Volume XXII 2019
ISSUE no.2
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Robustness of the watermark applied to compromised noise images

To cite this article: A.M. Travediu, M. V. Manoliu, C. Racuciu Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg.36-44.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I2-004

Robustness of the watermark applied to compromised noise images

Student Ana-Maria Travediu, MSc. Student, University Politehnica of Bucharest
Mitica Valentin Manoliu , Ph.D. Student Military Academy
Prof.Eng. Ciprian Racuciu Ph.D.University Titu Maiorescu University, Military Technical Academy
Email: ana.travediu@yahoo.com, manoliu_mit@yahoo.com, ciprian.racuciu@gmail.com

Abstract. Watermark is the concealment of digital information in a digital carrier signal. The main feature of the watermark is the robustness against changes that can be applied or can occur to the carrier signal which is vulnerable to external factors. Generally, the watermark is designed to have the following three properties: be imperceptible, inseparable from the document in which it was inserted, the same procedures applied to the carrier must be applied upon the watermark as well; We used the watermark applied to the image in the bit structure (LSB type) and tested it with different attack forms compared to the watermark applied on blocks in the image on the bit structure (LSB type) by modifying the information. This article looks for a comparison between the two research techniques to test it each one. We will demonstrate that this approach leads to the acceleration of the algorithm's operation without having a negative impact on the quality of the security solutions provided.

1. Information security

The current society is constantly expanding, which has led in the last years to an explosion in technology that undoubtedly has a huge influence on everyday life. The information that until recently was paper-based, now has electronic form. The need for security that people feel and the new dimension that information has at this time has led to the concept of information security.

Security means freedom or resistance to possible attacks by external forces that can not be controlled. Security recipients can be individuals and social groups, objects and institutions, ecosystems and any other entity or phenomenon vulnerable to unwanted changes through its environment.

Steganography is the practice of hiding a file, audio message, image or video in another file, sound, image or video. The word steganography is made up of Greek words "steganos", meaning "covered, hidden or protected", and "graphies" meaning "written".[1]

The advantage of steganography over cryptography is that the secret intended message does not draw attention to it as a control object. Clearly visible encrypted messages, no matter how unfounded they are, are of interest and can in themselves be incriminating in countries where encryption is illegal. While cryptography is the practice of just protecting the message, steganography takes into account the fact that a secret message is being concealed, as well as hiding the content of the message.

Steganography includes hiding information in computer files. In digital steganography, electronic communications may include steganographic encoding within a transport layer, such as a document file, image file, program, or protocol. Media files are ideal for steganographic transmissions due to their large size.[2]

An image can be inserted into another image like in the sender block functions (Fig 1.1). It results a watermarked image with the watermark image overlaps the host, original image.[3]

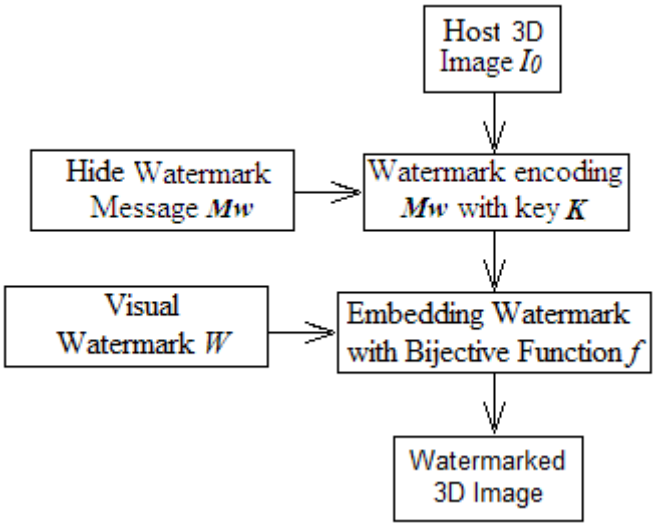

Fig. 1.1. Sender module's blocks[3]

2. Watermark

A watermark is a mark on certain types of paper, especially money, which is only seen if it is kept in strong light and used to stop illegal copying.[4]

A digital watermark is a type of marker hidden in a signal that has a high noise tolerance, such as audio, picture or video signals. It is usually used to identify the ownership or copyright of such a signal. "Watermarking" is the process of concealing digital information in a bearer signal. The digital watermark can be used to verify the authenticity or integrity of the bearer signal or to show the identity of the owners. It is frequently used for tracking copyright infringement. Since a digital copy of the data is identical to the original one, the digital watermark is a passive protection tool. It marks only the data, but does not degrade or control access to data.[5]

While steganography pursues imperceptibility to human senses, the digital watermark tries to control robustness as a top priority. The properties of a digital watermark depend on where it is applied. To mark media files with copyright information, a digital watermark must be robust enough against the changes that can be applied to the bearer. Instead, if integrity has to be ensured, a fragile watermark will apply.[1]

The method has two main modules (Fig.2.1), the sender and receiver. The sender is the part wherethe owner is protecting the produced images, adding a visual watermark over the host image.

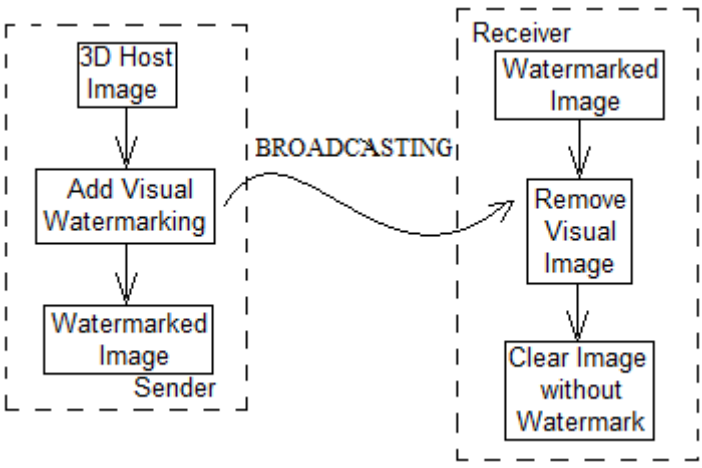

Fig. 2.1.Sender/Receiver 3D Image Watermarking Process[3]

3. Experiments and results

We implemented the randomly generated bitmap watermark with a bit watermark key built to meet design requirements on a chosen image, and we got the watermark image that was subjected to multiple attacks. We made the simplification to intensity, greyscale, to work with a single colour plan and not three plans like the RGB format.

3.1. Watermark applied to the image in the bit structure




Fig 3.1.Comparison regarding the quality of the image with watermark inserted in the bit structure

$$BER = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|w_2(i,j) - w_1(i,j)\right|}{MN}$$

$d = a \times b = \frac{M}{m} \times \frac{N}{n}$, where w is a d size watermark extracted from a pixel block.

Then we extracted the watermark and calculated the bit error rate (BER). For the case where the image was not attacked, the BER must be 0. The more brutal the attack and the more the bit error rate on the bit will increase. A fragile watermark will have a BER that will grow faster or a greater error than a robust watermark.[6]

The watermark image on LSB, bit1 and bit6 , was attacked and we obtained the following results:

Attack	**BER on bit 1**	**BER on bit 6**
blurring	0.4988	0.3925
brightening	0.1339	0.6730
Gaussian noise (0,0.0005)	0.4993	0.1354
median filter	0.3961	0.3763

Salt and pepper noise (0.0005)	2.4414e-04	2.6321e-04
JPEG compression (quality factor: 50)	0.4993	0.3254

Tab.3.1. Comparison regarding robustness at different attack forms

3.2. Watermark applied on blocks in the image on the bit structure

To decide the value of the watermark bit corresponding to a size block d the following decision function is used:

$$w' = \begin{cases} 0, \ if \ \sum_{i=1}^{a} \sum_{j=1}^{b} w(i,j) \le \frac{d}{2} \\ 1, \ if \ \sum_{i=1}^{a} \sum_{j=1}^{b} w(i,j) > \frac{d}{2} \end{cases}$$

To increase robustness, instead of inserting a watermark across the entire image area, we will redesign it into the redundant blocks with the LSB technique on bit 5.

Fig. 3.2. Generating the image containing the block watermark

This image was subjected to the attacks, and then we extracted the watermark from the image, passed it through a simple decision-making system that verifies in every redundant instance the value of each pixel and makes a decision about the true value based on most of the occurrence values:

Fig. 3.3. The image before the attack, the image after the blurring attack, the overall watermark, the original watermark

Fig. 3.4. The image before the attack, the image after the brightening attack, the overall watermark, the original watermark

Fig.3.5. The image before the attack, the image after the Gaussian noise attack, the overall watermark, the original watermark

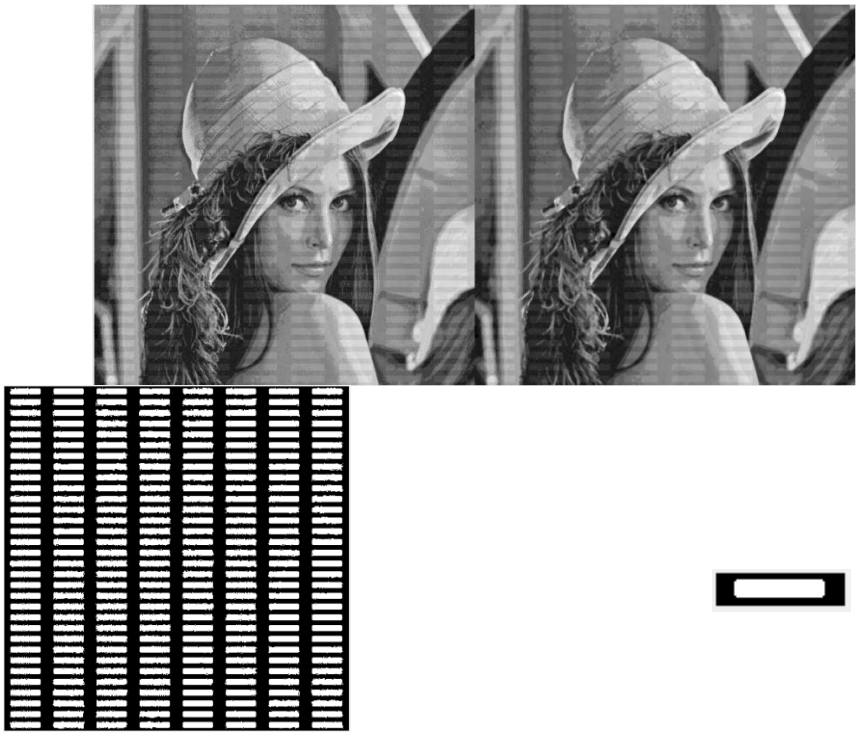

Fig.3.6. The image before the attack, the image after the median filter noise attack, the overall watermark, the original watermark

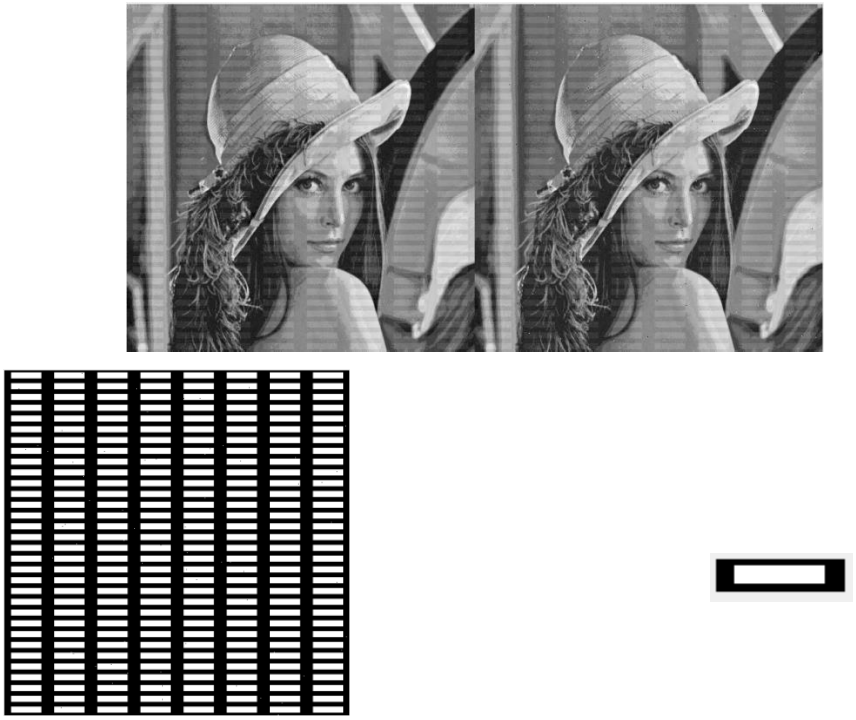

Fig. 3.7. The image before the attack, the image after the Salt and pepper noise attack, the overall watermark, the original watermark

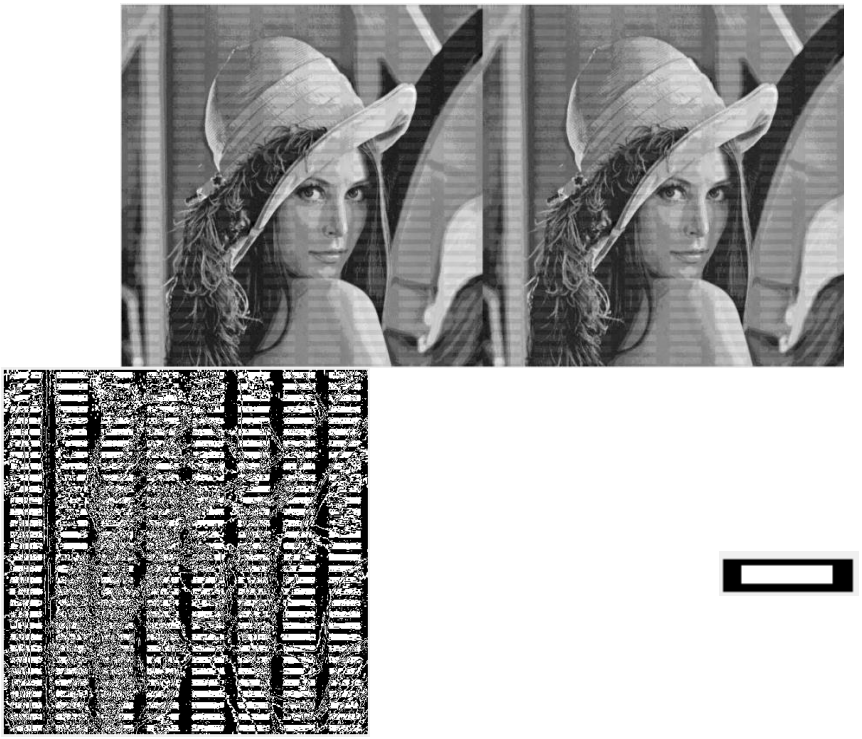

Fig. 3.8. The image before the attack, the image after the JPEG compression attack, the overall watermark, the original watermark

This type of watermark is more robust to attack, many of the watermarks extracted and subjected to the decision system, being identical to the original one.

4. Conclusions

As shown by the tests results, both the Watermark version of the bitmap and Watermark image applied on blocks in the image on the bit structure following the evolution of a multiple attack on an image. I used the processing with a single color plan, gray tones, and not three planes, such as the RGB format.

If the watermark is applied to the image in the bit structure and calculated the bit error rate (BER). For the case where the image was not attacked, the BER must be 0. The more brutal the attack and the more the bit error rate on the bit will increase. A fragile watermark will have a BER that will grow faster or a greater error than a robust watermark.(Fig.3.1). As a result of the multiple attack on bit 1 (LSB) and bit 6, we can see the values that lead to image alteration(Tab.3.1).

Using Watermark applied on blocks in the image on the bit structure To increase robustness, instead of inserting a watermark across the entire image area, we redesign it into the redundant blocks with the LSB technique on bit 5(Fig 3.2). The image was subjected to multiple attacks, and then we extracted the watermark from the image, passed it through a simple decision-making system that verifies in every redundant instance the value of each pixel and makes a decision about the true value(Fig 3.3, Fig 3.4, Fig 3.5, Fig 3.6, Fig 3.7, Fig 3.8).

Watermark applied on blocks in the image on the bit structure is more robust to attack, many of the watermarks extracted and subjected to the decision system, being identical to the original one.

References

[1] http://www.comm.pub.ro/preda/scm/cursuri/SCM_Cap4.pdf
[2] Alex Toumazis," Steganography", University of Cambridge, 2009
[3] Marius Rogobete, Ciprian Răcuciu - A Watermarking Framework for Image Protection. A case study, Symposium on Automated Systems and Technologies, St. Petersburg, Russia, May 2015
[4] Course note PAIC, Vertan Constantin
[5] Melinos Averkiou, "Digital Watermarking", University of Cambridge, 2009
[6] Marius Rogobete - Tehnici steganografice și watermarking, Editura Economică, București 2017, ISBN 978-973-709-806-1