International Journal of Digital Crime and Forensics
Volume 9 • Issue 4 • October-December 2017

Recognizing Substitution Steganography of Spatial Domain Based on the Characteristics of Pixels Correlation

Zhe Chen, University of Electronic Science and Technology of China, Chengdu, China
Jicang Lu, Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Pengfei Yang, Zhengzhou Information Science and Technology Institute, Zhengzhou, China
Xiangyang Luo, Zhengzhou Information Science and Technology Institute, Zhengzhou, China

ABSTRACT

Steganographic algorithm recognition is currently a key issue in digital image steganalysis. For the typical substitution steganographic algorithm in spatial domain, we analyze the modification way and construct the feature extraction source based on the adjacent pixels correlation; extract the special statistical feature which could distinguish the substitution steganography from other types of steganographic algorithms. Finally, a substitution steganography recognition algorithm is presented and tested by experiments. The experimental results show that, the proposed algorithm could recognize the substitution steganography in spatial domain efficiently, and the detection accuracy is better than existing algorithms.

KEYWORDS

Identifiable Feature, Modification Way, Recognition, Steganalysis, Substitution Steganography

INTRODUCTION

Digital steganography embeds messages into redundant data of covers such as digital image, video and text, and then transmits the stego ones with embedded messages through public channels, which could achieve the goal of transmitting secret message in a covert way. However, the technique has two sides, it can be used for national and social secure communication, and on the other hand it may also be used by criminals or terrorist organizations to endanger social security. Therefore, reliable detection of steganography, i.e. steganalysis, is significant and is also in urgent need for information security.

Developed through nearly 20 years, there have been a lot of achievements in steganography and steganalysis (Luo et al. 2008, Cheddad et al. 2010, Nissar et al. 2010, Denemark et al 2016, Boroumand et at. 2016, Denemark et al. 2017). However, there are still some bottleneck problems in steganalysis (Ker et al. 2013, Pibre et al. 2016, Tang et al 2016), such as steganographic algorithm recognition, secret message extraction and cracking etc. The main purpose of steganographic algorithm recognition is to recognize which kind of steganography is used in the stego image, which is the important premise of secret message extraction and cracking. There are little research achievements in steganographic algorithm recognition. And the existing methods are concentrate upon two aspects:

DOI: 10.4018/IJDCF.2017100105

one is based on the idea of two-class classification, only using a kind of features for conventional blind detection to classify and recognize stego and cover images (Pevny et al. 2008, Cho et al. 2010); the other one is to extract recognizable features based on the modification way of steganography, and then to recognize the steganographic algorithms (Lu et al. 2014). Pevny et al. (2008) and Cho et al. (2010) are mainly based on the first method to recognize steganographic algorithm, but did not analyze the unique features in specific steganography, which lead to poorer suitability and higher complexity; Lu et al. (2014) are based on the second method to recognize steganography, however, the research achievements are only for typical image steganography such as F5 and nsF5 in JPEG domain. It can be seen from existing studies that, reliable recognition of steganography is still needed to be researched for more typical steganographic algorithms, such as MB (Sallee 2004), Outguess (Provos 2001) and spatial steganography (Bender et al. 1996).

This paper aims at typical substitution steganography in spatial domain, firstly we analyze the principle, and then, construct the sensitive features that could capture the specific modification; finally train recognition classifiers and recognize substitution steganography from multi-class stegao images set. The experimental results show that, the proposed method can reliably recognize the stego images which are generated by substitution steganography from multi-class stego images.

This paper is organized as follows. The second section introduces the principle of substitution steganography in spatial domain by analyzing the embedding changes. In the third section, the modification characteristic of substitution steganography will be analyzed by considering the relationship between adjacent pixels. On the basis of that, the statistical feature based on the pixels correlation will be extracted, and then, the recognition method will be presented. In the experimental section, the efficiency of the proposed method will be tested using the well-known image database. The paper is concluded by the conclusions.

THE PRINCIPLE OF SUBSTITUTION STEGANOGRAPHY IN SPATIAL DOMAIN

The substitution steganography is not only one type of the most typical steganographic algorithms, but also one type of the earliest steganographic algorithms. The commonly used algorithms are LSB (Least Significant Bit) substitution steganography, MLSB (Multiple LSB, such as 2LSB and 3LSB) substitution steganography. In order to embed secret messages, this kind of steganography algorithm embeds secret messages in the way of directly replacing the LSBs of pixels in cover images, and the corresponding stego image is generated. The modification way in LSB substitution steganography can be described by the following equation:

$$\mathbf{I}'(i,j)=\begin{cases}\mathbf{I}(i,j)+1-2\times\mathrm{mod}\left(\mathbf{I}\left(i,j\right),2\right) & if\ s\neq \mathrm{mod}(\mathbf{I}(i,j),2)\\ \mathbf{I}(i,j) & else\end{cases} \tag{1}$$

where $\mathbf{I}(i,j)$ denotes the pixel value at position (i,j) in image pixel matrix $\mathbf{I}$ with size $M\times N$. $\mathbf{I}'(i,j)$ denotes the corresponding stego pixel, $1\le i\le M, 1\le j\le N$. $\mathrm{mod}(\cdot,2)$ denotes the function of modulo 2, and s is the secret message bit to be embedded.

In natural images, the higher the bit plane is, the more significant the pixel is. Generally, even if the lowest three bits planes are used to embed messages, there will not be significant changes in visual. At the same time, it can greatly increase the capacity during information embedding. Therefore, the substitution steganography which based on two or three-bit plane is also a hot research in spatial