the image is excruciating, such, military images a, medical images or sculpture conservation. For images like in the medical field, level insignificant changes are insupportable for of the prospective leeway of a surgeon mistaking the image. In other applications, such as remote recognizing it is also desired that the original protection television can be convalesced since of the essential high-precision landscape. In these belongings, an extraordinary thoughtful of data hiding method called reversible data hiding or lossless data hiding is used. Reversible data hiding (RDH) techniques are premeditated to disentangle the problem of lossless embedding of enormous messages in digital images so that after the embedded message is removed, the image can be refurbished fully to its original state before embedding befallen.

Phases of RDH:-

- Data Embedding
- Data Extraction

To embed the data in the image we need these inputs:

- The data to be embedded i.e. surreptitious data
- The protection data (cover image or host image)
- The key.

By conjoining these an appropriate algorithm is spawned which yield a stego image (stego cover) that can be warehoused or transferred. To the further end, the decoder or extractor collects the stego image and the stego key (optional) and extracts the data. In some algorithms, the decoder exertion is only to check that data is essentially embedded in the categorizer or not. It is in the case where the secret data are a logo originally placed in the cover to substantiate proprietorship.

A significant article of reversible data hiding is the reversibility, that is, one can confiscate the embedded data from the stego image to reestablish it to the inventive image.

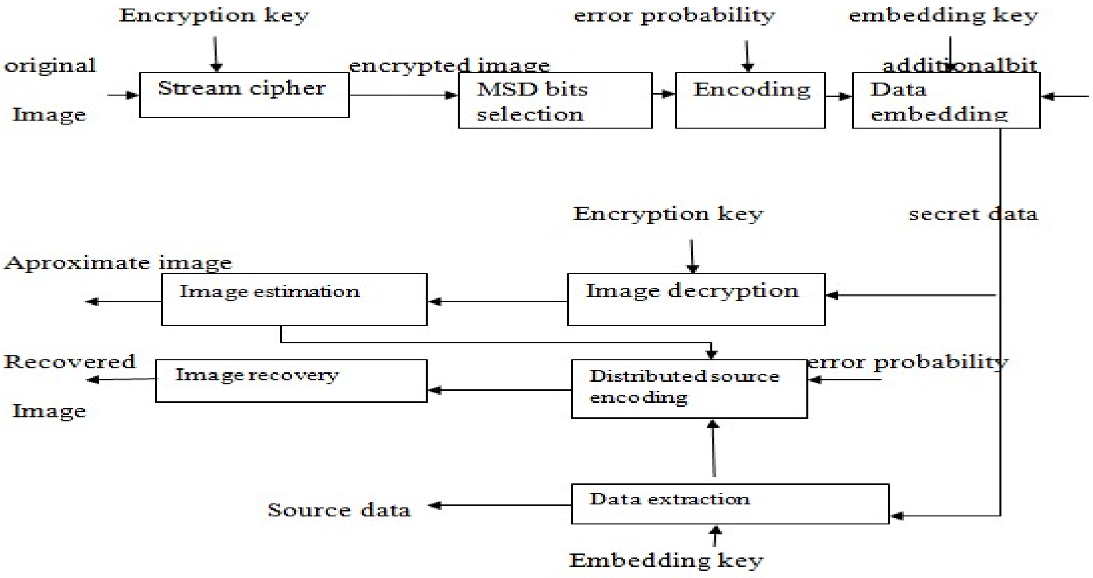

Fig.1 RDH using Distributed Source Coding

From the standpoint of evidence hiding, reversible data embedding hides some material in an arithmetical image such a way that only an approved party can decode the hidden data/information and also could restore the image to its primeval, creative state. The important metrics to determine the performance of reversible data-embedding algorithm are:

1) Payload capacity limit: determines the maximal amount of information that can be embedded.
2) Visual quality: determines how the visual quality of the embedded image is.
3) Complexity: determines the algorithm complexity.

LDPC:

Today, LDPC codes in coding theory one of the newest topics. Firstly developed in the early 1960's, they have practiced an amazing comeback in the last little years LDPC codes are already well-found with very profligate (probabilistic) encoding and decoding algorithms, unlike several other classes of codes. The question is that of the design of the cryptography such that these algorithms can recuperate the inventive code word in the face of greataggregates of clatter. The combinatorial tools make and new methodical using it possible to solve the design problem. The LDPC codes create not only smart from a speculative point of view but also perfect for real applications.

V.RESULT ANALYSIS

Several experiments were performed to evaluate the performance of the proposed system. Multiple techniques were used in order to prove our system better than the existing system. They are 1) Framework for RDH. 2) Histogram shifting. 3) Differential expansion.

Framework for RDH:

By first extracting compressible features of the original cover and then compressing them loss-lastly, spare space can be saved for embedding auxiliary data.

Histogram Shifting:

The difference histogram for most natural images would be similar to this, in the sense that did reference values with small magnitudes occur more frequently. Consider a process of select-in locations for expansion embedding from the set of expandable locations that involves selecting suitable bins from the histogram of expandable did erects. The bins whose dif- fervencies have smaller magnitude are given preference in the selection process because the smaller the magnitude of the expandable did Terence, the smaller the resulting distortion. Distortion resulting from expansion-embedding did erect with value 0 and 1 are equal (in a probabilistic sense, assuming equip-probable information bits). It is easy to see that did Terence values that are equidistant from 0.5 contribute equally towards the embedding distortion**.**

Differential expansion:

In this section, we combine the did Terence-expansion embedding technique with our proposed extensions. In these two algorithms, we use the histogram-based procedure for locationselection and use histogram shifting to enable the decoder to identify these selected locations.The two algorithms did err in the approach in which the decoder ideates the set of expandable locations. As we have seen from the discussion, the locations thatare not expandable have gray levels closer to the minimum or maximum and, thus, may over own upon expansion. In the rest algorithm, an over own map, indicating the locations that are not expandable, is embedded with the payload. In the second algorithm, age bits are interspersed with the payload to identify these locations.

Security:

Keys:

In the existing system, no secret keys are divided into parts so security provides is less. A single key is used for encryption an also for decryption. So a hacker can easily hack the key and get encrypt the con denial data.

In the proposed system the key is split into two parts. So two keys are used for encryption and after this, these two keys are again merged with additional two keys for more security purpose. So receiver needs these two keys for decrypting the data. If a hacker gets one key he can’t hack the data.

Room Reserved:

In the existing system, no room (bandwidth) is reserved while transferring the data from sender to receiver so the time required for transferring the data is more. In the proposed system room (bandwidth) is allocated while transferring data from sender to receiver so the time required for transferring the data is less compare to the existing system.

VI.CONCLUSION

Slepian–Wolf encoded with low-density parity-check codes used in selected bit series. Aswell as the receiver has encryption key only, the receiver can recover the original image exactly with more feature using an image estimation algorithm. In that case, the receiver has both embedding and encryption key then using distributed source decoding receiver Extract secret data and absolutely recover the original image.

REFERENCES

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

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3] X. Zhang, G. Feng, Y. Ren, and Z. Qian, “Scalable coding of encrypted images,” IEEE Trans. Image Process., vol. 21, no. 6,pp. 3108–3114, Jun. 2012.

[4] T. Kalker and F. M. J. Willems, “The Capacity of bounds andconstructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digit. Signal Process. (DSP), 2002, pp. 71–76.

[5] J. Fridrich, M. Goljan, and R. Du, “The Lossless data embedding to all image formats,” Proc. SPIE, Secur. Watermarking Multimedia Contents,vol. 4675, pp. 572–583, Apr. 2002.

[6] J. Tian, “Reversible data embedding using a difference expansion, ”IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8,pp. 890–896,Aug. 2003.

[7] D. Slepian and J. K. Wolf, “The Noiseless coding of correlated information sources,” IEEE Trans. Inf. Theory, vol. IT-19, no. 4, pp. 471–480, Jul. 1973.