Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 116 (2017) 334–341

Procedia Computer Science

www.elsevier.com/locate/procedia

2nd International Conference on Computer Science and Computational Intelligence 2017, ICCSCI 2017, 13-14 October 2017, Bali, Indonesia

Distributed Steganography Using Five Pixel Pair Differencing and Modulus Function

Fendi, Aswin Wibisurya*, Faisal

School of Computer Science, Bina Nusantara University, K.H. Syahdan 9, Palmerah, Jakarta Barat 11480 Indonesia

Abstract

FPPD steganography is one of steganography techniques that hides secret message by adjusting the difference between pixel pairs in 2x3 blocks. FPPD usually deals with using one cover image to hide any data. To make it practical, a steganography method needs to accommodate concatenated data of different types of media. The steganography method should also allow large data to be distributed on multiple cover images. Therefore, there should be indicator for the start, end, and media type of each component of secret data. The purpose of this research is to develop a FPPD based distributed steganography which allow addition of multiple secret message components across multiple cover images while informing the recipient of the media type of each secret message. This is done by applying a modulus function to to adjust the values of a block to represent the start, end, continuation, and media type of secret messages. The proposed approach results in PSNR value of 37.62, below the benchmark FPPD method. This decrease in PSNR is the result of modification to the pixel value of the reference point to provide means to embed data of different media types into several images.

Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.

Keywords: steganography, FPPD, distributed, modulus function

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: awibisurya@binus.edu

1877-0509
Peer-review under responsibility of the scientific committee of the 2nd International Conference on Computer Science and Computational Intelligence 2017.
10.1016/j.procs.2017.10.085

1. Introduction

Steganography is a method of hiding information so that it is not detectable by human. There are many methods of steganography, one of them is Pixel Value Differencing (PVD).

PVD is first proposed by Wu et al[1]. In this method, grayscale images are used as cover images. The cover image is scanned in zigzag manner to construct two-pixel blocks (P_i and P_{i+1}). The difference value between these pixels (d_i) is then calculated. A range table R, with table range from 0 to 255 is designed with n sub-ranges (R_k where k = 0,1,2,3,...,n). Each sub-range has lower and upper boundaries, l_k and u_k, with range width $w_k = l_k + u_k + 1$. The difference d_i is then mapped into the range table R to find the suitable sub range R_k. The width wk is used to determine the number of bits of the secret message ($t_i = \log_2 w_k$) to be embedded to the cover image. For embedding the secret image, a new difference (d') is determined by calculating the decimal value of secret message bits and the lower value of the sub-range l_k. The value of the two pixels, P_i and P_{i+1} is then adjusted according to d'. During extraction, the decimal value of bits embedded in each block is calculated by subtracting the difference between the two corresponding blocks in the stego image ($|d'_i|$) and the lower value l_k ($|d'_i - l_k|$). The decimal value is then converted into binary sequence and concatenated for all blocks in the stego image.

In order to increase the data hiding capacity, Chang et al proposed another PVD method [2] [3] using 2x2 block pixels. From the top left pixel ($P_{(x,y)}$), three pixel pairs are formed horizontally, vertically, and diagonally: PP0 = ($P_{(x,y)}, P_{(x+1,y)}$), PP1 = ($P_{(x,y)}, P_{(x,y+1)}$), PP2 = ($P_{(x,y)}, P_{(x+1,y+1)}$). Based on the difference between each of the pixel pair (d_i), these blocks are categorized into smooth or edged area. Edged blocks can hide more secret message bits than smooth block since changes to edged blocks are less noticeable to human eyes. After secret data are embedded, the value of each pixels get modified. However, this may result in the original point $P_{(x,y)}$ having different values. In this case, a selection rule is established to select the optimal reference pair, which result in the least MSE. Using the reference pair, the values of other pair is adjusted by maintaining the difference between the pixel values in the pair.

Liao, Wen, and Zhang [4] proposed a combination of PVD and LSB approach, also to improve data hiding capacity. The block used consists of 2x2 pixels.

Gulve and Joshi [5] proposed another steganography based on PVD approach called Five Pixel Pair Differencing (FPPD). In this method, the cover image is partitioned into a block of 2x3 pixels: $P_{(x,y)}, P_{(x,y+1)}, P_{(x,y+2)}, P_{(x+1,y)}, P_{(x+1,y+1)}, P_{(x+1,y+2)}$. The pixel $P_{(x,y+1)}$ is used as common pixel, thus 5 pixel pairs are formed: $PP_0 = (P_{(x,y)}, P_{(x,y+1)})$, $PP_1 = (P_{(x,y+2)}, P_{(x,y+1)})$, $PP_2 = (P_{(x+1,y)}, P_{(x,y+1)})$, $PP_3 = (P_{(x+1,y+1)}, P_{(x,y+1)})$, and $PP_4 = (P_{(x+1,y+2)}, P_{(x,y+1)})$

Secret data is then embedded using the PVD method. Difference d_i is calculated for each pixel pair. Then, a new difference is calculated by the sub range R which d_i falls into. The value of each pixel pair is then adjusted to the new difference. A pair with minimum change is selected as a reference pair. The rest of the pairs values are adjusted to the reference pair, maintaining the difference.

Gulve and Joshi [6] revised the FPPD method to increase data hiding capacity and avoid fall off boundary problem (pixel value adjusted to below 0 or above 255). In this revised method, the block is categorized into smooth ($d_i \leq 127$) or edged block ($d_i > 127$). Fall off boundary may happen while adjusting edged blocks. Therefore, instead of using the original PVD approach, LSB approach is used to embed data in edged blocks. Embedding data in smooth block is done using PVD approach.

In applying FPPD, some issues need to be addressed. The first issue is that the algorithm extracts data from all blocks in the image, assuming data are hidden in all blocks. If the secret message is short enough, it is only hidden in part of the blocks. A protocol needs to be implemented to tell the end of secret message sequence in the blocks.

The second issue is the hiding capacity of the steganography method. Using FPPD, approximately 82 kilobytes of secret message can be hidden in a cover image. As mentioned before, a secret message may be short enough. For efficiency, the rest of the blocks can be used to store other secret messages. If the messages are texts, they can be easily concatenated. However, to hide more than one types of content (text or image or other media), there needs to be an indicator of the start and the end of each secret message part. If combination of secret messages is large enough, the hiding capacity of a single cover image may not be sufficient. The solution is to span the secret messages across multiple cover images (distributed steganography).