Student Data Value Screen Using Steganography And Cryptography With Eof Method And Design Algorithm Case Study Campus of Universitas Budi Luhur Unit C Salemba

Ady Widjaja[1]
{ady.widjaja@budiluhur.ac.id[1]}

Faculty of Information Technology, Universitas Budi Luhur, Jakarta, 12260[1]

Abstract. Data on the value of students at the Universitas Budi Luhur Unit C Salemba needs to be secured from irresponsible people. The value data that is in campus salemba after collected per period values will be sent to the central campus in cileduk. The result of cryptography is data that is different from the original form and usually the data seems to be messy so it can not be known what information is contained therein (but actually can be returned to its original form through the description process). Application of EOF Steganography Method System (End Of File) aims to provide data security facilities, especially in terms of hiding data intended for companies, businesses and individuals. This research is based on increasing the flow of data packet delivery via email or media others that have a direct impact on increasing threats and data theft. This research was formed by the method of experimental research technique data collection using literature and documentation. Using the incorporation of steganographic and criti- cal techniques on the transfer of confidential information by developing DES algorithms can ensure better confidentiality of threats and data theft . Based on the tests that have been done, the application generated from this research has a good ability, especially in terms of functionality , realiabilit , usability, and effieciency. In general this application has a capability level of 82% or very good.

Keywords: Data Security, Steganography, Cryptography, End Of File (EOF), Data Encryption Standard (DES).

1 Introduction

1.1 Background

The problem of communication and information technology, now is the tapping of data and information in the global Internet network. The risks are quite high. The emergence of viruses, malware, spyware, malicious software (malicious software) that is able to tap and even steal information owned by someone, coupled with bermunculanny malicious hackers (blackhacker) capable of breaking the computer network either disebuah companies or government agencies [5].

Generally information security means protecting information from unauthorized persons accessing such information, disruption (information tapping), changes to original information or illegal use. Data security techniques or digital information are also growing

WMA-1 2018, January 20-21, Indonesia

DOI 10.4108/eai.20-1-2018.2281912

well and quickly. Some of the most common techniques used in data security are cryptography, steganography, digital signatures (digital signature), use of watermarks (etc.) [1],[2]. Cryptographic techniques are created with the primary objective of securing internet communication channels and has many methods developed to perform the process of encryption and decryption of data with the aim to maintain the confidentiality of messages or information submitted. Unfortunately this is also not enough to keep the information confidential or can only be accessed by certain people only, also needed technique to maintain the confidentiality of such messages or data [11]. The technique used to hide such confidential information is called steganography.

Steganography is the art and science of communication from the delivery of invisible messages (invinsible communication) [3]. This can be done by hiding information in other information, thus hiding the existence of information communicated from the sender to the recipient.

Steganography and cryptography are two different techniques that maintain the confidentiality and integrity of the data. The purpose of steganography is to hide secret messages in digital media in a way that does not allow anyone to detect the existence of such secret messages [9]. The main purpose of steganography is to communicate securely with secret messages through pictures [6],[7]. Steganography does not change the structure of the secret message, but it hides inside the media so the change is not visible [7],[8]. While cryptography protects messages from unauthorized individuals by changing their meaning [10].

Universitas Budi Luhur Unit C Salemba located in Sentra Salemba Mas Block ST, Jl. Salemba Raya No. 34-36 is a branch of Universitas Budi Luhur located at Jl. Ciledug Raya, North Petukangan, South Jakarta. Universitas Budi Luhur Unit C Salemba has 750 students. Every semester of Universitas Budi Luhur Unit C Salemba will send student value data to campus center. Currently the process of sending student value data to the central campus is still using courier services in the form of microsoft excel files. This mechanism is very vulnerable to the manipulation of value data made by certain parties because the file can be opened easily. Thus required an application that can ensure the security of microsoft excel file that is sent. Therefore the author tries to find solutions by creating applications with steganography and cryptography to insert confidential information into certain media. Value data stored in microsoft excel will be inserted into the image media so it can not be read easily by the parties - the parties are not responsible. The method used to insert the information is EOF (End Of File). In addition, the DES (Data Encryption Strandart) algorithm will be used to encrypt the value data before it is inserted.

1.2 Identification of Problems

One of the fundamental reasons with the research background that has been described, it can be identification problems in research are as follows:

1. Delivery of value data by courier from campus branch salemba to campus center prone to manipulation by certain parties because the file can be opened easily
2. Delivery of value data through internet media is also prone to wiretapping and theft by third parties.

1.3 Scope of Problems

The study was conducted at Universitas Budi Luhur Unit C Salemba branch because of the

limited time of this research is limited by the things listed as follows:

1. The designed application includes value data security for delivery through courier and media services
2. Value data sent only in the form of excel file
3. The insertion media used is a digital image or image
4. The method used with the method of End Of File
5. Algorithm used is DES (Data Encryption Standard)

1.4 Formulation of Problems

In connection with the problem found by researchers at Universitas Budi Luhur Unit C Salemba Branch, it makes the basis for doing research, such as:

1. Will the use of steganography and cryptography methods secure the value data sent from the branch campus to the central campus?
2. Will the EOF (End Of File) method and DES (Data Encryption Standard) encryption be used to insert value data?

1.5 Objectives and Benefits of Research

The purpose of this research is as follows:

1. Generate applications that can insert excel value data into images using EOF and DES encryption methods
2. Evaluate the implementation of the application that has been made
   The benefits of this research are to:

The benefits of this research are to:

1. The resulting application can be used to secure the value data at the time of delivery either through courier or internet media. The results of this study can contribute to science and technology, especially in the application of EOF and DES algorithms to insert secret messages into the image media or digital images.

2 Theoretical Basis

2.1 Steganography

The word steganography comes from the Greek word Steganos, which means "hidden or veiled" and graphien, "writing" so that it means "to write hidden or veiled writing" [Sellars, 1996].

Steganography is defined as the science and art to hide the secret message (hiding message) in such a way that the existence of the message is not detected by humans. [12],[13],[14]. Steganography is a branch of science that studies how to conceal a "secret" information in other information [4].

2.2 Criteria Data Hiding Steganography

Criteria to be considered in concealment of confidential data by using digital imagery as a container file are:

1. Imperceptibility
   The existence of the secret message can not be perceived by sensory. If the cover medium in the form of images, then the image of the stego medium penyisispan make the message difficult to distinguish by eye with his covertext- image. If covertext is audio (eg mp3 audio file , wav, midi, and so on), then the ear senses can not detect changes in its stegotext- audio.
2. Fidelity
   Container media quality does not change much due to insertion. After the addition of secret data, the image of the steganography still looks good. Observers do not know that in the image there is secret data.
3. Recovery
   Hidden message must be disclosed again (reveal) .Because the purpose of steganography is data hiding, then at any time - a secret message in the stego medium should be taken back to be used further.
4. Security
   Messages or confidential data that is concealed to a media must be secure, so that unauthorized parties can not know the existence of the inserted information.

2.3 Media Steganograpy

Some examples of secret message insertion media used by steganography include:

1 Steganography on Text
   Steganography in the text is divided into two applications, namely on soft-copy text and hard-copy text. In soft-copy text, steganography encodes data by changing the number of spaces after punctuation. While on hard-copy text , there are two methods: Line Shift Coding (shifting each line up or down) and Word Shift Coding (shifting a few words left or right)
2. Steganography on Image
   Most of the research and design of steganographic applications are on digital images . This is because an image with confidential information in it is more easily disseminated through the web or forum. To note is that when the information is hidden into the image file then the image is changed to another image format , then the hidden information will be lost.
3. Steganography on Audio
   Steganography can also be applied to digital sound . However, for steganography on audio files need to be careful in designing its steganographic algorithm, because the sound is more sensitive than the image. This means that digital sound is more easily damaged when steganography is added.
4. Steganography on Video
   Steganography on a video is very similar to steganography in the image , except that information is stored on every video frame. Steganography on digital video must be designed in such a way that the transition of images from one frame to another frame

must remain good and not visible modified. Because the digital video is relatively large in size than the digital image , then the inserted information can be more.

2.4 Definition of Cryptography

In the dictionary hackers, cryptography is defined as the science of studying writing in secret [15]. In a cryptographic algorithm, there are three elements are:

1. Encryption, ie the process of converting plaintext into ciphertext.
2. Decryption, ie converting ciphertext to plaintext.
3. The key, is the key used for encryption or decryption process

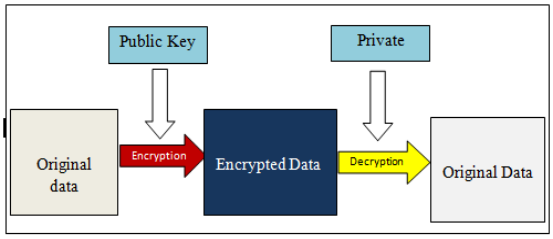

Fig. 1. Scheme processes on Cryptography method.

2.5 Format File

Digital imagery can be stored in various formats. Some digital image formats can utilize compression methods in image data storage. Compression can be lossy or lossless , depending on the type of format used.Compression that is lossy leads to a decrease in image quality, although in some cases the quality decrease can not be recognized by the eye humans.Beberapa digital image format that many met is BMP, JPEG, GIF and others.

2.6 Method End of File (EOF)

The EOF (End Of File) method is one technique that inserts data at the end of the file and development rather than the LSB (Least Significant Byte) method . This technique can be used to insert data the same size as the file size before inserted plus the size of data inserted into the file. In the EOF technique, the data inserted at the end is marked as a start recognition of the data and the final identifier of the data. In this technique, the data is inserted at the end of the file with a special mark as the start identifier of the data and the final identifier of the data.

2.7 DES Algorithm

DES (Data Encryption Standard) is a popular cipher block algorithm because it is used as a standard symmetric encryption algorithm. Actually DES is the symmetric encryption standard name, the name of the encryption algorithm itself is DEA (Data Encryption Algorithm), but the DES name is more popular than DEA . DES operates on a 64 bit block size. DES encrypts 64 bits of plaintext into ciphertext by using a 64 bit 48 bit internal key (internal key) or upa-key (subkey) internal. Key raised from external key (external key) length of 64 bits.

3 Design of Research

3.1 Method of Research

This study authors use descriptive qualitative research methods. Besides using the qualitative descriptive method, this research also uses simulation method to prove the effectiveness of the design result of the implementation that has been made. Qualitative research methods are used to examine natural sites, and research does not make treatment, because researchers in collecting data are emic, that is based on the views of data sources, not the views of researchers. In qualitative research, researchers interact with data sources. Although qualitative research does not make generalizations, it does not mean that qualitative research results can not be applied elsewhere. Generalization in qualitative research called transferability in the Indonesian language is called *ketralihan*. The point is that the results of qualitative research can be transferred or applied elsewhere, when the conditions of other places are not much different from the place of study [16],[17]. Likewise the final outcome of the design is expected to be flexible to apply anywhere as long as the infrastructure and needs are not much different. In this study, the authors use data collection techniques are:

Biblical Technique

1. Bibliography techniques
   Bibliography techniques focus on the study of various sources of literature.
2. Observation Technique
   Researchers see directly the implementation of the application of this system.

3.2 Step Research

The research steps are as follows:

1. Conduct an initial survey.
   This step aims to determine the extent to which the conditions of transactions execution of confidential information during this run.
2. Conducting literature study
   This research begins by conducting literature studies from several sources related to the discussion of data security with various techniques in application implementation
3. Create an application design
   After knowing the problems that occur in the field, the next step is to make the application design for the delivery of secret messages with cryptographic techniques and steganography.
4. Simulation and Testing
   From the process of encrypting the encryption of secret messages into excel files does not seem a significant difference when viewed in plain view.
5. Analysis of simulation results
   Compares security and time requirements for decryption of confidential messaging services before and after using steganographic and cryptographic integration techniques with the addition of EOF and DES algorithms.
6. Conclusion

This conclusion aims to explain the suitability of results designed to be applied to secret messaging applications at Universitas Budi Luhur Unit C Salemba if this application is implemented, and along with the fulfillment of the security aspects in the design of this application implementation by adding the algorithm.

3.3 Research Schedule

No.	Kegiatan	Bulan per tahun 2013-2014				
		Okt	Nov	Des	Jan	Feb
1	Pengumpulan Jurnal dan referensi	X				
2	Studi kepustakaan	X				
3	Menyusun proposal tesis	X	X	X		
4	Mengajukan proposal tesis			X		
5	Sidang proposal tesis				X	
6	Membuat rancangan	X	X	X	X	
7	Melakukan analisis terhadap rancangan				X	
8	Penarikan kesimpulan hasil analisis			X	X	
9	Membuat rekomendasi			X	X	
10	Penyusunan naskah tesis			X	X	X
11	Sidang Tesis					X
12	Perbaikan naskah tesis					X
13	Menyerahkan naskah akhir tesis					X

Fig. 2. Research Schedule.

4 Discussion Research

4.1 Cover Image used

Testing steganography method with EOF technique in this research will use digital image dataset by using JPG digital image format. Where the digital image dataset to be used amounted to 4 images. Digital image dataset which will be used as cover image in this research is bungamawar.jpg, bungamerah.jpg, bungaputih.jpg, daun.jpg Digital image dataset this can be seen in Figure 3.

Fig. 3. Digital Image Dataset Testing Steganography Technique.

In Figure 4, shows the resolution and image size information of the digital image data used as the cover image :

No	Nama Citra	Resolusi	Ukuran Citra (Byte)
1.	Bungamawar.jpg	5184 x 3456	6529917
2.	Bungamerah.jpg	5184 x 3456	4219132
3.	Bungaputih.jpg	5184 x 3456	53367960
4.	Daun.jpg	5184 x 3456	4291714

Fig. 4. Cover Image Data Information.

4.2 Secret Message

The secret message used in this application is a Microsoft Excel file (.xlsx) with an average size of 67 KB. The excel file information can be seen in Figure 5.

No	Name file value	Size(bytes)
1.	Value 0313.xlsx	68560
2.	Value 0513.xlsx	85599
3.	Value 0713.xlsx	64061
4.	Value 0913.xlsx	69393

Fig. 5. The final exam score file.

4.3 Test Result

4.3.1 Steps Application Testing

1. Open the apps

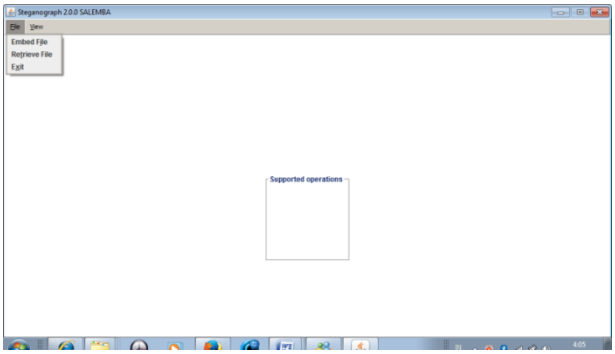

Fig. 6. Home Application page.

2. Click Menu embed file , then select select master file

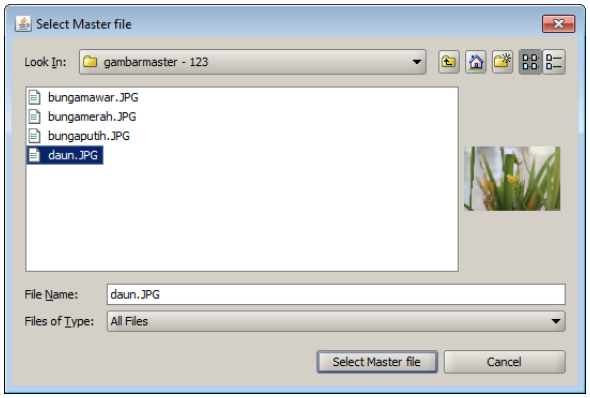

Fig. 7. Menu select master file(cover image) on embed file.

3. Select data file

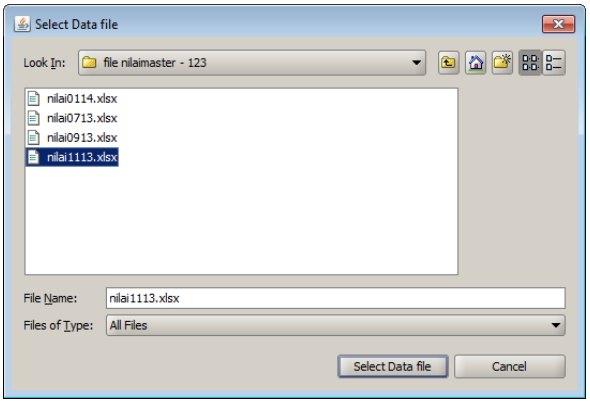

Fig. 8. Menu select output file (cover image) embed file.

4. Enter password (minimum 8 characters)

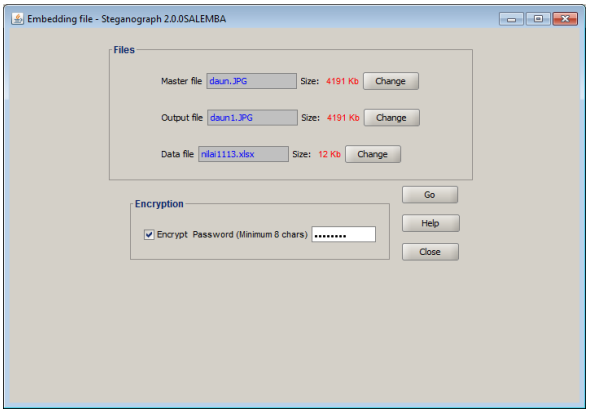

Fig. 9. Input menu password.

5. Click ok, will show the insertion process time

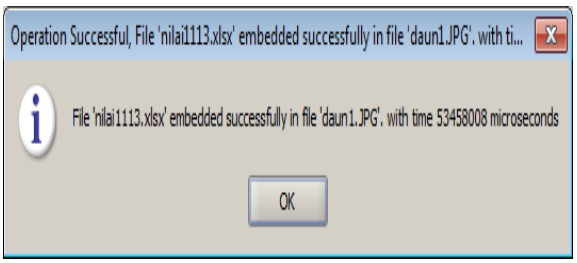

Fig. 10. The file embed menu is successful.

6. To open an inserted file, select Retrieve File

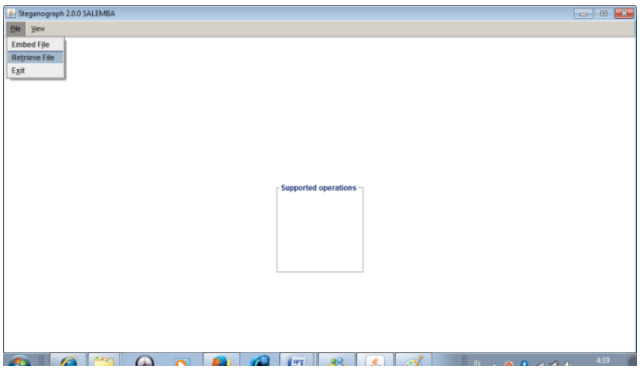

Fig. 11. Retrieve file menu.

7. Select master file

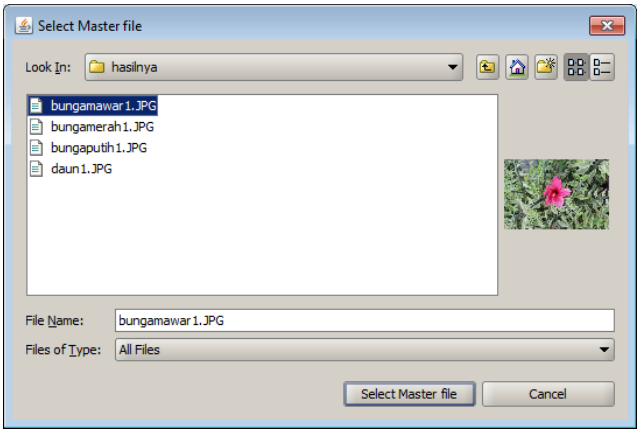

Fig. 12. Menu Select file retrieve.

8. Enter password

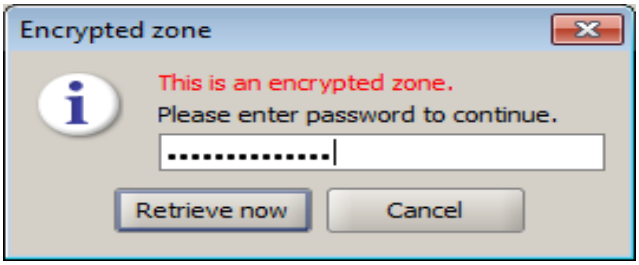

Fig. 13. Enter password.

9. The menu enters the password to open the retrieve file

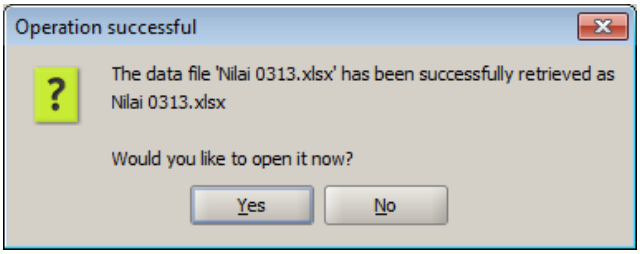

Fig. 14. Pop Up Retrieve.

10. Click Yes

CKDFAK	CPERIODE	CNIM	CNOTAB	KELOMPO	CNILSKS	NNILABS	NNILTGS	NNILMID	NNILUAS	NNILAKH	CJENIS	CUSERLOG	DTGLLOG	DTGLGAB
01	0313	11115302	KP011	SL	A	100,00	80,00	90,00	87,00	88,00		JITO		03/06/2013
01	0313	11115303	KP011	SL	A	100,00	80,00	88,00	90,00	88,00		JITO		03/06/2013
01	0313	11115302	KP011	SL	A	100,00	80,00	90,00	86,00	87,00		JITO		03/06/2013
01	0313	12115303	KP011	SL	A	100,00	80,00	90,00	90,00	89,00		MURYANTI		03/06/2013
01	0313	09115302	KP011	SL	A	100,00	80,00	85,00	88,00	87,00		MURYANTI		03/06/2013
01	0313	10115303	KP011	SL	A	100,00	80,00	86,00	86,00	86,00		MURYANTI		03/06/2013
01	0313	11115304	KP011	SL	A	100,00	80,00	87,00	90,00	88,00		SISTEM		03/06/2013
01	0313	12115303	KP011	SL	A	100,00	80,00	85,00	90,00	88,00		SISTEM		03/06/2013
01	0313	10115303	KP011	SL	A	100,00	80,00	86,00	88,00	87,00		SISTEM		03/06/2013
01	0313	12115303	KP011	SL	A	100,00	80,00	87,00	90,00	88,00		SISTEM		03/06/2013
01	0313	10115304	KP011	SL	A	100,00	80,00	90,00	87,00	88,00		SISTEM		03/06/2013
01	0313	10115303	KP011	SL	A	100,00	80,00	88,00	88,00	88,00		SISTEM		03/06/2013
01	0313	11115303	KP011	SL	A	100,00	80,00	86,00	86,00	86,00		SISTEM		03/06/2013
01	0313	10115302	KP011	SL	A	100,00	80,00	85,00	85,00	86,00		SISTEM		03/06/2013
01	0313	10115305	KP011	SL	A	100,00	80,00	90,00	88,00	88,00		SISTEM		03/06/2013

Fig. 15. Delivering the results of the file in the retrieve.

4.3.2 Results of Image Testing

The following test results are inserted files:

No	Nama file citra	Ukuran citra	Nama file excel (nilai)	Ukuran file excel	Ukuran file hasil	Waktu proses (ms)
1.	Bungamawar.jpg	6529917	Nilai 0313.xlsx	68560	6583398	16574959
2.	Bungamerah.jpg	4219132	Nilai 0513.xlsx	85599	4292608	16577961
3.	Bungaputih.jpg	5878522	Nilai 0713.xlsx	64061	5932603	10387823
4.	Daun.jpg	4291714	Nilai 0913.xlsx	69393	4349952	11652749

Fig. 16. Results of Image Testing.

Based on Figure 16 above if the file size cover image 6529917 KB and then inserted with file excel 68560 KB then the result file after inserted to 6583398 KB, there is addition of 53481 KB.

4.3.3 ISO 9126 Test Results

Testing based on ISO 9126. This is to test the application in terms of functionality, reliability, usability,and efficiency .

1. Results Recapitulation questionnaire for aspects Functionality, Reliability, Usability, Efficiency.

Aspek Penilaian	Skor Responden				
	5	4	3	2	1
	SS	S	R	TS	STS
Functionality	27	11	8	6	3
Reliability	19	5	4	4	1
Usability	20	15	6	2	1
Efficiency	10	10	2	-	-
Jumlah	76	41	20	12	5

Fig. 17. Results Recapitulation questionnaire for aspects Functionality, Reliability, Usability, Efficiency.

2. Final Score aspect Functionality, Reliability, Usability, Efficiency.
   Respondents' responses to aspects of functionality, Reliability, Usability, Efficiency of data security application of student value using steganography and cryptography:

Aspek Penilaian	Skor Aktual					Total Skor Aktual	Skor Ideal	%
	5	4	3	2	1			
	SS	S	R	TS	STS			
Functionality	135	44	24	12	3	218	275	79%
Reliability	95	20	12	8	1	136	165	82%
Usability	100	60	18	4	1	183	220	83%
Efficiency	50	40	6	-	-	96	110	87%
Jumlah	380	164	60	24	5	633	770	82%

Fig. 18. Final end of aspect Functionality, Reliability, Usability, Efficiency.

5 Conclusions & Suggestion

5.1 Conclusions

Based on the analysis and test results that have been done, it can be concluded as follows:

1. With this application, the value data owned by the Salemba branch campus becomes safe from unauthorized persons.
2. The use of End Of File (EOF) method resulted in less image quality, especially if it was observed by naked eye, so it would not make people suspicious that the image file contained a secret message.

3. Based on the data analysis obtained from questionnaires covering four aspects of the quality of the application prototype device ISO 9126 obtained an application quality score of 82% (very good).

5.1 Suggestion

Suggestions for further research and refinement of research on steganography techniques are as follows:

1. Integrating steganography techniques with cryptographic compression process in this application.
2. Add another file type that is used as cover or insertion media on the steganography process.
3. This app needs to be a web-based version. This is useful for this application can be used by many people.

References

[1]Al Muhammad Adel, "Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility.," 2010.

[2]D. Ariyus, Keamanan Multimedia, Penerapan Steganografi dalam berbagai bidang multimedia. Jakarta: Andi Publisher, 2009.

[3]A. Kahate, Cryptography and Network Security, 2nd Editio. Tata McGraw Hill, 2008.

[4]P. Cummins, Jonathan., Patrick, Diskin., Samuel, lau., Robert, Steganography and Digital Watermaking. 2004.

[5]P. M. K. A. Cheddad, J. Condell, K. Curran, "Biometric Inspired Digital Image Steganography," 15th Annu. IEEE Int. Conf. Work. Eng. Comput. Based Syst., pp. 159 – 168, 2008.

[6]C. Iswahyudi, "Penyisipan Pesan Rahasia pada Citra Digital dengan Teknik Steganografi," 2008.

[7]N. F. J. and S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software," Springer-Verlag (1998), 1998. [Online]. Available: http://www.jjtc.com/ihws98/jjgmu.html.

[8]H. F. Khalil Challita, "Combining Steganography and Cryptography," New Comput. Archit. Their Appl., no. The Society of Digital Information and Wireless Communications, pp. 199–208, 2011.

[9]S. A. Laskar and K. Hemachandran, "An Analysis ofSteganography and Steganalysis Techniques," Assam Univ. J. Sci. Technol., vol. 9, pp. 83–103, 2012.

[10]R. R. I. Miftahur Rahim, Achmad Hidayatno, "Teknik Penyembunyian Data Rahasia Dengan Menggunakan Citra Digital Sebagai Berkas Penampung," pp. 1–8, 2006.

[11]P. D. Mrs.Kavitha, Kavita Kadam, Ashwini Koshti, "Steganography Using Least Signicant Bit Algorithm," Int. J. Eng. Appl., vol. 2, no. 3, pp. 338–341, 2012.

[12]R. Munir, Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung: Informatika, 2004.

[13]R. Munir, Steganografi dan Watermarking. 2009.

[14]F. A. P. P. Ross J. Anderson, "On The Limits of Steganography," IEEE J. Sel. Areas Commun., vol. 16, no. Special Issue on Copyright & Privacy Protection., pp. 474–481, 1998.

[15] K. T. R. S. Ramesh, "An Automated Approach to Solve Simple Substitution Ciphers," Taylor Fr. Cryptologia, vol. XVII No.2, pp. 202–218, 1993.

[16]K. H. Shamim Ahmed Laskar, "Secure Data Transmission Using Steganography And Encryption Technique," Int. J. Cryptogr. Inf. Secur., vol. 2, no. 3, 2012.

[17]S. J. I. I. M. Anggrie Andriawan, Solikin, Implementasi Steganografi Pada Citra Digital File Gambar Bitmap (Bmp) Menggunakan Java. Bandung: Fakultas Ilmu Terapan, Teknik Komputer, 2012.