International Journal of Distributed Artificial Intelligence
Volume 11 • Issue 1 • January-June 2019

PVO-Based Multiple Message Segment Reversible Data Hiding

Sahil Chhabra, Department of Computer Science and Eng., Panipat Institute of Engineering and Technology, Samalkha, India

Neeraj Kumar Jain, Department of Computer Science and Eng., Thapar University, Patiala, India

Vipin Tomar, Department of Computer Science and Engineering, Panipat Institute Of Engineering and Technology, Samalkha, India

ABSTRACT

In this article, a reversible data hiding technique is proposed to embed multiple segments of a single message into a single cover image. This multiple message segment technique uses a pixel value ordering approach to embed the secret message. The splitting and randomization of the original secret message provides security from an attacker There are many digital formats for data hiding, like images, audio, and video, of which the digital image is the simplest format. Data hiding in image processing refers to inserting the secret message into digital images. Reversible data hiding (RDH) is a lossless technique, in which both the embedded secret message and the cover image is extracted by the receiver. The applications of RDH include medical and military imaging.

KEYWORDS

MMS, PVO, RDH, Security

1. INTRODUCTION

There are many digital formats for data hiding like image, audio and video in which digital image is simplest format. Data hiding in image processing refers to inserting the secret message into digital images. Reversible data hiding (RDH) is a lossless technique, in which both embedded secret message and cover image is extracted by the receiver. The applications of RDH include medical and military imaging.

Numerous RDH techniques have been introduced (Yang & Hwang, 2011; Celik, Sharma, Tekalp, & Saber, 2002; Tian, 2002; Awrangieb, 2003; Nosrati, Karimi, & Hariri, 2012) which are based upon lossless compression technique and histogram. Tian (2002) introduced the Difference Expansion (DE) method, in which difference between surrounding pixel values is calculated to embed the secret message. This expansion is done sequentially in the cover image, which generates the high Embedding Capacity (EC) and Peak Signal to Noise Ratio (PSNR) value. Alattar (2004) extends the technique of DE by generalized integer transform. Wang et al. (2010) improved the DE technique by taking the differences of correlated pairs of adjacent pixels. Kamstra and Heijmans (2005) introduced sorting technique that utilizes correlation between adjacent pixels efficiently. Histogram Shifting (HS) method of Ni et al. (2006), in which most frequent histogram bin are used for expansion and used for secret data bit embedding. Prediction Error Expansion (PEE) based RDH is introduced for the first time by Thodi and Rodriguez (2007) in which a pixel is predicted by its correlated pixel and then the histogram for these prediction errors is generated. The histogram splits into two parts, first is the inner and it is useful for secret bit embedding and the second is the outer region, which is used

DOI: 10.4018/IJDAI.2019010103

for shifting the remaining pixels. These outer region pixels provide a guarantee of reversibility of this technique. Some other PEE techniques (Hu, Lee, & Li, 2009; Sachnev, Kim, Nam, Suresh, & Shi, 2009; Hong, 2010; Li, Yang, & Zeng, 2011; Qu, Li, Zhao, & Ni, 2013) also provide improvement and achieve high EC, PSNR value and better visualization of stego image. Pixel value ordering (PVO) technique is firstly introduced by Li et al. (2013) in which sorted order of pixel value of cover image is used for computing the prediction. This order remains invariant after the secret data bits embedding, thus it used efficiently for the extraction of both cover image and secret message thus, achieves the reversibility. Block of cover image can embed up to 2-bit per pixel (bpp) and ensure the PSNR value more than 51.14 dB. Peng et al. (2014) improves the PVO technique, where the maximum (minimum) value pixel and second maximum (minimum) value pixel is equal for each block.

Wong et al. (2006) introduced Discrete Cosine Transform (DCT) based steganography technique in which multiple messages are embedded in a cover image. The Multiple Message Embedding (MME) technique is an extension of DCT based mod4 technique of Wong et al. (2007). Mod4 operation is used to embed the secret data in cover image and its technique is blind. The upper limit of embedding the number of secret messages successfully is 14, which enhance the security and also upgrade the quality of the stego image. Alnawok et al. (2008) introduced the multi-segment steganography technique, in which a single message is divided into multiple segments and these segments are embedded into a single cover image. Before embedding these segments, plain texts are encrypted into an encoded text by using a code table. This secret code table is already known to the receiver and is also embedded with secret message for cross checking it. All the characters of the secret message is converted into byte code and represented by 255 characters format. Thus, it provides more security for the secret message in the digital stego image.

In this paper, the PVO-based RDH Multiple Message Segments (MMS) has been proposed, in which segments of a single message are embedded in a cover image. These multiple segments increase the security of hidden message, because if one part of secret message is intruded by the attacker then it is not in understandable format till all parts of the secret message are intruded. Also, this technique does not need any extra encoding to convert the segments as the identification of segments is provided by modulo method.

The rest of the paper is organized as follows. Section 2 presents related work of Peng et al. (2014), section 3 describes the proposed techniques and modulo strategy for message segments partitions. Section 4 gives analysis and experimental results and finally section 5 concludes this paper.

2. RELATED WORK

Peng et al. (2014), Improved-PVO (I-PVO) technique creates the ranking for each pixel in the block and embed the secret data bits at both minimum and maximum pixel value. Li et al. (2013) PVO scheme embeds the secret data, when predictor value is equals to 1 at both smallest and highest pixel values of each block. I-PVO technique embeds the secret data when predictor value is equals to 1 as well as 0 for both smallest and highest pixel values of each block, which provides the Better EC and less distortion in the marked image.

First, cover image is partitioned into blocks. These blocks do not overlap each other, and size of each block is equal. Now pixel values of each block are sorted in ascending order. For a block *B* (b_1, …, b_n) are its n sorted value and ($b_{\phi(1)}$, …, $b_{\phi(n)}$) are sorted order of each pixel in the block. Where ϕ: {1,…,n} → {1, …, n} unique one to one function mapping such that: $b_{\phi(1)} \leq \ldots \leq b_{\phi(n),}$ b(p) < b(q) if $b_{\phi(p)} = b_{\phi(q)}$ and p < q. Now the predictor that predicts the $b_{\phi(n)}$ by its correlated second highest pixel, $b_{\phi(n-1)}$ and the prediction error is computed as:

$$dmax = bu - bv \quad (1)$$

Related Content