INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PRODUCING ENCRYPTED IMAGES BY RESERVING SPACE BEFORE ENCODING USING REVERSIBLE INFORMATION CONCEALMENT

M.Shanmuga Priya[1], S.Sherlin Vinolea Merlin[2], M.Vidhya[3], J. Anitha Shylin[4]

[1]*BE (CSE), ULTRA college of Engineering, Madurai, India*
[2]*BE (CSE), ULTRA college of Engineering, Madurai, India*
[3]*BE (CSE), ULTRA college of Engineering, Madurai, India*
[4]*Assisstant Professor, ULTRA college of Engineering, Madurai, India*

Abstract: - A Reversible data concealment produced in encrypted images has a magnificent property that the real cover can be lossless which is recovered after embedded data is extracted while protecting the image content's security and confidentiality. Each and every method contains embedded data by using reverse vacating room for the encrypted images some errors may occur on data extraction and in image restoration. Reserving room before encryption with a RDH algorithm that precedes traditional reversible data hiding, it is easy for the data hider to reversibly embed data in the encrypted image. In this paper, reversibility technique is used the data extraction and image recovery are free of any error. This algorithm used to "reserve space before encryption". We tend to 1st empty out space by using RRBE in embedding LSBs of some pixels into different pixels with a conventional RDH technique and so write the image. Hence, the positions of those LSBs within the encrypted image will be used to embed the data. In image encryption cipher technique is used for Data Extraction and Image Recovery.

Index: Reversible data concealment, security, image encryption, Data embedding, Image recovery.

1. Introduction

RDH is an algorithm to retrieve the cover image lossless after the data extraction. Whereas, this technique is widely used in military, law forensics the original cover distortion is not allowed. Encryption is an effective and popular means as it provides confidentiality and converts the original and meaningful content to incomprehensible one. In previous work RDH employs space by compression of images (i.e., vacating after the encryption is done). Hence large payload is not possible. To overcome this problem we introduce a concept reserve space by splitting image into smoother areas which increases the embedding rate [1].

Achieving the rate-distortion bound as long as the compression algorithm reaching entropy defines the equivalence between data compression and RDH for binary covers. RDH technique has emerged in recent years. Then, constructing a framework for RDH is done by first extracting compressible features of original cover and then compressing them lossless, spare space can be saved for embedding auxiliary data [2]. In RDH another promising strategy is used in which space is saved for data embedding by shifting the bins of gray values.

The confidentiality for images is done through encryption which is an effective means as it converts the original and meaningful contents to incomprehensible one [3]. Although few RDH techniques in encrypted images have

published yet, there are some of the promising applications if RDH can be applied to encrypted images. A reputation-based trust-management scheme enhanced with data coloring. Apparently, the cloud service provider has no right to introduce permanent distortion during data coloring into encrypted output.
Thus, coloring technique of a reversible data is based on encrypted data which is preferred [4]. Suppose a medical image database is stored the server in the data center can embed notations into an encrypted adaption of an image through a RDH technique. With the notation, the server can image or verify its integrity without having the knowledge of the original content, and thus privacy is secured.

2. Generation of Encrypted Image

Then the encrypted image is divided into several blocks. By flipping LSB of the half of pixels can be transferred as an embedded bit. The data extraction and image recovery proceed by finding which part has been flipped in one single block. This process can be realized with the help of spatial correlation in decrypted image. Then, by further exploiting the spatial correlation using a different estimation equation side matching is done to achieve much lower error rate. That is, the encrypted image must be decrypted first before data extraction. By separating the extraction from image decryption, an out space is emptied for data embedding the idea of compressing encrypted images. Encrypted data compressed can be formulated as source coding with side information that the compressed data in lossless manner by exploiting the syndromes of parity-check matrix of channel codes [6]. The proposed system not only separate data extraction from image decryption but also achieves excellent performance in two different prospects:

- Image recovery is free of any error and data extraction.
- Decrypted image containing data which is improved the range and is enlarged.

In this framework, a content owner encrypts the original image using a standard cipher with an encryption key [7]. The content owner hands over it to a hider and the encrypted image is been produced. (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according to data hiding key.

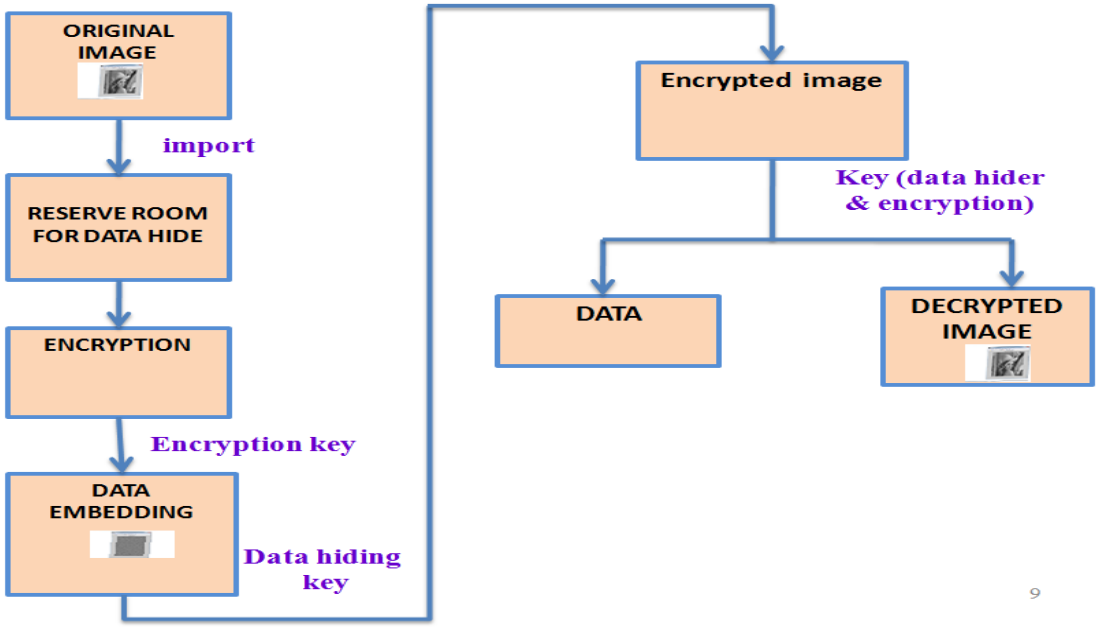

Figure.1 Architecture encrypted image, decrypted image

The new idea about reversible data hiding in encrypted image without loss can be achieved by proposed system. Reserving room before encryption in this we first lossless compress the redundant image and then encrypts it with respect to maintain privacy the implementation is carried in following ways.
In this we first empty out room i.e. creating space in the image before encryption of image the RDH task in encrypted image would be more natural and much easier and real reversibility is realized this can be achieved by

first lossless compress the redundant data of image in this way space is created for embedding data and then encrypts the image by different encryption technique [8]. Actually, to construct the encrypted image, LSBs are reversibly embedded onto messages and the rearrangement is done is done for the message to be generated at its final version [9].

2.1) Image Partition

This is used to construct the smoother area of image by RDH algorithm. This smoother area is used in future to embed the data. The input for this module is the cover image and length of the embedding data bits. The reserving room before encryption is a standard RDH technique, constructing a smooth area is the goal of image partition, on which standard RDH algorithms such as can achieve performance without loss of original image which is displayed generality, assume the original image is an 8 bits and its size is M×N and pixels $C_{i,j} \in [0,255]$, $1 \leq I \leq M \leq j \leq N$. the original image is extracted from the first owner, on rows along, containing blocks the number for the block is determined by the size of to be combined messages, which can be denoted as one. To say in detail about this, each and every block contains m rows, where, m= [l/N] and the number of blocks can be computed through n= m+1. An important point here is that each block is overlapped by pervious and/or sub sequential blocks along the rows. For each block, it defines a function measuring a first order smooth.

2.2) Embedding the image using self-Reversible method

The goal of self-reversible embedding is used embedding LSB planes considering as A onto B on RDH algorithm. Further then estimating the bugs of black pixels with the help of surrounding white pixels that may have been modified [10]. Error sequence is generated which can accommodate messages and can also implement multilayer embedding scheme by considering the modified B as "original" when needed. Exploiting can be done by all pixels of B, two estimating error sequences which are constructed in embedding messages in each and every single layer process.

2.3) Image Encryption

The output from the previous system is converted into secret image by XOR ciphering technique with the key and image [11]. The output is the ciphered image with space for embedding data. Then, after the rearrangement of the self-embedded image the encryption is done by constructing the encrypted image, which is initiated as E .the self-embedded image is obtained by the encryption version with the stream cipher. Considering a gray value ranging from 0 to 255 can be represented by 8 bits.

2.4) Data Embedding

For embedding only a small portion of messages: 1embedding data into peak points by making use of part error sequence and searching for proper points in the histogram of estimating errors. The comparison results are the first solution performs better than the other when cover image is relatively smooth with little fine-detail regions, In this data will be embed into the free space (LSB Planes) which is reserved during the encryption process. The key will be used to embed the data.

3. Usage of RRBE instead of VRAE

Vacating room after encryption (VRAE), in this encrypts the original image using a standard cipher with an encrypted key. Then the encrypted image is been produced, then the owner of the content produce it to data hider and the data hider can embed data into the encrypted image by lossless vacating some room according to a data hiding key.

But some of drawbacks of VRAE are,

- It Reduces the correctness of data extraction
- Larger payload of data impossible. For large payloads distortion may occur.

This proposed a novel method using RDH algorithm in images, for which vacating of room is done after encryption as done in previous methods, before encryption it reserves the room. In reversibility the data is extracted and image is recovered are free of any error. By using this larger payload data is possible.

Since data extraction is completely independent from image decryption, the order of them implies two different practical applications.

Case 1: Data Extracted from Encrypted Images

To manage and update personal information of images which are encrypted for protecting privacy only get permission to access the data hiding key and have to execute the data in a encrypted form. The order of data extraction before image decryption guarantees the feasibility of our work. Database manager gets the data hiding key, in which decryption is done on LSB-plane of and extracts the data which could read the decrypted version directly. When requesting for updating information of images takes place. Then process is operated entirely, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key. It avoids the leakage of the original content which is operated on the encrypted domain.

Case 2: Data Extracted from Decrypted Images

In Case 1, the extraction of the data is manipulated in encrypted form. On the other hand, there is a different situation that the user wants to decrypt the image first and extracts the data from the decrypted image when it is needed. In that encrypted images, the cloud server marks the images by embedding some notation, including the identity of the image owner, the identity of the cloud server, i.e., including the notation, the decrypted images are handled, trace the source and history of the data. Image decryption before/without data extraction is perfectly suitable for this case.

Case3: Data Hiding Key

This key is present at the data hiding center as well as receiver side the data hider can embed some auxiliary data into the encrypted image according to the data hiding key. The receiver maybe the content owner himself or can be an authorized party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to encryption key.

4. Related Work

The concealment using reversible and executing the encrypted image before vacating room is the paper format. This paper deals with the original work partition an encrypted image into block. The data extraction and image recovery can be achieved by examining the block smoothness. But it, reduce the correctness of data extraction. Watermarking concept providing efficient reversible technique based on a complete adaptive prediction-error expansion pixel. This paper presents by Prediction-error expansion (PEE) is an important technique of reversible watermarking which can embed large payloads into digital images with low distortion. Here the decryption key is need for the data retrieval.

Improved and reversible data concealment through encrypting images uses side match. This deal with The existing method encrypted images by a better scheme for measuring the blocks smoothness, decrease the error rate of extracted-bits. But, large payload of data is possible. Separable reversible data concealment in encrypted image is been used. In this paper, a data-hider may compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate some additional data. But in this only Small payload is possible.

5. Conclusion

Reversible data concealment in encrypted images in encrypted images is a new technology which is Drawing enormous attention because of its ability to uphold the content owners privacy and maintain integrity of data also real reversibility of data is realized, that is data extraction and image recovery are free from any error because of these requirements from cloud data management. Proposed methods implement RDH in encrypted images by vacating room before encryption, which is exactly opposed to the existing method of RDH in which we were vacating room after encryption. Thus the data hider gets advantage from the extra space which is created by vacating the room in previous stage to make data hiding process effortless because of proposed method. Thus the proposed method can take benefit of all previous RDH techniques for plain image and attain extremely good performance without loss of privacy and data's quality. the proposed method can achieve real reversibility, separate data from encrypted version of image and highly improve the quality of marked decrypted images.

REFERENCES

[1] W. Zhang, B. Chen, and N. Yu, "Capacity-approaching codes for reversible data hiding," in *Proc 13th Information Hiding (IH'2011), LNCS 6958*, 2011, pp. 255–269, Springer-Verlag.
[2] W. Zhang, B. Chen, and N. Yu, "Improving various reversible data hiding schemes via optimal codes for binary overs," *IEEE Trans. Image Process.*, vol. 21, no. 6, pp. 2991–3003, Jun. 2012.
[3] J. Fridrich and M. Goljan, "Lossless data embedding for all image formats," in *Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.
[4] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003.
[5] 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.
[6] 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.
[7] X. L. Li, B. Yang, and T. Y. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Dec. 2011.
[8] P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible image hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, 2009.
[9] L. Luo *et al.*, "Reversible image watermarking using interpolation technique,"*IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[10] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.
[11] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC, 1996.
[12] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data colouring," *IEEE Internet Comput.*, vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.
[13] 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.

M.Shanmugapriya, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

S.Sherin vinolia merlin, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai.

M.Vidhya, currently studying B.E. computer science and engineering in ultra college of Engineering and Technology for women at Madurai

Ms.J.Anitha shylin received her bachelor's degree from M.A.M College of engineering and Technology, Trichy(2012), and then did her Master Degree in computer science and engineering from Vins Christian College of Engineering , Nagercoil (2010), affiliated to. She is currently working as an Asst Prof in Ultra College of Engineering & Tech for Women, Madurai.