BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXII No. 1/2010	61 - 68	Seria Matematică - Informatică - Fizică

A New Version of a Steganographic System on Parallel Architecture CELL BE

Anca-Alexandra Purcărea[*], Bogdan Ţigănoaia[**]

[*] Politehnica University of Bucharest, Management Department, Bucharest, Romania
email: apurcarea@gmail.com

[**] Politehnica University of Bucharest, Computer Science Department, Bucharest, Romania
email: bogdantiganoaia@gmail.com

Abstract

This paper presents some considerations on the necessity of information protection and continuous development of steganographic systems. It also describes a new high capacity and robust method for hiding information on images. The image distortion after encoding the secret message is low and indistinguishable to the human eye. The security attributes (information availability, integrity, confidentiality, non repudiation) are discussed also in this article. Some parameters (system capacity, data integrity, image distortion etc.) of the proposed steganographic system are analyzed in order to draw a conclusion about its performances. A study of the CELL BE architecture is made and an efficient mapping of the application on it is proposed. New Cell BE programming facilities such as double buffering, SIMD instructions, mailboxes, events and DMA transfers are used.

Keywords: *information protection, steganographic systems, CELL BE architecture*

Introduction

Image processing domain [2] is in a continuous development and new research projects are available. One of these challenges is about the analysis and development of new steganographic systems. Information hiding is the process of hiding a stego-data, that means a secret message on an item of communication called cover data. The steganographic systems are a part of information hiding and mean the secret communication between two entities. According to Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, steganography is the science of hiding secret messages so that nobody, apart from the sender and the receiver, suspects the existence of such a message - security through obscurity. Information protection and steganography are used in the fight with the plagiarists, in copyright domain.

The steganography could be a good tool for proving the authenticity and originality. In this domain of information hiding, the most important request is a high level of imperceptibility (that means a minimum distortion on visual effect) followed by a high level of robustness and a high capacity. There are also important some system security parameters such as: information integrity, availability, non repudiation and confidentiality.

The SMK algorithm proposed by Seppanen, Makela, Keskinarkaus [4] and the steganographic system proposed by Kawaguchi and Eason [3] were the start point of our research. The parallel

architectures represent a new and good tool for the steganographic systems. A new version of the steganographic system in [5] is proposed. In that paper, the steganographic system uses two entities for communication: a simple encoder to code the secret message and a decoder to extract it. In this paper, some security parameters of the proposed steganographic system are analyzed and some modifications are made to the system.

The Necessity of Information Protection and Continuous Development of Steganographic Systems

Information protection for Romania comes from the actual society: the evolution of the cyber crime, the globalization phenomenon, the informational society (virtual shops, e-commerce, online transactions etc.), the information protection as a consequence of the NATO entrance and adhesion to EU. In the past ten years, Romania has made a remarkable progress. The NATO entrance in 2004 and Romania's adhesion to EU in 2007 has brought to our country not only a lot of benefits, but also a lot of responsibilities. Romania must have the capability to response to all the threats that daily occur. The IT domain that is in a continuously development is affected by the new threats. The communications infrastructures and the networks development daily bring a lot of securi*ty challenges*. The national security institutions in Romania have the instruments in order to protect information. But in the civil area, the information protection is a continuous challenge. Information means power and must be protected. It is true that information is perishable on time - you cannot protect information forever, but what is important is to protect the information a period of time so that, after that period, if the information becomes known, the impact is low. The need of information protection comes from the power mechanism: information is a key factor in taking decisions. On the other hand, there is a continuous need to have a complete and credible information. Information on electronic support is frequently used in our country: the Romanian institutions and companies work with this kind of information. As a comparison with the classic information, the information on electronic support can be keyed on malefic purposes. This is another reason for information protection. A system that works with classified information must have the following security attributes: availability, integrity, confidentiality, non repudiation. The development of the new steganographic systems is a necessity in our dynamic society. The new technologies help researchers to develop such systems. This should be in a strategic vision the desideratum of the management of a company which works with classified information.

Implementation of a New Version of a Steganographic System

Cell BE Architectural and Working Medium Descriptions

Cell BE architecture [7] consists of a chip with nine processors. In fig. 1 it is shown the block diagram of a Cell Broadband Engine architecture [8].

The PowerPC Processor Element (PPE) is a RISC core with 64 bit PowerPC architecture. Having a traditional subsystem of virtual memory, it is the main processor and it is responsible for the management of the resources and operating system. There are eight Synergistic Processor Elements (SPEs). They are optimized for SIMD (Single Instruction Multiple Data) operations and have an identical RISC architecture with the local data and instructions memory - local store. They also have a set of 128x128 bit registers and a capacity of 256 KB. SPEs use DMA (Direct Memory Access) transfers for moving data and instructions between the main store and the local store. The Element Interconnect Bus (EIB) is a high bandwidth bus through which the connections to peripherals are made - PPE processor and SPEs can communicate through EIB. This bus has a structure based on four rings for transferring data and a tree

structure for commands. PPE is responsible for the thread allocation and for the resources management between SPEs.

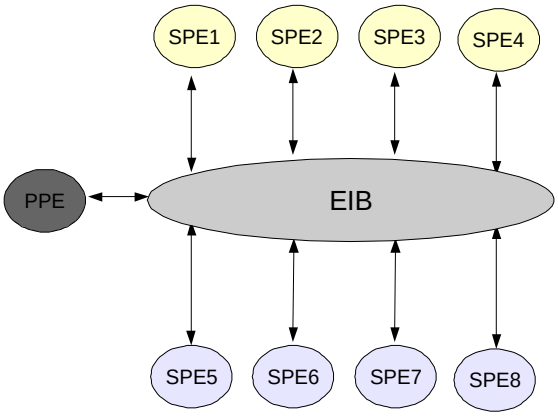

Fig. 1. The Cell BE architecture

The Linux Kernel on the SPEs controls SPE programs. SPE threads model is *M:N* and this means that *M* threads are mapped on *N* processing elements. In a Linux operating system, the main thread of a program is working on PPE and it can create one or many Linux tasks for Cell Broadband Engine. A Linux task for Cell BE has one or many Linux thread(s) that can work on PPE or SPE. A SPE thread is a Linux thread working on SPE. SIMD operations support is present on the Cell BE architecture.

PPE-SPE Communication

There are three important communication mechanisms [6]: mailboxes, events - notification registers by signals, DMA transfers. The mailboxes are queues that allow sending short 32 bit messages. The mailboxes can also be used for synchronization between SPEs. The Outbound Interrupt Mailbox – Events are used to avoid busy-waiting on PPE and to point out when a message arrives from one of the SPEs. The Memory Flow Controller consists of a controller for DMA transfers. DMA is used for moving a high volume of data between PPE and SPE. Double buffering is a mechanism which consists of multiple transfers by using a buffer. In the same time, new data is brought on SPE and old data is processed. So, the processing time on SPE is substantially reduced.

Steganographic System – a New, Original Version Proposed by the Authors

The steganographic system (fig. 2) has two elements: an encoder to hide the secrete message and a decoder to find the message. The pixels palette (this term is used in [1]) used to hide the message is the result of applying the K-means clustering algorithm, with some modifications. This algorithm chooses pixels by calculating the clustroids. A clustroid is a pixel that has the least distance to the other pixels on a cluster. After applying this algorithm, an uniform pixels palette is obtained. The *k* parameter in K-means algorithm was chosen 2 because for one piece of image we need two pixels in order to calculate the final clustroid. The modification of the clustering algorithm consists of the use of a threshold (in this paper 200) for deciding, at every step, what is the new clustroid. The distance between two pixels is measured with the formula:

$$D(P,Q)=\sqrt{(P_r-Q_r)^2+(P_g-Q_g)^2+(P_b-Q_b)^2}\,. \tag{1}$$

The algorithm proposed by the authors is the following:

Input: A piece of the image with quadratic dimension

1. choose two clustroids - *C1*, *C2* - for initialization (big distance between them)
2. **repeat** for every pixel
   - 2.1. calculate the distance between clustroids and the current pixel
   - 2.2. keep the minimum distance; let suppose that the minimum distance is toward the *C1* clustroid
   - 2.3. **if** the minimum distance > the chosen threshold **then**

     C1 ← the_current_pixel

     else *C2* ← the_current_pixel
3. apply previous step for the last two clustroids
4. **return** the final clustroid

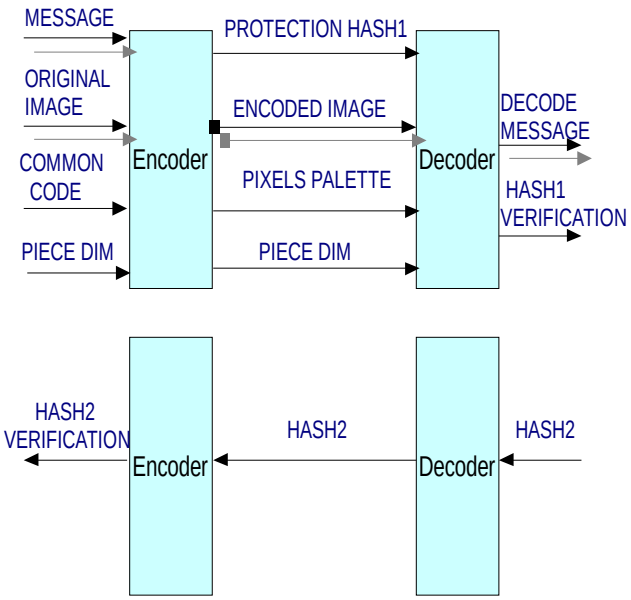

Fig. 2. The steganographic system: two transactions for one communication

Hence, for a piece of image, there is only one clustroid used for encoding. A pixels palette used for encoding consists of all these clustroids. All the three components from every pixel from the palette are used for encoding. There are used the last 5 bits from every *R,G, B* component of a pixel, so the distortion is acceptable. The Caesar encoding scheme is chosen to hide the message.

The Mapping of the Application on CELL BE Architecture

Having a high volume of data, it is necessary to use a parallel architecture - for calculating the *HASH1*, the pixels palette. The mapping of the application on the Cell BE architecture is shown in the fig. 3:

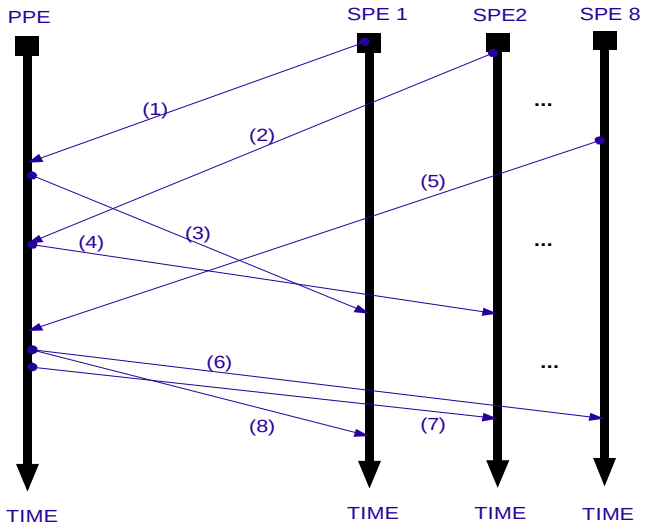

Fig. 3. The time diagram – the mapping of the application on Cell BE architecture

The image is initially on the PPE. PPE waits for requests from the SPE ((1) and (2) in the above figure). When a request from the SPE arrives, the PPE treats it and sends to the SPE ((3) and (4) in the above figure), by mailboxes, an address. This address is used by the SPE to transfer data by DMA from the main store to the local store. When SPE finishes processing data, it sends this data by DMA to the PPE ((5) in the figure above). It is a cyclic mechanism until the image is processed. When the image is processed, the PPE sends to the SPE the address 0 ((6), (7) and (8) in the above figure). This means that the SPE can terminate its execution. Finally, the PPE processes data and finishes its execution. Mailboxes, events and DMA transfers are used for communication. The encoder needs processing power for calculating the *HASH1* and pixels palette. The decoder needs a high processing power only for locally verifying the hash for data integrity. Then, using the pixels palette, it finds the message.

The Analysis of Security and Performance Parameters

Data integrity: In order to guarantee the data integrity, it is proposed a simple method that uses a hash of the encoded image which protects data. By this hash, it is very easy to detect if the image was analyzed and modified by someone. This *PROTECTION HASH1* (this hash is defined as the average of the averages of the pixels components for *every* piece of the image) gives to the system a high level of robustness. The purpose of someone who analyzes the encoded image is to destroy the secret message if he does not decode it. Verifying the hash on the decoder gives a high level of data integrity.

Authentication: Another security system requirement is about authentication. The system proposed in this paper uses a *COMMON CODE* through which the sender and receiver are identified. This is a shared code between the sender and the receiver and it is also encoded on the image.

Non repudiation: Non repudiation is another requirement of systems which work with information. The non repudiation assurance is done by *HASH2*, which is sent from the receiver to the sender. This hash is defined as the average of the following three elements: the piece dimension, the common code and the protection *HASH1*. The sender makes a verification of this *HASH2* in order to know if the encoded image arrives to the receiver and everything is OK.

Information confidentiality and availability: The last two functions of a security system are the availability and the confidentiality. Information confidentiality is ensured by encoding the message in the image. The information – the secret message, is available only for the sender and the receiver. The encoded image, the piece dimension, the pixels palette, the protection hash and *HASH2* are sent not cryptic.

System capacity: The system capacity is measured in bpp (bits per pixel) and varies depending on the number of bits used for encoding and the dimension of the piece of an image (fig. 4). The capacity increases with the decreasing of the dimension of the piece of the image (table 1. and table 2). For encoding, all components - *R, G, B* - of a pixel are used.

Table 1. The capacity depends on the dimension of a piece of the image (for an image of 256 x 256)

Image Dim.	Piece Dim.	Capacity (bits)
256 x 256	8	5*5*5*32*32
	16	5*5*5*16*16
	32	5*5*5*8*8
	64	5*5*5*4*4

Table 2. The capacity depends on the dimension of a piece of the image (for an image of 512 x 512)

Image Dim.	Piece Dim.	Capacity (bits)
512x512	8	5*5*5*64*64
	16	5*5*5*32*32
	32	5*5*5*16*16
	64	5*5*5*8*8

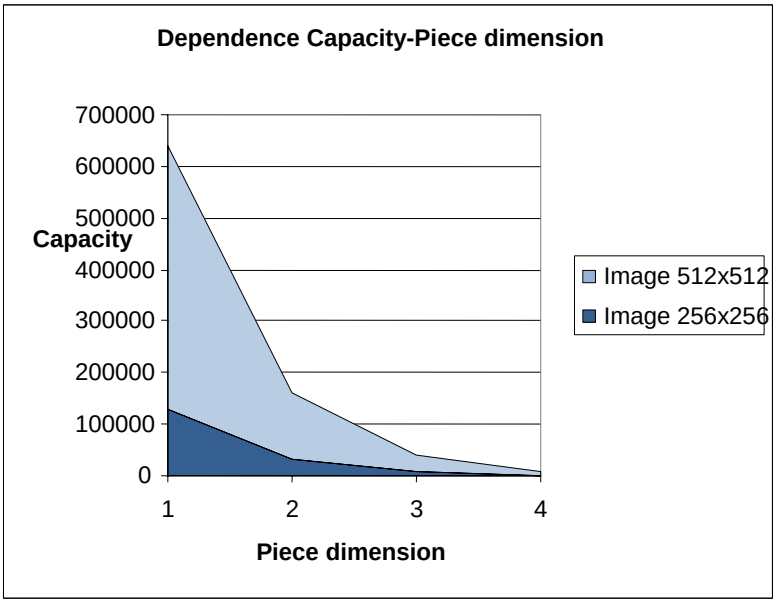

Fig. 4. The capacity depends on the dimension of one piece of the image

Distortion: The imperceptibility level includes the minimization of the distortion and the detectable level. The distortion is measured in this article by the formula:

$$PSNR = 20 \log\left(\frac{255}{\sqrt{MSE}}\right), \quad (2)$$

where *MSE* is the mean squared error for every pixel in the encoded and original image. For a 40 dB level of this parameter, there is no visual effect between the original image and the encoded image.

Experimental framework and example

The dimensions for the piece of the image were 16, 32 and 64. The parameter *k* was chosen 2 and the threshold for the clustering algorithm was 200. The images for tests were 256x256, 512x512 and 1024x768. All the experiments have a *PSNR* coefficient up to the 40 dB, so that at this value, there is no visual effect on the encoded image. One of the examples uses the image presented in fig. 5, where is hidden the secret message:

"Acesta.este.un.mesaj.ascuns"("This.is.a.hidden.message" in romanian).

There are no visual differences between the encoded and the original image (fig. 5 vs. fig. 6), but the first one contains the message.

Fig. 5. The encoded image

Fig. 6. The original image

Contributions, Future Work and Conclusions

The paper presents the necessity of information protection and *a new version of a staganographic system* is proposed. Some security parameters of the original proposed steganographic system are analyzed and some modifications are made to the system. An analysis of the most important parameters such as *capacity, distortion, robustness, data integrity* is made. A method for *maintenance of a high level of the data integrity* by calculating the encoded image hash is proposed. For *a dispersed secret message* in the image, it is proposed a new algorithm for finding the pixels *palette* used for encoding. The use of a parallel architecture (in order to have processing power for a high volume of data) for the development of such a system is another new element. *Other contribution consists in analyzing the security functions of the proposed system (authentication, availability, non repudiation, integrity, confidentiality). Some improvements are made to the old version of the steganographic system implemented on CELL BE architecture from IBM.* New concepts are also used: *double buffering, mailboxes, events, DMA transfers, SIMD instructions.* The paper offers *an efficient mapping of the application* on the architecture CELL BE, so that the resources and the programming facilities are optimally used. *The future work* is referring to other encoding schemes.

References

1. Brisbane, G., Safavi-Naini, R., Ogunbona, P. - High-capacity steganography using a shared color palette , *IEE Proceedings on Vision, Image and Signal Processing*, 9 December 2005, 152(6), 787-792, Copyright IEEE, 2005

2. Gonzalez, R., Woods, E. - *Digital Image Processing*, Second Edition, Prentice-Hall, Inc. Upper Saddle River, New Jersey 07458, 2002
3. Kawaguchi, E., Eason, R.O. - Principle and applications of BPCS-steganography, *International Symposium On Voice, Video and Data Communications, SPIE*, 1998
4. Seppnnen, T., Makela, K., Keskinarkaus, A. - Hiding information in color images using small color palettes, *Proc. Information Security, Third Int. Workshop, ISW*, December 2000, pp. 69-81
5. Tiganoaia, B., Iacob, F. - Low distortion and robust steganography on parallel architecture Cell Be using a pixels palette and a shared hash*, PUB Scientific Bulletin*, in press, 2010
6. * * * - Workshop Cell BE, Computer Science Department – IBM Laboratory*,* Politehnica University of Bucharest, 2007
7. * * * - *Cell Broadband Engine Architecture*, http://www-01.ibm.com/chips/techlib/techlib.nsf /products/ Cell_Broadband_Engine, accessed 2009
8. * * * - *Systems Architectures*, Course Notes, Computer Science Department*,* Politehnica University of Bucharest, https://anaconda.cs.pub.ro/asc/index.php/Laboratoare/ , accessed 2009

O nouă versiune de sistem steganografic pe arhitectura paralelă CELL BE

Rezumat

Acest articol prezintă câteva consideraţii asupra necesităţii protecţiei informaţiilor şi dezvoltării continue a sistemelor steganografice. Se mai descrie o nouă tehnică, de capacitate ridicată şi robustă, pentru ascunderea informaţiilor în imagini. Distorsiunea imaginii după codarea mesajului secret este redusă şi indistinctibilă ochiului uman. Atributele de securitate (disponibilitatea, integritatea, confidenţialitatea, non repudierea) sunt discutate în acest articol. Câţiva parametri (capacitatea sistemului, integritatea datelor, distorsiunea etc.) ai sistemului steganografic propus sunt analizaţi pentru a creiona o concluzie asupra performanţelor acestuia. Este realizat un studiu despre arhitectura CELL BE şi este propusă o mapare eficientă a aplicaţiei pe aceasta. Sunt folosite noi facilităţi de programare CELL BE cum ar fi double buffering, instrucţiuni SIMD, mailbox-uri, evenimente, transferuri DMA.