Implementation of Integration Blowfish Cryptography Methods with Blend Steganography to Improve Security Text Messages

By Imam Riadi

WORD COUNT 3726 TIME SUBMITTED 18-JUL-2017 10:17AM
PAPER ID 30572118

International Journal of Computer Applications (0975 – 8887)
Volume 132 – No.7, December2015

Implementation of Integration Blowfish Cryptography Methods with Blend Steganography to Improve Security Text Messages

Rahmad Zainul Abidin
Indonesia of Islamic University

Yudi Prayudi
Indonesia of Islamic University

Imam Riadi
Ahmad Dahlan University

ABSTRACT
Various techniques to ward off evil that uses information technology have been made, such as the delivery of messages by combining techniques Blowfish cryptography with steganography DCS (Dynamic Cell Spreading). However, DCS has a weakness when compared to steganography Blend. The disadvantage is the DCS insert text data in all the colors RGB. This will result in more pixels change and easily detected image embed text (stego image), while Blend is fewer the pixel changes. Based on DCS weakness, this research proposes the incorporation of steganographic techniques Blend as data embed technique and the Blowfish cryptography as data encryption technique.

This research testing process to MSE and PNSR analysis, to determine the rate of change of the original image (cover image) with stego image. Then Blend MSE PNSR results compared to the DCS.

The comparison showed that PSNR Blend value is higher than the value of DCS and MSE Blend value is lower than the value of DCS. Obtained conclusions that the method of integration Blowfish cryptography with Blend steganography is better than the DCS steganography.

General Terms
Information Security, Information hiding.

Keywords
Cryptography, Blowfish, steganography, Blend.

1. INTRODUCTION
Crime at this time already much involved in information technology and communications. Utilization of computers, mobile phones, email, the Internet and other digital devices can invite parties to commit crimes based communication technologies. Therefore, needed the techniques to secure the delivery of the text so that other people are not taking the text message to the crime.

Among the techniques to secure the delivery of text messages is by using steganography and cryptography [12]. Steganography is a method to hide a message within another message which other people do not know that the message in it there is a message that is more important. Steganography development goal is to maintain a data message is pasted on media digital image that can not be detected by other applications that in the digital image hidden secret text messages.

One technique delivery of text messages using steganography is Padmaa and Venkataramani study [7] that uses steganography algorithms Blend. Steganography Blend is a technique the development of steganography LSB or steganography previous . However, in this study only using steganography alone, a text message that will be inserted is not encrypted in advance. This data encryption is necessary, because according to Wijaya and Prayudi [11] to improve the security of the delivery of the text messages is combine the method of steganography and cryptography. Therefore, Padmaa and Venkataramani studi [7] research is necessary to develop techniques with combining steganography Blend with cryptographic techniques.

Technique text messaging with combining steganography and cryptography has also been done, such as the research that has been conducted by Wijaya [10]. Incorporation method using the Blowfish cryptography and steganography DCS (Dynamic Cell Spreading). However steganography DCS has a weakness when compared to steganography Blend. The disadvantage is the DCS insert text messages to all color bit RGB (red, green, blue). This will result in any more pixels to change color and the robustness in a text message when the stego image is manipulated / edited the text message data is easy lost or damaged. Unlike the steganography Blend in the insertion of data using the R indicator to trigger the data inserted into green or blue. So that the color of each pixel will be slightly discolored. R indicator is also causing the system to maintain a text message when the stego image edited the text message data is not easily lost or damaged.

Based on the explanation of weakness on research conducted Wijaya [10], this research take Blend technique as a method of security on steganography. As for the data encryption using the Blowfish as cryptography. The same cryptographic techniques this study with previous research, because according Haldankar & Kuwelkar [6] has become a Blowfish cryptographic algorithm that is fast, able to work at 26 clock cyle per byte, and process calculations using only simple addition and XOR.

So the focus of this research lies in how to build a system incorporation with a Blowfish cryptographic method with steganography Blend. is meant by establishing a system here is to create algorithms incorporation of these methods, then realized in the form of an application program as the implementation incorporation of the Blowfish cryptographic method with steganography Blend.

2. BASIS THEORY
In the basis of this theory will describe the theories that underlie this research in particular to secure the technical data on Cryptography and Steganography.

2.1 The Concept of Steganography
Steganography is the science and art of data hiding. A steganographic system in such a way hiding content of data into a cover of the media that can not be suspected by ordinary people that do not establish a suspicion to those who see it. In the past people used tattoos hidden or invisible ink to convey the contents of steganography. Current technology and computer networks provide an easy way to use communication networks for Steganography [3].

According Gutte [5] Modern Steganography objective is to maintain a media that is difficult to detect, but because the steganographic system still has weaknesses that leave a trail behind the cover of the media image so that the secret can be found. Even the secret contents were not disclosed.

2.2 The Concept of Blend Steganography

Steganography Blend sort are used to select the order line first randomly and then a color indicator or channel set embedding data between the other two channels (green and blue). In a color image, the color red can be chosen as a color indicator in which the most significant bits in each pixel. This is used to decide embedding data. Throughout this embedding process, the indicator color can not be changed, because the data to be hidden is usually embedded in a predetermined fashion k bits. This method is used for the pixel embedding process optimally to reduce mean-square error [8]. After the above-mentioned process is completed and 4 stego images generated every line of this compared to the corresponding line in the cover image. This step allows determining the relative deviation of each in relation to the cover image. The Blend algorithm in general can be seen in Figure 1.

Input : plaintext (secret data), key, cover image

Output :stego image with secret data embedded in it

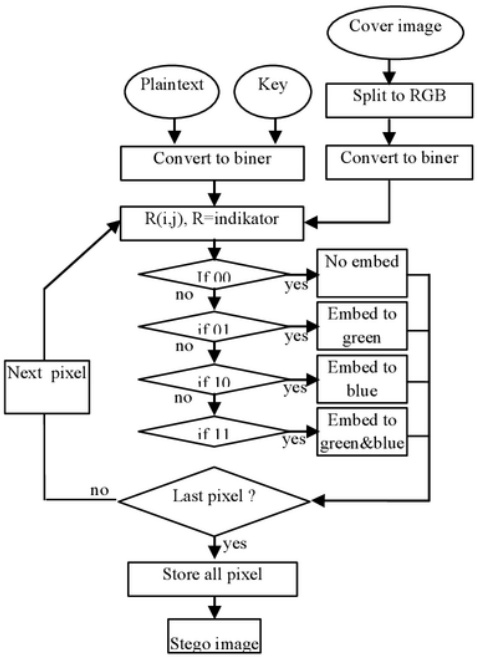

Figure 1 Steganography Blend Algorithm.

Explanation of steganography blend algorithms :

1. Convert plaintext and key to binary format.
2. Split cover image to RGB colour, then convert to binary format
3. Random squence generator to choose the order of row data to be inserted.
4. Check each pixel in R with the following conditions: Position 2 LSB for each pixel in the i line row and j column with R indicators:

   If R(i, j, 7,8) = 00 then no embed

   elseif R(i, j, 7,8) = 01 then embed to green

   elseif R(i, j, 7,8) = 10 then embed to blue

   Else embed k bits at Green and Blue
5. Repeat steps 4 the amount of data that will be embed in the cover image.
6. Store all pixels.
7. The result becomes 1 picture stego image.

2.3 The Concept of Cryptography

Cryptographic algorithm consists of an encryption algorithm (E) and decryption (D). The encryption algorithm using an encryption key (EK), whereas decryption using decryption key (DK). In general, encryption and decryption operations can be described mathematically as follows:

EK (EK) = C → E (encrypt process)

DK (C) = M → D (the decrypt process)

In which: M = plain text, C = ciphertext

At the time of the encryption process of encrypting messages with a key EK M and C. The resulting message decryption process, message C is described by using the key DK to produce a message M the same as before.

Therefore, the security of a message depends on the keys are used and do not depend on the algorithm used so that the algorithm published and analyzed, as well as products which can be produced using these algorithms in general. It does not matter if someone knows the algorithm that we use, as long as he does not know the key used, he still can not understand the message.

2.4 The Concept of Blowfish Cryptography

Kumar and Karthikeyan [13] explains that the Blowfish was designed by Bruce Schneier which is intended for 32-bit microprocessors up with cache memory. Blowfish was developed to meet the design criteria as follows:

1. Fast. In the optimal implementation of Blowfish can reach 26 cyle per byte clock.
2. Arranged neatly (compact). Blowfish can run on less memory than 5 kb.
3. Simple. Just use a simple operation that sum, XOR and search tables (lookup table) on a 32-bit operand.
4. The security was variable. Length key (key) can vary and can be as long as 448 bits (56 bytes).

The Blowfish algorithm can be seen in Figure 2 and explanation of cryptographic algorithms Blowfish

1. Form P-array initials as many as 18 pieces (P1, P2, P18) each worth 32-bit. Array P consists of eighteen key 32-bit subkey: P1, P2, ..., P18
2. Form S-boxes 4 pieces each worth 32-bit with input 256. The four 32-bit S-boxes each having 256 entries:

   S1,0, S1,1, ..., S1,255

   S2,0, S2,1, ..., S2,255

   S3,0, S3,1, ..., S3,255

S4,0, S4,1, ..., S4,255

3. Plaintext to be encrypted is assumed as the input, the plaintext taken as many as 64-bit, and what if less than 64-bits then we add bits, so that in later operations in accordance with the data.
4. The result of making earlier divided by 2, 32-bit first so-called XL, 32-bit second is called XR.
5. Next do the operation xor Pi XL = XL and XR = F (XL) xor XR
6. The results of the above operrasi be exchanged XL XR and XR becomes XL.
7. Do as much as 16 times, looping the 16th to do again the process of exchange of XL and XR.
8. On the 17th do surgery for XR = XR xor P17 and P18 XL = XL compl.
9. The last process re-XL and XR unite to become a 64-bit back.

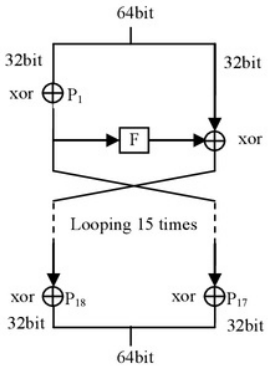

Figure 2 Blowfish Cryptography algorithm.

3. METHODOLOGY

The general flow of the design of Blowfish cryptography methods and steganography Blend can be seen in Figure 3.

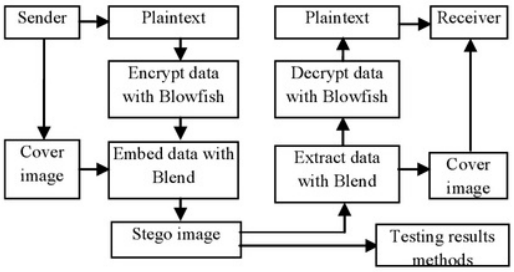

Figure 3 The general flow of the design of methods of cryptography Blowfish and steganography Blend

Explanation of figure 3 Flow Design implementation methods:

1. The sender input two files, namely the plaintext file as a text message that will be sent and the cover image file as an image file which is only used for confidential data plaintext.
2. Plaintext data is encrypted using Blowfish cryptography, the result is called cypertext.
3. The cypertext embedded on the cover image file with Blend steganographic techniques.
4. Results of that process into a file called stego image. Stego image will be performed on the test results, as will be explained later.
5. To retrieve the plaintext data back then extract the data carried on the stego image with Blend steganographic techniques. The output is a file cover image and cypertext.
6. Cypertext decrypted with Blowfish cryptographic, output in the form of plaintext.
7. Recipients get two files are plaintext or secret message and the cover image file.
8. The result of the output of this application form stego image file which is then tested the results of the method, which is described in the following discussion.

4. IMPLEMENTATION AND DISCUSSION

4.1 Program BlenBlow

In this phase will be the implementation of the integration program Blowfish Cryptography with Blend Steganography using Visual Basic 6.0. Programs are made known by the name of BlenBlow.

4.2 Sample Pictures and Plaintext

Sample text used to embed into the cover image in this study is of type TXT file size 5656 bytes

The image samples are taken from the laboratory database SIPI-USC (Signal and Image Processing Institute - University of Southern California) [9]. SIPI image database-USC is a collection of standard images that can be used to study drawing and image analysis. Sample pictures taken are images characterized by aerial photographs from space with color depth of 24 bits per pixel and the TIFF file format, that can be downloaded in *http://sipi.usc.edu/database/database.php* [1].

As for the test image file format is converted into type Bitmap (BMP), because BMP is the standard format used to display images and not change the color compression. Therefore, sample files will be converted first image from TIFF format into BMP with Microsoft Paint program. Figure 4 shows a sample image files as in this study.

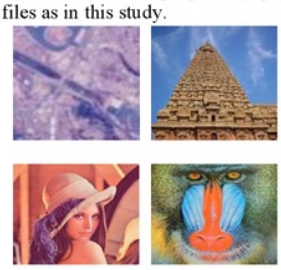

Figure 4 Sample image used

4.3 GUI Display BlenBlow

Applications designed in this study is called by the name of BlenBlow which can be seen in Figure 5.

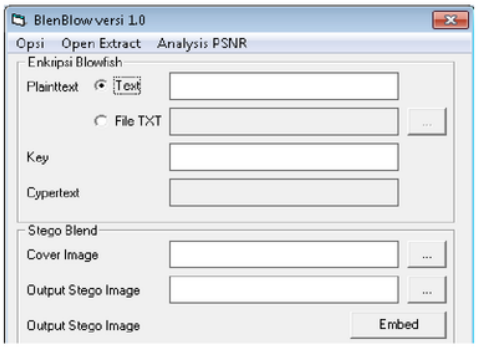

Figure 5 GUI display BlenBlow

4.4 Results and Analysis

Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum value of the signal measured by the amount of noise affecting the signal [2]. PSNR is a standard parameter for assessing the quality of an image objectively by comparing the noise cover image and stego image of the peak signal in decibels (dB) [2]. PSNR is often used to measure the quality of the original image file (cover image) to the image file inserts (stego image). To calculate the PSNR value, must first calculate the value of MSE (Mean Squared Error) using the equation:

$$MSE = \frac{1}{M.N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(f(x,y)-g(x,y)\right)^2$$

Description:

f (x, y) = the value of pixel cover image

g (x, y) = the value of pixel stego image

M, N = the dimension of the image

Then calculate the PSNR value using the following equation:

$$PSNR = 20.\log 10\left(\frac{255}{\sqrt{MSE}}\right)$$

In this research, PSNR is used to determine the noise level of the cover image and stego image. The higher the value PNSR the less changes in the cover image and stego image, meaning that steganography will be undetectable. MSE high value indicates poor quality of data embeded and value PSNR a high value indicates very good quality data embeded. Stego good image should have a value of PSNR above 35dB [4].

Security parameters used in the analysis is to measure the value PNSR PNSR on stego image steganography DCS and Blend. The higher the value, the more undetectable PNSR stego image, means the better in improving the delivery of text messages and the lower the value the better MSE in improving the delivery of text messages.

PNSR analysis process in this study using 4 sample images (cover image). At each sample image inserted text message with the technique of DCS and Blend. Then in each specified stego image PNSR value. PNSR value is then compared with the Blend DCS stego image. Table 2 and table 3 displays the comparison results of the analysis of DCS PNSR stego image and Blend.

Table 2 Comparison analysis stego image MSE PNSR DCS.

Sample image	Red		green		Blue	
	MSE	PNSR	MSE	PNSR	MSE	PNSR
Sky	3,15	40,49	3,85	39,87	3,73	40,11
Temple	3,19	40,29	3,69	39,53	3,66	40,03
Lena	3,12	41,33	3,74	40,36	3,75	40,46
Baboon	4,16	41,39	4,53	40,14	4,85	40,41

Table 3 Comparison analysis stego image MSE PNSR Blend.

Sample image	Red		Green		Blue	
	MSE	PNSR	MSE	PNSR	MSE	PNSR
Sky	0	∞	1,61	46,01	1,38	46,13
Temple	0	∞	1,55	45,32	1,68	45,76
Lena	0	∞	1,64	46,42	1,67	46,32
Baboon	0	∞	2,83	43,21	2,43	43,53

In Table 2 we can see that the value PNSR Sky image with DCS steganographic data embeded in Red worth 40.4943 and MSE value 3.1523, while the Blend steganography PNSR value ∞ and the value of MSE 0. Blend PNSR value is higher than the PNSR DCS and Blend lower MSE value of MSE DCS, then the resulting stego image on Sky Blend better picture of DCS. In the picture Temple value PNSR steganography DCS in Red worth 40.2948 and MSE value 3.1938, while the Blend steganography PNSR value ∞ and the value of MSE 0,0. Blend PNSR value is higher than the PNSR DCS and Blend lower MSE value of MSE DCS, then the resulting stego image in the picture Temple Blend better than DCS. At Lena image steganography DCS PNSR value in Red worth 41.3384 and MSE value 3.1203, while the Blend steganography PNSR value ∞ and the value of MSE 0. Blend PNSR value is higher than the PNSR DCS and Blend lower MSE value of MSE DCS, then the resulting stego image on the image Lena Blend better than DCS. Baboon on the image steganography DCS PNSR value worth in Red 41.3984 and MSE value 4.1637, while the Blend steganography PNSR value ∞ and the value of MSE 0. Blend PNSR value is higher than the PNSR DCS and Blend lower MSE value of MSE DCS, then the resulting stego image on the image Baboon Blend better than DCS.

At 4 the sample image PNSR Blend all grades higher than the value PNSR DCS and Blend lower MSE value of MSE DCS, then the parameter PNSR analysis concluded that Blend steganography is better than DCS steganography. Table 4 provides a summary of difference in value difference MSE PNSR DCS with Blend.

Table 4 MSE and PNSR value difference DCS with Blend

Sample image	Green		Blue	
	MSE DCS to Blend	PNSR DCS to Blend	MSE DCS to Blend	PNSR DCS to Blend
Sky	-2,24	6,14	-2,35	6,02
Temple	-2,14	5,79	-1,98	5,73
Lena	-2,1	6,06	-2,08	5,86
Baboon	-1,7	3,07	-2,42	3,12

In table 4 PNSR Blend value is higher than the value PNSR DCS and MSE Blend is lower then the value MSE DCS, it can be concluded that the steganography Blend better than DCS steganography.

Based on the results of resistance testing and analysis with PNSR, then the conclusion can be made tables that can be seen in Table 5.

Table 5 Conclusion The analysis of DCS and Blend

Test	Security parameters	Result DCS	Result Blend
MSE Analiysis	The lower the MSE value then the higher security stego image	4 image MSE DCS value is higher than Blend	4 image MSE DCS value is lower than Blend
PNRS Analiysis	The higher the PNSR value then the higher security stego image	4 image PNSR DCS value is lower than Blend	4 image PNSR DCS value is highes than Blend

In table 5 it can be concluded that the steganography Blend better than DCS in terms of the endurance (rebustness) test with the difference one of the edited images and better in terms of PNRS analysis with 4 images PNRS Blend value is higher than DCS. The conclusion of the steganography Blend feasible for use as security the delivery of a text message.

5. CONCLUSION

Based on the results obtained from the implementation process and discussion of the research Implementation Method Using Steganography Cryptography Blowfish Blend can be deduced:

1. Increased double security on the delivery of digital texts could implementaion of integration cryptography Blowfish with Blend steganography by using an application called BlenBlow.
2. Based on the results of the analysis can prove that the implementation of the program BlenBlow feasible to use text messaging more secure.

6. REFERENCES

[1]. Autoimager. http://www.autoimager.com/download.asp. Accessed on 1 September 2015

[2]. Ansari, Munawir. (2015). Compare Metode Hybrid Image Watermarking DWT-SVD with RDWT-SVD For Protection In Digital Image. Yogyakarta, Industrial Technology Faculty, Indonesia of Islamic Universitas.

[3]. Boora & Gambhir. (2013). Arnold Transform Based Steganography. International Journal of Soft Computing and Engineering (IJSCE). ISSN: 2231-2307, Volume-3, Issue-4.

[4]. Seddad, A., Condell, J., Curran, K., Kevitt, P.Mc., 2010. Digital Image Steganography : Survey and Analysis of Current Methods. Signal Processing, Elsevier. Northern Ireland, UK.

[5]. Gutte, Chincholkar and Lahane. (2013). Steganography For Two And Three Lsbs Using Extended Using Extended Substitution Algorithm. Ictact Journal On Communication Technology, March 2013, volume: 04, issue: 01.

[6]. Haldankar & Kuwelkar. (2014). Implementation Of Aes And Blowfish Algorithm. International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[7]. Padmaa. & Venkataramani. (2014). Encypted Secret Blend With Image Steganography For Enhanced Imperceptibility Dan Capacity. Tamilnadu India.

[8]. Poornima & Iswarya. (2013). AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.

[9]. SIPI, The USC-SIPI Image Database, website pada http://sipi.usc.edu, diakses pada 24 Agustus 2015.

[10]. Wijaya, Wijaya Satriya. (2014). Integration of DCS Steganography Method In Image With Blowfish Cryptography. Yogyakarta, Industrial Technology Faculty, Indonesia of Islamic Universitas.

[11]. Wijaya, Satriya. & Prayudi, Yudi. (2014). The Concept Of The Hidden Message Using Dynamic Cell Spreading steganographic techniques. Jurnal media informatika, ISSN: 0854-4743, Volume 2. NO. 1, PP 23-38.

[12]. Yadav. (2011). Information Security Using Blend of Steganography and Cryptography. Int. J. Comp. Tech. Appl., Vol 2 (6), 2023-2036. ISSN:2229-6093

[13]. Kumar and Karthikeyan. 2012. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. I. J. Computer Network and Information Security, 2012, 2, 22-28. DOI: 10.5815/ijcnis.2012.02.04

Implementation of Integration Blowfish Cryptography Methods with Blend Steganography to Improve Security Text Messages

ORIGINALITY REPORT

4%

SIMILARITY INDEX

PRIMARY SOURCES

1	Salman, Afan Galih, Bayu Kanigoro, Rojali, Kevin, and Santy. "Application Hiding Messages in JPEG Images with the Method of Bit-Plane Complexity Segmentation on Android-Based Mobile Devices", Procedia Engineering, 2012. Crossref	42 words — 1%
2	www.it.s-t.au.ac.th Internet	31 words — 1%
3	Soumendu Chakraborty, Anand Singh Jalal, Charul Bhatnagar. "LSB based non blind predictive edge adaptive image steganography", Multimedia Tools and Applications, 2016 Crossref	22 words — 1%
4	www.icei.pucminas.br Internet	17 words — < 1%
5	Siva Janakiraman. "Smart bit manipulation for K bit encoded hiding in K-1 pixel bits", 3rd International Conference on Trendz in Information Sciences & Computing (TISC2011), 12/2011 Crossref	13 words — < 1%
6	Sathisha, N., Amarashree, K. S. Babu, K. B. Raja, K. R. Venugopal, and L. M. Patnaik. "Non Embedding Steganography using Average Technique in Transform domain", 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 2013. Crossref	10 words — < 1%
	Reddy, H S Manjunatha, N Sathisha, Annu Kumari, and K B Raja.	

7	"Secure steganography using hybrid domain technique", 2012 Third International Conference on Computing Communication and Networking Technologies (ICCCNT 12), 2012. Crossref	8 words —	< 1%
8	Shiv Dutt Joshi. "Locating Text in Images using Matched Wavelets", Eighth International Conference on Document Analysis and Recognition (ICDAR 05), 2005 Crossref	8 words —	< 1%
9	Avinash, K. Gulve, and M.S. Joshi. "A Secured Five Pixel Pair Differencing Algorithm for Compressed Image Steganography", 2012 Third International Conference on Computer and Communication Technology, 2012. Crossref	7 words —	< 1%
10	V.C. Alves. "Implementation of cryptographic applications on the reconfigurable FPGA coprocessor microEnable", Proceedings 13th Symposium on Integrated Circuits and Systems Design (Cat No PR00843) SBCCI-00, 2000 Crossref	6 words —	< 1%

EXCLUDE QUOTES OFF
EXCLUDE MATCHES OFF
EXCLUDE BIBLIOGRAPHY OFF