SSB-4 System of Steganography using bit 4

J.M. Rodrigues[1], J.R. Rios[2] and W. Puech[1]
[1] Laboratoire LIRMM, UMR CNRS 5506, Université Montpellier II, France
[2] Compute Department, Universidade Federal do Ceará, Brazil

ABSTRACT

In this paper, a novel steganography method based on the spatial domain and in the human perception is proposed. It does not use the known LSBs bits to embed the information, instead the secret message is hidden in the fourth bit of the cover-image pixel. The main idea is to change the bit 4 of the pixel in the original image according the bit message. Than modify the other bits of the byte observing that the difference between the new pixel value and the previous one must be equal or smaller than four. We have compared our method with others that work in the spatial domain. We present the results obtained through subjective tests that are based on the levels of human perception. The great difference between our method and the others in the spatial-domain is the fact that we do not use the LSBs bits of the image for embedded the message.

1 INTRODUCTION

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography, but this has changed rapidly [9]. The search of a safe and secret manner of communication is very important nowadays, not only for military purposes, but also for commercial goal related to the market strategy as well as the copyright rights. To find other forms to communicate covertly is important. In this context, the steganography has great significance because it is based on the obscurity to keep the secrecy.

Steganography derive from the Greek and it means "covered writing". It is the art of communication in such a way that even the intention of communication can not be noticed (what can not be seen can not be modified). The goal of steganography is to hide data inside other "harmless" media. This media can be a digital image, audio, movie or any digital file that can carry a message. Images provide excellent carriers for hidden information and many different techniques have been introduced [8].

In our work we have applied the combination of the technique elements based on the spatial domain with the human visual system characteristics. We have masked the message in such a way that visually perceptible difference between the original image and the container does not exist.

The rest of this paper is organized as follows. Section 2 reviews, in progressive way, some methods based in the spatial-domain that use the Least Significant Bits. Section 3 we propose our steganography method, the SSB-4. In Section 4, some experimental results and analysis will be listed and discussed.

2 Methods in Spatial-Domain

2.1 Least significant bit substitution (LSB)

This is the simplest of the steganography methods based in the use of LSB, and therefore the most vulnerable. The embedding process consists of the sequential substitution of each least significant bit of the image pixel $c_\imath$, for the bit message $m_\imath$, where $\{\ 1 \leq\ \imath\ \leq l(m)\}$. For its simplicity, this method can camouflage a great volume of information [11].

This technique is quite simpleton and it presents a safety fault. It is necessary only a sequential LSB reading, starting from the first image pixel, to extract the secret message. This methods also generate a unbalanced distribution of the changed pixels, because the message is embedded at the top of the image.

2.2 Pseudo-random permutation

This technique was born as a solution for the problems of the previous method. Each one, the sender and the receiver of the image has a password denominated *stego-key* that it is employed as the seed for a pseudo-random number generator. This creates a sequence $\{x_1, x_2 \cdots x_{l(m)}\}$ which is used as the index to have access to the image pixel, so that:

$$C_{X_\imath} = m_\imath \qquad \{\forall\, \imath \in N \mid 1 \leq \imath \leq l(m)\}. \qquad (1)$$

The bit of the message $m_\imath$ is embedded in the pixel $C_{x_\imath}$ of the cover image, where the index $x_\imath$ is given by the pseudo-random number generator. All the methods based on the pseudo-random number generator must use an array to control the collisions [11].

The two main features of the pseudo-random permutation methods are the use of password to have access to the message, and the well-spread message bits over the image.

2.3 Cover regions and parity bits

This method is very similar to the previous one. The difference between them is the fact that each bit m_i of the message is stored in an area A_i of the image instead of a pixel. In this technique the image is divided in a minimum of $l(m)$ contiguous and disjoint regions and their use are defined by a pseudo-random number generator (PRNG).

The message bit is embedded thought the computation of the parity bit of a region I conform the following equation:

$$P(I) = \sum_{j \in i} LSB(C_j)\ mod_2. \quad (2)$$

It is necessary only one LSB flipping of any pixel of the region to change the parity region value.

3 THE PROPOSED METHOD (SSB-4)

Most of the camouflage processes use the redundant bits of the image to embed secret messages. Redundant bits are all bits that can be modified without altering the visual feature of the digital picture. In its great majority, the redundant bits are the LSBs. The big challenge in this work was to find a way of embedding the message in more significant bits of the image.

3.1 Hypothesi and Assertions

The SSB-4 is based in the following hypothesi/assertions:
Hypothesi-1: In an RGB-24 image, small variations in the channel color value is imperceptible to the human eye [3]. Our hypothesi is that changing of ± 4 units in the channel color value is imperceptible to HVS.
Assertion-1: The 4^{th} bit was chosen because it satisfies the hypothesi-1 and it is the most significant bit which provides the minimum change in the pixel values denoted in Hypothesi-1.
Assertion-2: The values of blue channel smaller than 4 or bigger than 251 will not be employed to embed information, because they do not satisfy the hypothesi-1.

3.2 Algorithm

The proposed method can be applied on images stored in anyone of the several types of existent file formats, as long as they use eight bits per color channel and make use of lossless compression. The main objective of our method is to change the bit 4 of the pixel, according the bit message, and after finding a way to modify these $\{1, 2, 3$ and $5\}$ remainder bits in order to reach the smallest difference between the new and previous decimal pixel values.
The process of the camouflaging through the SSB-4 works as follows:

Step-1: We compute the incrustation factor $E(l)$ using the cover image size $l(c)$, in pixels and the message size $l(m)$, in bits:

$$E(l) = \lfloor \frac{l(c)}{l(m)} \rfloor. \quad (3)$$

Step-2: The image is divided in at least $l(m)$ regions of size $E(l)$. They are disjoints and contiguous, each one of them will be used to store only one bit of the message. With this procedure, a uniform distribution of the message bits in the image is guaranteed.
Step-3: It is requested a password, that will be used as the seed for the pseudo-random number generator. This generator will produce numbers that indicate which region will be used to embed the message bits. Unlike some other methods, the password is not recorded in the image file.
Step-4: With the region i indicated by PRNG, we calculate its central pixel $P(i)$:

$$P(i) = \lceil \frac{E(l) \times (2i - 1) + 1}{2} \rceil. \quad (4)$$

Then we get the blue channel value of this central pixel. Our visual system has sensibility different to the three basic colors, being more sensitive to the green, red and blue lights, in this order [6]. We use the blue channel, so we became the modifications less evident.
Step-5: We analyze the value of the 4^{th} bit of this channel and compare it with the message bit. If the values that they represent are equals, nothing should be made. Otherwise, we change the value of the bit 4 in order to reflect the value of the message bit.

3.3 Practical example

Suppose the message bit is $zero$ and the value of the blue channel central pixel is 46. So, the value of the bit 4 is (1). It is necessary modify the bit 4 to $zero$ in order to embed the message. So, we have to search a new arrangement of the remainder bits $\{1, 2, 3$ or $5\}$ in order to have the smallest variation (maximum ± 4) in the color of the pixel. We can see on Table 1 that we have made modification on the remainder bits $\{2, 3$ and $5\}$ to obtain 48.

Table 1: A⇒Original blue color value, B⇒Best modification of the reminder bits.

		Binary value							
	Decimal	8	7	6	5	**4**	3	2	1
A ⇒	46	0	0	1	0	**1**	1	1	0
B ⇒	48	0	0	1	***1***	**0**	***0***	***0***	0

4 RESULTS

4.1 Subjective Test

Detecting an embedded message defeats the primary goal of steganography, that of concealing the existence of a hid-

den message [7]. As the Steganography is based in obscurity, the most important tests are related to the human perception [1]. These types of tests evaluate the invisibility or transparency and one of the most used is the subjective test. Its rules and recommendations were defined by the International Telecommunication Union [5, 4]. The subjective tests are made by people who look for visual differences between the images (original and container) trying to find which one of them is the original. If the percentage of success goes 50%, it can be concluded that the message is invisible. Truly, the analyzers will have to look for noises or imperfections, because theoretically all procedure of camouflage insert some kind of anomaly in the image.

For steganography exist appropriate pictures (great variety of brightness and color) and inadequate (long areas with same luminosity). In order to have significant results in the assays related to the human perception, we have chose images according these two approaches. We have used 60 images; 30 of the adapted type that we called Group-I (see example in Table 2) and 30 of the inadequate type that was denominated Group-II. For this last group, we create monochromatic photographs of $250X280$ pixels each (see example in Table 3). Optic-metric studies brings out that the HVS is very good to perceive points in surfaces with uniform colors. So, it is believed that if the solutions obtained for worst cases are satisfactory, certainly they will also be for the others.

In the subjective tests, each two images (original and container) were presented side by side for 100 different beholder, with the following question: *Which one is the original image?* The images were reorganized and submitted to the same 100 perceivers again. The results are showed in the following tables and in Figure 1.

Table 2: Group-I - Appropriated Images.

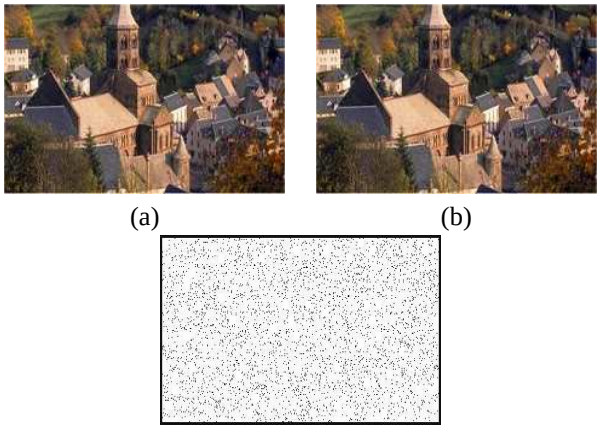
Image	Image size (pixels)	Message size (bits)	Success (%)
Pitcure-1	72.160	67.832	51
Pitcure-2	128.400	88.920	48
Pitcure-3	133.910	129.400	50

Table 3: The images have the same size 70.000 pixels and they have embedded the same message 67.832 bits.

Image	Color	(%) Success
1	RGB(255, 0, 4)	49
2	RGB(0, 255, 4)	50
3	RGB(0, 0, 251)	54

Analyzing the results for the Group-I (about 50%), we can conclude that the SSB-4 did not generate any indication that took the examiners to the correct identification of the original image.

For the images of Group-II, we have expected non-satisfactory results, however the experiments were very good for all tested colors, except the white color that presented 87% of rightness. The white color amplifies visually the noises and it stands out the imperfections.



(a) (b) (c)

Figure 1: a) Original Picture-1, b) Picture-1 embedding a message of 67.832 bits, c) Difference between (a) and (b).

4.2 Distribution Binomial

The use of PRNG for pixels selection becomes probabilistic the embedding process. So, it can be inferred that, if there are no addictions, the distribution of the number of modified pixels in the image should be binomial. Therefore, the probability of k pixels be modified in a total of n is given by:

$$p_k^{(n)} = \binom{n}{k}\, p^k\, (1-p)^{n-k}, \tag{5}$$

where p is the probability that a selected pixel has to be changed. Because there is no rule of formations for the message bits, we expected that $p = 1/2$, and the average number of changed pixels be around 50% of the image size. See Table 4.

Table 4: The probability p that a select pixel has to be changed.

Image Group I/II	Modified pixels	Standard Deviation σ Expected	Measured	Probability $\sigma = \sqrt{n}$
Pitcure-1	34.522	130,223	130,202	0,499
Pitcure-2	44.743	149,097	149,094	0,500
Pitcure-3	64.941	179,861	179,859	0,500
1,2	33.910	130,223	130,222	0,500
3	33.949	130,223	130,222	0,500

4.3 Comparison with other methods

We have applied the MSE (*Mean Square Error*) and the PSNR (*Peak Signal to Noise Ratio*) to compare SSB-4 with others methods. The results of the images of Groups I and II are displayed in the Table 5.

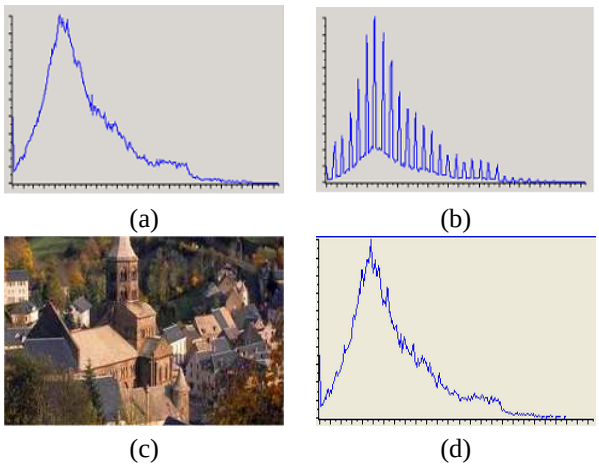
Table 5: Comparison with others methods, PSNR in dB.

	Image Group-I			Image Group-II		
	1	2	3	2	4	6
SSB-4	**42,4**	**44,0**	**42,6**	**40,6**	**40,6**	**40,6**
Contraband	46,4	46,3	46,5	48,1	43,4	43,4
InfoStego [2]	47,3	48,7	47,6	49,6	43,5	43,5
Secrets [10]	29,1	25,0	21,4	29,3	31,3	30,2
ThirdEye [12]	51,4	52,7	51,4	53,6	51,5	51,6
WbStego [13]	46,5	46,4	46,6	48,1	43,4	43,4

The SSB-4 showed favorable results. It presented very close PSNR values in relation to the other methods and in some cases, it was better. It is important to stand out that, the others methods use LSB and that implies in an alteration maximum of ± 1, while the SSB-4 accept alteration in the pixel of up to ± 4.

4.4 Histograms Analysis

The histograms of the carriers have presented great sequenced peaks, which turned the graphic strongly serrulated, exposing the presence of camouflaged information. This symptom is due to the size of the messages. For messages of smaller proportions in relation to image size, up to 10%, this phenomenon is not accentuated.



(a) (b) (c) (d)

Figure 2: a) Blue channel histogram of Figure-1.a, b) Blue channel histogram of Figure-1.b, c) Figure-1.a embedding a message of 4.208 bits, d)Blue channel histogram of (c).

5 CONCLUSION

This work presents a new spatial domain data hiding method used for steganography applications. The SSB-4 embeds the information in the fourth bit of the byte and make or not modifications on the remainder bits. With this approach, a stronger bit carries the information instead of the least significant bits and the impact in the pixel color is the same as the LSBs.

We showed that our method provide invisible cover-images by presenting the HVS perceptual test results, and statistical image properties. Future work will concentrate on improving the robustness of this technique using it in the frequency domain.

References

[1] FRIDRICH, J. Applications of Data Hiding in Digital Images. In *ISPACS'98 Conference* (1998).

[2] INFOSTEGO. http://www.antiy.net/infostego.

[3] ISMAIL AVCIBAS, N. M., AND SANKUR, B. Steganalysis using image quality metrics. In *IEEE Transactions on Image Processing* (February 2003), vol. Vol. 12, p. No. 2.

[4] ITU-R RECOMMENDATION BT.500-7. Method for the subjective assessment of the quality of television pictures. In *RBT* (1997).

[5] ITU-T RECOMMENDATION P.910. Subjective video quality assessment methods for multimedia applications. In *RBT* (1995).

[6] JAMES D. MURRAY, W. V. *Graphics File Formats*. O'Reilly & Associates, Inc., USA, April 1996.

[7] JOHNSON, N. F., AND JAJODIA, S. Steganalysis of images created using current steganography software. In *Proceedings of the Information Hiding Workshop* (Portland, Oregon, USA, April 1998).

[8] NEIL F. JOHNSON, ZORAN DURIC, S. G. J. *Information Hiding : Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1)*. Kluwer Academic Publishers, February 15, 2001.

[9] PETITCOLAS, FABIEN A. P. www.petitcolas.netfabien/steganographyindex.html.

[10] SECRETS. http://www.invisiblesecrets.com.

[11] STEFAN KATZENBEISSER, FABIEN, A. P. *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Boston - London, February 2000.

[12] THIRDEYE. http://www.webkclub.com/tte.

[13] WBSTEGO. http://wbstego.wbailer.com.