The Hybrid Methods of Column Transposition with Adaptive Minimum Error Least Significant Bit Replacement(AMELSBR) Using file jpg / jpeg and png

Wamilliana[1], Mustofa Usman[1], Astria Hijriani[2], Warsito[3], and Roni Setiawan[2]
[1]Dept. of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Lampung
[2]Dept. of Computer Science, Faculty of Mathematics and Natural Sciences, Universitas Lampung
[3]Dept. of Physics, Faculty of Faculty of Mathematics and Natural Sciences, Universitas Lampung

Abstract
The development of rapid technological demands a strong security system, especially in the process of sending digital data.The more layers of security the less chance the data will be stolen by unauthorized parties.In this case, cryptography is a concept to secure a message by encrypting the message so that is becoming difficult to be understood by others, while the art of steganography is to hide secret messages into other messages in such a way so that other people are not aware of the existence of something in the message. In this research, we built a hybrid system using Column Transposition and Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) web-based, with media messages to be sent as text file format (.txt), inserted into the media image file format (.jpg) as input (cover) and produces an image with the type of file (.png) as stego image. Using eight pictures with different colors dominant as cover, the result shows that AMELSBR managed to hide files and restore files that have been inserted earlier without causing distortion (noise) excessive stego image. The Column Transposition method affects the result of the manipulation of images such as brightness and contrast changes in pixel values. This increased the number of characters so that the number of columns and rows be increased.The images are resistant to image manipulation form of a cut (crop) and can restore the messages contained in the cropped image on the bottom and right with a certain scale cuts. Some media messaging such as WhatsApp, Line and Blackberry Messenger cannot return a message for applying the system of image compression algorithms while email can.

Keywords
Cryptography, steganography, column transposition, Replacement (AMELSBR).

1. Introduction

The rapid technological developments allow humans to communicate and exchange information away in a short time.With electronic media are connected through the internet makes communication a vital part that affects the lives. Most of people prefer to send a message via the short message service (SMS), email or social media (such as WhatsApp, Line, Blackberry Messenger, and so on) rather than sending messages through the post office because they can be done in a matter of seconds. However, delivering of messages using electronic media has a problem of security.The possibility of infiltration through the actions made by the network not authorized (hackers) to retrieve the data.To increase the security in data transmission process used cryptography and steganography.

Cryptography is the hieroglyph [1]. Cryptography has two main processes : encryption and decryption.The encryption process is to change the message to be sent (plaintext) into irregular shapes up to no meaning so that it is hard to understand (ciphertext), while the decryption process is restoring files encrypted (ciphertext) be added to form the original file(plaintext). Steganography is an art of hiding messages into other media [2]. The media that can be used to insert such messages, pictures, music, or video. The messages encrypted (ciphertext) which will then be inserted into one of these media produces an output image (stego image). In this paper we develop an applications which used the hybrid of classical cryptography which is column transposition and one of steganography method which is Adaptive Minimum Least Significant Bit Error Replacement (AMELSBR). Subsequently, in Section 2 we will discuss about column transposition and AMELSBR, and then we will discuss the implementation and results in Section 3, and is followed by conclusions in Section 4.

2. Materials and Methods

The reason for choosing image JPG / JPEG as the cover image is that this image format into an international standard format and images in these formats can be found easily in mobile phones and digital cameras. In addition, based on www.jpeg.org , the format image received ISO (International Standardization Organization) and IEC (International Electro technical Commission), while the PNG format (ping) is used as an output for PNG file using the compaction method does not eliminate part of the image (lossless compression), thereby reducing excessive noise in the image. The PNG file format also get a certificate of ISO and IEC in 2003. Before the message is

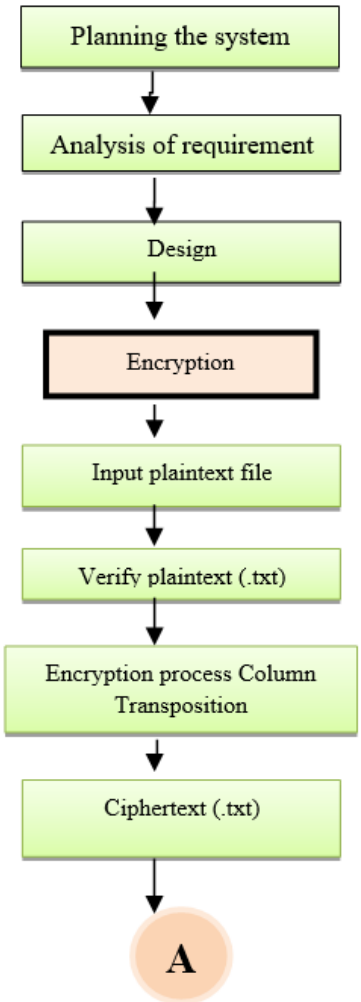
Manuscript received July 5, 2017
Manuscript revised July 20, 2017

inserted into an image, firstly the message encrypted with column transposition.

[5]. The steps being taken to encrypt messages include:

1. Reading the message file(plaintext)
2. Determining the size of the columns and rows
3. Mapping into columns and rows
4. Transposition of the column corresponding key.
5. Print the results of each column transposition (ciphertext)

Then the ciphertext file inserted in the cover image. Before pasted there are several processes that must be performed including checking the capacity of insertion and color variation value. The value of color variation is used to obtain K bits that will be used for the error value, conversion into a binary message, and insert a binary value into 3x3 pixel of RGB pixel [6]. After doing all of those steps we obtained a stegoimage as an output image. The following is the flowchart of the procedure:



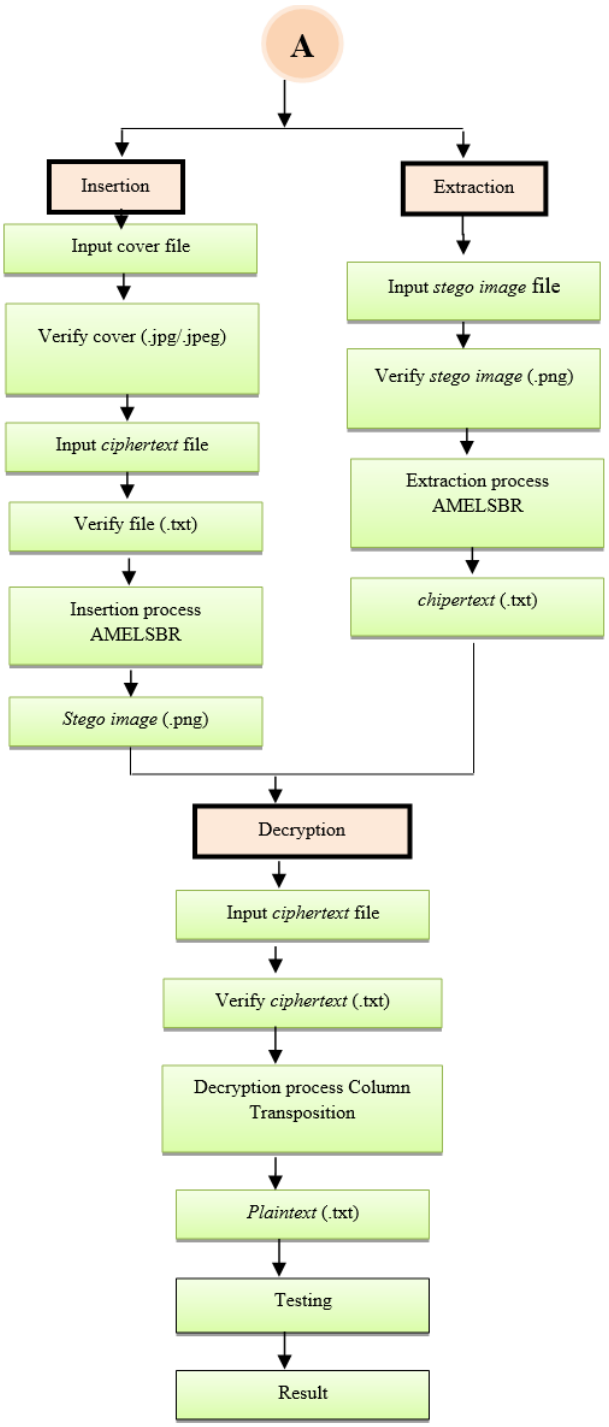


Fig. 1 Stages Research

3. Results and Discussion

The following table shows the images that used as the cover image.

Table 1: Cover Image

No	Image (JPG)	Pixel Size	Image Size (KB)
1		1280 x 800	277
2		1625 x 1080	201
3		1020 x 850	103
4		1024 x 768	76.6
5		1440 x 900	395
6		1600 x 1000	236
7		1600 x 1000	56.9
8		1024 x 768	135

The text **"The quick brown fox jumps over the lazy** dog **,.; '[] \ <> ?:" {} | = -_ +) (* & ^% $ # @! ~ `12345 67890**" will be inserted in the cover image. The reason for using this message is the same as [7]. This text firstly encrypted using transposition of the column. In this research we made that the rows and columns are dynamic, therefore to accommodate this feature we set a concept in the form of columns and rows for the determination of the size NxN (0<=N<=ROUND(SQRT(length message))). If the message length < N^2 then the value column = rows = (N-1), if the length of the message> N^2 then the value column = rows = (N + 1), whereas if the message length = N^2 then the value column = rows = N. That message is in length 84 (including the space character). Suppose that N = 9, N^2 = 81 will be entered in the condition where the message length> N^2 so the value column=rows=10 [5]. In a column transposition normally the space character is sometimes allowed nulls (space left blank).

In this research the space character is replaced with an underscore character, with the aim of showing the existence of a space character instead of nulls.

Table 2: Encryption Process

column / row	1	2	3	4	5	6	7	8	9	10
1	T	h	e	_	Q	u	i	c	k	_
2	B	r	o	w	n	_	F	o	x	_
3	J	u	m	p	s	_	O	v	e	r
4	_	t	h	e	_	L	a	z	y	_
5	D	o	g	,	.	;	‘	[	]	\
6	<	>	?	:	“	{	}	|	=	-
7	_	+	)	(	*	&	^	%	$	#
8	@	!	~	`	1	2	3	4	5	6
9	7	8	9	0						
10										

The random of even column and then followed by odd column is used as the key to encrypt the message. For example, the order of the columns that occurs when the array is a column transposition 2,4,6,8,10,1,3,5,7,9. To see the details column transposition in the case of earlier tests can be seen in Table 3 below.

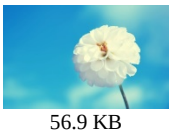
Table 3: Continuation of Encryption Process

column / row	1	2	3	4	5	6	7	8	9	10
1	h	_	u	c	_	T	e	Q	i	k
2	r	w	_	o	_	B	o	n	F	x
3	u	p	_	v	r	J	m	s	O	e
4	t	e	L	z	_	_	h	_	a	y
5	o	,	;	[	\	D	g	,	'	]
6	>	:	{	|	-	<	?	"	}	=
7	+	(	&	%	#	_	)	*	^	$
8	!	`	2	4	6	@	~	1	3	5
9	8	0				7	9			
10										

So the result of encryption (as ciphertext) are **"hruto> +! 8 _wpe, :(` 0 u__L; {& 2 covz [|% 4 __r _ \ - # 6 TBJ_D**

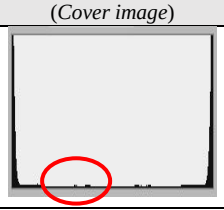
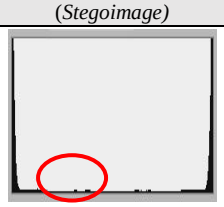
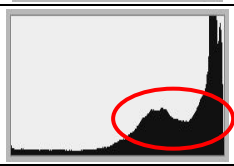
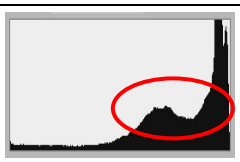
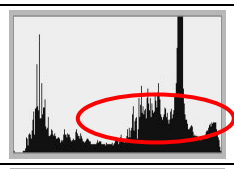
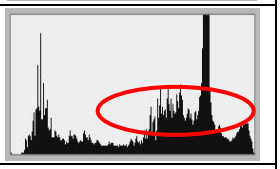
<_ @ 7 eomhg?) ~ 9 Qns _. "* 1 iFOa '} ^ 3 kxey] = $ 5 ". Then the ciphertext is inserted into the cover image to generate stego image. The comparison between the cover image and stego image can be seen in Table 4.

Table 4: Comparison Cover Image and Stego Image

No	*Cover Image*(.jpg)	*Stego Image*(.png)
1	 277 KB	 379 KB
2	 201 KB	 839 KB
3	 103 KB	 595 KB
4	 76.6 KB	 430 KB
5	 395 KB	 1980 KB
6	 236 KB	 1870 KB
7	 56.9 KB	 502 KB
8	 135 KB	 1010 KB

The size of the image (stegoimage) is getting bigger because there is an inserted message in the image. At a first glance the two images look the same and there is no difference. The histogram in Table 5 shows that the differences is very hard to be detected.

Table 5: Histogram of Cover Image and StegoImage

Image	Before Inserted (*Cover image*)	After Inserted (*Stegoimage*)
1		
2		
3		
4		
5		
6		
7		
8		

If stego image directly extracted without any change in the image (such as brightness, contrast and crop), then the chiper text can be extracted without changes to the original text file. To see the robustness of the method we do test the stego image by image changes through brightness images, contrast and crop.The reason to test using these three features because when someone get an image from somebody, the most common thing he done with the image is to do the brightness or contrast to see it

clearly. Moreover, someone who get the image may also do the cutting of the image. The following is the brightness changes made at intervals of -150, -120, -90, -60, -30, 30, 60, 90, 120, 150.

Table 6: Brightness Testing

Interval / Stego image	-150	- 120	- 90	- 60	- 30	+ 30	+ 60	+90	+120	+150
1	-*	-	-*	-	-*	-	-	-	-	-
2	-	-	-*	-*	-*	-*	-*	-	-	-*
3	-	-*	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-	-
8	-	-	-	-*	-	-*	-	-	-	-

(-): The message cannot be returned to the original message

(-*): There are some characters of the message back, but the file does not return to original message after decryption.

In the brightnest testing, there are some files that contained some character messages. However, after the decryption code does not create a message. This happens because of the changing in pixel value in the image causes the addition of a character.The addition of a number of characters affects the decryption process because of the number of columns and rows in the process of decryption and encryption must be the same in order to obtain the original message. Increasing the number of characters occurs in all messages in all stego image. To test image manipulation (contrast) is done at intervals of -50, -30, 30, 60, 90. The test results contrast can be seen in Table 7 below.

Table 7: Contrast Testing

Interval / Stegoimage	-50	-30	30	60	90
1	-*	-*	-*	-*	-
2	-*	-*	-*	-*	-
3	-*	-	-	-	-
4	-	-	-	-	-
5	-	-	-	-	-
6	-	-	-	-	-
7	-	-	-	-*	-
8	-	-	-	-	-

(-): The message cannot be returned to the original message

(-*): There are some characters of the message back, but the file does not return to original message after decryption

The result of testing on brightness gave no image can restore a message after the change of contrast. Although there are some files that recover some character messages after decryption, but no original messages were returned.

Next, we did testing by performing cropping at the top, bottom, right and left stego image by 1/3.The results of this test can be seen in Table 8 below.

Table 8: Crop Testing

Side / Stegoimage	Top	Bottom	Right	Left
1	-	√	√	-
2	-	√	√	-
3	-	√	-	-
4	-	√	-	-
5	-	√	√	-
6	-	√	√	-
7	-	√	√	-
8	-	√	-	-

(√): Files can be recovered.

(-): The message cannot be returned to its original message.

In the crop testing, returned messages contained in cutting the bottom and right with the 1/3 scale images.In addition to those three types of testing, we did also testing by sending stego image through social media, such as WhatsApp, Line, Blackberry Messenger (BBM) and Email. The test results can be seen in Table 9 below.

Table 9: Delivery stego image with media

Media / Stegoimage	*WhatsApp*	*Line*	BBM	*Email*
1	-	-	√	√
2	-	-	√	√
3	-	-	√	√
4	-	-	√	√
5	-	-	-	√
6	-	-	-	√
7	-	-	√	√
8	x	x	√	√

(√): File (message) can be recovered.

(X): The file is missing (no message is inserted in the *stego image).*

(-): The message cannot be returned in full.

The message inserted cannot be retrieved and tends to be lost because of media WhatsApp, Line and Black Berry Messenger implement image compression algorithms. The stegoimage is a PNG image when it is transmitted to the media is changed into JPG format when it is received. As a result, the pixel values change. The BBM can restore most of the messages due to the request of HD (High Definition) and email does not apply compression

algorithm so that the file is sent unchanged format and size.

4. Conclusion.

From the above discussion we can conclude that the use of JPG / JPEG provide much choice for the cover image, because it can be easily obtained. Image manipulation can restore images that allow the cutting beam (crop) the bottom and right. Column transposition method is not able tto fully support the image manipulation (brightness, contrast and crop because the pixel value of stego image changes and makes extra characters so that the number of columns and rows increases. Therefore, the decryption process cannot restore the original message. Some medias used to send stego image are not able to be used because they are not apply image compression algorithms not like email.

References

[1] Mollin, Richard.An Introduction to Cryptography Second Edition.Chapman and Hall / CRC, London. (2006).
[2] Sellars, D.An Introduction to Steganography, [Online].Available:http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html (2006)
[3] Lee, YK, and Chen, LH. An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement,[Online].Available: http://citeseer.ist.psu.edu/205600.html/lee99adaptive.pdf (1999).
[4] Stinson, D.R. Cryptography Theory and Practice. CRC Press.Florida. (1995)
[5] Munir, Renaldi. Kriptografi. Informatika, Bandung.(2006)
[6] Bailey, K., Curran, K., and Condell, J. "An Evaluation of Automated Methods In Stegodetection Images".Available:http://www.ittconference.com/anonftp/pdf/2004%20presentations/presentations/session%20a/Karen%20Bailey-1.ppt (2004)
[7] Wamiliana, Mustofa Usman, M. Azram, Faiz AM Elfaki, Astria Hijriani, and Pandya Panditatwa Adaptive Minimum Error Least Significant Bit Replacement Method for Steganography Using JPG/JPEG and PNG Files, Science International (Lahore), Vol 27 No. 6. Pp. 4987 – 4990. (2015)