International Journal of System Dynamics Applications
Volume 11 • Issue 2

Robust RDH Technique Using Sorting and IPVO-Based Pairwise PEE for Secure Communication

Aruna Malik, National Institute of Technology, Jalandhar, India
Rajeev Kumar, Kyungil University, South Korea

ABSTRACT

Reversible data hiding (RDH) is used extensively in information-sensitive communication domains to protect the integrity of hidden data and the cover medium. However, most of the recently proposed RDH methods lack robustness. Robust RDH methods are required to protect the hidden data from security attacks at the time of communication between the sender and receiver. In this paper, the authors propose a robust RDH scheme using IPVO-based pairwise embedding. The proposed scheme is designed to prevent unintentional modifications caused to the secret data by JPEG compression. The cover image is decomposed into two planes, namely HSB plane and LSB plane. As JPEG compression most likely modifies the LSBs of the cover image during compression, it is best not to hide the secret data in LSB planes. So, the proposed method utilizes a pairwise embedding to embed secret data into the HSB plane of the cover image. High fidelity improved pixel value ordering (IPVO)-based pairwise embedding ensures that the embedding performance of the proposed method is improved.

KEYWORDS

Pairwise Embedding, Pixel Value Ordering, Prediction Error Expansion, Robust Reversible Data Hiding, Sorting

INTRODUCTION

Due to advancements in digital communication over the internet, the sensitive information is prone to various security attacks. This has led to the need for proposing methods to address the security-related issues. Data hiding is a popular approach for information and data security where the main goal is to safely conceal or hide the secret data into some cover medium such as images, video, or audio. In some specific fields like telemedicine, biometrics, intrusion detect system, and military applications, it is required that the cover medium be not changed while retrieving the hidden data. It is because these applications are very information sensitive and even a small change in the information content can have menacing effects. To overcome this issue, Reversible image data hiding comes into the picture. Reversible image data hiding assures that the original cover image is recovered without causing any modification after we extract the secretly concealed data from it. Besides data security, this approach has also found its applications in watermarking. Watermarking consists of embedding some secret information in an image to preserve its copyright. This hidden information can be

DOI: 10.4018/IJSDA.20220701.oa6

extracted from the image to prove its ownership. The difference between the usage of reversible data hiding in watermarking and information security lies in the fact that in the former, less amount of data is embedded as compared to the latter. Reversible data hiding (RDH) can be used in order to protect the privacy of patient records. The patient information such as personal details, medical history, reports, etc. are sensitive pieces of information and their protection must be ensured when transmitted over internet. It can be used for covert communication in fields such as military, criminal investigations, or other applications requiring transmission of sensitive information over the internet. Another application is the centralized nature of cloud computing makes sensitive data susceptible to security attacks. In order to protect user-data over cloud, data coloring approach along with cloud watermarking is used. RDH can be employed in transmission of satellite information embedded in the satellite images. This ensures the protection of satellite data from unauthorized access. The major challenges to be addressed in any reversible image data hiding technique are to keep the image distortion low and making the payload carrying capacity high at the same time. Sometimes we are just interested in having a balance between the image distortion and data-carrying capacity. And one main feature of any data hiding method that makes it reversible is obvious i.e. reversibility, which means that after data extraction, the original grayscale cover image must be recoverable and there should not be any loss. There is the various application M. et al. (2020); Panda (2019); Bhardwaj (2020); Pierce et al. (2019); 855 (2018); Shukla et al. (2019) which can be implemented for secure data hiding communication.

Many RDH methods have been introduced that work in the compression domain Fridrich et al. (2001), spatial domain Tian (2003); Li et al. (2013a); Ni et al. (2006); Li et al. (2013b); Kim et al. (2008); Ou et al. (2014); Peng et al. (2014); Sachnev et al. (2009), transform domain Battisti et al. (2010), and encryption domain Huang et al. (2016). In the compression domain, cover-image is first losslessly compressed to make vacant space for the secret message Spatial domain methods directly manipulate the pixel values in a reversible manner hide secret data. In the transform domain, some transformations are applied to the image, and then the embedding is performed on the transformed image. In some fields to protect the original cover image from security compromises, image encryption and data hiding are used together i.e. encryption domain. Among these, spatial domain-based methods are the least complex. The spatial domain methods are based on difference expansion Tian (2003); Kim et al. (2008), histogram shifting Li et al. (2013a); Ni et al. (2006), sorting and prediction Sachnev et al. (2009); Kamstra and Heijmans (2005), prediction error expansion Li et al. (2013b); Ou et al. (2014); Peng et al. (2014); Thodi and Rodriguez (2007), pixel value ordering Li et al. (2013b); Peng et al. (2014) etc.

In 2003, difference expansion (DE) method proposed by Tian (2003) uses a pair of consecutive pixels and their corresponding difference is expanded to embed the data, which means a pixel pair is treated as a single embedding unit. This method was a turning point in the history of modern RDH. However, it lacked capacity control and various improvements have been proposed till date. The method of PEE was first introduced by Thodi and Rodriguez (2007) in which three-pixel neighborhood context of a pixel is used to compute its predicted value. Then the prediction error obtained from the difference of the original pixel and its predicted value is expanded to embed the secret data. The PEE method proved to be better than DE. Ou et al. (2013) presented a pairwise embedding style by considering a pair of prediction errors at the same time, called as pairwise PEE. It exploits the inherent correlation among the prediction errors and simultaneously modified the prediction error pair to embed the secret data. In pairwise PEE, the prediction error pair (0, 0) is expanded to (0, 0), (0, 1) and (1, 0) to accommodate $\log_2 3$ data bits into a single pair, while in the conventional PEE, each pair could only embed 1 bit of data. Moreover, pairwise PEE expands the error pair (1,1) to itself and (2,2) to embed 1-bit of data, while this error pair is simply shifted in conventional PEE. Sachnev et al. (2009) introduced a novel PEE-RDH scheme by incorporating the sorting of pixels according to their local complexities. They also proposed a new predictor i.e. ‘rhombus predictor’ to predict the value of a pixel from its four-pixel neighborhood. Ni et al. (2006) proposed a histogram shifting technique in