R.Brindha et al, International Journal of Computer Science and Mobile Applications,
Vol.5 Issue. 9, September- 2017, pg. 32-38 **ISSN: 2321-8363**
Impact Factor: 4.123

LOSSLESS AND REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES WITH PUBLICKEY CRYPTOGRAPHY: A REVIEW

R.Brindha[1], M.Hemamalini[2]
[1]Research Scholar, Department of Computer Science, A.V.C College(autonomous), brindha241094@gmail.com
[2]MCA., M.Phil., SET., Assistant Professor, A.V.C College(autonomous), maliniavcce@gmail.com

ABSTRACT: Image processing is processing of image in order to improve its quality. Now a day, more focus is on reversible data hiding (RDH) in encrypted images, so it maintains the excellent property that the original cover image can be easily recovered without any loss after embedded data. All previous Techniques embed data by reversibly vacating room from the encrypted images, which may be leads to some errors on data extraction and image restoration. A reserving room before encryption with a RDH algorithm and Least significant Bit (LSB) algorithm, histogram Shift (HS) algorithm, thus it is easy for the user to reversibly embed data in the encrypted image. The RDH and LSB algorithms, which can recover the original image without any loss from marked image after the hidden data have been extracted.
Keywords: Reversible data hiding, lossless data hiding, image encryption, public key cryptography, histogram shift and LSB.

I. INTRODUCTION

The problems of data security arise in many fields such as Medical image system, Remote sensing, Law-forensics, Military imaging, Social medias, Secrete agencies, require sensitive data transmission which should have high security. while the encryption procedures change over plain text content into mixed up cipher text, the information concealing insert extra information into spread media by slight alterations.

Information concealing can be performed with lossless reversible way. Purpose of data hiding is nothing but to maintain the security for sensitive data. Data hiding method is lossless if the display cover image containing embedded data is same as that of original cover image. To provide security to sensitive data we encrypt the cover image using encryption key [1].

Encryption is way to enhance the security of a messages or file by scrambling the contents so that is can be read only by someone who has the right encryption key to unscramble it. Information hiding technique is lossless if the display of cover signal containing installed information is same that of unique cover the fact that the spread information.

A RDH algorithm for encrypted images sender can reversibility embeds data into the encrypted images without using encryption key used by the owner. By this method the sender can implement reversible data embedding directly in the encrypted image without knowing the original contents image. Image encryption generates a pseudo random bit stream as encryption key uses the original image by a bitwise operation. Then the encrypted image sends to data hider [1].

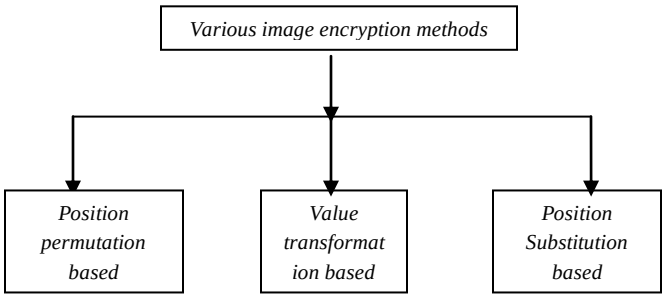
Data embedding all the data hider divides an encrypted image into non overlapping block size, and one data will be embedded into each block and then according to data hiding key, for each image block, LSB embedding technique where exact recovery of the embedded information. Signals are used for embedded distortion can transmit compressed description as part of the payloads and lossless recovery of original compression portions HS based RDH, high capacity and low distortion can be achieved efficiently. In this technique, space saved for data embedding by shifting the bits of histogram of gray values [1]. The LSB is the method of adjusting the carrier

Images LSB pixels. This technique is used for embedding images LSB plane of image in a deterministic order.LSB substitution is workable for GIF formats,
GIF image is significant bit is change the entire color palette will be changed. Thus its utilizes LSB Substitution for embedding the data into images, One of the basic LSB approaches is "Optimum Pixel Adjustment Procedure" [2].

II. VARIOUS IMAGE ENCRYPTION METHODS

The encryption algorithm performs various substitution and transformations on the plain text. The image encryption algorithm can be categories into three major groups,

- Position Substitution based algorithm
- Transposition based algorithm
- Value transformation based algorithm



Various image encryption methods

A. Position permutation (Transposition) based algorithms:

Transposition technique is a very different kind of mapping that is achieved by performing some sort of permutation on the plain image. The rearrangement of element can be done by bit, pixel and block wise the permutation of bits decreases the perceptual Information, permutation pixel and block produce high level n security. The permutation technique the bits in each Pixel are permuted using the permutation keys with the key length equal to 8. In the 8 pixel permutation are taken as a group and permuted with same size key. The combination of block, bit and pixel are used respectively[3].

B. Value transformation based algorithms:

This algorithm is based on the technique in the value of each pixel is change to some other value. The new value of pixel is evaluated by some algorithm in pixel, we take input as a pixel value compute it, with some formula produce a new value for that pixel value transformation based algorithm are digital signature and lossless image compression and encryption using SCAN, image crypto system, color image encryption using double random phase encoding, image encryption using block- based transformation algorithm and affine transform[3].

C. Position substitution based algorithms:

It can be combined, in this technique first pixels are reordered and then a key generator is used to substitute the pixel values[3].

III. RELATED WORKS

Zhang et al. It approaching the codes for reversible data hiding and improve the recursive code construction achieve the result that is rate distortion bound that uses the concept of compression algorithm. This system defines many befits such as reduce the distortion, improve the RDH schemes for spatial [4].

Ni et al. referred to as data hiding, has recently been proposed a technique for information assurance. Owing to data hiding, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the original hidden data have been extracted out. Classification of data compression algorithm can be referred to as lossy data hiding. It can be shown the most of the data hiding algorithm reported in the literature are lossy .major data hiding algorithm utilized spread spectrum, water-marking technique, either in DCT domain , round off error and /or truncation error may take place during data embedding[5].

Tian has proposed a system which uses different expansion method for embedding data in reversible manner for digital images. He describes how to measure the performance of the system by using concept of reversible data embedding. This can be measure through various factors such as the payload capacity limit. Visual quality and complexity this system uses the difference between two neighboring pixels. The LSB's of the differences are all zero and this embedded to the message. The system are no loss of data while performing compression and decompression [6].

Luo et al. Have used an interpolation technique for reversible image water-marking. It restore the original image without any distortion after performing the extract ion hidden data. In this system we can embedded large amount of convert data for imperceptible modification. Digital water-marking is the form of data hiding that are used to embed the convert information into digital signal. It provide low distortion rate and larger capacity [7].

Celik et al. presented by compressing quantization residues. They embedding lossless image compression algorithm with quantized values as side information, to efficiently compress quantization residual to obtain high embedding capacity. The compressed residual and the payload data are concatenated and embedded into the host signal via generalized LSB modification method [8].

Ke de Ma et al. proposed reversible data hiding in encrypted images by reserving room before encryption a new method, the content owner reserves a room for additional Data before encryption, by using traditional RDH method, embedding LSB of some pixel into other pixel and empty out the room and after that encrypt the image. Then the additional data is embedded on these rooms. On the receiver side, receiver can extracted and decrypted correctly. Limitation of this method is amount of the additional data is less [9].

Xinperg Zhang et al. in reversible data hiding in encrypted images based on progressive recovery proposed a new method for data hiding. There persons are involved in this process. Content owner encrypts the original image and upload cipher text into server. The data hider resides on the server divides the encrypted image into three channels and embed different amount of data into each one and make it marked encrypted image. The receiver can extract the additional data from marked encrypted image and plaintext image can recovered it can embed a large amount of data. But main disadvantage of this method is higher distortion rate [10].

Guo et al. proposed a novel procedure that In this scheme, given that multiple owners create an image distinct keys are given to only an authorized group of owners so that only when all the members in the group present their key scan the ownership of the image be verified. This process is based on generalized secret sharing scheme, multiple watermarks, one for each owner's key and one for the secret key are embedded so that both full ownership and partial ownership can be verified. Spread spectrum watermarking schemes, quantization watermarking schemes usually quantize the values of host images spatial domain or in the spectrum domain to a pre specified set of values according to binary watermarking bits. Thus, the watermark information is completely contained in the watermarked images and the watermarking detector can detect the embedded watermark blindly [11].

Wei Liu et.al suggested a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes. In this method they developed resolution progressive

compression, which has been shown to have much better coding efficiency and less computational complexity than existing approaches .Wei Liu and et.al observed that lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources such as images, they are trying to improve the compression efficiency. such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. Resolution progressive compression is used for this problem, which has much better coding efficiency and less computational complexity than existing approaches [12].

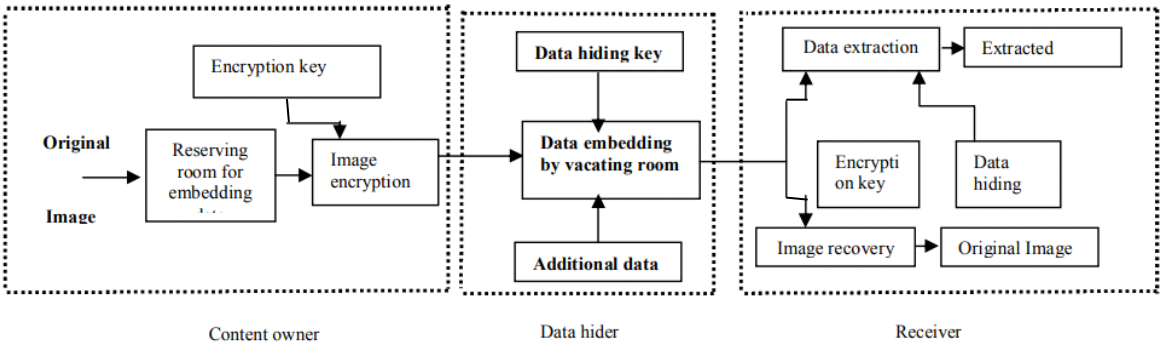
Shiguo Lian et.al suggested a different scheme composed of joint data-hiding and encryption schemes. In this system a part of cover data is used to carry the additional message and the rest of the data are encrypted, so that both the copyright and the privacy can be protected. Here motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients [13]. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be re watermarked.

IV. REVERSIBLE DATA HIDING IN ENCRYPTED IMAGES BY RESERVING ROOM BEFORE ENCRYPTION

In this framework in which the redundant image content is losslessly compressed and then Encrypts it with protecting privacy. RRBE consist four stages

[1]. Generation of encrypted image.
[2]. Data hiding in encrypted image.
[3]. Data extraction.
[4]. Image-recovery.

Reversible data hiding means extraction and image recovery is without any loss. If we reverse the order of encryption and vacating room, RRBE means firstly vacate room and then image encryption at sender side[1].



RRBE Framework

If uses three algorithms

[5]. Reversible Data Hiding (RDH)
[6]. Least Significant Bit (LSB)
[7]. Histogram Shift(HS)

RDH algorithm for encrypted images In which the sender can reversibly embed data into the encrypted images without using encryption key used by the content owner. By this method the sender can implement reversible data embedding directly in the encrypted images without knowing the original image content[1].

a) GENERATION ON ENCRYPTED IMAGE

To construct the encrypted image, divided into three steps:

[8]. Image partition
[9]. self-Reversible embedding
[10]. image encryption

At the beginning image partition step divides original image in two parts P and B : the LSBs of P are reversibly embedded into B with a standard RDH algorithm so that LSBs of A can be used for accommodating messages encrypt the re arranged image to generate[1].

b) DATA HIDING IN ENCRYPTED IMAGE

Once the data hider acquires the encrypted image, can embed some data does not access to the original image. The embedding procedure starts with encrypted version of P. data hider to read bits of information in LSB's of first encrypted pixels .encrypts according to the data hider sets a point out the end position of embedding process. Data hiding key to marked the encrypted image[1].

c) DATA EXTRACTION AND IMAGE RECOVERY

A lossless and reversible data hiding schemes for public-key-cryptography images are in this method With lossless scheme data embedding, and data does not affect the plaintext content and data extraction is also performed in encrypted domain. The additional data embedded by the reversible scheme cannot extracted before decryption, in which data extraction in either of the following in either of the two domains is feasible[1].

d) ADVANTAGES

[11]. It can perform compression as well as data encryption back side of image.
[12]. Easy to hide the large amount of data background of image.
[13]. High performance without data loss.
[14]. Free from any error.
[15]. No image distortion.

V. LITERATURE SURVEY OF COMPARISON TABLE

Paper	Authors, Year	Technique used	Advantages
Improving Various reversible data hiding schemes via optimal codes for binary covers,	W.Zhang, B.Chen, and N.Yu 2012.	Used Decompression Algorithm as the coding scheme for embedding data.	The proposed code construction is proved to be optimal when the compression algorithm.
Reversible image watermarking using interpolation technique	Luo et al, Zhang Xiong, 2010.	It utilize the interpolation-error, its different between interpolation value, and corresponding pixel value, to embed bit "1" or "0" by expanding.	Embed a large amount of cover data into images, and achieves better image quality the computational cost of the scheme is small.

Reversible Data Hiding With Optimal value Transfer	Xinpeng zhang,2013	The optimal rule of value modification under a payload distortion criterion is found by using an iterative procedure, and a practical reversible data hiding scheme is proposed.	The optimal transfer mechanism gives a new rule of value modification and can be used on various cover values.
Separable reversible data hiding in encrypted image.	Xian ting Zhang,2012	Separable reversible data hiding which consists of image encryption, data embedding and data extraction, image recovery phases.	Simple Less computation.

VI. CONCLUSION

RDH 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. To implement RDH in encrypted images by vacating room before Encryption, which is exactly opposed to the existing method of RDH in vacating room after Encryption.

Thus the data hider get advantage from the extra space which is created by vacating the room in previous stage to make data hiding process effortless because of this method.RDH Techniques for plain image and without loss of privacy and quality of data.

REFERENCES

[1]. Sharvi Dixit, Archana Gaikwad, IJESC "Public key Cryptography Based Lossless and Reversible Data Hiding in Encrypted Images",vol 6, issue no.4,2016.

[2]. Artz,D, "Digital Steganography: Hiding data within data", IEEE Internet computing , June 2001.

[3]. Gajendra Singh Chandel ,Vinod Sharma, Uday Pratap Singh , "Different Image Encryption Techniques-Survey and Overview ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 8, August 2016 ISSN: 2277 128X.

[4]. W.Zhang,X.Hu.X.Li,and N.Yu, "optimal Transition probability of reversible data hiding for general Distortion Metrics and Its Applications," IEEE Trans. On image processing, 24(1), pp.294-304, 2015.

[5]. Z.Ni.Y.Q.Shi, N.Ansari, and W.Su, "Reversible data Hiding,"IEEE Trans. Circuit Syst. Video Technol., vol.16, No.3, 354-362, Mar.2006.

[6]. J.Tian, Reversible Data embedding using a different Expansion, IEEE Trans. on Circuits and Systems For Video Technology,13(8),pp.890896,2003.

[7]. L. Luo et al. "Reversible image watermarking using interpolation technique, "IEEE Trans. vol.5, no.1, pp.187-193, Mar.2010.

[8]. Celik, et al, "Lossless Generalized-LSB data Embedding, IEEE Trans. on Image Processing, 14(2), pp.253266, 2005.

[9]. Kede Ma, Wei.Zhang, "Reversible data hiding in encrypted images by reserving Room before encryption", IEEE Trans. On information and security.vol.8, no.3, March 2013.

[10]. X.inpeng Zhang, Member ,IEEE "Reversible Data Hiding with optimal value transfer "IEEE Trans on multimedia, vol.15, no.2,February.2013.

[11]. H. Guo, N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing scheme", Multimedia Systems, vol9, no. 3, 2003.

[12]. W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images," IEEE Trans. Image Process, vol. 19, no. 04,,pp. 1097-1102, Apr 2010.
[13]. S. Lian, Z. Liu, Z. Ren, and H. Wang, “Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technology, vol. 17, no. 6, pp.774-778, Jun 2007.

