

Image Based Steganography Using Modified LSB Insertion Method with Contrast Stretching

Antoniya Tasheva, Zhaneta Tasheva, Plamen Nakov

Abstract: *The main objective of this research paper is to suggest a new steganography method based on a LSB insertion method and contrast stretching image histogram modification. The stego-images, obtained using the proposed data hiding method, are robust to RS steganalysis. The application of proposed method has comparatively higher secret data embedding capacity than classical LSB insertion method. The experimental results shows that the RS steganalysis fails to detect the presence of the secret message even its length is 50% of the maximum possible embedding length in the cover image.*

Key words: *Steganography, Data Hiding, LSB, Contrast Stretching, Histogram Modification.*

INTRODUCTION

Steganography is known long ago before the era of computer technologies, but gets more and more popular as the coverage of Internet gets wider and modern communication channels transmit massive amounts of information. Despite Cryptography, where secret data is being transformed into an unreadable message, Steganography lies on the idea of hiding the act of communication by embedding the secret message into other digital data, while maintaining its observable characteristics. The advantage of steganography to cryptography is the fact that the possible attacker doesn't know if there is communication process or not and thus may not conduct their attack. Nowadays, data hiding techniques are widely used for security and copyright protection purposes, as well as in authentication, fingerprinting and data mining. Usually, the cover data is some type of media – image, video, audio, or network protocols and other text. It is relied on the fact that humans' eyesight and hearing are not perfect and can't detect small changes in the colours or the sounds/frequencies.

Hiding information inside images is a popular technique nowadays. It is necessary to hide a message inside an image without changing its visible properties. To do this the cover image can be altered in some areas with many color variations, so the modifications will cause less attention. The most common methods for hiding information inside images involve the usage of the Least-Significant Bit (LSB), masking and filtering, and transformations of the cover image [5]. The changes in a cover image reflect its properties which determine the ability of the attacker to detect them easily by steganalytic algorithms. Attacks and analysis of hidden data may take several forms: detecting, extracting, and disabling or destroying hidden data [6]. The most commonly used attacks are lossy compression, geometrical modifications, denoising or image enhancement [11]. As these image processing techniques modify the content of the image bits, they make the hidden message recovery impossible.

Recent studies of steganography algorithms and steganalysis involve rule-based adaptive batch steganography, steganography in different colour models using an energy adjustment applying wavelets, lossless steganography for speech communications, histogram modification based data hiding techniques and data mining techniques for steganalysis [7], [8]. The stegoimages that are produced by using histogram modification data hiding techniques are robust against main geometrical attacks such as rotation, scattered tiles and warping, as well as other main attacks [12].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

CompSysTech'17, June 23–24, 2017, Ruse, Bulgaria

© 2017 Association for Computing Machinery. ISBN 978-1-4503-5234-5/17/06...\$15.00

<https://doi.org/10.1145/3134302.3134325>

Based on the above, the main objective of this research paper is to propose a new steganography algorithm based on LSB insertion method and some histogram modifications inherently resistant to main geometrical attacks. In this work, the proposed approach mainly utilizes the contrast stretching as histogram based image processing enhancement technique. The resulting stego-images are reasonably robust against RS stegoanalysis and with high secret data embedding capacity.

Rest of the paper is organized as follows. Fundamentals of the RS stegoanalysis and contrast stretching are explained in the section below. Section three contains some details of the proposed modified data hiding method. In section four are evaluated some experimental results from RS steganalysis of the proposed modified LSB insertion method with contrast stretching along with comparison of the results of classical LSB insertion method. Finally, some remarks are presented in the last section.

RELATED WORKS

This section presents the fundamentals of LSB data hiding method, contrast stretching, and RS and visual steganalysis which are fundamental for the proposed new data hiding method and its steganalysis.

LSB Insertion Method, RS and Visual Steganalysis

LSB Insertion Method is one of the most common data hiding methods which is based on manipulating the LSBs of the cover image by their direct replacing with the message bits [5]. Two common methods are used to determine the exact location where the secret message is to be placed into the cover image. They are sequential and pseudo-random methods. The sequential method starts on a specific pixel and inserts message bits in all subsequent pixels until the message is fully embedded. The pseudo-random method generates a pseudo-random sequence that determines the bytes of the cover image in which the secret message bits are embedded.

The advantages of the LSB method are its simplicity and higher hiding capacity. Its disadvantages are low robustness and easy destruction of embedded data by simple attacks. This type of steganography is detectable even if there is low embedding rate by RS steganalysis.

RS steganalysis is originally proposed as a reliable detection method of LSB steganography in color and grayscale images in 2001 [3] and has proved to be very effective steganalytic method that accurately estimates the length of the embedded message in a digital image, for several LSB insertion methods. The embedded message length is obtained by inspecting the lossless capacity in the LSB and the shifted LSB plane, because when a message is inserted in the LSB plane, its content is considered to become randomized and the correlation between the LSB and the shifted LSB plane is reduced.

Visual Attacks are the simplest form of steganalysis that involve inspection of the stego-image with the naked eye to identify any kind of degradation. Due to the direct human involvement, the visual steganalysis is not an effective method for testing large volumes of stego-images. A visual attack could be done directly by displaying the spatial domain of the whole image or by the observation of a LSB plane. Images typically contain approximately equal number of 1's or 0's in their LSB plane, whereas texts often have more 0's than 1's. This inconsistency can be observed by the human eye. A successful visual attack not only allows detecting inconsistencies within a stego-image, but it also reveals how the LSB insertion method operates (sequential or randomized embedding). It also allows estimation of the embedding message length [6].

Contrast stretching

Image enhancement is a process of improving the quality of a digital image by manipulating the dominance of some of its features or by decreasing the ambiguity between different image regions [4]. The aim of image enhancement is to improve the perception of image information for people or to provide a better input for an automated image processing. The enhancement operations are performed in order to modify the image brightness, contrast or the distribution of the color levels [2]. As a result the pixel values (intensities) of the output image $I_N(x,y)$ will be modified according to the transformation function $T(.)$ applied to the input values $I(x,y)$:

$$I_N(x,y) = T(I(x,y)) \quad (1)$$

Contrast stretching is one of the histogram-based image enhancement operations, that attempts to improve the contrast in an image by stretching the range of the intensity values to a desired range [1]. It is often used to brighten the original image if its histogram is mostly located on the left side. The idea is to stretch the contrast over the whole available range:

$$I_N(x,y) = 255 \cdot \frac{I(x,y) - I_{\min}}{I_{\max} - I_{\min}}, \quad (2)$$

where $I_N(x,y)$ is the intensity of the pixel (x,y) after the contrast stretching process, $I(x,y)$ is the intensity of the input pixel (x,y) , and I_{\min} and I_{\max} are the minimum and maximum intensity values in the input image, respectively.

As a result of such auto processing technique by full-scale histogram stretching (2) the image has a higher contrast and a better visibility of details.

In the case of dynamic histogram range expansion, the initial range of image intensity $[I_{\min}, I_{\max}]$ is expanded to new range $[\min, \max]$:

$$I_N(x,y) = \frac{I(x,y) - I_{\min}}{I_{\max} - I_{\min}} (\max - \min) + \min, \quad (3)$$

where $I(x,y)$ and $I_N(x,y)$ are the intensity levels of the input and output pixels, respectively.

MODIFIED LSB INSERTION METHOD WITH CONTRAST STRETCHING

The original LSB data hiding method is based on direct replacing of the Least Significant Bits (LSBs) of the cover image with the message bits. This simple process, however, is vulnerable to steganalytic methods, namely statistical steganalysis and RS-steganalysis. In order to develop an algorithm which avoids the above mentioned steganalysis, a further image processing is required to be done after hiding the message. This new process should not change the values of the LSBs of the produced stego-image, but must change the distribution of flipped bits. Moreover, the function of this process must be linear.

As one can see from equation (3), if $\min = I_{\min}$, i.e. the contrast stretching is done only for a new maximum value, the both transformations - contrast stretching and contrast compression are completely reversible. The contrast stretching is done by the formula

$$I_S(x,y) = \frac{I(x,y) - I_{\min}}{I_{\max} - I_{\min}} (\max - I_{\min}) + I_{\min}, \quad (4)$$

where \max is a new maximum image intensity, $\max > I_{\max}$. The contrast compression is realized by the equation

$$I_C(x,y) = \frac{I(x,y) - I_{\min}}{I_{\max} - I_{\min}} (\max - I_{\min}) + I_{\min}, \quad (5)$$

where $\max < I_{\max}$.

For a true color (24-bits) images we have used the compression and stretching operations on the Red, Green and Blue colors, described by the formula:

$$C_N(x,y) = \frac{C(x,y) - C_{\min}}{C_{\max} - C_{\min}} (\max - C_{\min}) + C_{\min}, \quad (6)$$

where $C(x,y)$ and $C_N(x,y)$ are color levels of the input and output pixels, respectively; C_{\min} and C_{\max} are minimum and maximum color level values in the input image, respectively; and min and max are minimum and maximum available color level values in output color histograms, respectively.

Stego-encoding

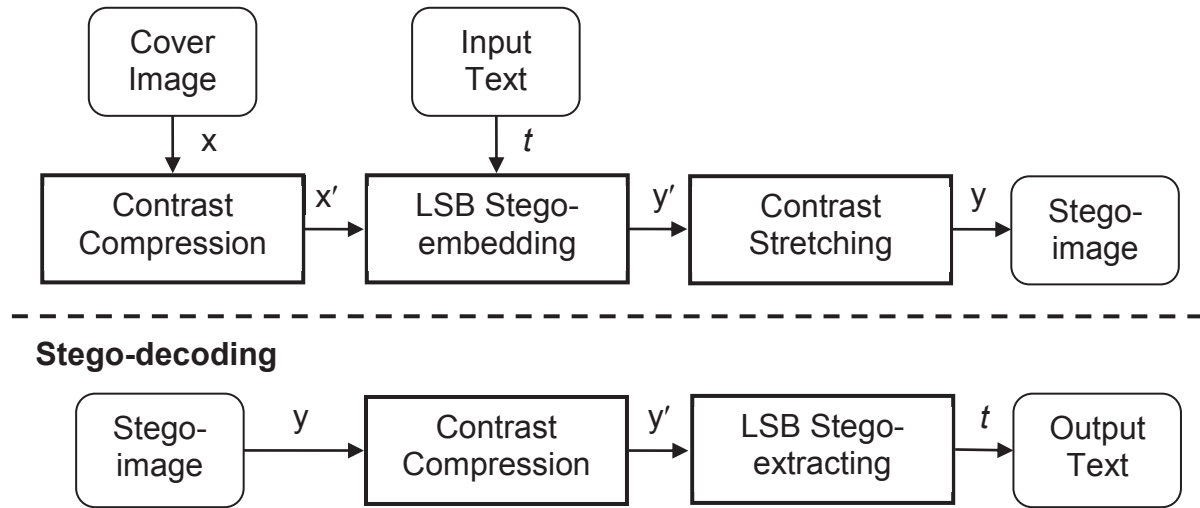


Figure 1. Stego-encoding and stego-decoding schemas of the proposed method

Since the histogram stretching changes the image quality, a contrast compression of the used cover image is necessary before the LSB embedding of the input text in order to keep the stego-image quality approximately equal to the cover image quality.

Thus the algorithm of proposed stego-encoding schema (see Figure 1) is:

Inputs: Cover image x with maximum color values R_m , G_m and B_m ; Input text t .

Steps:

1. A contrast compression of cover image x to the new lower maximum color values R_{mN} , G_{mN} and B_{mN} is done. As a result a compressed cover image x' is generated.
2. As a result of LSB stego-embedding of input text t into compressed cover image x' the compressed stego-image y' is produced.
3. Contrast stretching of compressed cover image x' back to initial maximum color values R_m , G_m and B_m , whereat the final stego-image y is done.

Output: Stego-image y

In order to extract the text hidden in a stego-image only two steps are necessary. The algorithm of stego-decoding schema shown in Figure 1 is:

Input: Stego-image y

Steps:

1. A reversed stego-image contrast compression is applied to the stego-image y with the used in step 1 of the stego-encoding schema maximum color values R_{mN} , G_{mN} and B_{mN} , which produces a compressed stego-image y' .
2. Extracting the output text t by LSB Stego-algorithm from compressed stego-image y'

Output: Output text t

EXPERIMENTAL RESULTS

The performance of the proposed LSB insertion with contrast stretching algorithm has been evaluated with ten RGB true color images. Text messages with approximately 10%, 20%, 30%, 40% and 50% of the maximum embedding size of every image were produced. The messages were embedded in cover images first with standard LSB insertion method and then with the proposed LSB insertion with contrast stretching method. Every test is performed with two preprocessing insertion text methods, without text encryption and with text encryption with pseudorandom bit generator [9], [10] and for 10%, 20% and 30% contrast stretching of the maximum colour levels of cover images. Thus 300 stego-images are tested, produced from 10 cover images, 5 input texts, and 2 insertion text methods and 3 contrast compressions.

RS Steganalysis

The RS steganalysis have been applied to the above mentioned 300 stego-images with two flipping masks $M = [0 \ 1 \ 1 \ 0]$ and $M = [1 \ 0 \ 0 \ 1]$. The results for the two used flipping masks are not significantly different. There are also no substantial variations in experimental results applying the RS Steganalysis to stego-images produced by proposed LSB insertion with contrast stretching method with preprocessing text compression and without it. Applying preprocessing text compression only affects the results of RS Steganalysis to stego-images produced by classical LSB insertion method. Therefore Table 1 presents calculated values of actual number of flipped pixels using the RS Steganalysis of "Butterfly.bmp" image for Red, Green and Blue colors, and its average value only for used preprocessing text compression. The rows with contrast stretching of 0% in the Table 1 show results from the classical LSB insertion method and other rows with contrast stretching of 10%, 20% and 30% show experimental results from proposed modified LSB insertion method with contrast stretching. Figure 2 shows the average values of actual number of flipped pixels (marked with stars) and the estimated percentage of flipped pixels (marked with a solid line) using the RS Steganalysis of "Butterfly.bmp" image.

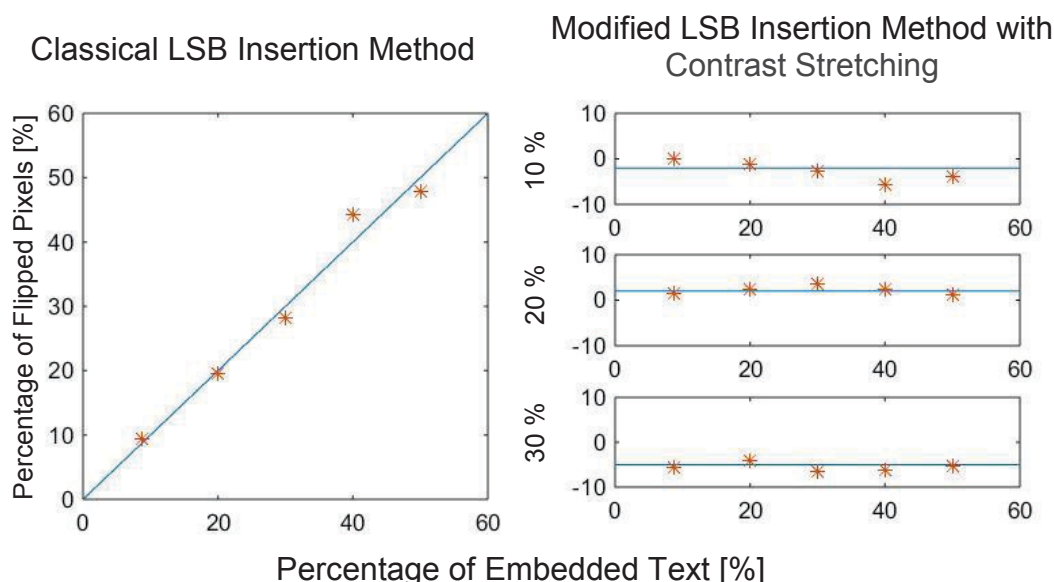


Figure 2. Estimated percentage of flipped pixels (solid line) and average actual number of flipped pixels (stars) using the RS Steganalysis of "Butterfly.bmp" image for classical LSB insertion method and modified LSB insertion method with contrast stretching 10%, 20% and 30%

Table 1. Values of actual number of flipped pixels using the RS Steganalysis of “Butterfly.bmp” image for Red, Green and Blue colors, and their average value

Text [%]	Contrast Stretching [%]	Red	Green	Blue	Average
10	0	0.1109	0.0813	0.0907	0.0943
	10	-0.0320	0.0850	-0.0499	0.0010
	20	0.0039	0.0689	-0.0286	0.0147
	30	-0.1174	0.0395	-0.0875	-0.0551
20	0	0.2138	0.1616	0.2117	0.1957
	10	-0.0403	-0.0510	0.0561	-0.0118
	20	0.0622	0.0480	-0.0381	0.0240
	30	-0.1114	0.0587	-0.0708	-0.0412
30	0	0.3088	0.2486	0.2911	0.2828
	10	-0.0578	-0.0710	0.0510	-0.0259
	20	0.0700	-0.0145	0.0528	0.0361
	30	-0.1364	0.0353	-0.0909	-0.0640
40	0	0.4754	0.3472	0.5077	0.4435
	10	-0.1284	-0.0898	0.0479	-0.0568
	20	0.0695	-0.0262	0.0261	0.0231
	30	-0.1136	0.0248	-0.0993	-0.0627
50	0	0.5271	0.4031	0.5063	0.4789
	10	-0.0877	-0.1178	0.0903	-0.0384
	20	0.0605	-0.0307	0.0101	0.0133
	30	-0.1130	0.0433	-0.0890	-0.0529

The difference between the estimated and the actual length of the embedded message with classical LSB insertion method is below 5%, which proves the effectiveness of RS steganalysis in estimating the message size. The experimental results from RS steganalysis of stego-images produced by proposed modified LSB insertion method with contrast stretching are quite different. Regardless of the length of the embedding message, even at 50%, the RS steganalysis fails to detect the presence of the secret message, i.e. it produces negative values for the estimated message length or the values are all below the 5%.

Visual Steganalysis

The direct visual inspection of the tested images did not identify any kind of quality degradation of stego-image compared to the cover image. In fact, in a normal communication scenario the cover image usually is not available to the attacker. A visual inspection of the LSB plane of the stego-images also did not reveal the presence of a message, because the pseudo-random LSB substitution steganography is used.

Figure 3 presents the original cover image Butterfly.bmp, stego-image with 50% text message embedded with classic LSB insertion method Butterfly_C50.bmp and stego-image with 50% text message embedded with modified LSB insertion method with contrast stretching 10% Butterfly_M50_S10.bmp. Moreover, quality measures used in image steganography evaluation, Mean Square Error (*MSE*), Peak Signal to Noise Ratio (*PSNR*) and Signal to Noise Ratio (*SNR*), are given.

Although, the visual differences between Stego-images produced with both methods were not observed, the smaller PSNR value with proposed modified LSB insertion method with contrast stretching determines the larger distortions. But, the reduction of PSNR is

within acceptable limits. Moreover, this is on account of increasing the embedded text up to 50% of the maximum possible length (100 % = 3 bits per pixel for true color images).


Cover image	Stego-images with 50 % Embedded Text Message	
	Classic LSB Insertion Method	Modified LSB Insertion Method with Contrast Stretching 10%
		
Quality Measures:		
MSE	0.0374	0,0126
PSNR	54.0844	46.2825
SNR	48.0934	40.2915

Figure 3. Cover image and stego-images produced with Classic LSB Insertion Method and Modified LSB Insertion Method with Contrast Stretching and its quality Measures

CONCLUSIONS AND FUTURE WORK

The proposed image steganography method, based on modified LSB insertion method with contrast stretching, is proved to be undetectable by RS steganalysis, which is successful in message length estimation of stego-images produced by classical LSB insertion. The analysis of experimental results shows that the RS steganalysis fails to detect the presence of the secret message even if its length is 50% of the maximum embedding length L_m in a $m \times n$ true color image ($L_m = 3.m.n/8$ [bytes]).

We're focusing our future research on estimating the contrast stretching level which will keep acceptable quality of stego-images produced by proposed modified LSB insertion method with contrast stretching.

REFERENCES

- [1] Al-amri, S. S., N. V. Kalyankar, and S. D. Khamitkar. Linear and non-linear contrast enhancement image. *International Journal of Computer Science and Network Security* 10.2, 2010: 139-143.
- [2] Bovik, A. C. *Handbook of Image and Video Processing*. Academic Press, 2000.
- [3] Fridrich, J., Miroslav Goljan, Rui Du, Reliable Detection of LSB Steganography in Color and Grayscale Images, *IEEE multimedia*, 8(4), 2001: 22-28.
- [4] Gonzalez R., C., R. Woods. *Digital image processing*. Prentice-Hall, Inc., 2002.
- [5] Kaur, A., Kaur, R., Kumar. A Review on Image Steganography Techniques. *International Journal of Computer Applications*, 2015, 123.4.
- [6] Laskar, S. A., Hemachandran, K. A Review on Image Steganalysis techniques for Attacking Steganography. In: *International Journal of Engineering Research and Technology*, Vol. 3. No. 1. ESRSA Publications, 2014.

- [7] Marçal, A. R., & Pereira, P. R. MARÇAL, André RS; PEREIRA, Patricia R. A steganographic method for digital images robust to RS steganalysis. In: *International Conference Image Analysis and Recognition*. Springer Berlin Heidelberg, 2005. p. 1192-1199.
- [8] Sajedi H. *Recent Advances in Steganography*. InTech. 2012.
- [9] Stoyanov, B., K. Kordov, A novel pseudorandom bit generator based on Chirikov standard map filtered with shrinking rule, *Mathematical Problems in Engineering*, 2014, art. no. 986174.
- [10] Tasheva, A., Nakov, O., & Tasheva, Z. About balance property of the p-ary generalized self-shrinking generator sequence. In: *Proceedings of the 14th International Conference on Computer Systems and Technologies*. ACM, 2013. p. 299-306.
- [11] Yalman, Y., & Erturk, I. A new histogram modification based robust image data hiding technique. In: *Computer and Information Sciences, 2009. ISCIS 2009. 24th International Symposium on*. IEEE, 2009. p. 39-43.
- [12] Yalman, Y., Akar, F., Erturk, I. Contemporary Approaches to the Histogram Modification Based Data Hiding Techniques. *RECENT ADVANCES IN STEGANOGRAPHY*, 2012, 53.

ABOUT THE AUTHORS

Assoc. Prof. Antoniya Tasheva, PhD, Department of Computer Systems and Technologies, Technical University of Sofia, e-mail: atasheva@ti-sofia.bg.

Prof. Zhaneta Tasheva, D.Sc., Department of Computer Systems and Technologies, Faculty of Artillery, Air Defense and KIS, National Military University of Bulgaria, and Department of Communication and Computer Technics, University of Shumen, e-mail: zh.tasheva@mail.bg.

Plamen Nakov, student, Department of Computer Systems and Technologies, Technical University of Sofia, e-mail: plamennkv@gmail.com

ACKNOWLEDGMENTS

This work is a result of a project supported by the National Science Fund, Ministry of Education and Science, Bulgaria via FINANCIAL SUPPORT FOR PROJECT OF JUNIOR RESEARCHERS – 2016 [Grant Number DM07/5 – 15.12.2016]