*International Journal of Research in Advent Technology, Vol.5, No.1, January 2017*
*E-ISSN: 2321-9637*
*Available online at www.ijrat.org*

# Review of Various Data Hiding Techniques

Ms. Harsha Mahajan[1], Prof. Pankaj Salunkhe[2]
*Department of Electronics and Telecommunication[1, 2], Yadavrao Tasgaonkar Institute of Engineering and Technology, Karjat, Maharashtra[1, 2]*
*Email: mahajanharsha9@gmail.com[1], pasalunkhe@gmail.com[2]*

**Abstract-** The techniques which are utilized to hide a secret message or secret image into a cover image so that the presence of secret data is not realized are called as data hiding techniques. Embedding a secret image into a cover image gives stego image. Digital image is the best media to store data. This provides large capacity for hiding secret information.

**Index Terms**- Data hiding, LSB substitution, Histogram Shifting, Difference Expansion, Prediction Error Expansion, Recursive Histogram Modification, Discrete Cosine Transform

## 1. INTRODUCTION

Nowadays technology is changing very rapidly as the world changes. In recent years with the growth of internet and communication techniques images from various sources transmitted for various applications such as military, Government, Banking. These images are having private and confidential information which is to be protected from leakages during transmission. Everybody wants secure network for secure transmission of information. More secure transmission techniques are required while using more secure information. Image encryption and Data hiding are two common approaches for secure image transmission. Digital image is a collection of pixels which are represented in the form of n*m (where n and m are no of row and column respectively). In image encryption and decryption process some encryption and decryption algorithm is required which makes use of characteristic property of image like high redundancy and spatial correlation in order to obtain scrambled image. At the receiver side using decryption algorithm information is extracted from scrambled image. The scrambled image can't give extra data before unscrambling and may stir an assailant's attention during transmission because of its irregularity in structure. In order to avoid this problem data hiding techniques are used in which secret message is hided in cover image so that existence of secret data can not be realized by anyone. Nowadays there are many methods developed for secure image transmission and data hiding. In this paper, review of various techniques is proposed for secure image transmission.

## 2. VARIOUS DATA HIDING TECHNIQUES

In image encryption technique the natural property of image such as high redundancy and strong spatial correlation are utilized to obtain encrypted image based on Shannon's confusion and diffusion properties. In order to obtain the secret image from encrypted image one has to have the correct key. However, due to randomness in structure it may arouse the attacker's attention during transmission. This problem can be avoided using various data hiding techniques described as follows. [1]

### 2.1. *LSB substitution*

Hiding of secret messages into a cover media so that the unwanted observer will not be able to read the hidden data is a technique of data hiding. Simple LSB substitution is one of the techniques of data hiding. In LSB substitution 8-bit grayscale images are selected for hiding the messages. Secrete messages are embedded into these 8-bit grayscale images to form a stego-images. In this technique the Least Significant Bits of cover image are manipulated by replacing by message bits. This technique is described by changing the pixels by bits of the secret messages. In order to improve the quality of stego-image Local Pixel Adjustment process (LPAP) is used. LPAP considers Last three significant bits and 4th but not all. LPAP is not optimal. In order to improve the capacity of simple LSB and improve the quality of stego-image Optimal Pixel Adjustment Process is implemented. Use of OPAP for simple LSB substitution the Worst Mean Square Error (WMSE) is reduced by half. So enhanced image quality can be obtained with low extra computational complexity. [2]

### 2.2 *Difference Expansion*

In reversible data embedding the original digital image content is completely restored. For lossless data embedding the quality degradation on the image after data embedding must be low. Difference Expansion technique provides high capacity, high visual quality and reversible data embedding for digital images. In

Difference Expansion method the differences of neighboring pixel values is calculated and some difference values are selected for expansion. These values are selected based on haar wavelet transformation.

Suppose a pair of pixel values $(x, y)$, $0 \leq x$ and $y \leq 255$.

Their integer average l and difference h are computed such that

$$l = \left(\frac{x+y}{2}\right) \quad \text{and}$$

$$h = x - y \text{.....(1)}$$

Let b be the bit which is to be embedded.

Taking inverse transform of equation (1)

$$x = l + \frac{h+1}{2} \quad \text{and}$$

$$y = l - \frac{h}{2} \text{.....(2)}$$

L and h are low frequency and high frequency signal components. The difference value h is represented into binary. Then b is appended into binary representation of difference value after LSB by which new difference value h is obtained. Then based on new difference value and original integer average value new values $(x', y')$ are calculated. From embedded pair $(x', y')$, the embedded bit b can be extracted and original pair $(x, y)$ is restored. Again new average and difference are calculated. Using Difference Expansion technique extra storage space can be discovered by exploring redundancy in image content. [3]-[4]

### 2.3 *Recursive Histogram Modification*

Recursive Histogram Modification is one of the new technique for Reversible Data hiding. In this technique the host sequence is divided into disjoint blocks and embed the message by recursively modifying the histogram of each block bit by bit manner. In this technique a host sequence with identical distribution is produced. The message which is to be embedded is usually encrypted before embedding. This message is a binary random sequence. In order to embed message recursively, the host sequence is divided into disjoint blocks in such a way the for n blocks (n-1) blocks having same length and last block has larger length. Message is embedded into each block. The embedding process in $i^{th}$ block outputs the message to be embedded into $(i+1)^{th}$ block. The embedding and extracting process are based on decompression compression algorithm of entropy coder. [5]

### 2.4 *Histogram Shifting*

Data hiding technique based on histogram shifting is used to embed data in cover media by shifting the histogram of image. This technique detects peak and zero points in the histogram. By shifting these peak and zero points data is embedded. It provides high data hiding capacity with low distortion. The input image is divided into blocks. Shifting of histogram is done on each block. Due to which data hiding capacity is enhanced and visual quality is improved as well. Embedding image within blocks is more in amount as compared with embedding within a single image. This technique does not allow overflow and underflow problem that is grayscale exceeds above 255or falls below 0. [7]

### 2.5 *Prediction Error Expansion*

Prediction Error Expansion technique considers for embedding the predictive errors. In this scheme the pixels are modified such that to expand two times the prediction error. Multiplying by two sets to zero the least significant bit of prediction error will create space for embedding data of one bit. Efficient predictors are developed in reversible watermarking for lossless compression eg, MED(Median Edge Detector), GAP(Gradient Adjust Predictor). Rhombus Predictors are most newly developed Prediction Error Expansion scheme. In this scheme the distortions introduced by watermarking are controlled by threshold. If prediction error is less than threshold, no overflow or underflow is generated which will transform the pixel and data of one bit can be embedded. [6]

## 3. CONCLUSION

In this paper, we have studied various techniques of data hiding in Image processing. As discussed earlier, in image encryption due to random nature of resultant image there are chances of leakage of confidential data. This limitation is overcome by using these data hiding techniques. The properties of digital image which are high redundancy and strong spatial correlation plays important role for implementation of these data hiding techniques.

## REFERENCES

[1] Ya-Lin Lee; Wen-Hsiang Tsai (2014): "A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations" IEEE Transactions on circuits and systems for video technology, pp. 695-703.

[2] C. K. Chan and L. M. Cheng (2004): "Hiding data in images by simple substitution", Pattern Recognition, pp. 469-474.

[3] J. Tian (2003): "Reversible data embedding using a difference expansion", IEEE Transactions on circuits and systems for video technology, pp. 890-896.

[4] Y. Hu, H-K Lee, K. Chen, and J. Li (2008): "Difference expansion based reversible data hiding using two embedding directions", IEEE Transactions on multimedia, pp. 1500-1512.
[5] W. Zhang, X. Hu, X. Li and N. Yu (2013): "Recursive Histogram Modification: Establishing equivalency between reversible data hiding and lossless data compression", IEEE Transactions on image processing, pp. 2775-2785.
[6] T. Nedelcu, R. Iordache, and D. Coltuc: "Three stages prediction-error expansion reversible watermarking".
[7] L. R. Mathew, A. C. Haran V.(2014): "Histogram Shifting based reversible data hiding", IJETT, pp. 482-485.

.