Computers and Electrical Engineering 43 (2015) 9–16

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

An analysis of computational models for accelerating the subtractive pixel adjacency model computation ☆

Marisol Rodriguez-Perez, Alicia Morales-Reyes, René Cumplido *, Claudia Feregrino-Uribe

Instituto Nacional de Astrofisica, Optica y Electronica, Sta. Ma. Tonantzintla, Puebla 72840, Mexico

ARTICLE INFO

Article history:
Received 20 August 2013
Received in revised form 5 January 2015
Accepted 9 January 2015
Available online 11 March 2015

Keywords:
Steganalysis
SPAM
FPGA
CUDA
GPU

ABSTRACT

Detecting covert information in images by means of steganalysis techniques has become increasingly necessary due to the amount of data being transmitted mainly through the Internet. However, these techniques are computationally expensive and not much attention has been paid to reduce their cost by means of available parallel computational platforms. This article presents two computational models for the Subtractive Pixel Adjacency Model (SPAM) which has shown the best detection rates among several assessed steganalysis techniques. A hardware architecture tailored for reconfigurable fabrics is presented achieving high performance and fulfilling hard real-time constraints. On the other hand, a parallel computational model for the CUDA architecture is also proposed. This model presents high performance during the first stage but it faces a bottleneck during the second stage of the SPAM process. Both computational models are analyzed in detail in terms of their algorithmic structure and performance results. To the best of Authors' knowledge these are the first design proposals to accelerate the SPAM model calculation.

1. Introduction

The increasing transmission of personal data, mainly through the Internet, has motivated the creation of new methods to protect information. Several algorithmic techniques have been developed to tackle main data protection problems. For example, cryptographic techniques have been developed to encode information against unauthorized access and steganographic methods aim at protecting sensible data without perceptible modifications, trying to be unnoticed to the third eye [1]. However, protecting data via covered communications are also used in terrorism and pornography [2,3], therefore it has been also necessary to develop inverse algorithmic techniques known as steganalytic methods which help to discover covered data in order to detect hidden information.

Steganalysis is classified in specific and universal. Specific steganalysis requires knowledge of the targeted steganographic method, thus limiting its application arena. On the other hand, universal steganalysis recognizes if an image has been modified by any steganographic technique [4]. To achieve its goal, universal steganalysis uses feature extraction techniques to train a classifier in order to distinguish distortions caused by steganographic methods. Depending on feature extraction domain, universal steganalysis is classified in spatial and transform.

☆ Reviews processed and approved for publication by the Editor-in-Chief.

* Corresponding author.

E-mail addresses: marisolr@inaoep.mx (M. Rodriguez-Perez), a.morales@inaoep.mx (A. Morales-Reyes), rcumplido@inaoep.mx (R. Cumplido), cferegrino@inaoep.mx (C. Feregrino-Uribe).

http://dx.doi.org/10.1016/j.compeleceng.2015.01.004

Designing steganalysis methods has focused on improving detection rates. However, computational cost of steganalytic techniques is high and optimizing processing times is nowadays necessary due to the massive amounts of data transferred through large networks. In order to improve the processing ratio, some authors have proposed steganalytic hardware implementations. For image data, Sun *et al.* [5] developed an FPGA-based architecture for the RS algorithm, a specific steganalysis method proposed by Fridrich *et al.* [6] which recognizes LSB (Least Significant Bit). The proposed architecture uses a three stage pipeline and was synthesized in a Xilinx Virtex II FPGA (now obsolete). In 2013, Gutierrez-Fernandez *et al.* introduced an FPGA-based architecture for transform domain universal steganalysis in JPEG images [7]. This architecture is based on JPEG's compatibility algorithm proposed by Fridrich *et al.* [8]. Authors proposed a pipeline scheme implemented in VHDL and synthesized in a Xilinx Virtex 6 FPGA. However, to the best of the authors' knowledge, hardware architectures for universal steganalysis on the spatial domain have not been reported.

Spatial features usually focus on modeling pixels neighborhoods. Such as the rich model proposed in 2012 by Fridrich *et al.* [9], where different pixel dependency sub-models are used as features. Using different types of sub-models facilitates detection of different embedding artifacts; however, dimensionality increases substantially. An ensemble is used for classification.

In 2010, Guan *et al.* proposed a method called Neighborhood Information of Pixels (NIP), in which, differences between pixels within the neighborhood and the central pixel are calculated and subsequently codified using rotation invariant [10]. The result is processed as a histogram removing empty values. In 2011, Arivazhagan *et al.* used 4×4 segments where pixels differences are calculated according to nine paths within the neighborhood [11]. Results between -4 and 4 are placed within a co-occurrence matrix and are used as characteristics vectors.

In 2010, Pevny *et al.* proposed a universal method where differences between neighboring pixels are modeled by first and second order Markov Chains [12]. This method was designed primarily for spatial based steganography, however, it demonstrated a good performance when detecting transform domain steganography. Because of its ability in both domains, this method is considered in this investigation from a hardware perspective to speed-up its process.

Among several universal steganalytic methods, the Subtractive Pixel Adjacency Model (SPAM) has shown a good performance for detecting stego-images watermarked with the most popular steganographic methods, both in the spatial domain and in the transform domain. The model is also scalable to color images, and its algorithmic design makes it a good candidate from a hardware architectural perspective. Moreover, many steganalytic methods share common processing tasks carried out in SPAM (pixel differences and transition probabilities). Therefore, the proposed computational models are flexible and can be adapted, as steganalytic processing cores, to other spatial domain techniques.

In this paper, two parallel computational models are investigated, an FPGA-based hardware architecture and a CUDA based algorithmic model is proposed for the first order SPAM model. A complete analysis of performance results in both implementation platforms is presented. In the next section, the SPAM model is detailed and analyzed from an architectural perspective. Section 3 presents both parallel computational models: an FPGA based architecture's design and a GPU programming model. Results are analyzed for each proposed approach in the same section. Final remarks are presented in Section 4.

2. Subtractive pixel adjacency model

The Subtractive Pixel Adjacency Model (SPAM) is a spatial domain method for features extraction in images with possible stego-data. This model has shown the best detection rate among other state of the art techniques. Moreover, operations required to obtain feature vectors are arithmetically simple which makes this model suitable for optimization from a hardware perspective. In [12], it is stated that correlation between neighboring pixels in a natural image can be used to detect some irregularities caused by stego-data. However, the resulting model would not be practical due to its dimension. To reduce model's dimension, it has been proposed using pixels differences versus pixel co-occurrences or neighborhood histograms. Thus, obtaining the difference model of several stego-images demonstrated that most significant information lay in small differences. Therefore, differences range is reduced together with its dimensionality.

The algorithm is mainly divided in three stages, see Fig. 1. First, the model calculates differences between pixels in eight directions $(\uparrow, \nearrow, \longrightarrow, \searrow, \downarrow, \swarrow, \longleftarrow, \nwarrow)$ in the spatial domain. For example, the horizontal differences are calculated by $A_{i,j} = I_{i,j} - I_{i,j+1}$ and $B_{i,j} = I_{i,j} - I_{i,j-1}$, where I is an (m, n) image, and $i \in [1 \ldots m],\ j \in [1 \ldots n]$. Second, to model pixel dependencies along the eight directions, a Markov chain is used between pairs of differences (first order chain) or triplets (second order chain). For dimensionality reduction of the transition probability matrix, only differences within a limited range are considered. Thus, the transition probability matrix is calculated just for pairs within $[-T, T]$. In [12], authors propose $T = 4$ for first order and $T = 3$ for second order, because of their relevance in steganalysis.

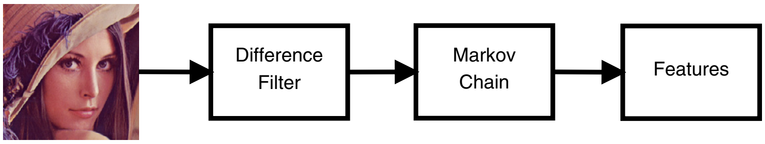

Fig. 1. SPAM main stages.