International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 2 089– 092

Reversible Data Hiding in Encrypted Image using Visual Cryptography

Nuzhat Ansari
PG Student, Dept. of CSE
Rajiv Gandhi College Of Engg. Research & Technology
Chandrapur. India
e-mail: ansari.rumi@yahoo.in

Prof. Rahila Shaikh
Asst. Professor, Dept. of Computer Technology
Rajiv Gandhi College Of Engg. Research & Technology
Chandrapur. India
e-mail: rahila.patel@gmail.com

***Abstract*:** In computerized world the protection of the data is essential. And one of the popular solution for data protection is encryption. In this method the ordinary signal is converted into unintelligible data for maintaining confidentiality. Now-a- days, reversible data hiding is gaining lot of popularity. This technique is nothing but hiding the data inside a cover file, so that the data and the cover file can be properly received at the receiver. In this paper, we propose an approach where reversible data hiding approach works before encryption to make data hiding process effortless. We also use visual cryptographic approach for encryption which help to protect the image during transmission. Sieving, Division and shuffling process of SDS algorithm are used which makes the proposed approach as keyless with the complete lossless image recovery and data extraction. The scheme is suitable for authentication based application where collective acceptance and decision making plays an important role. The main goal is to retrieve the original image with lossless process and minimum computation during image encryption/decryption by using keyless approach which reduces the task related to key management and key generation and also gives new direction towards the future.
Keywords *— image encryption, reversible data hiding, Visual Cryptography, Sieving, Division, Shuffling, Difference Expansion*

*****

I. INTRODUCTION

Security has gained a lot of importance with the advancement of information technology. Maintaining the secrecy and confidentiality of data in transmission has always being an issue of concern. Various traditional approaches like Cryptography, Steganography can be used to achieve security of data. . The cover image where the data is hidden is called a stegno-Image. In addition, the quality of cover image is important after using it for steganography. Data hiding conceals the existence of secret information while cryptography protects the content of messages.

Reversible Data hiding is the method of hiding data inside a cover file so that both the data and the cover file could be recovered lossless at the receiver. The transmitter side of such systems involves a cover image, additional data, encryption key and data hiding key. The original image will be encrypted, data will be hidden and then image will be transmitted. The receiver thus needs to decrypt the image and extract the data. For maintaining the security of images two different approaches can be employed that is one encrypting the image using the encryption keys and second approach can be without using the keys, where the image is divided into different shares to maintain the image secrecy. This allows the visual information to be encrypted in such a way that their decryption can be performed by human visual system. Unfortunately heavy computation cost and key management limit the employment of the first approach and the poor quality of the recovered image from the random shares limit the application of the second approach.

As long as images are concerned data hiding which cannot perceive between stego- image and cover image by human, the cover image still can get harmed in processing. Many different techniques have been proposed to get back the cover image lossless. The reversibility means not only embedding data but also original image can be precisely recovered in the extracting stage. Most hiding techniques perform data embedding by altering the contents of a host media. As a result the host image cannot be completely recovered after the bit extraction. These types of data hiding techniques are thus irreversible. Encryption of images with the traditional encryption algorithms such as RSA, DES etc. was found inapt due to some typicality of images such as its bulk size and also the correlation amongst the pixels. However in a number of domains such as military, legal and medical imaging although some embedding distortion is admissible, permanent loss of signal fidelity is undesirable. This highlights the need for Reversible (Lossless) data embedding techniques. Thus the proposed approach gives a novel technique for reversible data hiding using visual cryptography. With the scheme involving use of secret keys have limitations as regards key management. In addition in some cases the available keys for encryption are limited (restricted key space), also high computation involved in encryption. All these factors comprise the problem domain for using traditional encryption techniques in reversible data hiding. In opposite to this approach the method using visual cryptography techniques involve no use of keys for encryption keeping computational cost for encryption /decryption low.

The proposed technique involves splitting an image into multiple shares. The shares so generated reveal no information about the original secret image and to retrieve the secret image all the shares are required. The proposed technique is implemented with the SDS algorithm and involves three steps. In step one (Sieving) the secret image is split into primary colors. In step two (Division) these split images are randomly divided. In step three (Shuffling) these divided shares are then shuffled each within itself. Finally these shuffled shares are

combined to generate the desired random shares. This technique involves computation during the encryption and decryption stages and the results are to be viewed on the computer monitors hence it is natural for us to use the additive color model. The scheme that we present here is a (z, z) threshold scheme i.e. for retrieving a secret image that has been divided into z shares all z shares are required. No shares individually convey any information about the secret image, nor do a combination of subset of random shares. Introducing a framework for reversible data hiding for embedding data in an image by reserving room before encryption. Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient

A) Reversible Data Hiding:
Reversible data hiding is an approach where data is hidden in an encrypted image. A reversible data hiding is an algorithm, which can recover the original image losslessly from the stego-image after the hidden data have been extracted. This important technique is widely used in medical imagery, military imagery and law forensics where no distortion of original image is allowed.

B) Visual Cryptography:
Visual cryptography (VC) is a process where a secret image is encrypted into shares which refuse to divulge information about the original secret image. Its strength is a fact that the decryption of the secret image is through human visual system without computation.

II. Related Work

Lots of research has been done in the area of reversible data hiding. In last few years various efficient methods have been proposed for reversible data hiding and color image visual cryptography.

Reversible data embedding has drawn lots of interest recently. Being reversible, the original digital content can be completely restored. As the amount of information needed to be embedded (payload and original values in the embedding area) is larger than that of the embedding area and the space saved from compression will be used for embedding the payload. Jun Tian [1] introduced a DE technique, which discovers extra storage space by exploring the redundancy in the image content. Employing the DE technique to reversibly embed a payload into digital images. During data embedding, all changeable difference values are modified, by either adding a new LSB (via the DE) or modifying its LSB. To guarantee an exact recovery of the original image, the original values of those modified LSBs will also be embedded.

Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu and Fenghua Li in [2] has proposed a framework for reversible data hiding for embedding data in an image by reserving room before encryption. Since losslessly vacating room from the encrypted images is relatively difficult and sometimes inefficient.

Another promising approach has been proposed by Siddharth Malik, Anjali Sardana, Jaya in [3] which involve three main steps that are Sieving, Division and Shuffling to generate random shares. This approach promises the minimal computation requirement for generation of the original secret image from the random shares without any loss of image quality.

In the area of reversible data hiding José .R; Abraham .G, in [6] have proposed a novel scheme to reversibly hide data into encrypted grayscale image in a separable manner. Content owner encrypts the image by permuting pixels using encryption key. The data hider hides the data into the encrypted image by histogram modification based hiding by using data hiding key.

Using keyless techniques for encrypting the image involves various visual cryptography techniques which involves secret sharing of an image by dividing it into multiple shares. Combining the random shares generates the original image. Various schemes have been proposed for recovering the image losslessly from the random shares. Jithi P V, Anitha T Nair in [7] has proposed the scheme based on Progressive Visual Cryptography. In proposed method, a digital watermarking technique is used to generate meaningful shares. The secret image shares are watermarked with different cover images and are transmitted. At the receiving side the cover images are extracted from the shares and stacked one by one which reveals the secret image progressively.

Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, Eli in [10] proposed a novel reversible data hiding technique, which enables the exact recovery of the original host signal upon extraction of the embedded information. A generalization of LSB (least significant bit) modification is proposed as the data embedding method, which introduces additional operating points on the capacity-distortion curve. Lossless recovery of the original is achieved by compressing portions of the signal that are susceptible to embedding distortion, and transmitting these compressed descriptions as a part of the embedded payload. It represents a high-capacity, low-distortion, lossless data embedding algorithm. They employ the lossless image compression algorithm CALIC, with quantized values as side-information, to efficiently compress quantization residues to obtain high embedding capacity.

III. Proposed Work

The proposed method gives an efficient technique to overcome the limitations of existing schemes in the area of reversible data hiding. Reversible data hiding using images is the

technique by which the original cover image can be losslessly recovered. The proposed scheme suggests the novel approach for data hiding and image encryption. Since losslessly vacating the room from the encrypted image is relatively difficult and sometimes inefficient thus proposed scheme apply a method of vacating the room for data prior to the image encryption [1], thus vacated room can be used to hide the secret data. By reversing the order of encryption and data hiding we overcome the difficulty of finding the room for data from already encrypted image. In addition this scheme does not involve the use of keys for encryption, has low storage and bandwidth requirements, while also keeping the computation cost during encryption /decryption low.

Reserving the room for vacating the data involves partition of original image into two parts A and B then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages. Then next step is to embed the data into vacated area. Now after embedding the data this image will be encrypted using SDS algorithm. SDS algorithm involves the three main steps Sieving, Division and Shuffling. **Sieving** as the name suggests involves filtering the combined RGB components into individual R, G and B components. Having filtered the original image into the R, G and B components the next step involves **dividing** the R, G and B components into parts or shares.

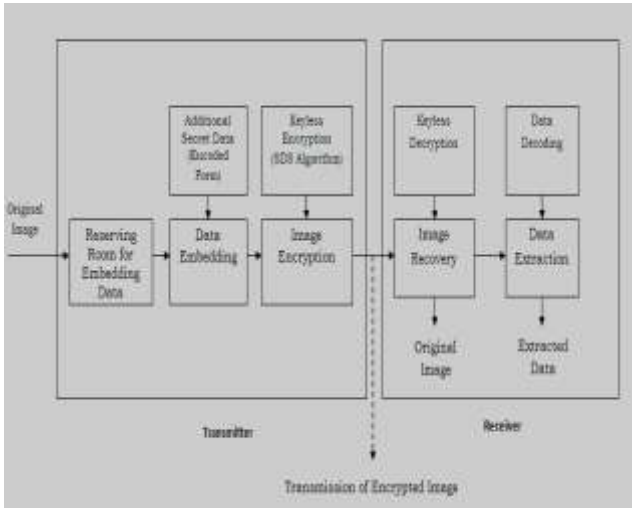

Fig.1: Framework for Proposed Scheme

A. Vacating room for embedding data:

Reserving the room for vacating the data involves partition of original image into two parts A and B then, the LSBs of A are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages.

B. **Image_Encryption_using_keyless_SDS_algorithm Sieving:** Sieving as the name suggests involves filtering the combined RGB components into individual R, G and B components. The granularity of the sieve depends the range of values that R/G/B component may take individually. To make the process computationally inexpensive, sieving uses the XOR operator.

Division: Having filtered the original image into the R, G and B components, the next step involves dividing the R, G and B components into z parts/ shares each.

R _ (RA, RB, RC, ----------, RZ)
G _ (GA, GB, GC, ----------, GZ)
B _ (BA, BB, BC, ----------, BZ)

While dividing it is ensured that each element in RA-Z, GA-Z and BA-Z is assigned values randomly, such that the entire domain is available for randomized selection; in case x = 8, then individual elements should be randomly assigned a value varying from 0- 255. The shares so generated should be such that (RA, RB, RC, ---------- RZ) should regenerate R and similarly for G/B components.

Shuffling: Though experimental results have shown that the random shares created by division in no way exhibit any resemblance to the original image, but as a second step towards randomizing the generated shares i.e. RA-Z, GA-Z and BA-Z , we perform the shuffle operation. This involves shuffling the elements in the individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from the same primary color. In other words RB decides how RA is shuffled, RC decides how RB is shuffled, ---------- RZ decides RZ-1 is shuffled and RA decides how Rz is shuffled. The shuffling operation uses the comparison operator on the LSB of the determining element to decide the shuffle sequence.

C. ***Original Image Recovery:***

The process of retrieving the original image involves sieving the random shares and retrieving R/G/B(A-shuffle) and R/G/B(B-shuffle), thereafter from the individual shuffled shares the original RA, GA , BA and RB, GB , BB are generated. Using these the original image is then generated. The retrieved image is same as original and no loss of picture quality occurs.

D. ***Data Extraction:***

After we get all the shares of the image the image can be reconstructed and from the reconstructed image the data can be retrieved. In the data retrieval process the new pixel value are considered and difference is calculated. The LSB of the difference is the bit which was hided. For this the data retrieval method require the index position of those blocks which were considered in hiding process and the pixel pairs position where the data is hidden as the input. Extracting the LSB and the embedded bit ‘b’, this gives the original value.

IV. CONCLUSION

Reversible data hiding in encrypted image is drawing lots of attention because of privacy preserving requirements. Thus proposed scheme provides a completely new framework for

reversible data hiding. Here in this approach I have used a new technique for reserving room before encryption of image. Thus the data hider can benefit from the extra space emptied out in previous stage before encryption to make data hiding process effortless. In the proposed approach we take advantage of visual cryptography approach for encrypting the image. Thus the image is protected in transmission and secret data is also transmitted securely. The employed technique involves the three main steps that are seiveing, division and shuffling the images. Thus random shares are so generated from shuffled shares of image are transmitted. As this approach does not involve any use of keys is keyless approach for image encryption with the complete lossless image recovery and data extraction.

V. REFERENCES

[1] Jun Tian "Reversible Data Embedding Using a Difference Expansion" Transactions on circuits and systems for video technology, VOL. 13, NO. 8, AUGUST 2003

[2] Kede Ma, Weiming Zhang, Xianfeng Zhao, Nenghai Yu, and Fenghua Li, " Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption" , IEEE Transaction on Information Forensics and Security, Vol.8, No.3, March 2013*)*

[3] Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption",2012 international conference on Communication systems and Network Technologies ©2012 IEEE

.

[4] Yu Jing, Song Wei,"Study on Reversible Data Hiding Scheme for Digital Images", 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics(CAR 2010) © IEEE

[5] Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Halftoning Technique",8th International Conference on Information Science and Digital Content Technology(ICIDT),© IEEE 2012

[6] Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference ©IEEE 2013

[7] Jithi P V, Anitha T Nair, "Progressive Visual Cryptography with Watermarking for meaningful shares", International Multi-Conference on Automation , computing , Communication , control and Compressed Sensing (iMac4s), 2013

[8] Wen-Chung Kuo, Shao-Hung Kuo, Lih-ChyauWuu, "High Embedding Reversible Data Hiding Scheme for JPEG", Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing,(IIH-MSP),Oct,2010. .

[9] Ching-Yu Yang, Chi-Hung Lin and Wu-Chih Hu, "Reversible Data Hiding for High-Quality Images Based on Integer Wavelet Transform", Journal of Information Hiding and Multimedia Signal Processing ©2012 ISSN 2073-4212.:

[10] Mehmet U. Celik, Gaurav Sharma, A. Murat Tekalp, Eli Saber, "Reversible Data Hiding", IEEE ICIP 2002.

[11] Ankit Chaudhary, J. Vasavada, J.L. Raheja, Sandeep Kumar, Manmohan Sharma, "A Hash Based Approach for Secure Keyless Stegnography in Lossless RGB Images", 22nd International Conference on Computer Graphics and Vision, GraphiCon'2012.

[12] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion",ICASSP 2009 © IEEE 2009

[13] J. Fridrich, M. Goljan, and D. Rui, "Lossless Data Embedding - New Paradigm in Digital Watermarking", In Special Issue on Emerging Applications of Multimedia Data Hiding, Vol. 2, pp. 185-196, February 2002

[14] Moni Naor and Adi Shamir, "Visual cryptography", in Proceedings of Advances in Cryptology EUROCRYPT 94, LNCS Vol. 950, pages 1-12. Springer-Verlag, 1994

[15] Yi-Hui Chen, Ci-Wei Lan, Chiao- Chih Huang, "A Verifiable Visual Cryptography Scheme", Fifth International Conference on Generic and Evolutionary Computing 2011.