Randomly Carrier Detection based Data hiding

1Anuja Bhondve & 2Akshada T Bhondave
1Department of Information Technology, Pimpri Chinchwad College of Engineering & Research, Ravet
2Department of Information Technology, AISSMS Institute of Information Technology, Pune

Received: April 02, 2019  Accepted: May 04, 2019

ABSTRACT: There is technique which involves communicating sensitive data with appropriate multimedia which is not visible is called data hiding. There is novel technique pixel prediction which is used for data hiding and it is based on minimum rate criterion. Novel technique pixel prediction maintains consistency between data hiding schemes. Previous pixel prediction system mainly focuses on two features, firstly discover how to obtain sharp PE histogram, and second for the given histogram how to improve the embedded performance. For achieving optimal embedding performance on generated random pixel prediction sequence we are introducing a novel optimized histogram modification scheme.

Key Words: Data hiding, Pixel Prediction, LSB.

Introduction
Data hiding technique involves putting sensitive information in host image with minimum changes in the image. In most of data hiding techniques, image becomes more distorted and we are unable to retrieve its original format. The cover media are permanently distorted due to the data embedding. In sector such as military or medical it is necessary to retrieve original cover image without any loss of information. There are different characteristics of data hiding technique such as: perceptibility, capacity, authentication, Security, Finger print and secret communication, [1] [2], Etc. that all can be achieved by using data hiding techniques.

In data hiding technique the information is embedded into image, after that original image gets distorted and cannot be restored to its original format. With the help of (RDH)[4][5] it is possible to extract cover image as well as embedded message from the embedded image. This technique is more needful in sensitive areas such as military, medical where recovery of original content is mandatory. Most of the proposed data hiding schemes are not based on pixel prediction and feature extraction. Specifically, this paper makes the following contribution:

1) Data hiding (DH) is a special embedding technique which guarantees about embedded messages as well as cover image should be extracted accurately and loss less.

2) To use Random Pixel Prediction (RPP). This is an important technique of DH for embedding large payloads into digital images with low distortion and to prove its superior performance

3) Amount of embedding capacity should be more compared with existing technology by using last two Least Significant bits (LSB) of pixels for embedding.
Related Work

A. Integer Transform Technique:
There is a technique which hides the information into integer wavelet coefficient of an image is called integer transform technique. To overcome drawback of existing system and to maximize holding capacity of system, integer transform technique uses data hiding technique and optimum pixel adjustment algorithm. In image data is hidden in random order and for extraction of data sender and receiver both are having public key. This technique is available for gray scale images only.

B. Difference Expansion:
To overcome drawback of previous system, for difference expansion Yongjian Hu [7] uses the predicted image pixel error instead of the pixel-pair difference. The recovery process contains two steps of manipulations. First in the inner/embedded region, and then the embedded/hidden bit is extracted from it. Original pixel value is resumed in shifted regions. For difference expansion which is based on reversible data hiding, contains two parts, first part is used to convey secret message and second part hold binary location map and header file.

C. Histogram Modification:
In histogram modification technique [6], neighbor pixels are strongly correlated so there is difference is expected to be very close to zero so this difference is utilized rather than simple pixel value. To complete the data hiding and extraction process at the sending side, first scan the image in an inverse s-order and calculate the pixel difference \( d \) between pixels \( x-1 \) and \( x \). Is completes the data hiding and extraction process in which only one peak point is used. With same data hiding techniques we can achieve large hiding capacities as well. However, without knowledge of peak points of every hiding pass recipient may not be able to retrieve the embedded message and the original host image.

System Design

The cover image and secret data are passed as an input to the system, which is illustrated by fig 2, then over a cover image system performs RPP to embed secret data into the image. Embedding operation shown in Algorithm 1 and to locate the exact position of pixel to store data shown in Algorithm 2.

Conclusion
Steganography technique is useful for sending or exchanging the data which is combined with randomized sequence of cipher bits provides a better means of secret communication between two parties with help of innocuous file and changes made in image are so subtle that someone is not able to locate it easily. Our system uses Random Pixel Prediction based on \( d=\text{seed} \) ranking in an image which is a significant improvement on current Steganography tools.

References
2. Wei-Liang Tai, Chia-Ming Yeh and Chin-Chen Chang,(2009), Reversible Data Hiding Based on Histogram Modification of Pixel Differences, IEEE Transaction on circuits and systems for video technology, Vol. 19, No. 6, pp. 906-910