Randomised Data Concealment with Reversibility Improved Data Hiding In Encrypted Images

S.Narayanan[1], M.Pravin Kumar[2], G.Ramprasad3 ,M.Mohan[4]
Panimalar Engineering College, Tamil Nadu, India
ssriramganesh1993@gmail.com[1] , pravinraj2392@gmail.com[2] ,
ramprasadg92@gmail.com[3] ,mohan.rm@gmail.com[4]

Abstract— Steganography is used to hide data like text, image audio from unauthorized user in different manner. Data hiding method for images suffer from performance issues like low embedding capabilities, distortion or do not recover the original image completely. A novel reversible data hiding method is proposed. The pixel to which data is embedded is estimated in a random manner, these pixels are shifted and data along with the estimation errors are embedded in the image and these pixels are encrypted using a standard encryption technique. The rest of the image is then encrypted using a standard encryption algorithm. The image and data can be encrypted before data concealment for added protection. The embedded data can be extracted before or after the image is decrypted. This is possible by implementing a data hiding key. Thus, with the data hiding key, only the embedded data can be extracted revealing no information about the carrier image. The image is decrypted and can be recovered using the location maps created during the histogram shifting process. The various encryption levels in this method ensure a secure system. The proposed model exhibits high PSNR values and offers complete recovery of the hidden data and image.

Keywords*: Steganography, Chaos-encryption technique, Data hiding.*

I. INTRODUCTION

The security is most important In general the concept of image processing is developed to conceal the data in a secured manner by means of steganography, because of these implementation data can be highly secured in many possible ways. In this paper, we are going to develop a new method to encrypt the images in such a way that the security level of the data concealment will be increased. We are going to implement an algorithm for encrypting images such that pixel will be determined in randomized manner and the estimation of pixels will be done before the encryption of the image. Then the data will be embedded in the respective pixel and after that the pixel will be rearranged and then the process of encryption will be handled so that the data concealment will be as we expected.

II. RELATED WORK

Lossless data hiding in uncompressed image formats was discussed by Jessica Fridrich et al, (1), where uncompressed image formats can be used for embedding data by dividing the pixels into disjoint sets according to grayscale levels and using a discrimination function to flip LSB of the sets. Also they gave a method for embedding data in palette images such as GIF, by exploiting the limited colour palette of GIF images. Jun Tian gave reversible methods for reversible data hiding by exploiting the redundancy of the carrier (2). In the methods outlined, the data is embedded in pixels or groups of pixels that are chosen by a mathematical formula.

In another paper, (3), Tian proposed a reversible watermarking method to hide data by using a difference value of selected pixels that have been chosen by a formula. Diljith et al., (4) brought out another technique called ‘expansion-embedding’ based on improvements of Tian’s algorithm. They suggested prediction error expansion to the difference expansion technique by proposing a model of histogram selection of pixels on probabilistic models based on the amount of distortion possibly introduced. This method provides double the embedding capacity than of difference expansion and also exhibits higher PSNR. Hyoung Joong Kim et al., (5) improved difference expansion by implementing a new simplified location map of the rearranged pixels and formulating a new expansion theorem. It works by identifying the number of times a pixel can be unambiguously expanded to embed data, without overflow of the information. By this method they exhibited higher performance than Tian's method in terms of distortion and embedding capacity. However an uncompressed location needs embedding space in the image. Vasiliy Sachnev et al., in their paper (6), give a method which eliminates the need for location map. They use a prediction algorithm through which pixels are calculated for embedding. The prediction errors are embedded along with the data for extraction and image recovery purposes.

In their paper, Yongjian Hu et al., (7), discussed a new method using Difference Expansion for reversible data hiding. They worked on the auxiliary information needed to recover the original during the extraction process. The information may be the location map of the pixels that is used when histogram shifting. They worked on the prediction errors when estimating pixels and embedded them along with the secret data. This means that the errors are dependent on the data payload alone, improving Tian's method (2). This method, however, does not guarantee a sharp histogram. Xiaolong et al., in their paper (8), give a method by which data is embedded adaptively by analysing the histogram. The pixels are grouped according to smooth and rough regions. Data embedded in the smooth regions is slightly more than that of those embedded in the rough regions. This results in a sharper histogram of prediction errors improving image quality and increasing the image capacity.

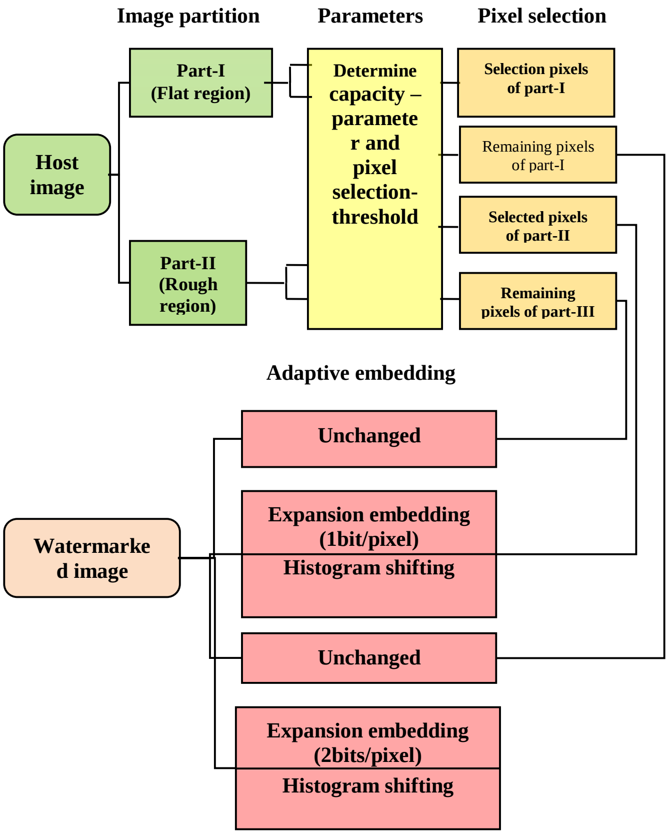
Image partition
Parameters
Pixel selection
Part-I (Flat region)
Host image
Part-II (Rough region)
Determine capacity – paramete r and pixel selection-threshold
Selection pixels of part-I
Remaining pixels of part-I
Selected pixels of part-II
Remaining pixels of part-III
Adaptive embedding
Unchanged
Watermarke d image
Expansion embedding (1bit/pixel)
Histogram shifting
Unchanged
Expansion embedding (2bits/pixel)
Histogram shifting

Figure 1: Embedding Mechanism for adaptive pixel expansion and pixel selection

The payload capacity of the carrier image is a major concern and therefore compressing data would reduce the possibility of distorting the image and increase the embedding capacity. Some algorithms may encrypt the secret data before embedding. Mark Johnson et al., [9] proposed a method of reversing the order of compression and encryption. They deal with only the secure communication and transmission of data and do not discuss the embedding of data in a carrier. This is discussed in (10), with commutativity between encryption and watermarking in mind. Commutativity between encryption and watermarking is a concern and Shiguo Lian et al., achieved this by encrypting the Motion Vector Differences and the Intra Prediction Mode signs in H.264/AVC encoding/compression. Watermarking is then performed. However,the methods of encryption and watermarking can be done in any order. In (11), Wei Liu et al., propose to compress the image progressively in resolution to allow the decoder to study low resolution version of the images and use the inferences to decode higher resolution. Lossless data embedding, i.e., embedding data in a way that no data is lost during data recovery is a very important factor in reversible data hiding. The popular LSB data embedding is effective but may introduce distortion. A generalized LSB embedding scheme is discussed in (12).

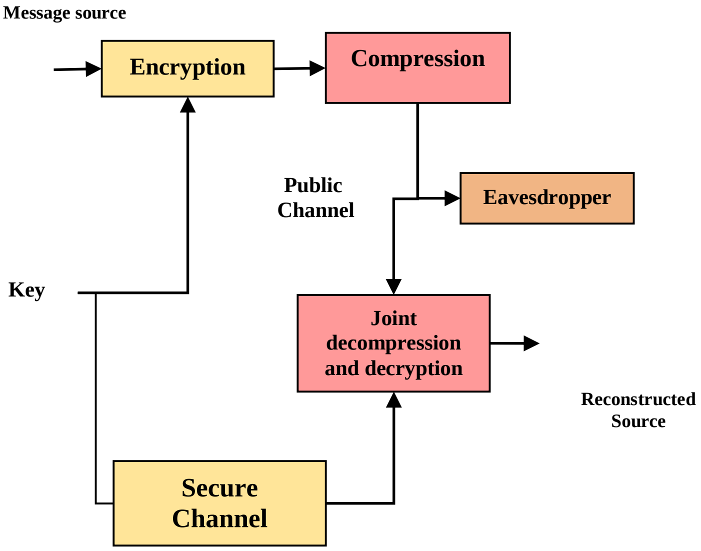

Figure 2: Compressing encrypted data and the encryption key is unavailable during compression.

By compressing regions of signal that are prone to distortion, Mehmet U. Celik et al., demonstrated that higher embedding rates can be achieved to a given distortion value. This Lossless Data Embedding was discussed by Xinbo Gao Et Al., [13], to improve the histogram based data embedding, they incorporated merits of Generalized Statistical Quantity Histogram Shifting by identifying the 'embedding zones' of the image. They successfully applied the method to JPEG format and exhibited high pure embedding capability. In data hiding; reversibility should be distortion-free.
A reversible data hiding technique is discussed in [14] for grayscale images. Here, the image is scanned and the histogram is analysed to identify the peak and zero point. The peak corresponds to the highest value to which maximum number of pixels assume. The zero, corresponds to the value, that is assumed by no pixel. According to the high values, the pixels are shifted by 1 if the bit to be embedded is 1. Xinpeng Zhang in his paper, [15], discusses a way to embed data after encryption by embedding the data in sets pixels of the carrier that have been formed in a pseudo-random manner of the carrier according to the data hiding key. The data is embedded by flippping the three LSB's of two sets based on whether the data hiding key value is 1 or 0. In another paper, [16], he, modifies the embedding algorithm by compressing the LSB of encrypted pixels that have been permuted by the data hiding key. By this method, Zhang improved his previous technique, exhibiting higher embedding capacity. In their paper [17], Sian-Jheng Lin et al., give methods to reduce the distortion by calculating the probabilities of the transitions in signal. They then use scalar embedding scheme with a square error distortion to reach the rate distortion bound. In Zhang's paper [15], the smoothness of the histogram is not fully exploited. Wien Hong et al., propose a method in their paper, [18], by using side match technique, i.e, smoothening the block boundaries of image. By this, he reduced the error rate of Zhang's work from 1.21% to 0.34% in prediction errors.

A reversible watermarking algorithm using interpolation technique is discussed in [19]. Interpolation error , error in calculating a pixel from surroundings. This is further classified into left and right interpolation errors. All this information is used in embedding the data and also used in the recovery of the carrier image. Lingling An et al., in their paper [20], provide a robust watermarking framework by incorporating Property Inspired Pixel Adjustment and Statistical Quantity Histogram.Weiming Zhang et al., by studying the above, proposed a method for reversible data hiding in encrypted images by histogram shifting after pixel estimation [21]. They embedded the estimation errors along with the embedding data to achieve high embedding capacity and also achieved higher PSNR values than previous methods. This technique is also secure and exhibits resistance to known attacks as collusion attacks and desynchronisation [22].

III. Current Existing Methods

There are many encryption methods and development like steganography watermarking compression method, reversible data embedding method is used, recursive code construction, compression of LSBs of the encrypted image to create a sparse space method are the methods used in the existing system such that the data concealment is obtained. In all these method the level of security is achieved but the security is destroyed by some unauthorized access to extract the secret data. In every particular the drawbacks obtained in all these methodology are Image distortion, Compressing overflow location maps and Inability of code reconstruction to reach rate-distortion bound. And we have discussed these major problems and made the proposed in a better manner.

When we discuss about the previous implementation there exists two rule, they are Fredkin rule and Conway's rule. They are the past implementation of chaos encryption method. The simple Fredkin rule means about half the cells are going to be alive in any specified iteration, which lends itself to a good statistical spread of data, moreover doesn't peter out or steady after a limited number of generations.

Conway's Rules

1. Process Conway's rules for game of life for each cell, add up the cells:
2. Count the cells neighbours.
3. A living cell with less than 2 living neighbours will die of loneliness.
4. A living cell with 2 or 3 neighbours remains alive
5. A living cell with more than 3 neighbours dies of overcrowding.
6. An empty cell with exactly 3 neighbours becomes alive.
7. Commit the changes.

This may seem secure, but, if the initial stages of the algorithm or the seed value are identified, the implementation can be successfully recreated to arrive at the original data. For this, we use the methods outlined in (23).

IV. Proposed Method

In this method, we are going to implement a novel combination of algorithm to achieve a high level of security in securing the secret data.

a) Encryption and Embedding

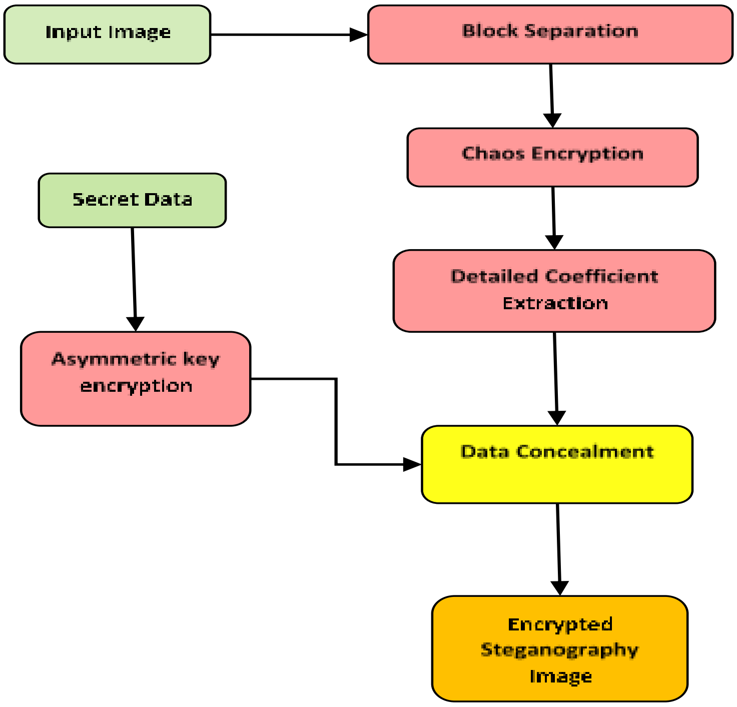
Input Image
Block Separation
Chaos Encryption
Secret Data
Detailed Coefficient Extraction
Asymmetric key encryption
Data Concealment
Encrypted Steganography Image

Figure 3: Proposed Encryption & data embedding flow

The diagram which is represented above is the implementation method of the proposed system. The initial step of this method is to separate the image into several blocks, then, the image is encrypted using the chaos technique:

1. Considering the data of the plain image as matrices of blocks of data, we use the properties of circulant matrix and take advantage of the permutation in row and column along diagonal and anti-diagonal.
2. The permuted matrix is then split into equal parts according to rows.
3. The control parameter is determined by finding the modulus values of the element and the column value.
4. The image is then encrypted using modulo addition of the values determined.

The pixels are estimated and the data is embedded in that particular block efficiently. After the process of rearranging the pixels concealing data, image will be encrypted using Asymmetric Key encryption method so that the total encryption process will be completed. And the determined key will be combined with the encryption of images to make a better way of data concealment.

b) Decryption and Data Extraction

In the side of decryption the image which is encrypted will be obtained by the receiver and that image will be decrypted and the suitable key will be used to extract the secret data. There are two keys to decrypt the image i.e. the key which is used to decrypt the image and the key which is used to extract the data. If any third person access to it, will not get the data which is concealed because he cannot obtained the concealed pixels and the key which is need to extract the data since the key and pixel also encrypted with that same image. Hence the proper encryption and decryption will be made and the secured data concealment will be successfully achieved.

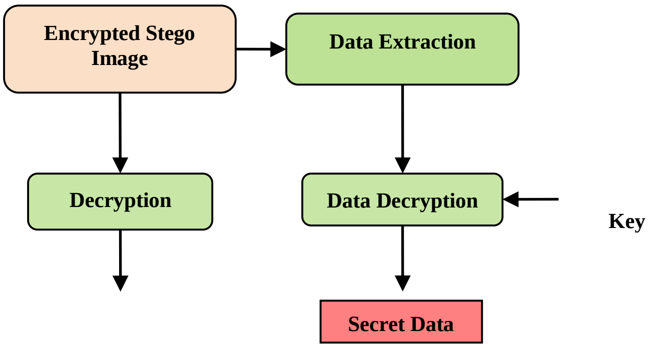

Figure 4: Proposed Data extraction & image restore flow

V.IMPLEMENTATION AND PERFORMANCE

The implementation of this proposed method has two modules, they are encryption and decryption. Both the module has several process but those are the module which play a major factor in this method. The encryption which is going to be implemented here is a combination of two encryption algorithm i.e. the standard encryption algorithm and the special encryption algorithm. Since the procedure is already explained in the methodology here we will determine how it process to obtain required result. The special encryption algorithm used is chaos encryption algorithm as explained before, the chaos encryption algorithm will encrypt the pixels before the data embedding and room is created by histogram shifting to embed the data into those respective pixels in a randomized behaviour so that the security range will be increased when compared to previous methods.

RSA data encryption algorithm

Step 1: Choose two distinct prime numbers p, q.

Step 2: Calculate the product of the numbers (n).

Step 3: Find a number e, such that e lies between 1 and n and also e and n are coprime.

Step 4: Calculate d as the multiplicative inverse of e.

Step 5: Release e as public component and use d as private.

The decryption will be extracting the data which is embedded in that particular pixel hence the secret data is obtained. Experimental results show that the technique offers excellent data embedding rates and high PSNR values.

Features of proposed method

The proposed system has several advantage, they are listed below

- The rate of secret data concealment will be higher since there is double encryption process.
- The rate of distortion appeared will be less since the proper sequence process will be carried out.
- The new implementation in this method is the determination of pixel where the pixel will be determined randomly and the estimated pixels will not be known to the proceeding professional that much secured system will be generated.
- Less computational period for image encryption will be done.

So we say this method is better than the previous existing method since all the previous disadvantages are enhanced and given importance to each and every individual factor involved in it.

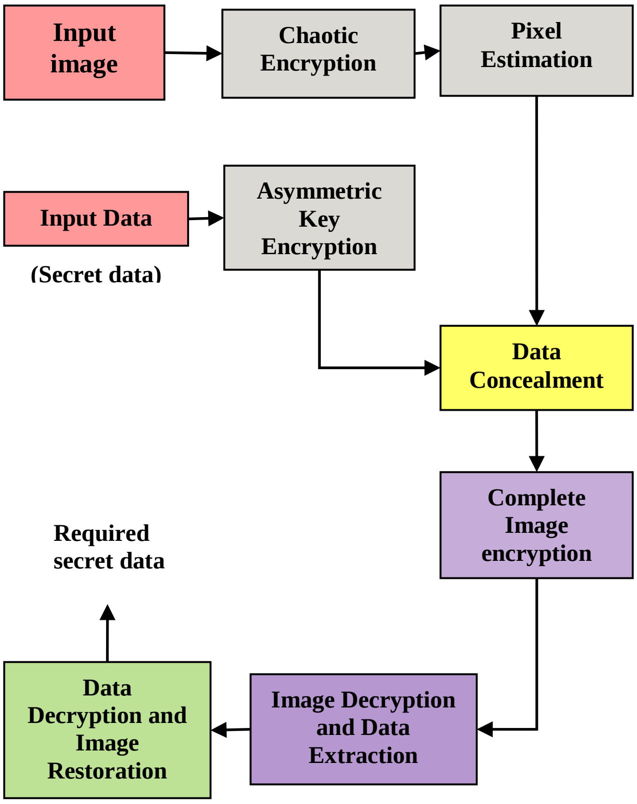
Input image
Chaotic Encryption
Pixel Estimation
Input Data
(Secret data)
Asymmetric Key Encryption
Data Concealment
Complete Image encryption
Required secret data
Data Decryption and Image Restoration
Image Decryption and Data Extraction

Figure 7: Proposed Architecture Diagram

V. EXPERIMENTAL SETUP

For initial tests, standard test image Lena (512 x 512) is considered to demonstrate the feasibility of the proposed method. The complete reversibility of the image has been successfully achieved by comparing the test image with the resultant recovered image. On comparing the results with other methods discussed we can arrive at some parameters that can be used to gauge the performance of the proposed method. They are embedding capacity and accuracy of estimation. These parameters can be varied to obtain different results.

The results obtained largely correspond to the ones observed by Zhang et al.,[23] the proposed method can keep the PSNR at 53dB when the embedding rates are around 0.04bpp. Introducing error correcting codes does not affect the embedding capacities. Also, by increasing the data and subsequently the location maps the data embedding rate remains more or less the same. The proposed method achieves high PSNR near 67 dB for low embedding rate and stabilizes for rates 0.075-0.1. The complexity has been reduced and the time taken for the encryption and decryption is low due to using optimized algorithms as AES. We can conclude that, the proposed method can be comfortably used where the main objectives are data hiding and extraction.

VI. FUTURE WORK

The method can be improved by exploring parallel computing. This can possibly allow for more complex features to be added to the proposed system, thus enhancing it.

VII. CONCLUSION

These papers propose a new combination of algorithm to have more secured data concealment. The encryption implemented in this paper is more efficient when we study the existing methods. Encryption is the most important factor in case of data concealment , in this paper there is a double encryption technique which is allotted of secret data and image individually. Data embedded in the respective coefficient will be in a randomised manner through Chaos encryption algorithm and the image will be encrypted through a standard encryption algorithm.

VIII. REFERENCES:

(1) Lossless Data Hiding for all Image Formats. Jessica Fridrich, Miroslav Goljan, Rui Du. San Jose : s.n., 2002. Spie Proceedings of Photonics West, Electronic Imaging, Security And Watermarking Contents.

(2) Reversible Data Hiding us

(3) ing Difference Expansion. Tian, Jun. 8, s.l. : IEEE Transactions On Circuits And Systems For Video Technology, August 2003, Vol. 13, pp. 890-896.

(4) Reversible Watermarking using Difference Expansion. Tian, Jun. s.l. : Journal of Image Processing and Computer Vision.

(5) Expansion Embedding Techniques for Reversible Watermarking. Diljith M. Thodi, Jeffrey J. Rodríguez,. 3, s.l. : IEEE Transactions On Image Processing, March 2007, Vol. 16.

(6) A Novel Difference Expansion Transform for Reversible Data Embedding. Hyoung Joong Kim, Vasiliy Sachnev,Yun Qing Shi,Jeho Nam,Hyon-Gon Choo. 3, s.l. : IEEE Transactions On Information Forensics And Security, September 2008, Vol. 3, pp. 456-465.

(7) Reversible Watermarking Algorithm Using Sorting and Prediction. Vasiliy Sachnev, Hyoung Joong Kim, Jeho Nam, Sundaram Suresh, Yun Qing Shi. 7, July 2009, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 19, pp. 989-999.

(8) DE-Based Reversible Data Hiding With Improved Overflow Location Map. Yongjian Hu, Heung-Kyu Lee, Jianwei Li. 2, s.l. : IEEE Transactions On Circuits And Systems For Video Technology, February 2009, Vol. 19, pp. 250-260.

(9) Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection. Xiaolong Li, Bin Yang, Tieyong Zeng. 12, s.l. : IEEE Transactions On Image Processing, December 2011, Vol. 20, pp. 3524-3533.

(10) On Compressing Encrypted Data. Mark Johnson, Prakash Ishwar,Vinod Prabhakaran,Daniel Schonberg,Kannan Ramchandran. 10, s.l. : IEEE TRANSACTIONS ON SIGNAL PROCESSING, October 2004, Vol. 52, pp. 2992-3006.

(11) Commutative Encryption and Watermarking in Video Compression. Shiguo Lian, Zhongxuan Liu, Zhen Ren, Haila Wang. 6, June 2007, Ieee Transactions On Circuits And Systems For Video Technology, Vol. 17, pp. 774-778.

(12) Efficient Compression of Encrypted Grayscale Images. Wei Liu, Wenjun Zeng, Lina Dong, Qiuming Yao. 4, April 2010, IEEE Transactions On Image Processing, Vol. 19, pp. 1097-1102.

(13) Lossless Generalized-LSB Data Embedding. Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp, Eli Saber. 2, s.l. : IEEE Transactions On Image Processing, February 2005, Vol. 14, pp. 253-266.

(14) Lossless Data Embedding Using Generalized Statistical Quantity Histogram. Xinbo Gao, Lingling An, Yuan Yuan, Dacheng Tao, Xuelong Li. 8, August 2011, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 21, pp. 1061-1070.

(15) Reversible Data Hiding. Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, Wei Su. 3, March 2006, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 16, pp. 354-362.

(16) Reversible Data Hiding in Encrypted Image. Zhang, Xinpeng. 4, April 2011, IEEE Signal Processing Letters, Vol. 18, pp. 255-258.

(17) Separable Reversible Data Hiding in Encrypted Image. Zhang, Xinpeng. 2, April 2012, IEEE Transactions On Information Forensics And Security, Vol. 7, pp. 826-832.

(18) The Scalar Scheme for Reversible Information-Embedding in Gray-Scale Signals: Capacity Evaluation and Code Constructions. Sian-Jheng Lin, Wei-Ho Chung. 4, August 2012, IEEE Transactions On Information Forensics And Security, Vol. 7, pp. 1155-1167.

(19) An Improved Reversible Data Hiding in Encrypted Images Using Side Match. Wien Hong, Tung-Shou Chen, Han-Yan Wu. 4, April 2012, IEEE Signal Processing Letters, Vol. 19, pp. 199-202.

(20) Reversible Image Watermarking Using Interpolation Technique. Lixin Luo, Zhenyong Chen, Ming Chen, Xiao Zeng, Zhang Xiong. 1, March 2010, IEEE Transactions On Information Forensics And Security, Vol. 5, pp. 187-193.

(21) Robust Reversible Watermarking via Clustering and Enhanced Pixel-Wise Masking. Lingling An, Xinbo Gao, , Xuelong Li, Dacheng Tao, Cheng Deng, Jie Li. 8, August 2012, IEEE Transactions On Image Processing, Vol. 21, pp. 3598-3611.

(22) Reversibility improved data hiding in encrypted images. Weiming Zhang, Kede Ma, Nenghai Yu. s.l. : Elsevier, 29 June 2013, Signal Processing, pp. 118-127.

(23) Video Fingerprinting and Encryption Principles for Digital Rights Management. Deepa Kundur, Kannan Karthik. 2004. Vol. 92.

(24) Chaotic Image Encryption Algorithm Based on Circulant Operation. Xiaoling Huang, Guodong Ye, Kwok-Wo Wong. Hindawi Publishing .19 June 2013.