ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT METHOD FOR STEGANOGRAPHY USING JPG/JPEG AND PNG FILES

Wamiliana[1*], Mustofa Usman[1], M. Azram[2], Faiz A. M. Elfaki[2], Astria Hijriani[3], and Pandya Panditatwa[3]

[1]Department of Mathematics, Lampung University, Indonesia

[2]Department of Sciences, Faculty of Engineering, IIUM, Kuala Lumpur, Malaysia

[3] Department of Computer Science, Lampung University, Indonesia

[*]Email: wamiliana.1963@fmifa.unila.ac.id

ABSTRACT*: Nowadays, the security of data transmission is one of the important aspects in digital data transmission. In this era, sending messages via computers or other gadgets are highly used, the attackers can easily intercept the data during transmission process. Therefore, if there is a secret message, then it can be easily seen. One method for sending data without making curiosity is using the steganography where a secret message can be transmitted in such a way so that attackers are not aware of the existence of something in the message. In this research, we built a digital steganography system using Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) method. We use .jpg file for hiding the message, .png file for the output, .txt for the message. The procedures for applying AMELSBR method are Capacity Evaluation, Minimum Error Replacement and Error Diffusion. The result shows that the AMELSBR method is able to manage for hiding and restoring files without causing excessive distortion (noise) in stego image, and has a possibility of returning most files for image manipulation such as the change of image brightness and contrast for the black and white color dominan. However, the method is resistant to image cutting (crop).*

Keywords: Steganography, Adaptive Minimum Error Least Significant Bit Replacement, brightness, contrast, crop

INTRODUCTION

Data in digital format is an important media in this era. The rapid development in information technology influences the way of life, including the dependency of people to computers or other electronics devices. Using digital media a message can be received within seconds, not hours or even days like before. We can notice this phenomenon where now there are not so many people send greetings card by air mail (post). They prefer sending it by short message service (SMS), email, or social media (facebook, twitter, etc) to post. However, sending a message or information using electronic media has a problem, security. It is possible that the adversaries or hackers intercept the secret information during data transmission. To overcome this problem we can use cryptography or steganography.

Sending secret messages using cryptography technique may overcome this problem, but since the secret message is encrypted and the result is a meaningless message, it may cause curiosity of people. Thus it is possible that some people who are very curious about the message try to do cryptanalysis to attack or open the secret message. Therefore Steganography is an alternative technique to overcome this problem.

Steganography is an art of hiding a message into another message [1]. This method use other media for hiding data or secret information during transmission process. Steganograhy in general is quite secure and does

not make people curious because the secret information is embedded into certain file. The file for hiding the secret information usually pictures, voice, etc.

The method used in this application is Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR). This method proposed by Lee and Chen [2]. In this method, the process of inserting the secret information is done into three stages which are: Capacity Evaluation, Minimum-Error Replacement and Error Diffusion. AMELSBR also used by [3] but they used picture under .bitmap files on both cover and stegoimage. In this research we use cover object (file for hiding the secret information) in .jpg or .jpeg file, and the stegoimage (output) in .png file, and the data (secret information) is in .txt file. Next, we will discuss the method of adopting the AMELSBR briefly in Section 2, and then we willl discuss the Implementation and Results in Section 3, and followed by Conclusion in Section 4.

2. MATERIALS AND METHOD

[2] proposed the Adaptive Minimum Error Least Significant Bit Replacement method, in which they used black and white picture as cover. Later, [4] implemented this method using 24 bit true color image, while [3] implemented this method using .bitmap file for both cover and stegoimage. In our method we use .jpg or .jpeg file for cover because these types are produced millions every day by digital cameras or mobile phones. The picture below describes the stages of our research:

Before doing insertion process we must evaluate the capacity of the cover and find the value of *color variation*. After finding the value of color variation, this value is processed to get the capacity for K bit, and then determine if we need to change the k +1th bit by embedding error value. The embedding process in AMELSBR method start by dividing the cover into blocks size 3 x 3 pixels [5]

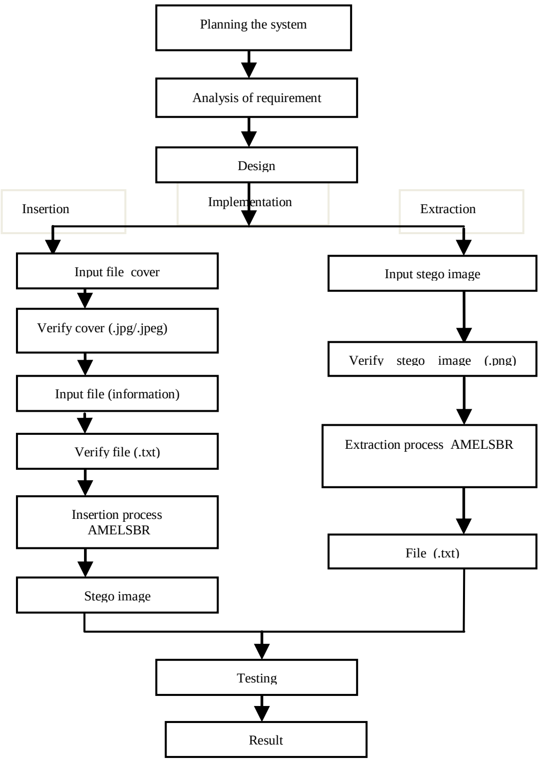


Fig. 1: Research stages

.

The steps for insertions process are :

a. Input file picture (cover)
b. Verify the file picture (must be in .jpeg/.jpg format).
c. Input file (secret information)
d. Verify the file picture (must be in .txt format).
e. Process using AMELSBR.

The steps for extraction /retrieval process are:

a. Input file picture (stego image).
b. Verify the stego image file (must be in .png format).
c. Process using AMELSBR.

We use .jpeg or .jpg for input cover. The reasons for using these files are:

a. On the legal site www.jpeg.org is stated that everyday millions of pictures taken by digital cameras or mobile phones are on the .jpg format [1]. This fact tells us that pictures on .jpg or .jpeg format are in common used.
b. .jpg also recorded at International Standardization Organization (ISO),
c. .jpg also recorded at International Electrotechnical Commission (IEC).

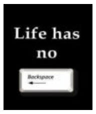
For output (stego image) we use .png. The reasons for using this file are [6]:

a. .png pictures are *lossless compression* [6],
b. .png is recorded at International Standardization Organization (ISO),
c. .png is recorded at International Electrotechnical Commission (IEC),
d. .png is recorded at World Wide Web Consortium (W3C).

3. IMPLEMENTATION AND RESULTS

We use 5 files (. jpg) as input cover where every file differs on size as in table 1.

Table I: The Five Files Use For Testing (Jpg)

NO.	PICTURE (.JPG)	SIZE (CM)	PIXEL SIZE	MEMORY SIZE (KB)
1.		8,47 x11,29	240 x 320	6,68
2.		20,99 x 13,44	595 x 381	9,00
3.		31,75 x 19.86	900 x 563	74,7
4.		36,12 x 28,89	1024 x 819	116
5.		21.17 x 15.06	600 x 427	333

The process of insertion and extracting are running smoothly and in general we cannot see the different between the cover image and the stegoimage (see Table 2). We use .txt file which is “***The Quick Brown Fox Jumps Over the Lazy Dog,.;'[]\<>?:"{}|=-_+)(*&^%$# @!~`1234567890***”.

Table 2: The Cover and Stegoimage

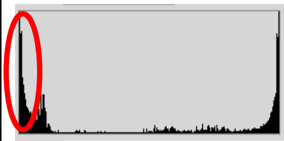
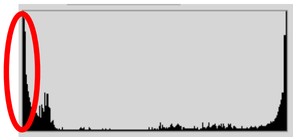
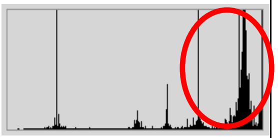
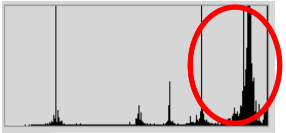
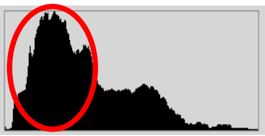
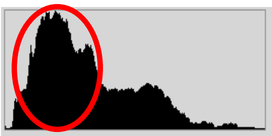
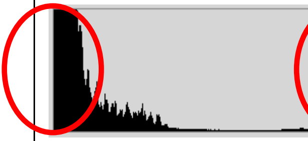
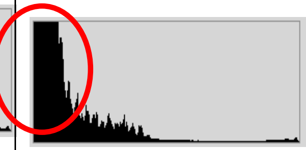
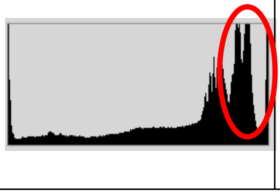
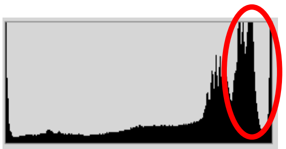
NO.	Picture (.jpg)	Stego Image (.png)
1	 6,68 KB	 25,3 KB
2 .	 9,00 KB	 35,6 KB
3 .	 74,7 KB	 516 KB
4 .	 116 KB	 462 KB
5 .	 333 KB	 458 KB

The reason to use this file is the sentence consists all of a to z letters, numbers, and the characters on common keyboard. The testing is done with 30 repetitions. Table 3 show the histograms of the file before insertion and after insertion (stegoimage).

From table 3 we can see that there are a little differences between the histogram of cover and stego image. If there is no action done to the stego image (such as cropping, changing brightness or constrast), the .txt file inserted on all of the cover files can be extracted without any changing as in the original file.

In order to know what is the effect of some actions done to stego image, we do some testing on the stego image by changing the brightness and constrast, and also doing crop. The intervals for changing brightness and contrast are -150, -120, -90, -60, -30, 30, 60, 90, 120, 150. Note that we do changing on stegoimage, not cover image. The testing is running 30 times for every changing interval.

Table 3: Histogram of Cover and Stegoimage

NO .	Histogram before file is inserted (cover)	Histogram after file is inserted (stego image)
1.		
2.		
3.		
4.		
5.		

The result for brightness and contrast testing can be seen on the in tables 4, 5 and 6:

Table 4: Brightness Testing

Interval Scale / Stegoimage	-150	-120	-90	-60	-30	30	60	90	120	150
1	-	-	√	√	√	√	√	-	-	√
2	√	-	√	-	√	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-

Note : √ : the file is able to be extracted (retrievable)
- : the file cannot be extracted

After testing by changing the interval scale of brightness we can conclude that out of ten interval scales, 60% the .text file can be retrieved (extracted) from the stegoimage 1 that has white dominan (rgb(255,255,255)) or black dominan (rgb(0,0,0)), and 30% from stegoimage 2. Similar with brightness testing, the result of contrast testing on ten interval scales also shows that 70% the .txt file can be extracted for stegoimage 1 and stegoimage 2. For other stegoimage, the .txt files inserted cannot be extracted .

Table 5: Contrast Testing

Interval scale / Stegoimage	- 150	- 120	- 90	- 60	- 30	30	60	90	120	150
1	√	√	√	√	√	√	√	-	-	-
2	√	√	√	√	√	√	√	-	-	-
3	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-

The last testing is cropping. We do crop the stigma by cutting 1/3 part of stegoimage. The cropping (cutting) is done on the top, bottom, right, and left sides of the stegoimage. We repeat the testing 30 times for every stegoimage.

Table 6: Crop Testing

Sides / Picture	Top	Bottom	Right	Left
1	-	√	√*	-
2	-	√	√	-
3	-	√	√	-
4	-	√	√	-
5	-	√	√	-

√* : only partially can be extracted.

From Table 6 we can see that for every stegoimage, we can retrieve or extract the the message (.txt file) when the cropping is done on 1/3 parts of the bottom or on the right sides of the stegoimage.

We also want to note here that after cropping 1/3 parts on the right side of stegoimage 1 we did not get the original file. Only part of the file can be extracted which is :

***The Quick Brown Fox Jumps Over the Lazy Dog,* 1234567890.**

.

CONCLUSIONS

From the experiments we can conclude that based on our data, the .jpg/.jpeg files are good alternative choices of media covers for steganography technique because these files are easily found and most of digital cameras produce these files. If there is no action done to the stegoimage, then the original file can be extracted easily without any changing. In addition, using only usual sight, there are no differences between the stegoimages and the covers. However, the user might pay attention when modify the stegoimage. Most of brightness and constrast changing will make the files are not able to be extracted. But, most cropping on 1/3 parts of the right or bottom of the stegoimages will recover or extract the original files. Therefore, we also can conclude that AMELSBR methods inserts the .txt file on the top and left side of the cover file. Besides, the size of the inserted files also must be under consideration.

REFERENCES

[1] Sellars,D. *An Introduction to Steganography*. [Online]. Available: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/ stego.html, (2006).

[2] Lee, Y. K., and Chen, L. H. An *Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*, [Online]. Available : http://citeseer.ist.psu.edu/205600.html/lee99adaptive.pdf, (1999).

[3] Prayudi, Y and Kuncoro, S. P. "Implementasi Steganografi Menggunakan Teknik Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)". The national Seminar: Application of Information Technology (SNATI), Yogyakarta, (2005).

[4] Gan, M. D. *Chameleon Image Steganography*. [Online]. Available: http://chameleonstego.tripod.com/downloads/Chameleon_Technical paper.pdf,(2003).

[5] Bailey, K., Curran, K., and Condell, J. "An Evaluation of Automated Stegodetection Methods In Images"[Online]. Available: http://www.ittconference.com/anonftp/pdf/2004%20presentations/ presentations/session%20a/Karen%20Bailey-1.ppt. (2004).

[6] Bither, Bill. *Benefits of the PNG Image Format*,. [Online]. Available : http://www.atalasoft.com/png , (1999).