Lecture Notes in Networks and Systems 149

Prasant Kumar Pattnaik
Mangal Sain
Ahmed A. Al-Absi
Pardeep Kumar *Editors*

Proceedings of International Conference on Smart Computing and Cyber Security

Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2020)

Springer

Lecture Notes in Networks and Systems

Volume 149

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

More information about this series at http://www.springer.com/series/15179

Prasant Kumar Pattnaik · Mangal Sain ·
Ahmed A. Al-Absi · Pardeep Kumar
Editors

Proceedings of International Conference on Smart Computing and Cyber Security

Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2020)

Springer

Editors
Prasant Kumar Pattnaik
School of Computer Engineering
Kalinga Institute of Industrial Technology
KIIT Deemed to be University
Bhubaneswar, India

Mangal Sain
Division of Information and Communication Engineering
Dongseo University
Busan, Korea (Republic of)

Ahmed A. Al-Absi
Department of Smart Computing
Kyungdong University Global Campus
Gangwondo, Korea (Republic of)

Pardeep Kumar
Department of Computer Science
Swansea University, Bay Campus
Swansea, UK

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-981-15-7989-9 ISBN 978-981-15-7990-5 (eBook)
https://doi.org/10.1007/978-981-15-7990-5

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The 1st International Conference on Smart Computing and Cyber Security—Strategic Foresight, Security Challenges and Innovation (SMARTCYBER 2020), took place in Kyungdong University Global Campus, Gosung, Gangwondo, South Korea, during July 7–8, 2020. It was hosted by the Department of Smart Computing, Kyungdong University, Global Campus, South Korea.

The SMARTCYBER is a premier international open forum for scientists, researchers and technocrats in academia as well as in industries from different parts of the world to present, interact and exchange the state of the art of concepts, prototypes, innovative research ideas in several diversified fields. The primary focus of the conference is to foster new and original research ideas and results in the five board tracks: smart computing concepts, models, algorithms, and applications, smart embedded systems, bio-Inspired models in information processing, technology, and security. This is an exciting and emerging interdisciplinary area in which a wide range of theory and methodologies are being investigated and developed to tackle complex and challenging real-world problems. The conference includes invited keynote talks and oral paper presentations from both academia and industry to initiate and ignite our young minds in the meadow of momentous research and thereby enrich their existing knowledge.

SMARTCYBER 2020 received a total of 143 submissions. Each submission was reviewed by at least three Program Committee members. The committee decided to accept 37 full papers. Papers were accepted on the basis of technical merit, presentation and relevance to the conference. SMARTCYBER 2020 was enriched by the lectures and insights given by the following seven distinguished invited speakers: Prof. Prasant Kumar Pattnaik, School of Computer Engineering, Kalinga Institute of Industrial Technology; Professor Ana Hol, Western Sydney University, Australia; Professor Aninda Bose, Senior Editor Springer India; Prof. Evizal Abdul Kadir, UIR, Indonesia; Dr. James Aich S, CEO Terenz Co. Ltd, South Korea; Prof. Mangal Sain, Dongseo University, South Korea; and Prof. Ahmed A. Al-Absi, Kyungdong University Global Campus, South Korea. We thank the invited speakers for sharing the enthusiasm for research and accepting our invitation to share their expertise as well as contributing papers for inclusion in the proceedings.

SMARTCYBER 2020 has been able to maintain standards in terms of the quality of papers due to the contribution made by many stakeholders.

We are thankful to the General Chairs, Prasant Kumar Pattnaik, KIIT Deemed to be University, India; Ahmed A. Al-Absi, Kyungdong University, South Korea; Mangal Sain, Dongseo University. We futher thank the Program Chairs, Baseem Al-athwari, Kyungdong University Global Campus, South Korea; Pardeep Kumar, Swansea University, UK; Deepanjali Mishra, KIIT Deemed to be University, India, for their guidance and valuable inputs.

We are grateful to Prof. John Lee, President of Kyungdong University (KDU) Global Campus, South Korea, and Honorary General Chair, SMARTCYBER 2020, for his constant support and for providing the infrastructure and resources to organize the conference. We are thankful to Prof. Sasmita Rani Samanta, Pro-Vice-Chancellor, KIIT Deemed to be University, India, Honorary General Chair, SMARTCYBER 2020, for providing all the support for the conference.

Thanks are due to the Program and Technical committee members for their guidance related to the conference. We would also like to thank the Session Management Chairs, Publications Chairs, Publicity Chairs, Organizing Chairs, Finance Chairs and Web Management Chair who have made an invaluable contribution to the conference. We acknowledge the contribution of EasyChair in enabling an efficient and effective way in the management of paper submissions, reviews and preparation of proceedings. Finally, we thank all the authors and participants for their enthusiastic support. We are very much thankful to entire team of Springer Nature for timely support and help. We sincerely hope that you find the book to be of value in the pursuit of academic and professional excellence.

Bhubaneswar, India — Prasant Kumar Pattnaik
Gangwondo, Korea (Republic of) — Ahmed A. Al-Absi
Busan, Korea (Republic of) — Mangal Sain
Swansea, UK — Pardeep Kumar

Contents

Author Index

P. K. Pattnaik et al. (eds.), *Proceedings of International Conference on Smart Computing and Cyber Security*, Lecture Notes in Networks and Systems 149,
https://doi.org/10.1007/978-981-15-7990-5

SMARTCYBER 2020

Springer Scopus

KDU MAN OF MISSION KYUNGDONG UNIVERSITY 취/업/사/관/학/교 경동대학교

CONFERENCE SCHEDULE

July 7th 2020,

10:00 AM ~ 12:20 PM (15 minutes / paper)
Session-1: Smart Computing Concepts, Models, Algorithms, and Applications
10:00 AM ~ 12:20 PM (15 minutes / paper)
Session-2: Smart Embedded Systems
10:00 AM ~ 12:20 PM (15 minutes / paper)
Session-3: Bio-Inspired Models in Information Processing
10:00 AM ~ 12:20 PM (15 minutes / paper)
Session-4: Technology
10:00 AM ~ 12:20 PM (15 minutes / paper)
Session-5: Security

Compilation of Presentation and Discussion for Best Paper Award

01:30 PM ~ 02:00 PM
Inaugural Session SmartCyber 2020 by KDU Global Leaders and General Chairs
02:00 PM ~ 02:30 PM
Keynote Speaker-1: Professor Prasant Kumar Pattnaik (Kalinga Institute of Industrial Technology, India)
Title: Applications of MCDM Technique in Sensor Cloud Environment
02:30 PM ~ 03:00 PM
Keynote Speaker-2: Professor Ana Hol (Western Sydney University, Australia)
Title: Business Transformations within Intelligent Eco-systems
03:00 PM ~ 03:30 PM
Keynote Speaker-3: Professor Aninda Bose (Senior Editor, Springer, Asia) Title: TBD.

July 8th 2020,

02:00 PM ~ 02:30 PM
Keynote Speaker-4: Professor Evizal Abdul Kadir (UIR - Indonesia)
Title: Intelligent Ubiquitous Sensor Applications (Scanning, Sensing, and Actuating)
02:30 PM ~ 03:00 PM
Keynote Speaker-5: Dr. James Aich S (CEO Terenz Co. Ltd, South Korea)
Title: Artificial Intelligence: The leap to Precision Healthcare
03:00 PM ~ 03:30 PM
Keynote Speaker-6: Professor Mangal Sain (Dongseo University, South Korea)
Title: The end of middleware?
03:30 PM ~ 04:00 PM
Speaker-7: Professor Ahmed A. Al-Absi (Kyungdong University Global Campus, South Korea)
Title: Enhanced Parallel Computing Framework for Big Data Processing in Cloud Environment
04:00 PM ~04:30 PM
SMARTCYBER 2020 Team Meeting & Discussion
04:30 PM ~ 05:00 PM
Closing SMARTCYBER 2020 & Launch of SMARTCYBER 2021 Webpage

https://global.kduniv.ac.kr/int **https://icceconference.com/**

SMARTCYBER 2020
The 1st International Conference on Smart Computing and Cyber Security
Department of Smart Computing, Kyungdong University, Global Campus, South Korea

경동대학교 KYUNGDONG UNIVERSITY

THE 1st INTERNATIONAL CONFERENCE ON SMART COMPUTING AND CYBER SECURITY
July 7th ~ 8th, 2020 - Kyungdong University, South Korea

SMARTCYBER 2020
Springer Scopus

SMARTCYBER 2020 SCHEDULE

July 7th 2020; Day One Schedule

TIME	Session-1: Smart Computing Concepts, Models, Algorithms, and Applications	Session-2: Smart Embedded Systems	Session-3: Bio-Inspired Models in Information Processing	Session-4: Technology	Session-5: Security
	Chairs: Dr. Md Azam Hossain ; Dr. Samaresh Mishra	***Chairs:*** Dr. Nguyen Ngoc Cao ; Dr. Evizal Abdul Kadir	***Chairs:*** Dr. Md. Nur Alam ; Dr. Kueh Lee Hui	***Chairs:*** Dr. Baseem Al-athwari ; Dr. Sasmita Mohanty	***Chairs:*** Dr. Grace C. Kennedy ; Dr. Ahmadxon Kamolov
10:00	Exploring Generative Adversarial Networks for Entity Search and Retrieval	Implementation of Motorcycle Monitoring using Bluetooth with an Android-Based Microcontroller Using Arduino	Customer Sentiment Analysis using Cloud App and Machine Learning Model	Blockchain Technology to Support Employee Recruitment and Selection in Industrial Revolution 4.0	Proposal of Pseudo-random Number Generators using PingPong256 and Chaos Maps
10:20	A Comparative Analysis of Data Mining Analysis Tools	DGA Method Based on Fuzzy for Determination of Transformer Oil Quality	Mood Enhancer Based on Facial Expression using Machine Learning and Virtual Assistant Technology – an Android App	Blockchain Based Solution for Effective Employee Management	Text File Protection Using Least Significant Bit (LSB) Steganography and Rijndael Algorithm
10:40	Classification of Multiple Steganographic Algorithms using Hierarchical CNNs and ResNets	Real Time Access Control System method using Face Recognition	Deep Learning-Based Apple Defect Detection with Residual SqueezeNet	Android Based Online Attendance Application	Graph Theory based Numerical Algorithm to Secure WSAN Network with Low Delay and Energy Consumption
11:00	Towards a Sentiment Analyzer for Low-Resource Languages	Robotic Process Automation Challenges Overview	Apple Defect Detection Based on Deep Convolutional Neural Network	Integrating Complete Locomotive Assistance and IoT Based Health Care for the Disabled	Secure Marine Communication under Distributed Slotted MAC
11:20	Satellite Image Segmentation and Classification using Fuzzy C Means Clustering and Support Vector Machine Classifier	Smart Parking Management System in Shopping Malls	Apple Defects Detection Based on Average Principal Component using Hyperspectral Imaging	The determinants of Internet Financial Reporting for Investor Decision Making: Evidence from Indonesia Companies	Detection of Network Intrusion and Classification of Cyber Attack using Machine Learning Algorithms: A Multistage Classifier Approach
11:40	Development of an Information System for the Collection and Processing of Big Data in Construction	IoT Technology with Marine Environment Protection and Monitoring	Early Detection of Alzheimer's Disease from 1.5T MRI Scans using 3D Convolutional Neural Network	The Application of Technology Acceptance Model to Asses the Role of Complexity toward Customer Acceptance on Mobile Banking	Genetic Algorithm for Decrypting user's Personal Information
12:00	Exploring the Volatility of Large-Scale Shared Distributed Computing Resources	Smart Sensing System for Detection and Forecasting Forest Fire in Riau Province, Indonesia		Resource Allocation in the Integration of IoT, Fog, and Cloud Computing: State-of-the-art and Open Challenges	Automatic Detection of Security Misconfigurations in Web Applications
12:20					Decentralized Privacy Protection Approach for Video Surveillance Service
1:30~2:00 PM	Inaugural Session SMARTCYBER 2020 by KDU Global Leaders and General Chairs				
	Keynote Day-1:				
2:00~2:30 PM	Speaker-1: Professor Prasant Kumar Pattnaik (Kalinga Institute of Industrial Technology, India)				
2:30~3:00 PM	Speaker-2: Professor Ana Hol (Western Sydney University, Australia)				
3:00~3:30 PM	Speaker-3: Professor Aninda Bose (Senior Editor, Springer, Asia)				

July 8th 2020; Day Two Schedule

	Keynote Day-2:
2:00~2:30 PM	Speaker-4: Professor Evizal Abdul Kadir (UIR - Indonesia)
2:30~3:00 PM	Speaker-5: Dr. James Aich S (CEO Terenz Co. Ltd, South Korea)
3:00~3:30 PM	Speaker-6: Professor Mangal Sain (Dongseo University, South Korea)
3:30~4:00 PM	Speaker-7: Professor Ahmed A. Al-Absi (Kyungdong University Global Campus, South Korea)
4:00~4:30 PM	SMARTCYBER 2020 Team Meeting & Discussion
4:30~5:00 PM	Closing SMARTCYBER 2020 & Launch of SMARTCYBER 2021 Webpage

Note: **The sessions will be conducted as panel discussions in which authors give a presentation (15 minutes) of their papers, and then take (5 minutes) live questions from the panel moderators and audience. The event will be organized virtually on Zoom Software, in this regard, we have created exclusive online login and the credentials will be shared with authors only. In case you have any problem in using Zoom software, you are requested to please go through it, to enable you to join SMARTCYBER-2020 on time. For any inquiries, feel free to contact us at *smartcyber2020@gmail.com* or *absiahmed@kduniv.ac.kr***

Text File Protection Using Least Significant Bit (LSB) Steganography and Rijndael Algorithm

Apri Siswanto[1], Yudhi Arta[1], Evizal Abdul Kadir[1], Bimantara[1]

[1]Department of Informatics Engineering, Faculty of Engineering Universitas Islam Riau, Indonesia

{aprisiswanto@eng.uir.ac.id, yudhiarta@eng.uir.ac.id, evizal@eng.uir.ac.id, bimbimjabrikz@gmail.com}

Abstract. Nowadays, thousands of kilobytes personal data are transmitted every day through insecure communication media (such as the internet, computer networks, communication systems, etc.). This makes data vulnerable to information theft, especially for fraud, illegal trade and so on. So, there is a need for protecting the information in its storage and transmission. To improve data and information security, in this study, we propose a Least Significant Bit (LSB) steganography to insert message information in a 24-bit jpg image and Rijndael cryptography that is used to encrypt jpg images so that message information can be secured from unauthorized parties.

Keywords: Encryption, cryptography, LSB steganography, Rijndael, information hiding

1 Introduction

The rapid development of computer technology has triggered crimes that exploit the weaknesses of computer network transmission systems. One form of crime is hackers try to retrieve data and information through the transmission of computer networks or known as a man in the middle attack [1]. Transfer of essential data on companies, agencies, or the military is vulnerable to attack if it only relies on a standard security system[2]. Confidential information can be taken and used by irresponsible parties. So, this must be given special attention by the parties concerned. Some ways to overcome this problem is to secure the message using the information hiding technique. Information hiding is a field of science that studies how to hide messages so that they cannot be perceived (both visually and audial). There are two ways techniques used in information hiding i.e. cryptography and steganography [3].

Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, and authentication [4]. While Steganography is the science that studies, researches, and develops the art of hiding information. Steganography can be classified as one part of communication science [5]. In the digital information era, steganography is a technique and art of hiding

information and digital data behind other digital data, so that digital information is invisible.

Recently, some methods can carry out attacks on steganography by utilizing the weaknesses of steganography. These methods are Visual Attacks and Statistical Attacks [6]. Visual attacks explain the difference between noise and visual patterns, while statistical attacks to detect the steganography method used. Because the method of attack on steganography has been found, problems arise how to provide security for data so that data can be hidden. Besides, confidentiality can also be maintained from the parties who are not authorized to access it. Therefore, to increase data and information security, in this study, we implement message encryption (cryptography) while hiding data and information in image files.

This paper is organized as follows. Section two describes Rijndael and LSB steganography theory. Then, section three introduced literature review where different methods of hiding information are discussed. Next, Section four discusses the research method of this paper. After that, section five explained results and discussion. Finally, section six presents conclusions and references used at the end.

2 LSB Steganography and Rijndael Algorithm

LSB is a technique commonly used in encryption and decryption of confidential information. The way the LSB method works is to change the redundant bits of the cover image that have no significant effect on the bits of the secret message. Figure 1 showed the mechanism of the LSB method in 8-bit images by utilizing 4 bits LSB [7].

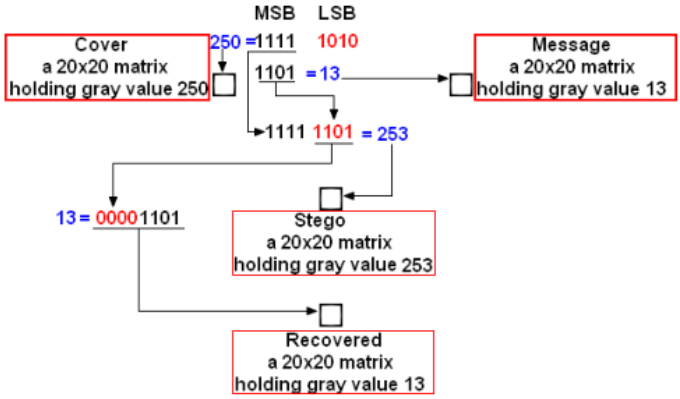


Figure 1: LSB Mechanism

Figure 1 showed the application of LSB using pixel-based image media with an 8-bit value (gray value). Each pixel consisting of 8 bits is divided into two parts, namely 4 bits MSB (most significant bits) and 4 bits LSB (least significant bits). The LSB part is changed to the value of the message to be inserted. After being sprinkled with a secret message, each pixel is rebuilt into a complete image resembling the original image media. The advantages of LSB is less suspicious in human eyes, easy to implement, and High perpetual transparency. On the other hand, the disadvantages of LSB include robustness and sensitivity to filtering, and scaling, rotation, the addition of noise in the image, and cropping can damage confidential messages [8].

The Rijndael algorithm used substitution, permutation, and a number of rounds. Each round used a different internal key. The key of each round is called around key. However, unlike DES operates bit-oriented, Rijndael operates in byte orientation. The goal is to minimize software and hardware resources. The Rijndael algorithm works on 128-bit blocks with 128-bit keys with the AddRoundKey process. AddRoundKey is to do XOR between the initial state (plaintext) and the cipher key [9]. This stage is also called initial round. The process carried out in each round is:

1. SubBytes: byte substitution using a substitution table (S-box).
2. ShiftRows: shifting array state lines in wrapping.
3. MixColumns: scrambles data in each state array column.
4. AddRoundKey: perform XOR between the current state of the round key.

The Rijndael algorithm has three parameters [10]:

1. plaintext: a 16-byte array, which contains input data.
2. ciphertext: an array of 16-byte size, which included the results of encryption.
3. key: an array of 16-byte size, which contains a ciphering key (also called a cipher key). With 16 bytes, both the data block and the 128-bit key can be stored in all three arrays (128 = 16 x 8).

3. Related Research

Data security and confidentiality are essential aspects needed in the process of exchanging data on the internet network. Two techniques can be used for data protection, namely cryptography and steganography. Several studies related to cryptography and steganography, for example, Syawal, et al., [11] proposed text message encryption using Vigenere cipher algorithm and LSB technique for inserting messages into images. The proposed encryption was programmed in MatLab 2014b. The object of research is to enter text into the image to produce hidden files and cannot be accessed by unauthorized parties.

Then, Purba et al., [12] has conducted a study Implementation of Text Message Steganography into Sound Files (.Wav) with Byte Distance Modification in the Least Significant Bit (Lsb) Algorithm. The purpose of this study is to hide files with the extension .txt and files ending in .Wav. Data bits are hidden or secured using LSB into the audio media. The result of the study found that the bit values are inserted into the audio media are still looks like normal so as not to arouse suspicion of the listener. Then if extracted, it will get back the whole bit values that have been inserted.

Therefore, the results of the research show that the resulting wav stego file has a good level of imperceptibility, fidelity, and recovery.

Utomo and Purnomo [13] has been proposed Image Steganography with the Least Significant Bit Method for Protection of Communication in Online Media. In this study, a message is inserted in the image file to be extracted again into a message. This method is done to secure the message and avoid unauthorized parties from utilizing the message.

The research conducted by Utomo and Purnomo, Purba et al., Syawal et al., and the research that the authors did together secure data by hiding the data into other data. The difference is in the object under study, the research method and the programming language used in developing the system. Like Purba, hide the .txt file into the file extension .Wav. Syawal used a different algorithm. And Utomo securing the message on the image file can then be extracted again into a message.

4 Research Methodology

The LSB Steganography and Rijndael algorithm are implemented using the Visual basic net programming language. We used modified LSB steganography method as a medium that will hide text file information in the form of each bit data value into the image media bit values. Data bits that will be hidden or secured with LSB into the jpg image media. The proposed encryption scheme is like the figure 1.

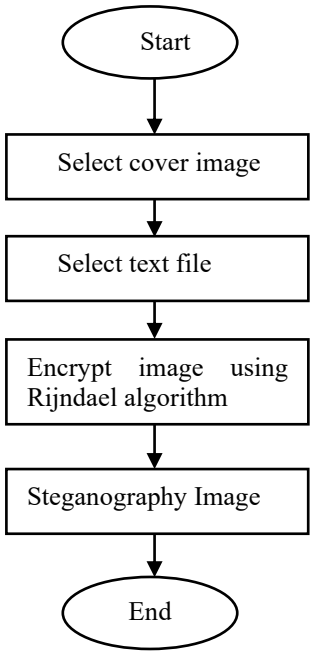


Fig. 1. Encryption process

In the encryption and decryption process, users must input object image files that will be steganography with text files that will be encrypted. Then the data is encrypted with the Rijndael algorithm. The Rijndael algorithm did the encryption process used substitution and permutation process. For the decryption process, the user enters the steganographic image file and then decomposes it with the Rijndael algorithm so that the ciphertext file returns to the original text file. See details in figure 2 the decryption process.

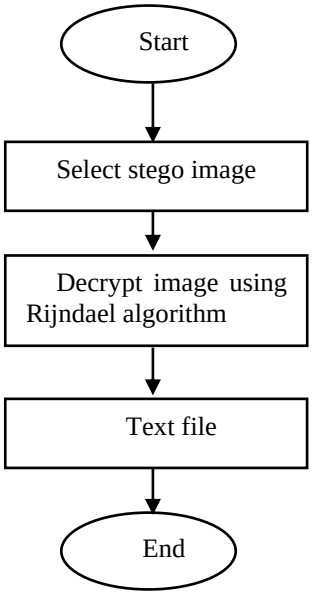


Fig. 2. Decryption process

5 Result and Discussion

This research output is an encryption scheme to secure text file. In simple application, the process steps is insert text files as a hidden message into a digital image. It is built using Visual Basic Net programming language, which has several supports for digital image programming. To accommodate the image when the process of hiding and reading the message, it used picture box control. The interface display of the application is like Figure 3.

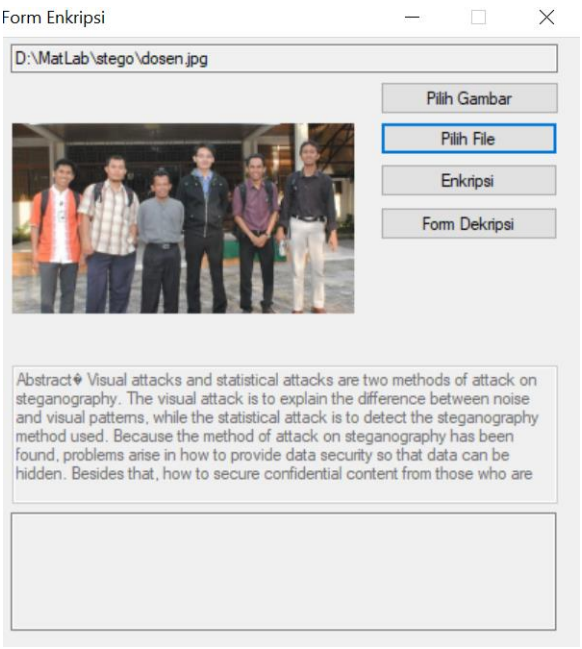
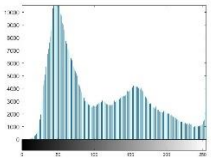
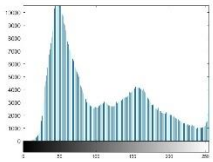
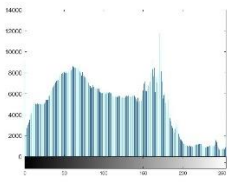
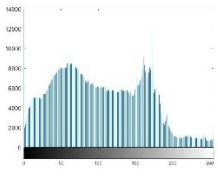


Fig. 3 Encryption decryption interface application

The first evaluation conducted was a histogram analysis. We have compared histogram analysis of the original image and stego image that has been inserted with the text file. The result is in table 1.

Table 1. Histogram analysis

Original image (A)	Stego image (B)	Histogram A	Histogram B
			
			

To determine image quality, the method of peak signal to noise ratio (PSNR) is used as a comparison of the quality of stego image with the original image (cover image). The term peak signal-to-noise ratio (PSNR) is a term in the field of engineering that states the ratio between the maximum possible signal strength of a digital signal and the noise power that affects the correctness of the signal. Because many signals have a wide dynamic range, PSNR is usually expressed on a logarithmic decibel scale [14]. The formula for calculating PSNR is as follows:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2] \quad (1)$$

$$PSNR = 10.log_{10}(\frac{MAX_1^2}{MSE}) \quad (2)$$

PSNR was defined through the signal-to-noise ratio (SNR). SNR is used to measure the level of signal quality. This value is calculated based on the comparison between the signal and the noise value. Signal quality is directly proportional to the SNR value. The higher the SNR value, the better the quality of the signal produced. Table 2 showed the results of calculation of valuesPSNR which is represented on a decibel scale (dB) [15].

Table 2. MSE, PSNE and MSE results

Image		MSE	PSNR	NSR
Cover Image	Dosen.jpg	414.9138	22.0142	15.7063
Stego Image	Dosen1.jpg	410.4317	21.9629	15.6550
Cover Image	Kolam.jpg	408.2399	22.0304	15.3456
Stego Image	Kolam1.jpg	404.2999	21.9541	15.2694

As the results of calculations in Table 1 show that the insertion of a text message with different sizes will produce different MSE and PSNR values. The larger the message file size, the higher the MSE value and the smaller the PSNR value, and vice versa the smaller the message file size, the smaller the MSE value and the higher the PSNR value. If the PSNR value is low, it can be said that image quality is getting worse, meaning that the image quality is physically bad. Whereas if the PSNR value is large, the image quality is still good, which means that the damage to the image is relatively small.

6 Conclusion

From the research that has been done, it can be concluded several things, namely steganography is a very efficient and powerful technique that allows to send text files safely and hidden. The LSB method that is applied to the message hiding process does not significantly affect the quality of the cover image.

References

[1] B. A. Forouzan and D. Mukhopadhyay, *Cryptography and Network Security (Sie)*: McGraw-Hill Education, 2011.

[2] A. Siswanto, A. Syukur, and I. Husna, "Perbandingan Metode Data Encryption Standard (DES) Dan Advanced Encryption Standard (AES) Pada Steganografi File Citra," in *Seminar Nasionl Teknologi Informasi dan Komunikasi 2018*, 2018, pp. 190 - 197.

[3] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," *International Journal on New Computer Architectures and Their Applications (IJNCAA),* vol. 1, pp. 199-208, 2011.

[4] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*: CRC press, 1996.

[5] R. Rahim, H. Nurdiyanto, R. Hidayat, A. S. Ahmar, D. Siregar, A. P. U. Siahaan*, et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," in *Journal of Physics: Conference Series*, 2018, p. 012003.

[6] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *International workshop on information hiding*, 1999, pp. 61-76.

[7] M. Pelosi, N. Poudel, P. Lamichhane, D. Lam, G. Kessler, and J. MacMonagle, "Positive Identification of LSB Image Steganography Using Cover Image Comparisons," 2018.

[8] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal processing,* vol. 90, pp. 727-752, 2010.

[9] R. Munir, "Pengantar Kriptografi," *Penerbit Informatika Bandung,* 2010.

[10] R. Munir, "Steganografi dan Watermarking," *Departemen Teknik Informatika, Institut Teknologi Bandung. Diakses dari http://informatika. stei. itb. ac. id/~ rinaldi. munir/Kriptografi/Steganografi% 20dan% 20Watermark ing. pdf,* 2004.

[11] M. F. Syawal, D. C. Fikriansyah, and N. A.-U. B. Luhur, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," *Jurnal TICom,* vol. 4, 2016.

[12] J. V. Purba, M. Situmorang, and D. Arisandi, "Implementasi steganografi pesan text ke dalam file sound (. wav) dengan modifikasi jarak byte pada algoritma least significant bit (LSB)," *Dunia Teknologi Informasi-Jurnal Online,* vol. 1, 2012.

[13] P. Utomo and B. E. Purnama, "Pengembangan Jaringan Komputer Universitas Surakarta Berdasarkan Perbandingan Protokol Routing Information Protokol (RIP) Dan Protokol Open Shortest Path First (OSPF)," *IJNS-Indonesian Journal on Networking and Security,* vol. 1, 2012.

[14] D. F. Alfatwa, "Watermarking Pada Citra Digital Menggunakan Discrete Wavelet Transform," *Bandung: Institut Teknologi Bandung,* 2005.

[15] M. M. Amin, "Image Steganography dengan Metode Least Significant Bit (SLB)," *Jurnal Computer Science Research and Its Development (CSRID),* vol. 6, 2014.