Eurographics Italian Chapter Conference (2007)
Raffaele De Amicis and Giuseppe Conti (Editors)

Ramses: a Visual Steganographic System

S. Battiato[1], G. Di Blasi[2], G. Gallo[1], S. Patti[1]

[1]Department of Mathematics and Computer Science, University of Catania, Catania, Italy
[2]Department of Linguistics, University of Calabria, Rende, Italy

Abstract

Steganography is the art of "secret communication". Its goal is to transmit a message (information) hidden inside another visible message. The typical visible message used in many steganographic systems is a digital image and the embedded message is usually hidden by working in the Fourier domain. In this paper we present Ramses, a novel approach to the steganography based on the Puzzle Image Mosaic (PIM) technique ([DGP05]) which uses the metaphor of the hieroglyphic writing to hide the message in the image. The message is first coded by a sequence of small irregular images and then merged inside another image together with many other small images. We prove that the Kerckhoff's principle required by a steganographic technique is satisfied and experimental results show how it is very difficult to detect the hidden message.

Categories and Subject Descriptors (according to ACM CCS): I.3.3 [Computer Graphics]: Picture/Image Generation
E.3 [Data Encryption]: Public key cryptosystems

1. Introduction

Steganography studies methods to perform secret communications between two entities interested in sharing the content of a secret message but also in hiding the act of communicating it. Steganographic algorithms (also called "stego-algorithms") hide the secret information into different types of "natural" cover data such as sounds, images and videos. The resulting altered data is usually called stego-data and it should be perceptually indistinguishable from its natural cover. Another research field of the steganography, called stego-analysis, tries to analyze altered cover data in order to understand if it embeds a message or not.
Digital images are one of the most used natural covers data to transmit the secret message and usually the message is embedded by slightly modifying the JPEG DCT coefficients of the image ([WAL91], [UPH07]).
In this paper we present a novel approach to the steganography which uses the metaphor of the hieroglyphic writing to hide the message in the image, we call this technique Ramses. Differently from all previous techniques Ramses does not hide the message into the image by any sort of mathematical transformation, but directly shows the message in the image confused with many other "messages". Ramses is based on a recent technique in the field of digital mosaic creation called Puzzle Image Mosaic (PIM) [DGP05]. Given an input image PIM uses a set of image tiles of arbitrary shapes to compose a picture that, if seen from a distance, resembles the input image. By using PIM, Ramses first codes the message by a sequence of small irregular images and then merges them into an input cover image.
We also prove that our system is "secure" under the hypothesis of the "Kerckhoffs' principle" ([KER83]). Kerckhoffs' principle says that a stego-system should be secure even if everything about the system, except the key, is public knowledge.
Steganography is strictly related to watermarking, a technique allowing to add hidden copyright notices or other verification messages to sounds, images and videos. Such hidden message usually contains information about the author of the signal. Steganography and watermarking are similar and use the same technical approaches, but their aims are different: watermarking hides a "mark", steganography hides a message. On the other hand, steganography and watermarking have many common goals: they want to hide "something" without altering the cover data, the "thing" has not to be recognized by a malicious user and has to be robust under several digital attacks (noise, zooming, cutting, etc.), finally the (malicious) user has not to be able to detect the existence of the hidden "thing".
Steganography is also related to cryptography, a technique

allowing to send a message in an encrypted form. Cryptography's primary purpose is to hide the meaning of the message (like steganography), not the existence of such message (differently from steganography).
The rest of this paper is structured as follows: in Section 2 we present some related works in the field of Puzzle Image Mosaic and steganography, Section 3 is devoted to the description of the PIM algorithm, while Section 4 describes Ramses and proves the correctness (Kerckhoff's principle) of our approach. Finally Section 5 shows some experimental results. Section 6 closes the paper proposing some ideas to extend and improve Ramses.

2. Related Works

2.1. Puzzle Image Mosaic

Digital mosaics are images composed by a collection of small images called "tile". The tiles "tessellate" a source picture to reproduce it in a "mosaic-like" style. The same source image can be converted into different kind of digital mosaics depending on which dataset of tiles is used and which constraints are imposed for positioning, deformations, etc.; a complete review on digital mosaic techniques can be found in [BDFG07].
During the Italian Renaissance, the painter Giuseppe Arcimboldo [STR99] invented a form of painting where he did not paint faces in flesh, but with clumps of vegetables and other materials slightly deformed to better match human features. He called this technique "the composite head". Puzzle Image Mosaic is a digital image processing technique inspired by the form of art invented by Arcimboldo.
The first attempt to emulate the Arcimboldo's idea was proposed by Kim and Pellacini [KP02]. They introduce a mosaicing technique, called Jigsaw Image Mosaic (JIM), where they compose the final picture by using image tiles of arbitrary shapes. A similar idea can be found in the photo-mosaic approach ([SH97]), but the final effect is very different and interesting (Figure 1).
To solve the problem they redefine a mosaic as the tile configuration able to minimize a "mosaicing energy function", in this way they introduce a general energy-based framework for mosaicing problems that can be viewed as a generalization of the algorithms presented in [HAU01] and in [SH97]. The energy function E used by Kim and Pellacini is defined as:

$$E = w_C \cdot E_C + w_G \cdot E_G + w_O \cdot E_O + w_D \cdot E_D \qquad (1)$$

where:

1. the color energy term E_C penalizes configurations that do not maintain the color of the input image;
2. the gap energy term E_G penalizes configurations that have too much empty space in the final image;
3. a big overlap between tiles gives large overlap energy E_O;
4. the deformation energy E_D penalizes configurations where tiles are highly deformed.

Figure 1: *The Jigsaw Image Mosaic.*

The stego-algorithm described in this paper uses the PIM algorithm [DGP05] as better specified below.

2.2. Steganography

Several visual stego-algorithms have been proposed in these last decades, for example, we may cite two classic algorithms used in [MSS05] to study how several recently proposed statistical models can be used for stego-analysis. They consider Jsteg [UPH07] and MHPDM [TBHK03].
Jsteg embeds a message in the least significant bit of JPEG DCT coefficients. The algorithm operates in two steps. First, it reduces the number of entries in the color palette of the cover image, and then it embeds a message in the least significant bits of the three RGB components, without expanding the number of colors beyond 256.
The MHPDM algorithm works by altering the least significant bit of a subset of the JPEG DCT coefficients of an image. If the 64 coefficients of each DCT block are indexed from zero following the usual zig-zag order, only coefficients 1 through 20 are candidates for modification. The rest are left untouched, since values of coefficient with index 0 (DC) are far from being independent and coefficients 21 through 63 are highly quantized during the JPEG process.

3. The PIM Algorithm

The PIM algorithm has been presented in [DGP05]; this approach is based on the Antipole strategy ([CFP*05]) and leads to good results in an acceptable computation time (Figure 2). The technique reformulates the problem as a search problem in a large database of small images taking into account some important features of the image to speed up the search process. Today, Magic Mosaics [Mag06] produces puzzle image mosaic posters and banners using a modified version of this software. To reach this goal the authors have

Figure 2: *The Puzzle Image Mosaic.*

to map a tile (shape and color) into the metric space X in order to create the Antipole data structure. The shape of a tile is composed by the pixels of the image having a non-transparent color. So, they perform the following steps:

1. evaluate the shape's mass center;
2. subdivide the shape into 90 segments, obtaining 90 vertices;
3. compute the (Euclidean) distance of each vertex from the mass center and normalize the value in [0,1] (the normalization is performed in order to make the distances "scale independent").

This leads to a vector x composed by 90 components: x is the feature vector of the image in the data structure. The shapes distance is computed evaluating the Euclidean distance between feature vectors. The computation takes into account all the possible shifting between the two arrays (that is all the possible mutual rotations of the two shapes). This operation is performed in order to make the distance "rotation independent" and "starting point independent"; since a shape is subdivided into 90 segments a rotation error of at most 4 degrees ($\pi/45$ radians) is committed. The final algorithm can be summarized as follows:

1. start with an input image;
2. perform the directional guideline detection by using the same technique proposed in [DG05];
3. perform the morphological operation "dilate" obtaining the image G (the dilation is performed only for better aesthetic results and it does not affect the subsequent steps);
4. compute a Voronoi diagram V of the same size of the input image (the set of points is randomly chosen and its cardinality is user selected);
5. merge the images G and V obtaining the image R;
6. for each region R_i of R:
   a. perform the algorithm described above in order to obtain the feature vector x of R_i (x can hence be used to perform the search in the Antipole tree);
   b. perform the best matching;
   c. perform a color shifting in order to align the median color of the selected tile with the median color of R_i;
   d. rotate and resize the tile to fit and paint it over the region.

4. The proposed stego-algorithm: Ramses

In order to hide a message inside an image we modified the basic PIM algorithm. Ramses uses the metaphor of the hieroglyphic writing to hide the message in the image. For this reason, the first step of the algorithm is devoted to the "translation" of a message into a sequence of small images following the same idea used by the old Egyptians. The description of the method used to perform this step is beyond the scope of this paper and inscribes itself into the area of the linguistics sciences (see [DE 64] for a very good introduction to the problem).
After this step we have a message coded by a sequence of small irregular images, then we have to merge it inside another image together with many other small images. To reach this goal we modify the algorithm proposed in the previous Section by adding another step between the steps 5 and 6. In particular given the image R, let N be the cardinality of the Voronoi regions and let n be cardinality of the coded message, the algorithm can be summarized as follows:

1. for each image I of the message:
   a. perform the algorithm described in the previous Section in order to obtain the feature vector x of the image;
   b. evaluate N/n regions and find the best matching region R_i between the regions and the image I;
   c. perform a color shifting in order to align the median color of I with the median color of R_i;
   d. rotate and resize I to fit and paint it over the region.

This approach has two basic advantages with respect to a simple "random" approach:

1. we limit the overlapping between images;
2. the message images can be found sequentially by scanning the image in the classic scan-line approach (top-down, left-right) in the same order of the original message.

The remaining regions are merged by using the same approach proposed in step 6 of the algorithm in the previous Section.
Now, we have to prove that our system is "secure". We have to suppose that everything about the system, except the key, is public knowledge, we have to define the "key" and prove that it is no possible to detect the message without the key. The proof is visually intuitive. In our system we suppose that both the sender and the receiver (and eventually a malicious user) have the same cover image, the same database

of small images and the same Voronoi diagram. The key is represented by the seeds of the Voronoi regions used to transmit the coded message. Suppose that a malicious user wants to detect the message without knowing the key; even if he has the cover image, the database and the Voronoi diagram, he will not be able to find which seeds have been used to send the secret message. Moreover, if $N \approx n$ then many regions will contain an image message and it could be easy for a malicious user to detect the entire message by using some statistical brute force approaches, while if $N \gg n$ then the message is sufficiently "dispersed" into the regions and also a brute force approach could require an exponential time to detect the message.

5. Experimental Results

To illustrate the effectiveness of the proposed technique we report some pictorial examples. The algorithm has been implemented in Java2 Standard Edition 1.4.2 and all experiments have been carried out on a PC Athlon XP-M 1800+, 192MB RAM, with Windows XP Home Edition. To allow the real testing of the performances of the proposed technique an applet is available in [BDGP07], at the same URL is also possible to download a JGimp plug-in and a Java application. Our implementation at this time does not rely on any particular graphic hardware acceleration.
Figures 3 and 4 show the typical outputs of our technique; Figure 3a (resp. 4a) shows the cover image used to transmit the message, while Figures 3c and 3d (resp. 4c and 4d) show respectively the output generated by PIM and Ramses; it is plain that the two figures are indistinguishable and it is not possible to detect the secret message hidden inside Figure 3d (resp. Figure 4d). Finally, Figure 3e (resp. 4e) shows the message image which could be retrieved by the receiver user.

6. Conclusions and Future Works

In this paper we presented Ramses, a novel approach to the steganography. Actually, the software requires a manual user intervention for the creation of the message and for the interpretation of the received image. Future works will be devoted to the creation of an automatic system able to:

1. code a string message into a sequence of images;
2. create and send the cover image;
3. receive the cover image and decode it into the original string message.

References

[BDFG07] BATTIATO S., DI BLASI G., FARINELLA G., GALLO G.: Digital mosaic frameworks - an overview. *Computer Graphics Forum, in press* (2007).

[BDGP07] BATTIATO S., DI BLASI G., GALLO G., PATTI S.: The ramses applet www.dmi.unict.it/∼gdiblasi/ramses/ramses.html, jgimp plug-in and java application www.dmi.unict.it/∼gdiblasi/ramses/ramses.jar.

[CFP*05] CANTONE C., FERRO A., PULVIRENTI A., REFORGIATO RECUPERO D., SHASHA D.: Antipole tree indexing to support range search and k-nearest neighbor search in metric spaces. *IEEE/TKDE 17*, 4 (2005), 535–550.

[DE 64] DE SAUSSURE F.: *Course In General Linguistics*. Peter Owen London, 1964.

[DG05] DI BLASI G., GALLO G.: Artificial mosaics. *The Visual Computer 21*, 6 (2005), 373–383.

[DGP05] DI BLASI G., GALLO G., PETRALIA M.: Puzzle image mosaic. In *Proc. IASTED/VIIP2005* (2005).

[HAU01] HAUSNER A.: Simulating decorative mosaics. In *Proc. SIGGRAPH2001* (2001).

[KER83] KERCKHOFFS A.: La cryptographie militaire. *Journal des sciences militaires IX* (1983), 5–38, 161–191.

[KP02] KIM J., PELLACINI F.: Jigsaw image mosaics. In *Proc. SIGGRAPH2002* (2002).

[Mag06] Magic mosaics, http://www.magicmosaics.com/.

[MSS05] MARTIN A., SAPIRO G., SEROUSSI G.: Is image steganography natural? *IEEE/TIP 14*, 12 (2005), 2040–2050.

[SH97] SILVERS R., HAWLEY M.: *Photomosaics*. Henry Holt, 1997.

[STR99] STRAND C.: *Hello, Fruit Face! : The Paintings of Giuseppe Arcimboldo*. Prestel, 1999.

[TBHK03] TZSCHOPPE R., BAML R., HUBER J., KAUP A.: Steganographic system based on higher-order statistics. In *Proc. SPIE* (2003).

[UPH07] UPHAM D.: Jpeg-jsteg-modifications of the independent jpeg groups jpeg software for 1-bit steganography in jfif output files ftp://ftp.funet.fi/pub/crypt/steganography/.

[WAL91] WALLACE G.: The jpeg still picture compression standard. *Communications of the ACM 34*, 4 (1991), 30–44.

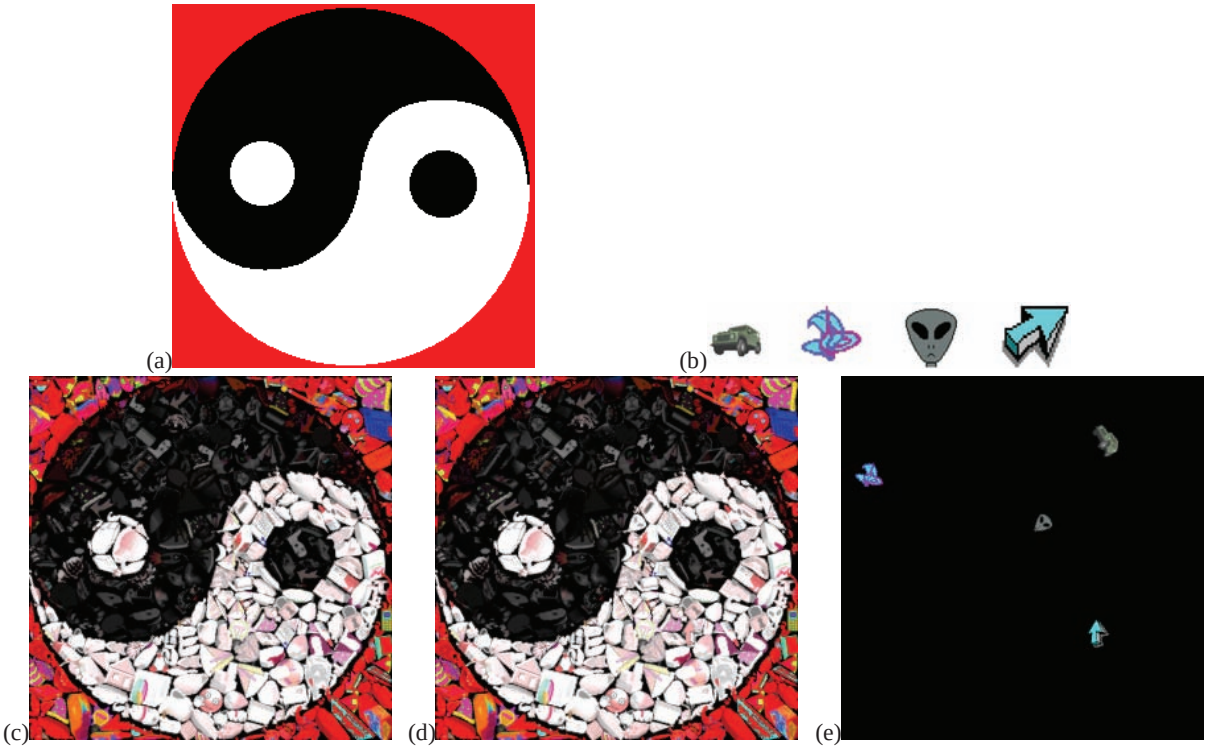

Figure 3: *An example of Ramses, (a) the orginal (cover) image, (b) the message, (c) the PIM image, (d) the Ramses image and (e) the message image.*

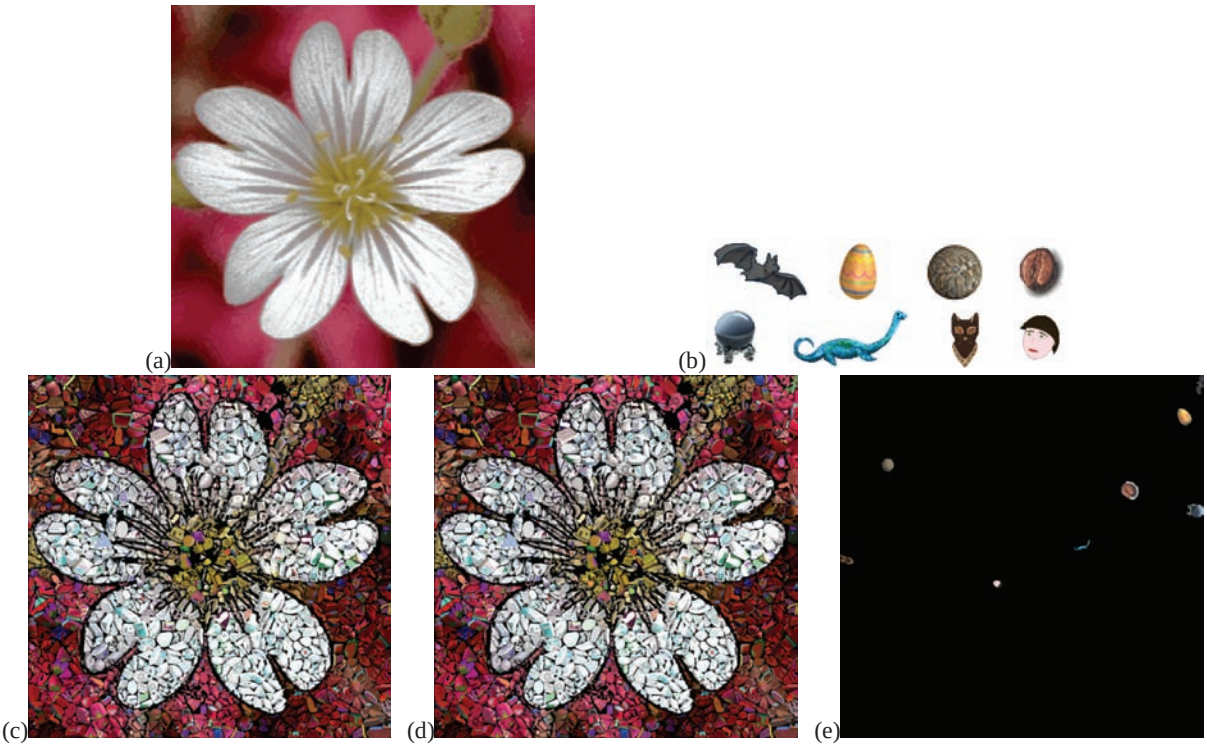

Figure 4: *Another example of Ramses, (a) the orginal (cover) image, (b) the message, (c) the PIM image, (d) the Ramses image and (e) the message image.*