ISSN 2278-7763

Study on Separable Reversible Data Hiding in Encrypted Images

Rini.J ,4th Semester M.Tech ,Dept. of Computer Science and Information Systems ,FISAT Angamaly ,Kerala, India
riniklbm@gmail.com

ABSTRACT

This work proposes a Secure and authenticated discrete reversible data hiding in cipher images deals with security and authentication. In the first phase, a content owner encrypts the original uncompressed image using an encryption key. Then, a data hider may compress the least significant bits of the encrypted image using a data hiding key to create a sparse space to accommodate some additional data. With an encrypted image containing additional data, if a receiver has the data hiding key, receiver can extract the additional data though receiver does not know the image content. If the receiver has the encryption key, can decrypt the received data to obtain an image similar to the original one. If the receiver has both the data hiding key and the encryption key, can extract the additional data and recover the original content.

Keywords
Cryptography, Steganography, Reversible data hiding,

1. INTRODUCTION

The amount of digital images has increased rapidly on the Internet. Image security becomes increasingly important for many applications, e.g., confidential transmission, video surveillance, military and medical applications. For example, the necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over networks. To decrease the transmission time, the data compression is necessary. The protection of this multimedia data can be done with encryption or data hiding algorithms. Since few years, a problem is to try to combine compression, encryption and data hiding in a single step. For example, some solutions were proposed in to combine image encryption and compression. Two main groups of technologies have been developed for this purpose. The first one is based on content protection through encryption. There are several methods to encrypt binary images or gray level images. The second group bases the protection on data hiding, aimed at secretly embedding a message into the data. Nowadays, a new challenge consists to embed data in encrypted images. Previous work proposed to embed data in an encrypted image by using an irreversible approach of data hiding or data hiding, aimed at secretly embedding a message into the data. A new idea is to apply reversible data hiding algorithms on encrypted images by wishing to remove the embedded data before the image decryption. Recent reversible data hiding methods have been proposed with high capacity, but these methods are not applicable on encrypted images.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data medication. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over the internet, many techniques have been developed like: Cryptography, Steganography. While Cryptography is a method to conceal information by encrypting it to cipher texts and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats.

In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner
does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes. With the lossy compression method an encrypted gray image can be efficiently compressed by discarding the excessively rough

ISSN 2278-7763

and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients.

Data hiding is a technique that is used to hide information in digital media such as images, audio, video etc. The information that is hidden depends upon the purpose of application. Owing to data hiding, some distortion may occur in the original cover medium and cannot be inverted back to the original medium. Such a data hiding is called lossy data hiding. But in applications such as medical image system, law enforcement, remote sensing, military imaging etc it is desired to recover the original image content with greater accuracy for legal considerations. The data hiding scheme that satisfies this requirement is called reversible or lossless data hiding. Reversible data hiding was first proposed for authentication and its important feature is reversibility. It hides the secret data in the digital image in such a way that only the authorized person could decode the secret information and restore the original image. Several data hiding methods have been proposed. The performance of a reversible data embedding algorithm is measured by its payload capacity, complexity, visual quality and security. Earlier methods have lower embedding capacity and poor image quality. As the embedding capacity and image quality improved, this method became a covert communication channel. Not only should the data hiding algorithm be given importance. The image on which the data is hidden should also be highly secured.

2. REVERSIBLE DATA HIDING

Reversible data hiding in images is a technique that hides data in digital images for secret communication. It is a technique to hide additional message into cover media with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analyzed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. Many reversible data hiding methods have been proposed recently .As is well known, encryption is an effective and popular means of privacy protection. In order to securely share a secret image with other person, a content owner may encrypt the image before transmission. In some application scenarios, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. For example, when medical images have been encrypted for protecting the patient privacy, a database administrator may aim to embed the personal information into the corresponding encrypted images.

It may be also hopeful that the original content can be recovered without any error after decryption and retrieve of additional message at receiver side. Traditionally, data hiding is used for secret communication. In some applications, the embedded carriers are further encrypted to prevent the carrier from being analysed to reveal the presence of the embedment. Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before data hiding is actually performed, such as military images or confidential medical images.

In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. A major recent trend is to minimize the computational requirements for secure multimedia distribution by selective encryption where only parts of the data are encrypted. There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all. Selective encryption aims at avoiding the encryption of all bits of a digital image and yet ensuring a secure encryption.

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored after extraction of the hidden message. As an effective and popular means for privacy protection, encryption converts the ordinary signal into incomprehensible data, so that the general signal processing typically takes place before encryption or after decryption. However, in some circumstances that a content owner does not trust the service provider, the ability to manipulate the encrypted data when keeping the plain content secret is desired. When the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may compress the encrypted data due to the limited channel resource. 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. Data hiding is referred to 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

ISSN 2278-7763

the original media. That is, cover media has permanent distortion even after the hidden data have 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. Performance of a reversible data-embedding algorithm Reversible data embedding, which is also called lossless data embedding, embeds invisible data (which is called a payload) into a digital image in a reversible fashion. As a basic requirement, the quality degradation on the image after data embedding should be low. An exciting feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. Reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original state. The performance of a reversible data-embedding algorithm can be measured by the following

.

Payload capacity limit
Visual quality
Complexity

The distortion- free data embedding is the motivation of reversible data embedding. Data will certainly change the original content by embedding some data into it. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. From the application point of view, since the difference between the embedded image and original image is almost unnoticeable from human eyes, reversible data embedding could be thought as a secret communication channel since reversible data embedding can be used as an information carrier.

3. Separable Reversible Data hiding

As name itself indicates that it is the reversible data technique but which is separable. The separable means which is able to separate .In other words, we can separate the some things, activities using suitable criteria. Here in separable reversible data hiding concept. The separation of activities i.e. extraction of original cover image and extraction of payload (data which was embedded).This separation requires some basic cause to occur. In separable data hiding key explained by Xin peng Zhang the separation exists according to keys. Here at the receiver side, there are three different cases are encountered. The separation of extracting the data and getting the cover media come to be exists. That's why it is called as Separable Reversible Data hiding.

4. Compression

Compression of encrypted data has become considerable research interest in recent years. The traditional way of securely and efficiently transmitting redundant data is to first compress the data to reduce the redundancy, and then to encrypt the compressed data to mask its meaning. At the receiver side, the decryption and decompression operations are orderly performed to recover the original data. However, in some application scenarios, a sender needs to transmit some data to a receiver and hopes to keep the information confidential to a network operator who provides the channel resource for the transmission. That means the sender should encrypt the original data and the network provider tend to compress the encrypted data without any knowledge of the cryptographic key and the original data. There are several techniques for compressing/decompressing encrypted data have been developed. This paper a presented lossy compression method in which an encrypted grey image can be efficiently compressed by discarding the excessively rough and _ne information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. The compression ratio and the quality of reconstructed image vary with different values of compression parameters. In the encryption phase of the Zhangs system, only the pixel positions are shuffled and the pixel values are not masked. With the values of elastic pixels, the coefficients can be generated to produce the compressed data.

5. Existing System

In existing system reversible data hiding technique the image is compressed and encrypted by using the encryption key and the data to hide is embedded in to the image by using the data hiding key. At the receiver side he first need to extract the image using the encryption key in order to extract the data and after that he'll use data hiding key to extract the embedded data. It is a serial process and is not a separable process.

Disadvantages

Principal content of the image is revealed before data extraction.

If someone has the data hiding key but not the encryption key he cannot extract any information from the encrypted image containing additional data.

ISSN 2278-7763

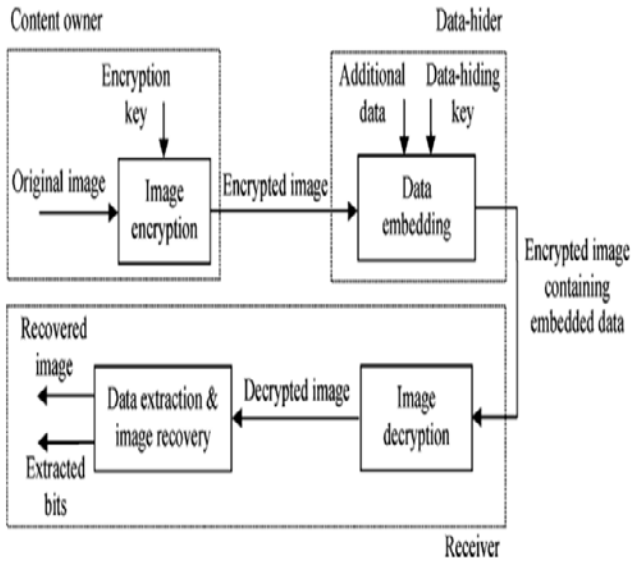


Figure 1: Existing system

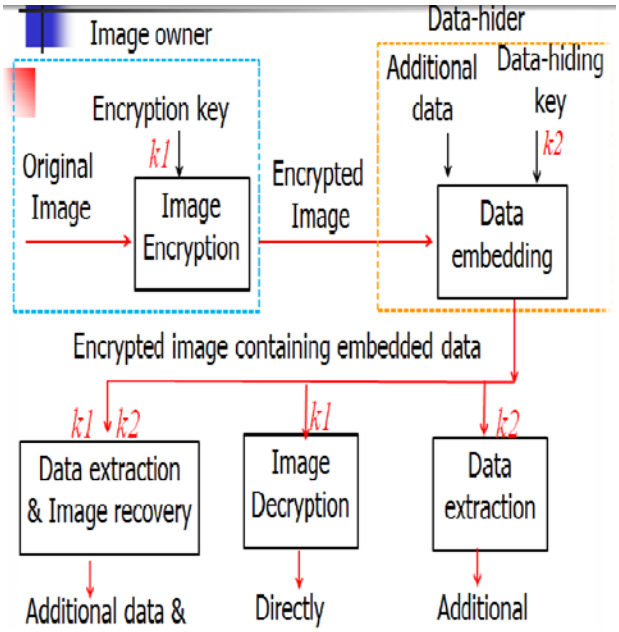


Figure 2: Proposed system

6. Proposed Scheme

The proposed scheme is made up of image encryption, data embedding and data extraction, image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

Advantages

If the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content.
If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data.
If he receiver has both the data-hiding key and the encryption key, can extract the additional data and recover the original image without any error when the amount of additional data is not too large.

7. IMPLEMENTATION MODULES

7.1 Image Encryption

In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from
cipher code, scientific community have seen strong interest in image transmission. However, illegal data or image access has become more easy and prevalent in wireless and general communication networks. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, data or image encryption /decryption [2] is essential, furthermore. As such in this paper, a scheme based on encryption has been proposed for secure image transmission over channels.

Assume the original image with a size of N1 * N2 is in uncompressed format and each pixel with gray value falling into [0, 255] is represented by 8 bits. Denote the bits of a pixel as bij0,bij1,....bij7 where 1<i<N1 and 1<j<N2,the gray value as P i ,j and the number of pixels as N (N= N1 * N2).In encryption phase, the exclusive-or results of the original bits and pseudo-random bits

ISSN 2278-7763

$$B_{i,j,u} = b_{i,j,u} \oplus r_{i,j,u}$$

are calculated. where r,i,j,u are determined by an encryption key using a standard stream cipher. Then B,i,j,u, are concatenated orderly as the encrypted data.

7.2 **Data Embedding**

This module implements an additional data embedding and enclosed into Data-Hiding Key. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. In the data embedding phase, some parameters are embedded into a small number of encrypted pixels, and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters. The detailed procedure is as follows According to a data-hiding key, the data hider randomly selects Np encrypted pixels that will be used to carry the parameters for data hiding. Here, Np is a small positive integer, for example, Np=20. The other (N-Np) encrypted pixels are permuted and divided into a number of groups, each of which contains L pixels. The permutation way is also determined by the data-hiding key. For each pixel-group, collect
the M least signi_cant bits of the L pixels, and denote them as B (k,1) , B (k,2) B(k,M*L) where k is a group index within [1,(N-Np)/L] and M is a positive integer less than 5.The data-hider also generates a matrix G , which is composed of two parts. The left part is the identity matrix and the right part is pseudo-random binary matrix derived from the data-hiding key. For each group, which is product with the G matrix to form a matrix of size (M
* L-S). Which has a sparse bit of size S, in which the data is embedded and arrange the pixels into the original form and re-permutated to form a original image.

$$\begin{bmatrix} B'(k,1) \\ B'(k,2) \\ \vdots \\ B'(k,ML-S) \end{bmatrix} = \mathbf{G} \cdot \begin{bmatrix} B(k,1) \\ B(k,2) \\ \vdots \\ B(k,ML) \end{bmatrix}$$

Fig: Sparse space obtaining by matrix multiplying

7.3 **Image Decryption**

This module implements an Image Decryption Process .The content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method in is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. When having an encrypted image containing embedded data, a receiver firstly generates ri,j,k according to the encryption key, and calculates the exclusive-or of the received data and ri,j,k to decrypt the image. We denote the decrypted bits as bri,j,k . Clearly, the original most significant bits (MSB) are retrieved correctly. For a certain pixel, if the embedded bit in the block including the pixel is zero and the pixel belongs to S1, or the embedded bit is 1 and the pixel belongs to S0, the data-hiding does not affect any encrypted bits of the pixel. So, the three decrypted LSB must be same as the original LSB, implying that the decrypted gray value of the pixel is correct. On the other hand, if the embedded bit in the pixels block is 0 and the pixel belongs to S0, or the embedded bit is 1 and the pixel belongs to S1 , the decrypted LSB.

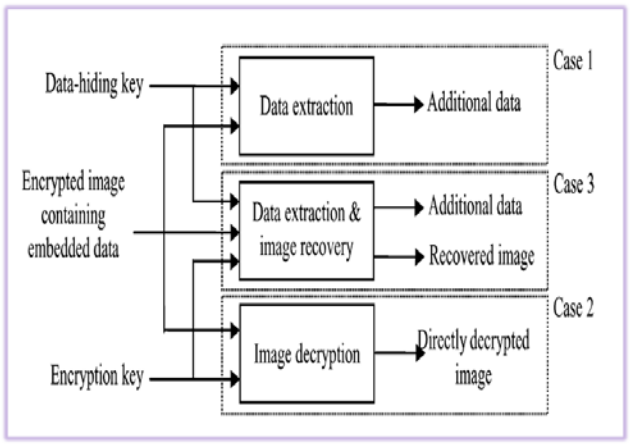
$$\begin{aligned} b'_{i,j,k} &= r_{i,j,k} \oplus B'_{i,j,k} \\ &= r_{i,j,k} \oplus \overline{B_{i,j,k}} \\ &= r_{i,j,k} \oplus \overline{b_{i,j,k} \oplus r_{i,j,k}} \\ &= \overline{b_{i,j,k}}, \qquad k = 0, 1, 2. \end{aligned}$$

7.4 **Data extraction**

If the receiver has both the data-hiding, he may aim to extract the embedded data According to the data-hiding key, the values of M,L and S, the original LSB of the Np selected encrypted pixels, and the (N-Np) * S/L - Np

ISSN 2278-7763

additional bits can be extracted from the encrypted image containing embedded data. By putting the Np LSB into their original positions, the encrypted data of the Np selected pixels are retrieved, and their original gray values can be correctly decrypted using the encryption keys. In the following, we will recover the original gray values of the other (N-Np) pixels.



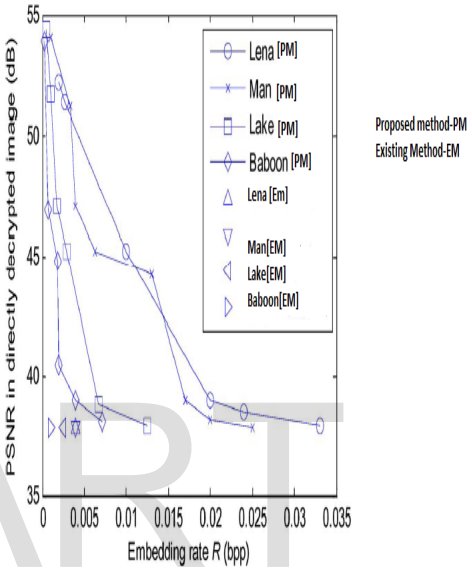
This project proposes a novel scheme for separable reversible data hiding in encrypted image. In the proposed scheme, the original image is encrypted
using an encryption key and the additional data are embedded into the encrypted image using a data-hiding key. With an encrypted image containing additional data, if the receiver has only the data-hiding key, he can extract the additional data though he does not know the image content. If he has only the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the embedded additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original image without any error when the amount of additional data is not too large.

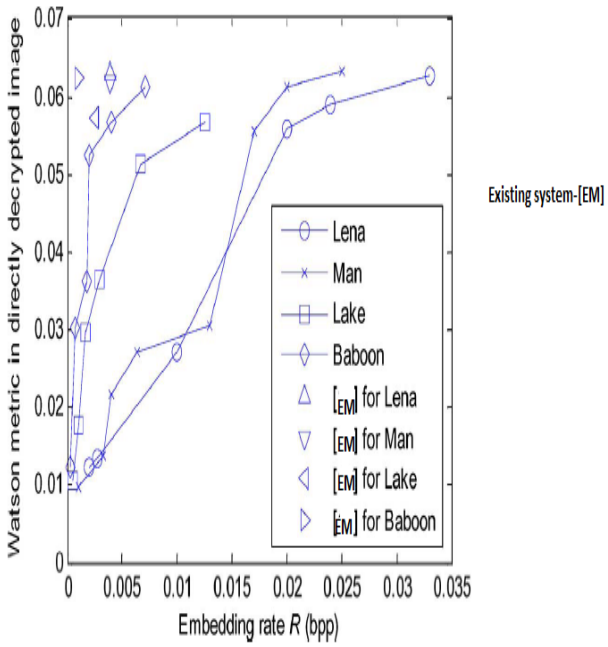
8. EXPERIMENTAL RESULTS

Here, three quality metrics were used to measure the distortion in directly decrypted image:

- PSNR
- The Watson metric
- A universal quality index.

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. PSNR simply indicates the energy of distortion caused by data hiding, the Watson metric is designed by using characteristics of the human visual system and measures the total perceptual error, which is DCT-based and takes into account three factors: contrast sensitivity, luminance masking and contrast masking. Additionally, the quality index works in spatial domain, as a combination of correlation loss, luminance distortion and contrast distortion. Higher PSNR, lower Watson metric or higher means better quality. In these figures, while the abscissa represents the embedding rate, the ordinate is the values of PSNR,Watson metric or quality index.





ISSN 2278-7763

9. CONCLUSION AND FUTURE SCOPE

In this paper, a novel scheme for separable reversible data hiding in encrypted image is proposed, which consists of image encryption, data embedding and data-extraction/image recovery phases. In the first phase, the content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, he can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. With an encrypted image containing additional data, the receiver may extract the additional data using only the data hiding key, or obtain an image similar to the original one using only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large. If the lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method in compatible with encrypted images generated by pixel permutation is not suitable here since the encryption is performed by bit-XOR operation.
The lossless compression method is used for the encrypted image containing embedded data, the additional data can be still extracted and the original content can be also recovered since the lossless compression does not change the content of the encrypted image containing embedded data. However, the lossy compression method compatible with encrypted images generated by pixel permutation is not suitable here since the encryption performed by bit-XOR operation. In the future, a comprehensive combination of image encryption and data hiding compatible with lossy compression deserves further investigation. The implemented a Novel Reversible method can be enhanced in future by using the following provisions A MLSB technique can also be applied after embedding when there is lot of change in the pixel to retain nearest to the original value.

10. REFERENCES

[1].Chi-Kwong Chan Hiding data in images by simple LSB substitution.
[2].Kazem Ghazanfari,Shahrokh Ghaemmaghami LSB++: An improvement to LSB+ steganography.
[3].Xinpeng Zhang E_cient data hiding with plus-Minus one or two.
[4].Robust data hiding technique based on LSB matching.
[5].Spread spectrum image steganography.
[6].Altering based approach to adaptive steganography.
[7].Chung-Li Hou,ChanChun Lu,Shi-Chun Tsai and Wen-Guey Tzeng An optimal Tree Based Parity Checking.
[8].Weiqi Luo,Jiwu Huang Edge adaptive image steganography based on LSB matching revisited.
[9].Xinpeng Zhang Separable reversible data hiding in encrypted messages

