ISSN 23499842(Online), Volume 1, Special Issue 2(ICITET 15), March 2015
International Journal of Innovative Trends and Emerging Technologies

REVERSIBLE DATA HIDING USING AES ALGORITHM

MOHANAPRIYA.S[1] PRADEEPA.A[2] SINDHU.S[3] GNANAVEL.R[4]
[1,2]UG Department of computer science, [3,4]Assistant professor Department of computer science,
[1,2,3,4]Rajalakshmi Institute of Technology Chennai,Tamil Nadu,India
[1]mohnselvaraj@gmail.com [2]pradeepman23@gmail.com [3]sindhu.s@ritchennai.edu.in [4]gnanavel.r@ritchennai.edu.in

***Abstract*— The aim of this paper is to transmit data to the recipient in secure manner. Reversible data hiding (RDH) is a technique that embeds secret data into a image in reversible manner. The secret data to be sent is embedded into an image and then transmitted to the receiver. In existing system, the secret data is embedded into an uncompressed image for transmission and LSB technique is used for encrypting an image.In proposed system, any sort of image is taken as input and then converted into JPEG format. Further they are compressed which may increase the efficiency. Here Huffman coding technique is used for image compression. Added to this the data is embedded in an image. Here both secret data and image gets encrypted using AES algorithm and then secret data is embedded into the encrypted image. Finally key is exchanged between sender and receiver through the image. With the help of the key the receiver can be able to retrieve both image and the Secret message. By doing compression before encryption will make the system more efficient.**

Keywords:Encryption,EmbeddingDecryption,Extraction, Restoration.

I INTRODUCTION

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image.It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the buildup of noise and signal distortion. Image processing techniques involve treating the image as two-dimensional signal and applying standard signal processing techniques to it.

Some of the efficient algorithms used in image processing are RSA, AES etc. In some cases techniques like Huffman coding, least significant bits for image encryption process.This paper is concerned about transmitting confidential data by embedding it into an encrypted image. Huffman coding technique is used to compress an image, this technique is mainly used to transmit data in well-organized manner which provides security without any data loss during the process of transmission. Image of any format is converted to JPEG image and encrypted where the encrypted data is embedded into it. Both embedded and encryption key has sent to receiver. The receiver extracts the data and image with the key.

There are two parties in the entire workflow of encryption embedding extraction restoration. They are: sender and receiver, which are described as follows.

***Sender*:** Select the image in which the data is going to be hide. The image gets converted into JPEG format for high image quality.The image gets compressed to reduce its memory size without any image distortion. Compressed JPEG image gets encrypted using AES(Advance Encryption Standard) algorithm. Similarly the secret data which we going to be embed into an image also encrypted by the same algorithm.

Receiver: The encrypted image and encryption key is obtained by the receiver.By using this encryption key, the sender can encrypt both image and data or either data or an image by using RDH technique.

II LITERATURE REVIEW

In Image processing for transmission there are many threats like data hacking. Hacker will crack the secret data which is to be shared between sender and receiver.This type of transmission used in the field of army military purpose, medical field and all other field which needs secured transmission. Some of the issues faced are under follows. In some cases the data is embedded in the image for secured transmission.The image which is transmitted is not encrypted so that they can be easily hacked by the hacker[9]. Secret data is embedded into the encrypted image. It is easy to find the key for encrypted image hence the image is decrypted and data is extracted[11].Selecting and the positioning the pixel for embedding the data in the image so that they can be transmitted. When placing the data in the image the position of the pixel will be changed[10]. The original image gets directly encrypted by LSB technique and data gets embedded into an encrypted image. Data gets hidden into an encrypted image of least significant free space available. There is specific position for hiding that is last most bit of an image. During the process of retrieval data may loss (i.e.)Data can be cracked since it is easy to find message bits are available in last bit of an image[12].

III EXISISTING SYSTEM

In Existing system an image is taken as input which gets encrypted and data is hidden by LSB Technique. In LSB algorithm, the message bit is taken from the message byte and then that particular bit will be embedded inside the least significant bit of an image or video or audio file. This is done because The message embedded in the least significant bit of an image file will not draw the suspicion of the hacker as the minute difference that would be made in the pixel value of the image file will not be perceived by the normal naked human eye.The message that will be embedded in the LSB of an audio file will not create suspicion to the hacker as that change would not be perceived by the human ear. The same concept works out even with video file[12].

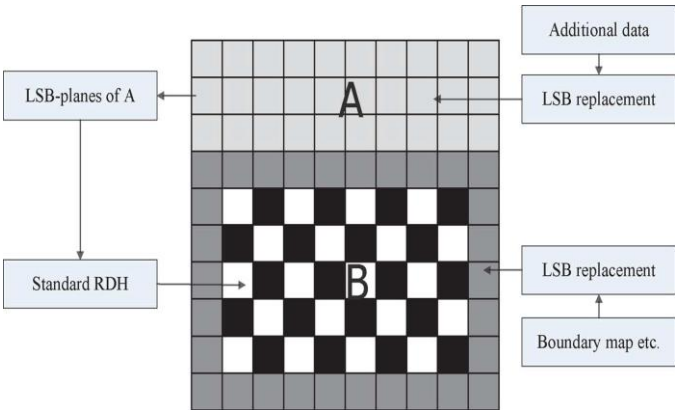


Fig 1. Image partition and data embedding using LSB technique

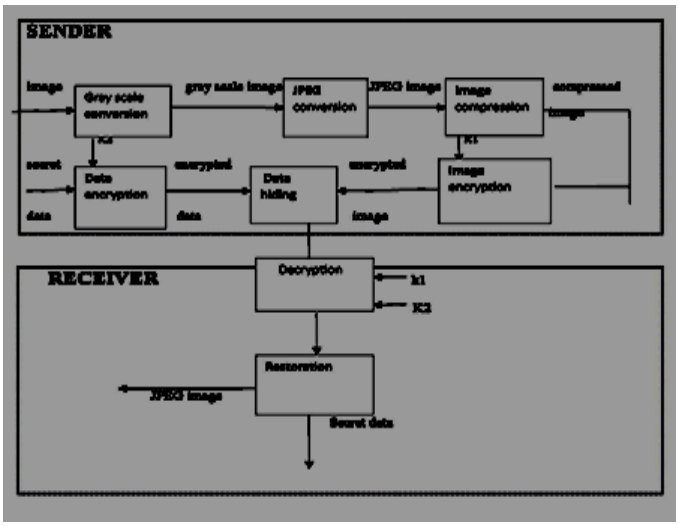
The above fig 1 explains the concept of least significant bit
The Cover image is split in two parts namely A & B. Then the LSB of A is allowed to be reversed and then they are placed in the LSB of B. Then the LSB replacement is done finally the LSB are replaced in the A part of the image[12].

As the name suggests, this algorithm is used for replacing the least significant bits of the carrier image with the bits of the message that is to be hidden**.**The one's bit of a byte is used to encode the hidden information. Suppose we want to encode the letter A (ASCII 65 or binary 01000001) in the following 8 bytes of a carrier file.

01011101 11010000 00011100 10101100
11100111 10000111 01101011 11100011
becomes
01011100 11010001 00011100 10101100
11100110 10000110 01101010 11100011

The above mentioned binary codes are image bits.Last bit of binary code is replaced with the message bits where the secret data gets hidden into an image.

IV WORK FLOW DIAGRAM



The above work flow diagram explains the process flow of this paper.An image with any extension is taken as an input and the image is converted to gray scale that is binary format for mission understanding purpose.

Then the converted image is renewed to JPEG format which obviously increases the image size to reduce the image size compression concept is included in this system. Then the image size gets decreased. Reduced image is then encrypted with some key. Secret data which is to be transmitted is encrypted and embedded into that encrypted image. Then the image and key is shared with the receiver. Finally the receiver restores the data from the image by using the key.

V PROPOSED SYSTEM

In proposed system any type of cover image is taken as input, then it is converted into JPEG image then the image is compressed and converted using Huffman algorithm. Image encryption has to be done here to improve its security. Image encryption is done with AES algorithm which is most standardized secured algorithm used in most of encryption and decryption process. The encryption and embedding are controlled by encryption and embedding keys given by the sender. Reversible data hiding technique is going to be used now sender has his own choice of giving keys to receiver that is it may be both key ,it may be data key(embedding key)alone or it may be encryption key alone. With the help of this key receiver could obtain Image and data if and only if he has both encryption and embedding key. If receiver has only data key he could extract only Secret data. Extraction is done after Decrypting the received content. Here decryption has done with same AES algorithm only.By this way a data is sent to the receiver in a very confidential manner. Which is very important in many fields like army, military, airforce etc.

A. Huffman coding:

Huffman codes can be used to compress information Like WinZip – although WinZip doesn't use the Huffman algorithm JPEGs do use Huffman as part of their compression process.The basic idea is that instead of storing each character in a file as an 8-bit ASCII value, we will instead store the more frequently occurring characters using fewer bits and less frequently occurring characters using more bits. On average this should decrease the file size (usually ½).Un compressing works by reading in the file bit by bit start at the root of the tree If a 0 is read, head left.If a 1 is read, head right When a leaf is reached decode that character and start over again at the root of the tree Thus, we need to save Huffman table information as a header in the compressed file.

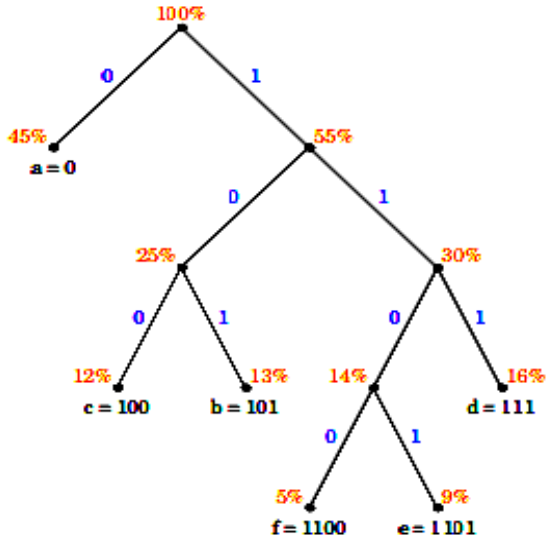


Fig 2. Representation of a binary code as binary tree.

Huffman coding is optimal when each input symbol is a known independent and identically distributed random variable having a probability that is an the inverse of a power of two. Prefix codes tend to have inefficiency on small alphabets, where probabilities often fall between these optimal points. The worst case for Huffman coding can happen when the probability of a symbol exceeds $2^{-1} = 0.5$, making the upper limit of inefficiency unbounded. These situations often respond well to a form of blocking called run-length encoding. For a set of symbols with a uniform probability distribution and a number of members which is a power of two, Huffman coding is equivalent to simple binary block encoding, e.g., ASCII coding. This reflects the fact that compression is not possible with such an input. Huffman coding is done with two major step which is explained as follows.

STEP 1:

I. Sort the gray levels by decreasing probability.
II. Sum the two smallest probabilities.
III. Sort the new value into the list.
IV. Repeat 1 to 3 until only two probabilities remains.

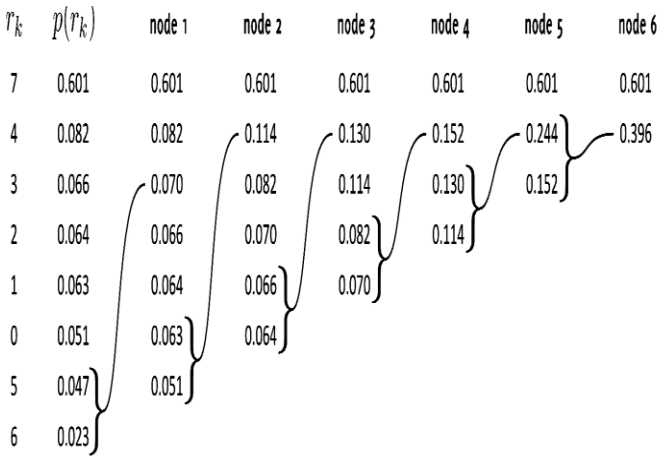


Fig 3.Probablity of Color values of an image

STEP II:

I. Give the code 0 to the highest probability, and the code 1 to the lowest probability in the summed pair.
II. Go backwards through the tree one node and repeat from 1 until all gray levels have a unique code.

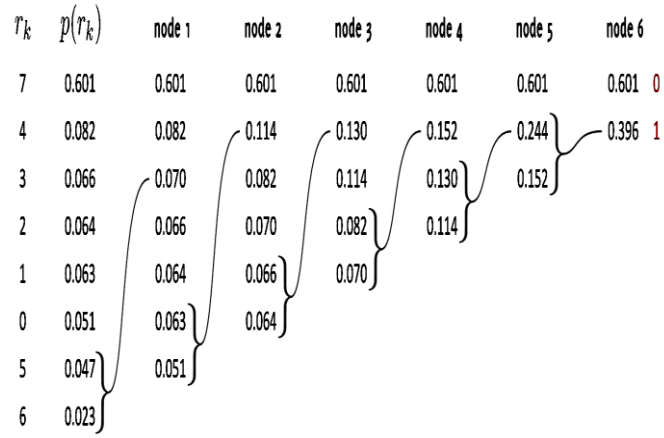


Fig 4.Assigning Binary value for Least minimum and Least maximum Probablity.

r_k	$p(r_k)$	code	node 1		node 2		node 3		node 4		node 5		node 6	
7	0.601	0	0.601	0	0.601	0	0.601	0	0.601	0	0.601	0	0.601	0
4	0.082	110	0.082	110	0.114	101	0.130	100	0.152	11	0.244	10	0.396	1
3	0.066	1000	0.070	111	0.082	110	0.114	101	0.130	100	0.152	11		
2	0.064	1001	0.066	1000	0.070	111	0.082	110	0.114	101				
1	0.063	1010	0.064	1001	0.066	1000	0.070	111						
0	0.051	1011	0.063	1010	0.064	1001								
5	0.047	1110	0.051	1011										
6	0.023	1111												

Fig 5.Binary value of color image.

B. AES algorithm

AES- Advanced Encryption Standard

AES is available in many different encryption packages, and is the first publicly accessible open cipher approved by the National Security Agency (NSA) for information when used in an NSA approved cryptographic module AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware. AES is a variant of which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per sec* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:10 cycles of repetition for 128-bit keys.12 cycles of repetition for 192-bit keys.14 cycles of repetition for 256-bit keys.It processes data block of 4 columns of 4 bytes is state.It operates on entire data block in every round. It has 9/11/13 rounds in which state undergoes.it has four steps namely ,Byte substitution, Shift rows ,Mix columns ,Add round key.

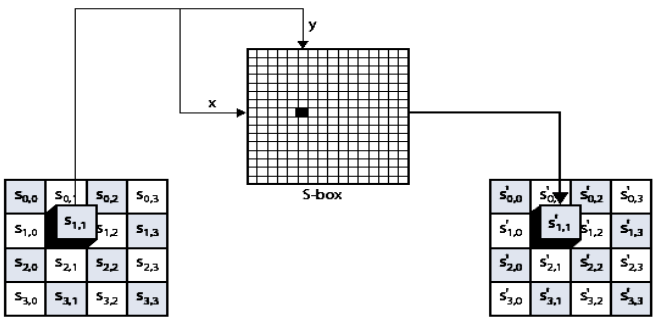


Fig 5.Byte Substitution

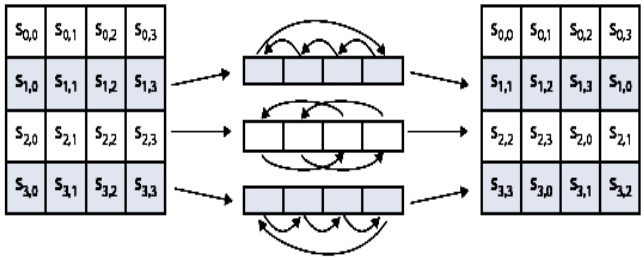


Fig 6.Shift Rows

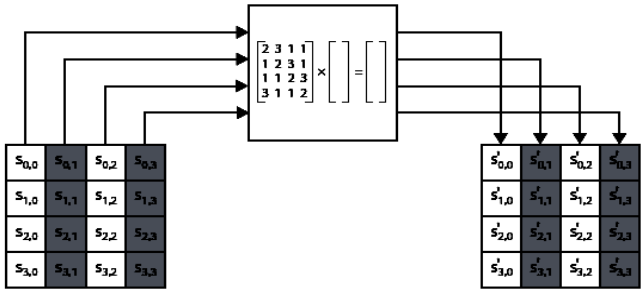


Fig 7.Mix Columns

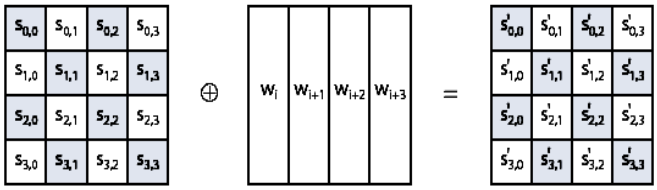


Fig 8.Add Round Key

VIII COMPARISON ANALYSIS

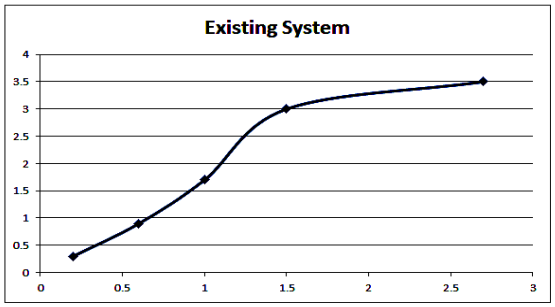


Fig 9.1

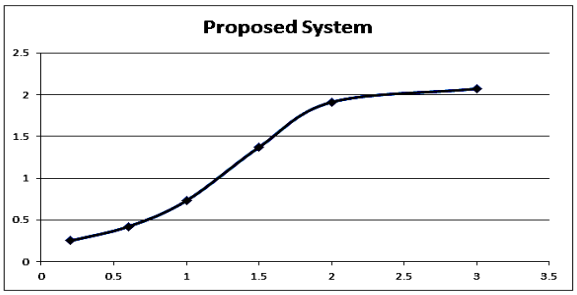
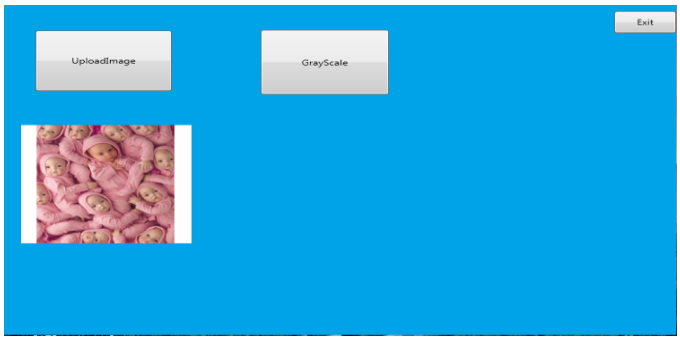


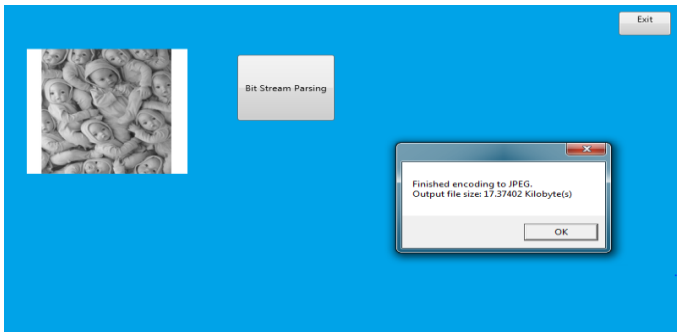
Fig 9.2

VII EXPRIMENTAL RESULTS

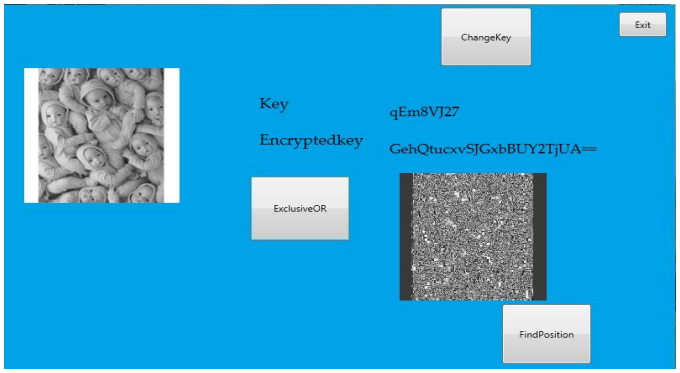


a.Upload Image

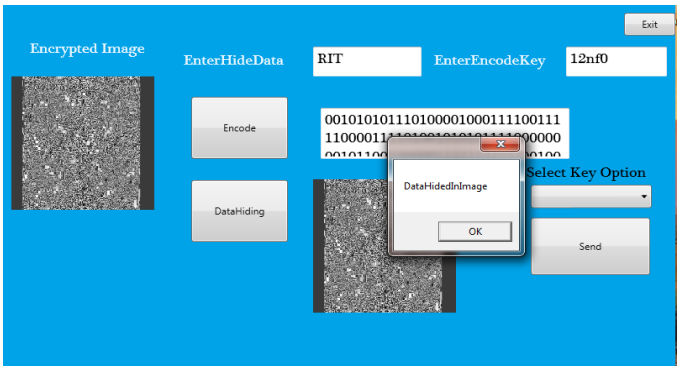
b.JPEG Image Conversion



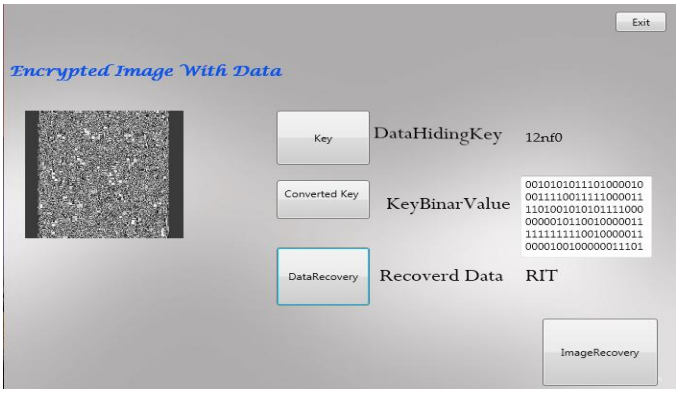
c.Compressed Image.



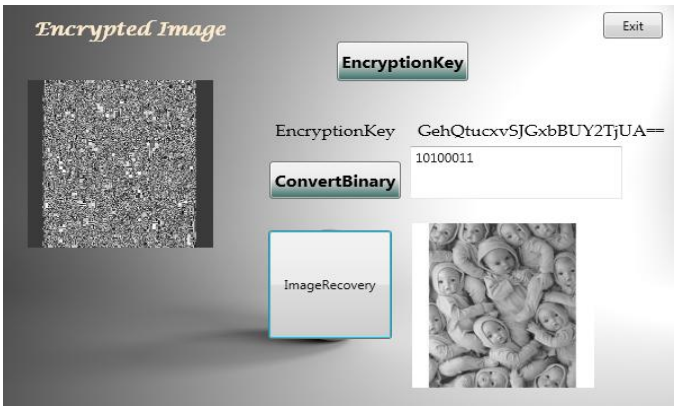
d.Encrypted Image



e.Data Hidden



f.Data Recovered



g.Image Recovered

VI CONCLUSION

In this paper Reversible data hiding technique is used for providing choice to sender by which he could have his own rights to provide embedding key or encryption key or both key. Huffman coding is used for image compression purpose which decreases the memory size of an JPEG image leads to increase in transmission speed.AES algorithm is used which is more secured standardized algorithm in which data cannot be cracked by the hacker easily.

VIII REFERNCES

1) M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-sellerwaermarking protocol based on composite signal representation," inproc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.
2) J. Fridrich and M. Goljan, "Lossless data embedding for all image for- mats," 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.
3) W. Hong, T. Chen, and H. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process. Lett., vol.19, no. 4, pp. 199–202, Apr. 2012.
4) T. Kalker and F. M. Willems, "Capacity bounds and code constructions for reversible data-hiding," in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.
5) S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," IEEE Trans. Circuits Syst. Videotechnol., vol. 17, no. 6, pp. 774–778, Jun. 2007.
6) 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.
7) L. Luo et al., "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
8) N Memon and P. W. Wong, "A buyer-seller watermarking protocol,"IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649, Apr. 2001.
9) Z. Ni, Y. Shi, and N. Ansari et al., "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar.2006.
10) G.S.Raman, C.Surya, R.Balaji Ganesh "Reversible Watermarking Based on Prediction Error Expansion and Pixel selection on Image" volume:2,April 2013.
11) X. Zhang, "Reversible data hiding in encrypted images," IEEE signal process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.
12) K. Ma, W. Zhang, and X. Zhao et al., "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, 2013.