IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 5, Ver. II (Sep - Oct .2015), PP 01-07
www.iosrjournals.org

Reversible Data Hiding in Encrypted Images using Rhombus Method by RRBE

[1]Jewel Vincent Chittilappilly, [2]Tressa Micheal,
[1]Department of Electronics and Communication Engineering Rajagiri School of Engineering and Technology Kochi, Kerala
[2]Assit. Professor Department of Electronics and Communication Engineering Rajagiri School of Engineering and Technology Kochi, Kerala

***Abstract**: Nowadays the data security and data integrity are the two challenging areas for research. Usually, hiding data destroys the host image. However in RDH , if the embedded image is deemed authentic, we are able to reverse it to the precise copy of the initial image before the embedding occurred. Encryption is an effective and popular method to provide confidentiality for images. In the proposed method, the first step is to empty out room by embedding LSBs of some pixels into other pixels by a Rhombus method. Then encrypt the image, so that the positions of these LSBs in the encrypted image can be used to embed data. Later on, data is hidden and the entire image is again encrypted. This method ensures that extraction of data and recovery of image is free of any error.*

I. Introduction

Reversible data hiding is a technique to embed additional image into another image , for example military or medical images, in a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden image[1]. Hiding data inevitably destroys the host image even if the distortion introduced by hiding is imperceptible to the human visual system. However, there are some sensitive images like medical image sharing, multimedia archive management and image trans-coding wherever any distortion because of data embedding is intolerable and also the availableness of the initial image is in high demand. To the present finish, a solution known as reversible data hiding (RDH) is proposed, in which the host image are often totally restored after data embedding.RDH is a hybrid method which mixes numerous techniques to make sure the reversibility. Its feasibleness is mainly because of the lossless compressibility of natural images. For example, even slight changes in medical pictures aren't accepted because of a possible risk of a medical practitioner giving a wrong explanation of the image. Hence, reversible data hiding techniques provides a answer to the problem of how to embed a message in digital images in a lossless manner in order that the image are often fully restored to its original state before the embedding occurred. Encryption is an effective means of privacy protection. To share a secret image with other person, a content owner may encrypt the image before transmission. In some cases, a channel administrator needs to add some additional message, such as the origin information, image notation or authentication data, within the encrypted image however he does not know the original image content. It may be also expected that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. That means a reversible data hiding scheme for encrypted image is desirable[1]. Data hiding is defined as a process to hide data (representing some information) into cover media. That is, the data hiding process links two sets of data, a set of the embedded data and another set of the cover media data. In most cases of data hiding, the cover media becomes distorted due to data hiding and cannot be inverted back to the original media. Hence the cover media has permanent distortion even after the hidden data has been removed. In some applications, such as medical diagnosis and law enforcement it is desired that the original cover media can be recovered efficiently with no loss. The marking techniques satisfying this requirement are referred to as reversible, lossless, distortion-free or invertible data hiding techniques.

II. Proposed Scheme

RRBE consists of 4 stages such as:

A. Generation of Encrypted Image.

For the construction of the encrypted image, there are three stages: image partition, self reversible embedding and image encryption. At the beginning, image partition step divides original image into two parts A and B.

The general framework of RRBE is as shown below:

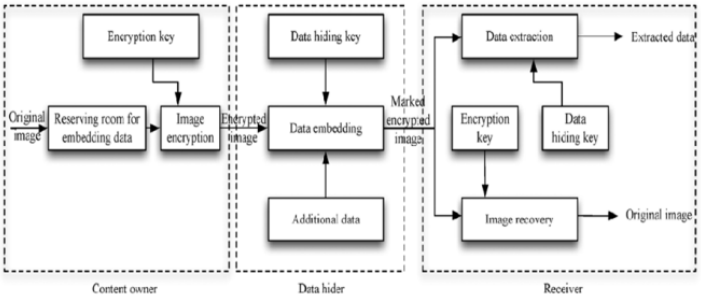

Fig 1: General Framework of RRBE

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; at last, encrypt the rearranged image to generate its final version.

1) Image Partition: The main goal of this method is to partition the original image C into two parts A and B so that we can achieve an area B upon which we can perform RDH. Original image C is an 8 bits gray-scale image with its size M*N and pixels C_{ij} [0,255], 1< i< M , 1< j< N divides into two parts A and B.

2) Self reversible embedding: The main goal of this step is that LSBs of A are reversibly embedded into B with a standard RDH algorithm called Rhombus method and room is also reserved for embedding data so that LSBs of A can be used for accommodating messages.

Rhombus Method: To predict the pixel value position U_{ij}. Neighboring four pixel of U_{ij} are used in the form of rhombus. Here this five pixel comprise a cell which is used to hide one bit of data. Even and odd pixels are used for data embedding.

1.Calculate U_{ij},$U_{ij}=U_{i},j-1+Ui+1,j +U_{i},j+1+U_{i}-1,j/4$

2. Based on the value U_{ij} then we calculate error e,where $e=U_{ij} - U_{ij}$

3. The error e expanded to hide information and applied LSB replacement E=2e M=E + Bit Vij=M +Uij

4. After data hiding the original value U_{ij} is changed to V_{ij}

3) Encryption: After self- reversible embedding, the image encrypts to construct the encrypted image by XOR method. In this method, the encryption key is XOR-ed with every pixel of the image. A general flowchart is shown in fig.2a

4) Data Hiding In Encrypted Image: Here data hider will hide the data into the reserved place on the encrypted image-which is the LSB of A. It again encrypts using data hiding key and get marked as encrypted image.

5) Data Decryption and Image Recovery: At the receiver side the data extraction is completely independent from image decryption. The data can be retrieved using the data hiding key. In data extraction, reverse rhombus method is used. Here first V_{ij} is changed to original value U_{ij} and then we calculate:

$$M=V_{ij}-U_{ij}$$
$$M= Bit + E$$

To retrieve the hiding data we calculate:

$$Bit = M \bmod 2$$
$$E=M-Bit$$
$$e=E/2$$
$$Uij=e+Uij'$$

After the data extraction LSB of B can reversibly be embedded into A and we can recover the Original image using decryption key. The general flowchart is as shown in fig.2b.

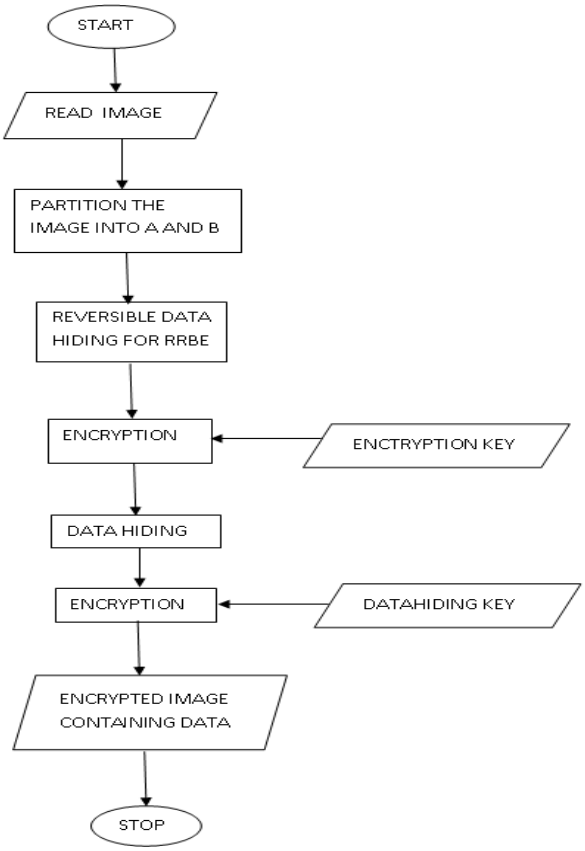

Fig 2a: Encryption Flow Diagram

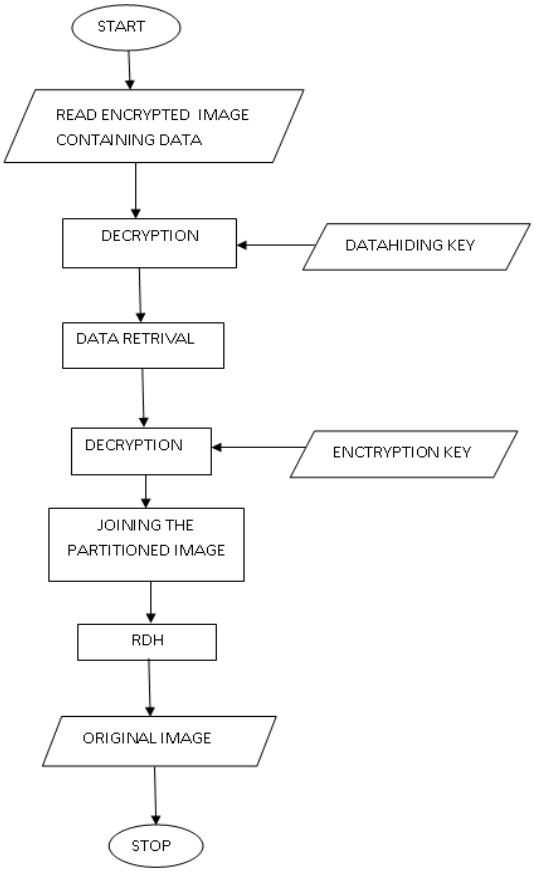

Fig 2b: Decryption Flow Diagram

III. Motivation

Since data security and data integrity are the two challenging areas for research nowadays there are so many research in progress on the field like internet security, steganography, cryptography. This work describes the concept of reversible data hiding and encryption technique. When it is desired to send the confidential/important/secure data over an insecure medium it is customary to encrypt as well as compress the cover data and then embed the confidential/important/secure data into that cover data. For achieving this facility there are various data hiding techniques, compression techniques, encryption/decryption techniques available.

Reversibility gives the ability to retrieve the exact original input data after the extraction process. This technique is used to embed additional message into a cover media, such as military or medical images, in a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Reversibility can be used to attach crucial information to the media without changing their original contents.

By embedding an authentication code that has a close relationship to the host image, reversible data hiding provides a self authentication scheme without any extra support. Reversible data hiding techniques have also been proposed for various fields such as Medical Image Processing ,Multimedia archive management, Image trans-coding Video error-concealment coding.

IV. Scope And Objective

Reversible data hiding in encrypted images is a new topic getting attention because of the secured environmental requirements. Data hiding in reversible manner provides double security for encrypted images. The existing system contains some disadvantages so the future scope is to remove the disadvantages by adding reversible manner means, data extraction and recovery of image are free of errors. In future it may be possible that memory space can be reserved before encryption which requires less amount of time for data extraction and image recovery. Lots of work in this research area is done but there are number of problems in existing systems. So the objectives to be recovered in the future may be:

1) The extracted data contains the errors as there may be data loss.
2) The problem of availability of memory space can occur. It is time consuming process.
3) The key contents of original image are restored back, so image quality should not be hampered.

The extracted data may contain errors because if there is no availability of sufficient space then some data may lost and that's why there is data missing at the receiver side which may called as data with error. Again the unavailability of memory space is the big problem, as some space is created at the time of data embedding which is the time consuming process. After data extraction the image recovered does not contain the qualities as was the original cover. Some distortions are there into that image.

V. Related Work

The earliest reference to reversible data embedding found is the Barton patent [3], filed in 1994. In his invention, the bits to be overlaid will be compressed and added to the bitstring, which will be embedded into the data block. Honsinger, et al., reconstructed the payload from an embedded image, then subtracted the payload from the embedded image to losslessly recover the original image. Macq [4] proposes an extension to the patchwork algorithm to achieve reversible data embed-ding. Fridrich, et al., develop a high capacity reversible data-embedding technique based on embedding message on bits in the status of group of pixels. They also describe two reversible data-embedding techniques for lossy image format JPEG. De Vleeschouwer, et al., proposed a reversible data-embedding algorithm by circular interpretation of bijective transformations. Kalker, et al., provide some theoretical capacity limits of lossless data compression based reversible data embedding and give a practical code construction. Celik, et al.[5] presented a high capacity, low distortion reversible data-embedding algorithm by compressing quantization residues. They employ the lossless image compression algorithm CALIC, with quantized values as side-information, to efficiently compress quantization residues 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. The experimental results show that the PSNR and capacity are satisfying. Nasir Memon and Ping Wah Wong worked on a buyer-seller watermarking protocol which is the concept of digital watermarking. In this protocol they stated that the seller does not get to know the exact watermarked copy that the buyer receives. Hence the seller cannot create copies of the original content containing the buyer's watermark. However, in case the seller finds an unauthorized copy, he can identify the buyer from whom this unauthorized copy has originated and furthermore also prove this fact to a third party by means of dispute resolution protocol. Hence, the buyer cannot claim that an unauthorized copy may have originated from the seller. The watermark embedding protocol is based on public key cryptography and has little overhead in terms of the total data communicated between the buyer and the seller. Nasir Memon and Ping Wong stated the concept of hiding the data in encrypted form of the data. Here seller is doing data (fingerprint/Watermark in this case) embedding while he does not know the original data content. The data is in

the encrypted form. Shiguo Lian and 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. Thus, the watermark can be extracted from the encrypted videos, and the encrypted videos can be re-watermarked[6]. Xinpeng Zhang presented a practical scheme satisfying the above-mentioned requirements.

A content owner encrypts the original image using an encryption key, and a data-hider embeds additional data into the encrypted image using a data-hiding key yet he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the activity of data extraction is not separable from the activity of content decryption. In other words, the additional data must be extracted from the decrypted image, so that the principal content of original image is opened before data extraction, and, if someone has the data-hiding key but not the encryption key, he is not able to extract any information from the encrypted image containing additional data [1]. Jun Tian developed a simple and efficient reversible data embedding method for digital images in which he explored the redundancy in the dig-ital content to achieve reversibility. Both the payload capacity limit and the visual quality of embedded images are among the best in the literature. As a basic requirement, He achieved the policy that quality degradation on the image after data embedding should be low[8]. Sergio Vicente,D. Pamboukian and Hae Yong Kim invented the technique that selects a set of low visibility pixels and uses the Golomb code to compress the predictions of these pixels. This compressed data and the net payload data are embedded into the image. In this technique, predictions of low visibility pixels are compressed using the Golomb code create space to store the hidden data. The technique was applied to several kinds of binary images and, in average, only 453 pixels were compressed to get space to store 128 bits of net payload data. This algorithm employs two techniques, difference expansion and generalized least significant bit embedding, to achieve a high embedding capacity, while keep the distortion low. The reported results of Lena image is shown in Table 1. It seems until now this algorithm reaches the highest capacity.

Zhenfei Zhao and et.al showed a reversible data hiding method for natural images. Due to the similarity of neighbor pixels' values most differences between pairs of adjacent pixels are equal or close to zero. In this work, a histogram is constructed based on these difference statistics. In the data embedding stage, a multilevel histogram modification mechanism is employed. As more peak points are used for secret bits modulation, the hiding capacity is enhanced compared with those conventional methods based on one or two level histogram modification. Moreover, as In the data extraction and image recovery stage, the embedding level instead of the peak points and zero points is used.

Most of the data hiding techniques are not reversible completely. The well known LSB technique is not completely reversible due to bit replacement without memory. Earliest technique is based on LSB replacement. In Data compression technique, the data to be embedded as well as related information's of the image used for data recovery is compressed. Compressed data is embedded directly into the cover media using LSB replacement. Celik et al.[5] proposed a data hiding technique in which each image pixel is quantized using L-level scalar technique. The residues yielded after quantization is compressed using a lossless compression algorithm called CALIC. Compressed residues along with the to-be embedded bits are embedded into the quantized image using LSB replacement. Distortions introduced on the watermarked image by this method are comparatively high.

The first several lossless data hiding algorithms belong to this category. Since fragile authentication does not need much data to be embedded in a cover media, the embedding capacity in this category is not large. Normally from 1k to 2k bits. Bartons patent in 2000 [3] may be the earliest one. His algorithm was developed for authentication of digital media, including JPEG and MPEG coded image and videos. The main idea is to losslessly compress the bits to be overlaid and leave space for authentication bit-string. No specific performance result has been reported. Honsinger et al.s patent in 2001 is the second lossless data hiding technique used for fragile authentication. Their method is carried out in the image spatial domain by using modulo 256 addition. In the embedding, $Iw = (I + W) \bmod 256$,where Iw denotes marked image, I original image, W is the payload comes from the hash function of the original image. In the authentication side, the payload W can be reconstructed from the marked image, then subtract the payload from the marked image to losslessly recover the original image. By using modulo 256, over/underflow is avoided. However, the marked image may suffer from the salt-and-pepper noise during possible grayscale flipping over between 0 and 255 in either direction due to modulo 256 addition. This issue will be addressed later in this paper. Fridrichs group explored a deep research on lossless data hiding techniques and developed some algorithms. Their first algorithm [11] is in the spatial domain, which losslessly compresses the bit-planes to leave room for data embedding. In order to leave sufficient room for data embedding, it needs to compress a relatively high level bit-plane, which usually leads to visual quality degradation. They also describe two reversible data hiding techniques for lossy compressed JPEG

image. The first technique is based on lossless compression of biased bit-streams derived from the quantized JPEG coefficients. The second technique modifies the quantization matrix to enable lossless embedding of one bit per DCT coefficient. In addition, Fridrichs group extended the idea of lossless authentication to MPEG-2 video.

All the above mentioned techniques aim at fragile authentication, instead of data hiding. As a result, the amount of hidden data is rather limited. Hence, Goljan et al. [9] presented a first lossless marking technique that is suitable for data embedding. The details are as follows. The pixels in an image are grouped into non-overlapped blocks, each consisting of a number of adjacent pixels. For instance, it could be a horizontal block having four consecutive pixels. A discrimination function is established to classify the blocks into three different categories, Regular, Singular and Unusable. (The authors use the discrimination function to capture the smoothness of the groups.) An invertible operation F can be applied to groups. That is, it can map between a pair of gray level values, resulting in F(R)=S,F(S)=R, and F(U)=U. It is reversible since applying it to a gray level value twice produces the original gray level value. This invertible operation is hence called flipping F. The main idea for lossless embedding is that they scan the image group-by-group and losslessly compress the status of the image the bit-stream of R and S groups (the RS-vector) with the U groups simply skipped as overhead to leave room for data embedding. By assigning a 1 to R and a 0 to S they embed one message bit in each R or S group. If the message bit and the group type do not match, the flipping operation F is applied to the group to obtain a match. The data to be embedded consist of the overhead and the watermark signal. While it is novel and successful in reversible data hiding, the amount of data that can be hidden by this technique is still not large enough. From what is reported in [9], the estimated capacity ranges from 0.011 to 0.092 bits per pixel (bpp). This may not be high enough for some applications.

Another problem with the method is that when the capacity increases, the visual quality will drop severely. Xuan et al. proposed a high capacity lossless data hiding technique based on the integer wavelet transform (IWT) [10].IWT is used in the algorithm to ensure the lossless forward transform and inverse transform. After IWT, the bias between 1 and 0 in the middle and high bit-planes of IWT coefficients becomes much larger than that in spatial domain. Hence, those coefficient bit-planes can be losslessly compressed to leave a large space for data embedding. Histogram modification is used in this algorithm to prevent the over/underflow problem. The experiments show that the capacity can reach 0.057 to 0.36 bpp, quite larger than the previous algorithms. While the PSNR of marked images are not very high due to histogram modification there is no any annoying artifact and the visual quality is satisfying. Further improvement has been made, resulting in both higher embedding capacity and visual quality. Ni et al. [11] proposed a new lossless data hiding technique based on the histogram modification. This algorithm utilizes the zero or minimum points of the image histogram and modifies the pixel value to embed the data. In the image histogram, they first find a zero point (no pixel assumes that gray value) and a peak point (a maximum number of pixels assume that gray value).Then they move the histogram between zero point and peak point toward zero point by one unit and leave the histogram near the peak point empty. Finally the histogram in peak point is moved to its neighbor or kept intact to finish the embedding of 1 or 0. This algorithm has a quite large capacity (0.019 to 0.31 bpp) while keeping a very high visual quality for all images (the PSNR of marked images versus original images is guaranteed to be higher than 48 dB). This PSNR performance is much higher than any other algorithms at the same data embedding rate.

Tian recently presented a new high capacity reversible data embedding algorithm in [8]. This algorithm employs two techniques, difference expansion and generalized least significant bit embedding, to achieve a high embedding capacity, while keep the distortion low. It seems until now this algorithm reaches the highest capacity.

Faheem Masoodi et al., presents a self-contained and comprehensive analysis of linear feedback shift registers and their application in stream ciphers. This research focuses on analyzing the mechanism of an LFSR, the two implementation variations and various properties of LFSR, which play a vital role in stream cipher design. The security aspects of LFSR based stream ciphers and different techniques to enhance it is described.[13]

VI. Experiments

A standard image Lena is taken as shown in Fig. 3(a), to demonstrate the feasibility of proposed method. Fig. 3(b) is the encrypted image containing embedded messages and the decrypted version with messages is illustrated in Fig. 3(c). Fig. 3(d) depicts the recovery version which is identical to original image.


Fig 3(a)

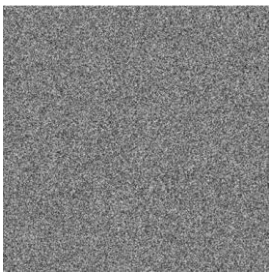
Fig 3(b)


Fig 3(c)


Fig 3(d)

VII. Conclusion

Reversible data hiding is drawing a lot of attention because of the privacy-preserving requirements from cloud data management as well as encryption techniques. Previous methods implement RDH in encrypted images by vacating room after encryption, as opposed to which we proposed by reserving room before encryption. Thus the data hider can benefit from the extra space emptied out in previous stage to make data hiding process effortless. The proposed method can take advantage of all traditional RDH techniques for plain images and achieve excellent performance without loss of privacy. Furthermore, this method can achieve real reversibility, separate data extraction and greatly improve on the quality of marked decrypted images.

References

[1] X. Zhang, "Reversible data hiding in encrypted image", IEEE Signal Process, vol. 18, no. 4, Apr 2011,pp. 255-778.

[2] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang, "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification", IEEE Transactions on Information Forensics and Security, VOL. 8, NO. 7,July 2013.

[3] J. M. Barton, "Method and Apparatus for Embedding Authentication Information Within Digital Data", U.S. Patent 5 646 997, 1997.

[4] B. Macq, "Lossless multi resolution transform for image authenticating watermarking, in Proc. EUSIPCO", Sept. 2000, pp. 533536.

[5] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding, in Proc. Int. Conf. Image Processing", vol. II, Sept. 2002, pp. 157160.

[6] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and watermarking in video compression", IEEE Trans. Circuits Syst. Video Technol, vol. 17, no. 6, Jun 2007, pp.774-778.

[7] Sun Jing, Yang jing-yu, Fu De-sheng, "Research On the Security of Key Generator in Stream Ciphers", The 1st International Conference on information Science and engineering (ICISE2009) pp. 1831-834

[8] J. Tian, "Reversible data embedding using a difference expansion", IEEE Trans. Circuits Syst. Video Technol, vol. 13, no. 8, Aug 2003, pp. 890-896 Y. Lim, J. Choi, and M. Kim, "Probabilistic Sound Source Localization", International Conference on Control, Automation and Systems 2007, October 2007.

[9] C. N. Sakamoto, W. Kobayashi, T. Onoye, and I, Shirakawa, "DSP Implementation of Low Computational 3D Sound Localization Algorithm", IEEE Workshop on Signal Processing Systems, pp. 109-116, September 2001.

[10] Z.Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding, IEEE Trans. Circuits Syst. Video Technology", vol. 16, no. 3, pp. 354362, Mar. 2006.

[11] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding new paradigm in digital watermarking", EURASIP J. Appl. Signal Processing, vol. 2002, no. 2, pp. 185196, Feb. 2002.

[13] W. Liang and Long Jing, "A cryptographic Algorithm Based on Linear Feedback Shift Register", 2010 International conference on computer application and system Modeling (ICCASM 2010), v15, pp 526-529

[14] Faheem Masoodi,Shadab Alam,M U Bokhari, "An Analysis of Linear Feedback Shift Registers in Stream Ciphers", International Journal of Computer Applications (0975-8887)Volume 46 No.17, May 2012.