Ann. Acad. Rom. Sci.
Ser. Math. Appl.
ISSN 2066-6594 Vol. 9, No. 1/2017

ROBUSTNESS OF THE SECRET MESSAGE IN STEGO FILE AGAINST FLIP AND ROTATION ATTACK*

Hristo Paraskevov† Stanimir Zhelezov‡
Boryana Uzunova-Dimitrova§

Abstract

This paper provides an algorithm to achieve robustness with the extraction of the secret message from a Stego file after an applied attack from the flip, rotate type, or any random combination thereof. The LSB method is at the base of the algorithm, which is applied with a column modification when reading the matrix of pixels. Ratios are used, such as PSNR and embedding efficiency. To assess the results histogram and steganalytic analyses are applied as well. It is experimentally proved that the proposed method can be successfully applied to extract the secret message with these attacks, even if an LSB Inversion attack is attached to the file as well.

MSC: 68U10, 68P30, 94A08, 94B05

keywords: Active Stego Attack, Data Hiding, Steganography

*Accepted for publication on January 12-th 2017

†paraskevov@gmail.com Faculty of Mathematics and Computer Science, Shumen University, Shumen, Bulgaria; Paper written with financial support of project RD-08-119/2016 Steganography in mobile devices and 3-dimensional modeling

‡stanzhelezov@yahoo.com

§uzunova_b@abv.bg

1 INTRODUCTION

Information is one of the most valuable things in the people‘s modern life and with the development of multimedia technologies and computer networks access to it has become very easy. This deepens one of the oldest and still extremely topical, but unresolved problem - reliable protection from unauthorized access to confidential information, which in most cases is in a digital form.

Information protection is required during the document flow within state and non-state organizations and companies, in the personal correspondence, in the transmission of information over modern telecommunication channels, to protect the intellectual property of audio, film and photo products. It is also necessary to protect the data stored in personal computers. There are different ways to protect data, one of which is the application of Steganography methods. Nowadays Steganography has taken its niche in providing information security.

According to [1] the main requirement to the Stego system is resistance to passive and active opponents. Robustness must be perceived as keeping the secret message even after deformations in the process of transmission or storage. The Stego capacity and robustness are always in conflict. The larger the Stego capacity, the smaller the robustness and vice versa.

In [2] the task of robustness of the stegosystem to passive attacks is formalized as a test of statistical hypotheses. For that purpose a test function of a stegodecoder that gives binary decision on the presence or absence of an embedded message has been introduced. With the help of this function the offender can evaluate the messages found in the unclassified channel.

This paper gives an overview of several types of active attacks against Stego files and the extent of the changes they cause is assessed. An algorithm for protection is proposed in extracting the secret message after the implementation of the reviewed Stego attacks. Robustness is achieved using a special marker placed within the Stego file before embedding a secret message. An assessment and comparison have been made of the proposed algorithm with the help of a statistical and histogram analysis and ratios such as: efficiency coefficient and peak signal to noise ratio (PSNR).

For the experimental studies there was established a base of 100 images in BMP (24-bit) and 100 images in PNG format (with no compression) of a size about 150KB. Generated texts from LoremIpsum are utilized as secret messages varying in size, according to the experiment.

It is experimentally proved that the proposed algorithm successfully extracts the secret message from all of the files after various types of attacks

being made.

2 LITERATURE REVIEW AND BACKGROUND

2.1 Literature Review

The methods in the spatial domain are used most often for the good of stegoprograms because of the the good concealing (invisibility) of the messages, the great Stego capacity and the easy implementation.

One of the best literary reviews for this Steganography is made in [3]. This type of Steganography includes the Least Significant Bit (LSB) method [4, 5, 6, 7] and numerous modifications thereof. The direct methods embed information directly into the bits of the container (with images in the pixels).

With the LSB method both schemes of embedding hidden messages are possible - consistent and scattered. The scattered embedding [8] scatters the message randomly (using a random number generator) in the bytes of the entire container. The LSB methods can be divided into two main types: LSB replacement and LSB matching [9]. With the first type there is a direct substitution of the least significant bits with those of the message. With the second type bytes are being selected, in which the least significant bits of the container coincide with the bits of the message. As a result, the statistical and the other characteristics do not change significantly in the container.

Similar to the replacement of bits with the LSB method, the block BPCS steganography conceals secret data by block substitution. Every bit field of the image undergoes segmentation to identical blocks of pixels (usually 8x8) which are classified into informative and noise-like blocks [10]. Each Steganography method or its modification, an approach or algorithm aims to extract successfully the secret message from the recipient without any losses. To reduce the chance of deciphering the most common solutions there are being added cryptographic means, there are used special means of permuting the message (Arnold transform) and others.

These and other measures would not provide a solution to another important issue in the implementation of the stego communication, namely providing countermeasures against possible attacks against the transmitted data. In [4] both an overview of some types of attacks and comparison of different methods how to submit them are made.

2.2 Background

The main objective of steganography is to attain maximum invisibility of the change after embedding a message hidden in the carrier file. In pursuit of this objective several tasks are formed, some of which are: what is the shape, size and number of the carrier files, what Stegoalgorithm to use, how to increase the reliability of extracting the secret message when there is an intentional attack to the Stego file and others. Protecting a message from an attack means it should be made resistant to external interference, for which countermeasures for particular actions could be undertaken. Robustness lies in the fact that whether after an attack by a third party the presence of the message could be detected, whether one can extract the information, whether there could be added information called noise to help expose the message or whether one can damage or destroy the message in order to break contact between the sender and the recipient of the message.

According to Figure 1 the possible attacks that can be applied to the Stego communication are passive and active.

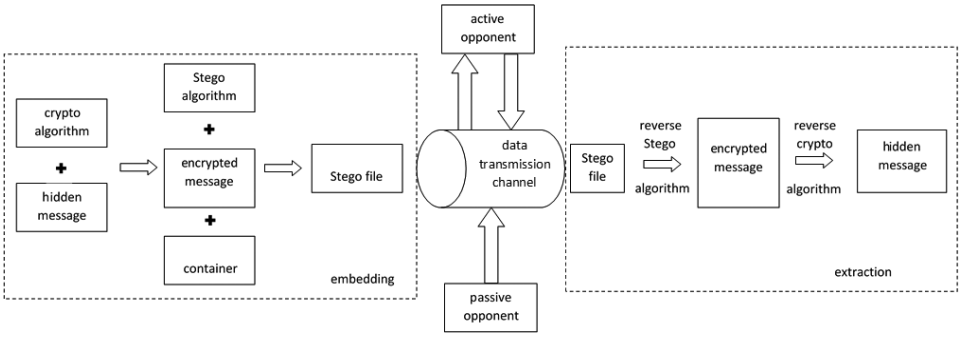

Figure 1: A model of a stegosystem.

To the passive attacks refer those which do not make adjustments to the graphic matrix of pixels and are intended only to listen to the communication channel, analyze the traffic subsequently, but without interfering in it.

To the active attacks refer those which make direct changes to the graphic matrix of pixels - rotation by degree (rotate), mirror rotation (flip) along the horizontal or vertical of the image, inversion of all least significant bits in the image, cutting out part of the image (crop), adding noise to the image, adding different color filters, sharpening of one or more colors and others. With all these changes any defects would be outlined that can expose the hidden message. The Rotate Attack - it is rotating the image, which can be easily applied, for example by using a photo viewing program. Upon

rotation of 90, 180 or 270 degrees there will not be made any changes in the values of the matrix of pixels of the image, but will keep it rotated.

The Flip Attack - could be applied in two versions: rotation by the horizontal and rotation by the vertical using a a photo viewing program. With this attack again there is no direct intervention in the values of the matrix of pixels of the image, but again the hidden message will be lost due to a change in the positions of the pixels.

It is possible to combine both Rotate and Flip Attacks to maximize hindering the extraction of the message. The LSB Inversion Attack is a kind of sterilization procedure that turns the values in the least significant bit to their opposites. If it is 0 it becomes 1, if it is 1 it becomes 0. This spoils the message, wherever it is located in the graphic file.

3 THE PROPOSED METHOD

In order to counter the attacks rotate, flip or their random combination, the addition of a marker in the Stego file is proposed. For this reason, the choice of location, size and type of marker represents a very important selection and a step of the operation of the algorithm. It is through this marker that the image could be brought to its normal position subsequently.

A possibility is added to neutralize the LSB Inversion attack in case one cannot find the marker when extracting the message. The LSB method is selected for an embedding algorithm, but with a column modification which represents a change in the reading of the matrix of pixels of the image, column by column rather than row by row.

The reason for this change in the direction of reading is to hamper attempts by third parties to disclose the message. The algorithm can work with BMP and PNG containers without limitation in size, but it is recommended that the size of the carrier file would not exceed 500 KB on grounds of unsuspicion.

3.1 Embedding Process

- The container file name, the extension of the new Stego file and the message that will be hidden into the container are entered.

- It is verified whether the size of the message would take more space than the size of the container after embedding. If the message would not fit into the container a message is displayed that the container is rather small for that message.

- It is verified whether the graphic file is from the RGB color scale, and if it is not a system message is displayed for incorrect color model and a file in RGB is required.
- After that the message is embedded together with the marker.
- A message for the successful embedding is displayed and the new Stego file is created with the specified extension at the input.

3.2 Recovery Process

- A Stego file name is entered from which the message will be extracted.
- It is verified whether the color scale is RGB, and if it is not an error message is displayed.
- The presence of the special marker is verified:
  - *backslash* if the marker is in its normal position, the algorithm continues with the message extraction;
  - *backslash* if the marker is not found in its expected position, the algorithm finds the marker, sets the image into its normal position and continues with the message extraction;
  - *backslash* if the marker is not found in its expected position, and could not be found within the file an attempt to neutralize the LSB Inversion attack is made. If the marker is found the algorithm continues with the message extraction, otherwise the processing is terminated;
  - *backslash* if the marker is not found, the processing is terminated.
- The message is extracted from the container.

4 EXPERIMENTS AND RESULTS

Python programming language is selected for the program realization of the proposed algorithm. One of the advantages of that language is that there is a great set of instruments for working with images.

A created data base with the volume of 100 images in the BMP format and 100 images in the PNG format serves as containers. These images are downloaded from the Internet with almost the same size ranging between 150-151KB.

Table 1: Coefficient of efficiency of a large and small text in BMP and PNG files

Image	Resolution		Coefficient of efficiency	
	Width	Height	Large Msg	Small Msg
BMP Image(1)	193	262	0.1240754	0.0121491
BMP Image(2)	259	194	0.1248656	0.0122265
BMP Image(3)	225	225	0.1239308	0.0121349
BMP Image(4)	259	194	0.1248656	0.0122265
BMP Image(5)	300	168	0.1244841	0.0121891
PNG Image(1)	284	177	0.1248110	0.0122221
PNG Image(2)	318	158	0.1248706	0.0122269
PNG Image(3)	275	183	0.1246696	0.0122073
PNG Image(4)	239	211	0.1244125	0.0121823
PNG Image(5)	259	194	0.1248656	0.0122265

The hidden text messages are randomly generated by Lorem Ipsum, with the size of 18816 bytes and 1837 bytes, respectively designated as a large (Large msg) and small (Small msg) message.

When assessing the results two ratios are taken into consideration: embedding efficiency and Peak signal to Noise Ratio (PSNR).

Embedding efficiency is the ratio of the size of the message that can be embedded in the container to the size of the container. By this index the extent of filling of the container towards the secret message is calculated.

$$E_e = \frac{V_{mes}}{V_c} \tag{1}$$

where:
V_{mes} volume of the secret message in KB or MB
V_c volume of the container in KB or MB.

In order to assess the extent of changing the Stego file towards the container the ratio PSNR is calculated.

$$PSNR = 10 \log_{10} \left(\frac{L^2}{MSE} \right) \tag{2}$$

where:
L is the maximum value which is used for color identification

MSE represents the cumulative mean square error between the original and the altered image with dimensions MxN, calculated by the formula:

$$MSE = \frac{1}{MN}\left[\sum_{i=1}^{M}\sum_{i=1}^{N}\left(f(i,j) - f'(i,j)\right)^2\right] \tag{3}$$

To calculate the embedding efficiency ratio many experiments with files of both BMP and PNG formats with two different-sized messages have been made. Several of them were randomly selected as the values of the ratio are given in Table 1.

The results obtained with Large Msg, show that the proposed algorithm entirely satisfies the requirements of the LSB method because the maximum amount of the hidden message is 1/8 of the size of the carrier file.

To determine the extent of change of the carrier file, Table 2 shows a sample of the calculations of PSNR for all files within the created database.

Table 2: PSNR with a large and small text in the BMP and PNG files

Image	PSNR	
	Large Msg	Small Msg
BMP Image(1)	56.2510229	66.5060446
BMP Image(2)	53.4948633	63.7029486
BMP Image(3)	56.3355592	66.2664526
BMP Image(4)	63.4417178	73.5036246
BMP Image(5)	54.8133128	63.6587126
PNG Image(1)	56.2619112	66.3094490
PNG Image(2)	56.3644753	65.8723360
PNG Image(3)	55.7159502	65.5518688
PNG Image(4)	56.1743256	66.2419477
PNG Image(5)	56.3865227	66.4391713

From the results it is seen that the extent of invisibility is high, which provides grounds for continuing the research towards robustness with extracting the message after the attacks in question.

A comparison is made in Table 3 between images that are alike where one and the same information has been hidden by means of both the SilentEye program and the proposed method. From the results obtained it is evident that the noise level is lower when using the proposed method.

Histogram analysis

Table 3: PSNR with a large text in the BMP and PNG files between the "SilentEye" and the Proposed method

Image	PSNR	
	SilentEye	Proposed
BMP Image(1)	52.7291150	56.2510229
BMP Image(2)	52.5829221	53.4948633
BMP Image(3)	52.6480900	56.3355592
BMP Image(4)	60.3758582	63.4417178
BMP Image(5)	53.0257589	54.8133128
PNG Image(1)	52.8604215	56.2619112
PNG Image(2)	52.8696059	56.3644753
PNG Image(3)	52.7940312	55.7159502
PNG Image(4)	53.3054027	56.1743256
PNG Image(5)	52.2089748	56.3865227

The following figures (Fig. 2 to 4) show a histogram analysis of the image in the BMP and PNG format with a large message embedded.

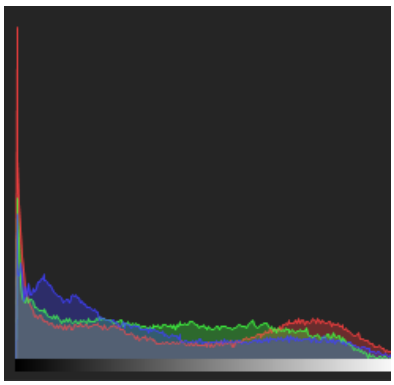

Figure 2: Original BMP

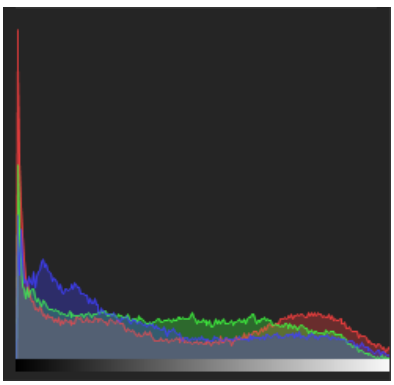

Figure 3: With a large text BMP

It is evident that the differences in the histograms of the original and the stego files are insignificant, which indicates an even change of the values in the application of the algorithm.

Analysis to detect the hidden message

The analysis for unsuspicion of the stego file occupies an important part in assessing each Stego method. For this purpose, the hidden message is

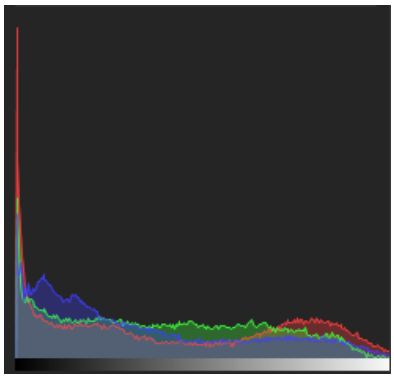

Figure 4: Original BMP

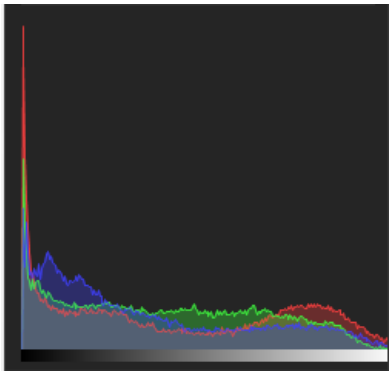

Figure 5: With a large text BMP

embedded in images that are the same with a maximum size for the particular file. To calculate the probability of detecting a hidden message two methods are used. One is the Chi-square - for statistical Steganalysis and the other one is described in [11]. The results obtained show that the Chi-square method detects the hidden message in 27% of the files, and the second method - in 34%.

The last experiments are aimed at exploring the algorithm for robustness when extracting secret messages after the attack. Table 4 shows the results after applying the self-attack or in combination on randomly selected files from the base with images when extracting messages.

The results indicate that secret messages can be successfully protected by the proposed algorithm despite the attacks described in Table 4.

5 CONCLUSIONS

This report provides an approach to ensure robustness in extracting the secret message from a Stego file after flip and rotate attacks. The ability to counteract these attacks becomes possible with the use of specially defined marker placed before embedding of the message itself. After the experimental studies it was established that the proposed algorithm brings low changes in the carrier file, satisfies the LSB method in terms of the capacity of embedded message and securely extracts the secret message after the attacks flip, rotate and LSB Inversion or their random combination.

For the future development of the tested algorithm there could be used a variety of generators of pseudo random sequences [12, 13] with the aim of spread spectrum embedding of the information.

Table 4: Extracting messages after various attacks

Image	Attack	Extract a message
BMP Image(1)	Rotate 90°	Yes
BMP Image(2)	Horizontal Flip	Yes
BMP Image(3)	Rotate 180°	Yes
BMP Image(4)	Rotate 270°	Yes
BMP Image(5)	Vertical Flip	Yes
PNG Image(1)	Rotate 90° + Horizontal Flip	Yes
PNG Image(2)	Rotate 270° + Vertical Flip	Yes
PNG Image(3)	Rotate 180° + LSB Inversion	Yes
PNG Image(4)	Rotate 180° + Horizontal Flip	Yes
PNG Image(5)	Vertical Flip + *Rotate*90° + LSB Inversion	Yes

6 ACKNOWLEDGMENTS

This work was supported in part by Project RD-08-119/2016 Steganography in mobile devices and 3-dimensional modeling. The Project is realized by the financial support of the Konstantin Preslavski University of Shumen, Bulgaria.

References

[1] Agranovskii, A., A. Balakin, V. Gribunin i S. Sapojnikov. *Steganografiq, cifrove vodqne znaki i steganoanaliz.* Moskva: Vuzovskaq kniga ,2009, ISBN 978-5-9502-0401-2

[2] Gribunin V., I.Okov i I. Turincev. *Cifrovaq steganografiq.* Moskva: Solon-Press, 2002.

[3] Ming, C., Z. Ru, N. Xinxin and Y. Yixian, Analysis of Current Steganography Tools: Classifications & Features. Proceedings of the 2006 International Conference (IIH-MPS06)

[4] Koduri, N. Information security through image steganography using least significant bit algorithm. M.S. thesis. University of East London, retrieved 13 april 2012.

[5] Johnson, N., S. Jajodia, Exploring steganography: Seeing the unseen,*IEEE Computer*, 31(2)(1998) 26-34.

[6] Judge, J. Steganography: Past, present, future. SANS Institute publication, *http* : *//www.sans.org/reading*$_r$*oom/whitepapers/stenganography/*552.*php*, 2001.

[7] N. Provos, N., P. Honeyman, Hide and seek: An introduction to steganography, *IEEE Security and Privacy*, 01 (3)(2003)32-44.

[8] Marvel, L., C.Boncelet, C. Retter.Spread Spectrum Steganography. IEEE Transactionson image processing. 8:08, 1999.

[9] P. Moulin and R. Koetter, Data-hiding codes, *Proceedings of the IEEE*, 93 (12)(2005) 2083-2126.

[10] H. Verma, A Singh and R. Kumar, Robustness of the Digital Image Watermarking Techniques against Brightness and Rotation Attack, *(IJCSIS) International Journal of Computer Science and Information Security*, Vol. 5, No. 1, 2009

[11] Mansour, R. F., Awwad, W. F., Mohammed, A. A., A robust method to detect hidden data from digital images. Journal of Information Security, 2012, 3(2), 91.

[12] Kordov, K. M. Modified Chebyshev map based pseudo-random bit generator,*American Institute of Physics Conference Series*, Vol. 1629. 2014.

[13] Kordov, K. Modified Pseudo-Random Bit Generation Scheme Based on Two Circle Maps and XOR Function, *Applied Mathematical Sciences* 9.3 (2015): 129-135.