ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization*

**Vol. 2, Issue 3, March 2014**

# Inverse Data Hiding in a Classical Image by Using Scalable Image Encryption

C. Shahul Hameed[1], S.A.K. Jainulabudeen[2] and P. Mohamed Nazeem[3]

Assistant Professor, Dept of IT, Panimalar Engineering College, Chennai, India[1]
Assistant Professor, Dept of CSE, Panimalar Engineering College, Chennai, India [2]
Assistant Professor, Dept of CSE, Panimalar Engineering College, Chennai, India[3]

**ABSTRACT**: Data hiding is the process of hidden embedding data into data sources such as audio, video, or image signals without changing the perceptual quality. The most common techniques in data hiding is the use of least significant bit and the use of redundancy in the cover image by performing lossless compression. The encryption is a general method for providing privacy protection such as confidentiality, integrity and authentication of data. The hiding of data ideas for encrypted images is made of encryption of image, embedding of data and extraction of data. In the encryption phase, initially the images are encrypted with the encryption key associated with data to be embedded on that encrypted image with data hiding key. In the decryption phase, the embedded image (associate with data) is extracted and decrypted with encryption key and encrypted data is extracted and decryption is made using data hiding key. Though, in both encryption and decryption process same encryption key and data hiding key is used. The objective of the work is to provide an efficient data hiding technique and Image Encryption in which the data and the image can be retrieved independently.

**KEYWORDS**: Cryptography, Image Encryption, Scalable Image Encryption, Huffman Coding.

## I. INTRODUCTION

Cryptography is the science of writing a hidden code (or) the study of mathematical techniques related to aspects of data security such as confidentiality, data integrity, entity authentication and data origin authentication. The basic cryptographic ideas used are Symmetric (or) Hidden key cryptography and Asymmetric (or) Public key cryptography. It employs complex computational algorithms for encryption and decryption. In order to reduce the complexity, Cryptography ideas can be used. The main need of cryptography is to hide the data with the hidden key without knowing to the user. The fast progression of data exchange in electronic way, data security is becoming important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. Security is an important issue in storage communication and communication of images, and encryption is one of the ways to ensure security. Images are different from text. Although the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. In order to transmit hidden images to other people, a variety of image encryption ideas have been proposed. The security of message transmission is very important in the modern computerized and interconnected world. Security problems, such as modification, forgery, duplication, and others, on the Internet have been focused on inevitably.

It has proposed an encryption method using image steganography concept and PLIP model. These image encryption ideas have the advantage of the lossless recovery of the original message. However, due to the disturbances in the transmission media, it makes harder to execute the decryption algorithm for the encrypted data with noise. In this paper, proposed a new encryption method to recover the original image without distortion. In this proposed system, three methods are implemented for image encryption. First method is inverse data hiding method in which the image is encrypted by doing XOR operation bit -by-bit. The second method is Huffman coding method in which the image is scrambled using periodicity.

The third method is Scalable image encryption method. By comparing all these methods, it can be viewed that, Scalable image encryption provides better image quality. The proposed algorithm is simulated in mat lab and their PSNR values are calculated. The paper is organized as follows. In section II, inverse data hiding method and Huffman

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization

Vol. 2, Issue 3, March 2014

coding are introduced i.e. how the original image is encrypted and decrypted. It also explains the security provided by the watermarking technique. Section III, gives the simulation results and section IV draws the conclusion.

## II. RELATED WORK

In [2] authors have proposed Securing Images by Secret Key Steganography. Most watermarking methods introduced that require concealment is less detectable or undetectable, while others exist that are based on the types of concealment that do not require an indiscernibility. It is within this framework and to ensure the security, at storage and transmission of digital data, our work, a new crypto-watermarking method using symmetrical injection of noise on architecture of multilayer neural networks performed to compression images. Data hiding is a technique which embeds data imperceptibly into cover images, so that people will not perceive the existence of the hidden data. Data hiding techniques often utilize the weaknesses of the human visual system in differentiating small color or a grayscale difference is given in [3]. A well-known method is least significant bit (LSB) modification which changes the LSBs of the pixels of an image to embed information. In [4] scheme through data hiding, which could improve the level of security and confidentiality, is introduced. This paper presents a simple lossless scheme for medical image processing. The method is distortion –tolerant in application, since the original image can be recovered without distortion. This scheme is applicable for images of various sizes. In particular, embedding patient information into a medical image through data hiding could improve the level of security and confidentiality that is essential for diffusion of medical information system. Such security provides integrity of medical images and corresponding documentations, along with protection of confidential information. In [5] authors have proposed a scheme to embed data in binary images, including scanned text, figures and signatures. The method manipulates flippable pixel to enforce specific block. In this paper, the hidden data can be extracted without using the original image, but it can be extracted after high quality printing. In [6] authors have proposed an information transmission scheme which combines the cryptosystem and information hiding ,is mainly based on RSA encryption algorithm and the HSV characteristics of 24 bit s BMP image. The scheme is simple and easy to implement. To better protect the security of information, this paper proposed an information transmission scheme which combined the cryptosystem and information hiding. The scheme pre-treated the information firstly by making use of the RSA arithmetic which belongs to the public key cryptosystem, and then took advantage of the improved LSB which based on the Human Visual System to make the cryptograph hid in the 24 bits BMP image and transmitted it.

## III. ENCRYPTION SCHEME

### A. *Inverse Data Hiding:*

The inverse data hiding scheme is used for encrypting the images. It is mainly used to embed additional message into some distortion, with an inverse manner so that the original content can be perfectly restored after extraction of the hidden messages. The proposed scheme is the content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. The data embedding algorithm hides data into the encrypted image using (least significant bit) LSB method with hidden key.According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. Within an encrypted image containing additional data, a receiver must first decrypt it using the encryption key and the decrypted version is similar to the original image.The detailed instructions are as follows:

1. Determine an image, which is determined as a cover image.
2. Convert the cover image to binary
3. Random bits are generated which act as the encryption key
4. XOR operation is performed between the random bits generated and cover image
5. Convert the above binary image to greyscale image. Thus, encrypted image is obtained.

*LSB method:*

This method is used to hide the data in encrypted images. In 8-bit gray scale images are selected as the cover media. Cover-images with the hidden messages embedded in them are called stego-images.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization

Vol. 2, Issue 3, March 2014

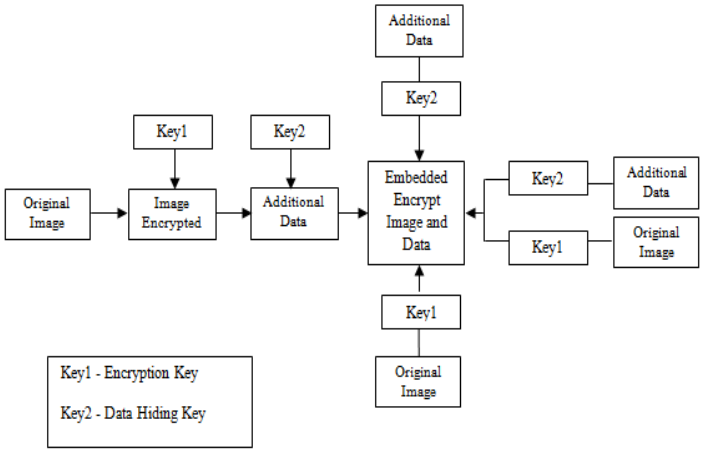


Fig.1. System Architecture

For data hiding methods, the image quality refers to the quality of the stego-images. One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity. This allows a person to hide data in the cover image and make sure that no human could detect the change in the cover image. The LSB method usually does not increase the file size, but depending on the size of the data that is to be hidden inside the file, the file can become noticeably distorted.

The detailed procedures as follows:
1. Determine an encrypted image (cover image).
2. Determine the message or data that should be hidden into the cover image.
*3.* Convert all the pixel values of the encrypted image from grayscale to 8-bit binary values.
*4* Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.
*5.* The original image along with the data is recovered with less distortion and the PSNR value is calculated.

B. *Image Encryption in Huffman Coding:*

Several encryption algorithms including DES, AES, Triple DES, were used in past few years. But variable length codes get more attention from researchers in little time. It is a code that maps source symbols to variable length of bits like Huffman coding. It represents the data in few bits and in few memory locations. It creates binary tree. The process starts by set of symbols/letters and their respective frequencies in ascending or descending order. Each symbol with its frequency is a leaf node at start. Next step is to select two symbols with smallest frequencies, add their frequencies and assign it to parent node, until only one node remains which is called the root node. Assign 0's and 1's to all the nodes and translate the codes by reading from leaf to root node.The detailed instructions are as follows:

1. Determine an image, which is determined as a cover image.
*2.* Convert the cover image to binary
*3.* Random bits are generated which act as the encryption key
*4.* XOR operation is performed between the random bits generated and cover image
*5.* Convert the above binary image to greyscale image. Thus, encrypted image is obtained.

*LSB method:*

This method is used to hide the data in encrypted images. In 8-bit gray scale images are selected as the cover media. Cover-images with the hidden messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. One of the common techniques is based on manipulating the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization

Vol. 2, Issue 3, March 2014

least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity. This allows a person to hide data in the cover image and make sure that no human could detect the change in the cover image. The LSB method usually does not increase the file size, but depending on the size of the data that is to be hidden inside the file, the file can become noticeably distorted. The detailed procedures as follows:

1. Determine an encrypted image (cover image).
2. Determine the message or data that should be hidden into the cover image.
3. Convert all the pixel values of the encrypted image from grayscale to 8-bit binary values.
4. Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.
5. The original image along with the data is recovered with less distortion and the PSNR value is calculated.

C. *Scalable Image Encryption:*

Scalable image encryption algorithm is a wonderful technique for encrypting and compressing the data (Images and Videos). It is specifically designed for the colored images, which are 3D arrays of data streams. Because of the explosion of networks and the huge amount of content transmitted along, securing video content is becoming more and more important. There are traditional approaches to encode the data, which perform encryption on bit stream of data. The several interesting features, such as scalable encryption, the main goal of scalable encryption is to reduce the amount of data to be encrypted. The general approach for scalable encryption is separated in two parts, public part which is unprotected and private part i.e. protected part. There is a lot of development in the communication field and a huge amount of data is transmitted through the channel daily. For secure transmission of data, there is a great demand for securing these multimedia data, resulting in encrypting the data. Most of the conventional algorithms are not useful for image encryption because of the redundant data contained in an image, strong correlation between the pixel value of the image and the complexity of the algorithm is high. For this purpose, scalable encryption is used, which provide security and confidentiality for secure transmission of data through the network.

D. *Algorithm for Scalable Encryption:*

Step 1: Input and colored image (which contains R, G, B pattern).Input image can be browsed from anywhere.
Step 2: R, G, B pattern will be in the form of matrix. Save this matrix in a variable.
Step 3: In this algorithm I have used the technique of confusion and diffusion, which means that each pixel of the input image is replaced by another value and that value will be generated by random number generator. In this algorithm Lorentz function is used to generate the random numbers.
Step 4: After generating the random numbers, that random numbers will be XORed with the original pixel.
Step 5: The output will be an encrypted image.

*LSB method:*

This method is used to hide the data in encrypted images. In 8-bit gray scale images are selected as the cover media. Cover-images with the hidden messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity. This allows a person to hide data in the cover image and make sure that no human could detect the change in the cover image. The LSB method usually does not increase the file size, but depending on the size of the data that is to be hidden inside the file, the file can become noticeably distorted.

The detailed procedures as follows:

1. Determine an encrypted image (cover image).
2. Determine the message or data that should be hidden into the cover image.
3. Convert all the pixel values of the encrypted image from grayscale to 8-bit binary values.
4. Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.
5. The original image along with the data is recovered with less distortion and the PSNR value is calculated.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization

Vol. 2, Issue 3, March 2014

## IV. EXPERIMENTAL RESULTS

In this proposed system, selecting the classical image of 256x256 cameraman.tif, Brain.gif with 256 gray levels as the original image and adopt the inverse data hiding method, Huffman Coding and Scalable image encryption algorithm for image encryption. MATLAB 2010 is used to simulate the experiment.

### A. *Inverse Data Hiding Method:*

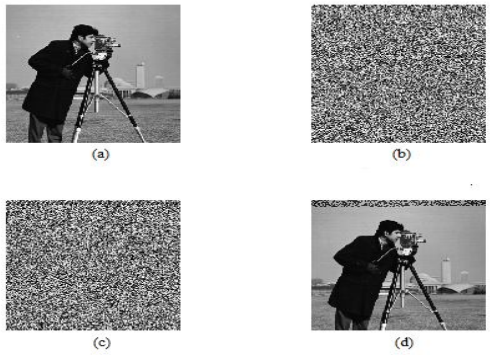


Fig.2. (a) Original image, (b) Encrypted image (c) Encrypted image with Encrypted message and (d) decrypted image.

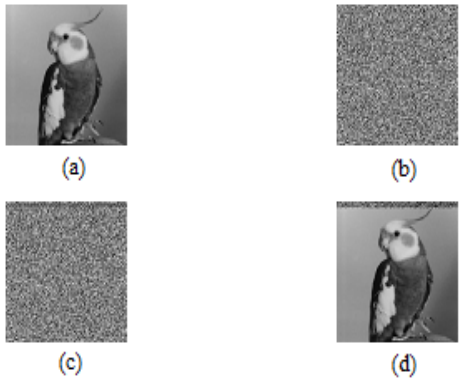


Fig.3.(a)Original image(b) Encrypted image (c) Encrypted image with Encrypted message (d) Decrypted image.

The test images Bird, Cameraman sized 256 *256 shown in Fig.2 (a), Fig.3 (a) was used as the original cover in the experiment. After image encryption, the 8 encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Fig. 2(b), Fig.3 (b).Then embedded data into the encrypted image by using LSB method. The encrypted image with message is given as Fig. 2(c),Fig.3(c).The decrypted is shown in Fig.2(d),Fig.3(d)and the values of PSNR is 51.4 dB,53.5dB.Finally, the embedded data were extracted and the original image was perfectly recovered from the decrypted image.

### B. *Huffman Coding*

The test image Baboon, Barbara sized 256 x 256shown in Fig.4 (a), Fig.5 (a) was used as the original cover in the experiment. Make the parameter in the Huffman hidden, the images are shown in Fig.4 (b), Fig.5 (b) and Fig.4(c), Fig.5(c).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization

Vol. 2, Issue 3, March 2014

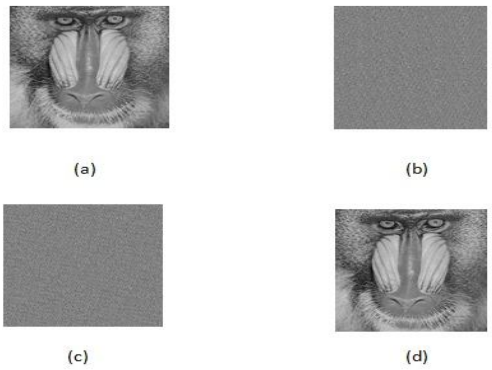


Fig.4.(a)Original image, (b)Encrypted Image, (c) Encrypted images with Encrypted message (d) Decrypted image.

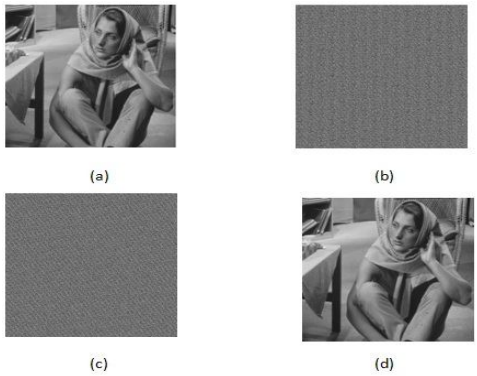


Fig.5. (a) Original image, (b) Encrypted image (c) Encrypted image with Encrypted message and (d) Decrypted image.

The decrypted image is given as Fig.4 (d), Fig.5 (d) and the PSNR is 91.6 dB, 94.6Db. The number of times may be selected according to visual effect. It is safe to keep the hidden of the parameters and the iteration times, but the attacker can also attract through the method of statistics analysis and exhaustion. So still need to change the pixel value to encrypt further.

C. *Scalable Image Encryption*

The test image Baboon, Barbara sized256 *256shown in Fig. 6(a) was used as the original cover in the experiment. Then, a data is embedded into the encrypted image by using LSB method. The encrypted image with message is given Fig.6 (b) and 6(c), is the encrypted file by data hiding key. Fig. 6(d) shows the extracted data that was decrypted by the data hiding key. The value of PSNR caused by data embedding is 65.6 dB. The number of times may be selected according to visual effect. Through the Scalable Image Encryption, it realizes the scrambling and attains the purpose of encryption. It is safe to keep the hidden of the data and the iteration times, but the attacker can also attract through the method of statistics analysis and exhaustion. The test demonstrate that it is impossible to get the original data when input the wrong key which provides the protection to the hidden data. Scalable Image Encryption algorithm is based on the theory of a special kind of inverse arithmetic for modular and exponent.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization

Vol. 2, Issue 3, March 2014

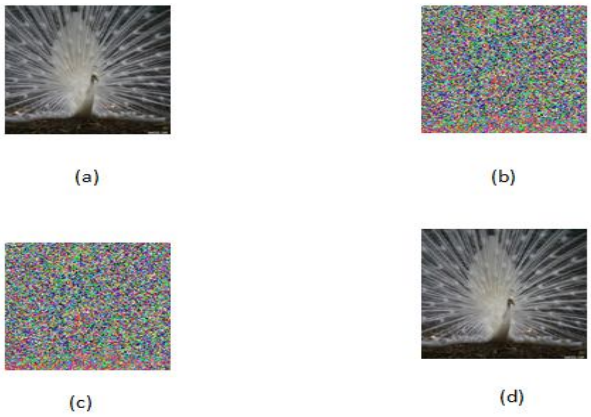


Fig.6.(a) Original image, (b) Encrypted image (c) Encrypted images with Encrypted message (d) Decrypted image.

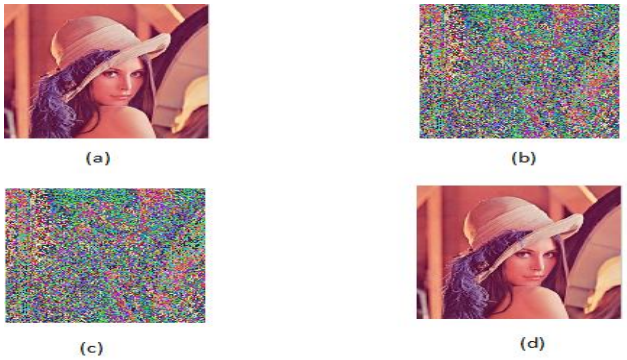


Fig.7. (a) Original image, (b) Encrypted image (c) Encrypted image with Encrypted message and (d) decrypted Image.

## V. CONCLUSION AND FUTURE WORK

In this paper, discussed and demonstrated that the image encryption algorithm is efficient and highly secure. All parts of the proposed encryption system were simulated using MATLAB. The scheme can resist most known attacks, such as statistical analysis and brute-force attacks. By comparing these entire algorithms the Scalable image encryption gives the best image quality and has high level of security with less computation. It is highly robust towards cryptanalysis.This work can be extended to implement image encryption using neural networks and for many securities, authentication purpose it can be used. It can be also used in many emerging fields. Because of the rapid development of information technology, it is becoming increasingly difficult to maintain a satisfactory level of information security. New information security theory and advanced technologies are required urgently. Most encryption methods are designed for text information, and some encryptions are easily to be attacked.

## REFERENCES.

1. Xinpeng Zhang, "Reversible Data Hiding in Encrypted Images", IEEE International Conference on Signal Processing Lett., Vol.18, No.4, pp. 255-258, 2011.
2. Y. Benlcouiri, M.C. Ismaili and A. Azizi, "Securing Images by Secret Key Steganography", Applied Mathematical Sciences, Vol.6, No. 111, pp. 5513-5523, 2012.
3. C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition., vol. 37, pp. 469-474, 2004.
4. Chen.G, Mao.Y and Chui C.K. "A Symmetric Image Encryption Scheme based on 3rd Chaotic Cat Maps", Chaos, solutions and fractals 21, pp. 749-761, May 2004.
5. Daemen.J and Rijimen.V, "The Design of Rijimdeal; AES – The Advanced Encryption Standard", Springer, 2002.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization*

**Vol. 2, Issue 3, March 2014**

6. James Bowley and laura Rebollo – Neira ,"Sparsity and Something Else' : An Approach to Encrypted Image Folding", IEEE signal Processing Lett., Vol.18, No.3, pp. 189 – 192, 2011.
7. V.Naveenkumar, Santosh Hariharan, and Kumar Rajamani "Data hiding scheme for medical images using lossless code for mobile HIMS", IEEE International conference on Communication system and networks, pp.1-4, 2011.
8. Min Wu, and B. Liu, "Data hiding in digital binary image", IEEE transactions on multimedia, vol 6, no.4, 2004.
9. SantoshHariharan, V.Naveenkumar, and MrigankRochan, "An improved anti-counterfeiting technique for credit card transaction system" IEEE International conference on communication system and networks, pp. 1-4, 2011
10. Tan Fei, Liao Shaojun,"Research and implementation of data hiding based on RSA and HVS", IEEE International conference on e-business and e-commerce, pp.1-4, 2011.
11. Cheng Zhi-Gang, Yue-li cui, Zheng Wei, "Image Encryption and hiding based on Wavelet Packet Transform and Bit plane decomposition" IEEE International conference on Wireless Communications, Networking and Mobile Computing, (pp1-4), 2008.
12. Sos Agaian, and Yicong Zhou, "Image Encryption using the image steganography concept and PLIP model", IEEE International conference on System Science and Engineering, pp 699-703, 2011.
13. Lhoussain EL Fadil, and Youssef Za, "Enhancer EPR Data Protection using Cryptography and Digital Watermarking", IEEE International Conference on Multimedia and computing systems, pp 1-5, 2011.
14. Wein Hong, Tung-shou Chen and Han-Yan Wu, "An Improved Inverse Data Hiding in Encrypted Images using side Match", IEEE Signal Processing Lett., Vol. 19, No.4, pp. 199- 202.2012.
15. Subramania Sudharsanan, "Shared Key Encryption of JPEG Color Images", IEEE Trans. on consumer Electronics., Vol. 51, No.4, pp.1204 - 1211, 2005.