UNIVERSITI TEKNOLOGI MARA | Cawangan Melaka

PUBLICATION DATE | 1 SEPTEMBER 2021

i-JaMCSIIX 2021 Exploring ideas

International Jasin Multimedia & Computer Science Invention and Innovation Exhibition

International Jasin Multimedia & Computer Science Invention and Innovation Exhibition (i-JaMCSIIX 2021)

15 FEBRUARY 2021 - 31 MARCH 2021

VIRTUAL COMPETITION • INNOVATION & INVENTION • PUBLICATION OPPORTUNITIES

EXTENDED ABSTRACT

UiTM CAWANGAN MELAKA KAMPUS JASIN

ISBN:
978-967-15337-0-3

WEBSITE | https://jamcsiix.wixsite.com/2021

i-JaMCSIIX 2021

Exploring ideas

International Jasin Multimedia & Computer Science Invention and Innovation Exhibition

i-JaMCSIIX
Universiti Teknologi MARA Cawangan Melaka Kampus Jasin
77300, Merlimau, Melaka
Web: https://jamcsiix.wixsite.com/2021

PUBLISHED BY:

i-JaMCSIIX

Universiti Teknologi MARA Cawangan Melaka
Kampus Jasin

77300 Merlimau, Melaka

Tel: 062645000

Email: jamcsiix@uitm.edu.my

Web: https://iamcsiix.wixsite.com/2021

ISBN: 978-967-15337-0-3

ORGANIZING COMMITTEE

PATRON	ASSOC. PROF. DR. ISMADI MD BADARUDIN
ADVISOR 1	NOR FADILAH TAHAR @ YUSOFF
ADVISOR 2	DATO' TS. DR. MOHD NOR HAJAR HASROL JONO
PROJECT LEADER	TS. NURUL NAJWA ABDUL RAHID @ ABDUL RASHID
PROJECT LEADER 2	ANIS AFIQAH SHARIP
TREASURER 1	SITI MAISARAH MD ZAIN
TREASURER 2	NURUL ZAHIRAH ABD RAHIM
SECRETARY 1	NOR AIMUNI MD RASHID
SECRETARY 2	NUR NABILAH ABU MANGSHOR
PUBLICATION	**DR. RAIHAH AMINUDDIN**
	DR. NOR AIZA MOKETAR
	DR. SITI FEIRUSZ AHMAD FESOL
JURY	**TS. RAIHANA MD SAIDI**
	DR. ELIN ELIANA ABDUL RAHIM
	NOR INTAN SHAFINI NASARUDDIN
REGISTRATION	**FADZLIN AHMADON**
	HAJAR IZZATI MOHD GHAZALLI
	SITI AISYAH ABDUL KADIR
PROMOTION	**MOHAMAD ASROL ARSHAD**
	ZUHRI ARAFAH ZULKIFLI
	FADILAH EZLINA SHAHBUDIN
MULTIMEDIA	**NORSHAHIDATUL HASANA ISHAK**
	HAZRATI ZAINI
	NUR FARAHIN MOHD JOHARI
	FAIQAH HAFIDZAH HALIM
	MOHAMMAD BAKRI CHE HARON
	MUHAMMAD HAMIZ MOHD RADZI
AWARD	**FARAH NADZIRAH JAMRUS**
	FADHLINA IZZAH SAMAN
	NURULHUDA ZAINUDDIN
	HAZWA HANIM MOHAMED HAMZAH
	MOHD HAFIFI MOHD SUPIR
	ADI HAKIM TALIB
CERTIFICATE	**NUR SYUHADA MUHAMMAT PAZIL**
	MARIATHY KARIM
	UMMU MARDHIAH ABDUL JALIL
	NOOR WAHIDA JAMIL
TECHNICAL & PROTOCOL	**DR. AHMAD FIRDAUS AHMAD FADZIL**
	ALBIN LEMUEL KUSHAN
	MOHD NABIL ZULHEMAY
SPONSOR	**TS. NURUL NAJWA ABDUL RAHID @ ABDUL RASHID**
	SHAHADAN SAAD
	FARIDAH SAPPAR
	SYAFNIDAR ABDUL HALIM
	SITI NURAMALINA JOHARI
LANGUAGE EDITOR	NUR AQILAH NORWAHI
	MOHD AMIRUL ATAN

BRONZE SPONSOR

AINON SYAZANA AB HAMID
ANITA MOHD YASIN
BUSHRA ABDUL HALIM
FARIDAH SAPPAR (Ts.)
FATIMAH HASHIM
HAZRATI ZAINI
MASTURA MANSOR
MASWATI SUFFIAN
NOORAZILAH IBRAHIM
NOR ADILA KEDIN
NOR AIZA MOKETAR (DR.)
NOR AZIDA MOHAMED NOH
NOR INTAN SHAFINI NASARUDDIN
NURUL HIDAYAH MAT ZAIN (Ts. DR.)
NURUL NAJWA ABDUL RAHID @ ABDUL RASHID (Ts.)
NURULHUDA GHAZALI (Ts.)
RAIHAH AMINUDDIN (DR.)
SALEHAH HAMZAH
SHAHITUL BADARIAH SULAIMAN
SITI AISYAH ABDUL KADIR
SITI NURAMALINA JOHARI
SITI RAMIZAH JAMA
SURYAEFIZA KARJANTO (DR.)
SYAFNIDAR ABDUL HALIM
UMMU MARDHIAH ABDUL JALIL
ZAINAB OTHMAN
ZURAH ABU

LIST OF REVIEWERS

FADILAH EZLINA SHAHBUDIN
FADZLIN AHMADON
FARAH NADZIRAH JAMRUS
HAJAR IZZATI MOHD GHAZALLI
HAZRATI ZAINI
NOR AIZA MOKETAR (DR.)
NOR INTAN SHAFINI NASARUDDIN
NURUL NAJWA ABDUL RAHID @ ABDUL RASHID (Ts.)
RAIHAH AMINUDDIN (DR.)
RAIHANA MD SAIDI (Ts.)
SHAFAF IBRAHIM (Ts. DR.)
SITI FEIRUSZ AHMAD FESOL (DR.)
SITI MAISARAH MD ZAIN
SITI NURAMALINA JOHARI
SURYAEFIZA KARJANTO (DR.)

CONTENTS

ID	PROJECT TITLE	PAGE
JM008	Automation in Pneumonia Detection	1
JM017	Terengganu Cultural Trail: Using Videography in a Participant-observer Study to Enhance Cultural Heritage Appreciation Among Children.	5
JM019	Cassava Leaf Disease Detection System using Support Vector Machine	8
JM021	Learning Mathematics using Fun-Math Mobile Application for Pre-School	12
JM024	OSH-DBG as a Method of Digital Problem-Solving for Learning Construction Safety and Health Course	16
JM026	"What to Cook?" Mobile Application	19
JM028	Learning Arabic Communication Skill Through Mobile Application	23
JM034	Enhanced Gamification in Study Skills	27
JM039	Flexible Learning Using ANATEKS Flexi e-Content Medium: An Innovative Effort in Times of Covid-19 Pandemic	31
JM043	Web-Application for Securing Message Using LSB Algorithm Steganography and Hybrid Encryption	35
JM045	Web-Based Science Lab Inventory System for Faculty of Pharmacy in UiTM Bertam	39
JM046	Dental Treatment Orientation for Children using Role Playing Game	43
JM047	EZ Forecast 2.0: A System of Univariate Models	47
JM048	Arduino-based Farm Feeder Helper	51
JM050	PictoEZodit (E-Comic In Teaching Practice)	55
JM054	i-CHEMTORIALS (Interactive Chemistry Tutorials)	59

JM056	Chemical Composition and Biological Activity of Momordica charantia (Bitter Melon)	63
JM059	Lima Sekawan: An Entrepreneurial App Based Introductory Tools for Kids	66
JM064	A Study on Factors Toward Household Willingness on E-Waste Recycling in Seremban	69
JM070	PEFE (Plant Eco-Friendly Energizer)	73
JM071	An Intelligent of ANN Towards Agarwood Oil Compounds Pre-processing Based on Stepwise Regression Method to Improve the Oil Quality	76
JM080	Paddyville: Learning Paddy Cultivation through Role-Playing Game	80
JM089	Agarwood Oil Quality Classification Using One Versus All Strategies in Multiclass on SVM Model	84
JM099	The Development of E-Content 'Sci-Anime2021'for PDPR during Covid-19 Era	87

i-JaMCSIIX 2021
Exploring ideas
International Jasin Multimedia & Computer Science Invention and Innovation Exhibition

Web-Application For Securing Message Using LSB Algorithm Steganography And Hybrid Encryption

Muhammad Khairul Amin bin Mohd Nai[1] , Nurul Huda Nik Zulkipli[2], Siti Rahayu Abdul Aziz[3]

[1,2,3] Universiti Teknologi MARA, Malaysia

khairulamin9710@gmail.com, nurulhuda8459@uitm.edu.my, rahayu748@uitm.edu.my

Abstract— **The study of data security has become a critical issue as data communication across computer networks has grown. Sending data through normal network traffic poses a high risk, particularly in the case of a man-in-the-middle attack, and even if the user uses encryption on the data, it poses a risk because it raises suspicions about the nature of the data. The objective of this study is to develop a web application for securing messages using steganography with the Least Significant Bit (LSB) Algorithm and Hybrid Encryption that encrypts user input and conceals it in an image file to provide the highest level of security for messages sent and received. The steganography technique is used to mask the data as it hides inside insusceptible image files and is secure to send through normal traffic since Rivest–Shamir–Adleman (RSA) algorithm is used as an additional layer of security, which can only open it via the intended target with its private keys. The benefit of using this system is the messages are hidden in an ordinary-looking image file, and it will be undetectable and unaffected. Even if the steganalysis is successfully decrypted, the hybrid features of encryption will undoubtedly impede or significantly will slow down the decryption process in terms of security.**

Keywords—steganography, hybrid encryption, security, LSB Algorithm

I. INTRODUCTION

In this era of modern technology, one of the biggest concerns is the security of data exchanged through the Internet. Many researchers have devised a variety of techniques to limit the risk, including cryptography. Even still, cryptography is not enough since hackers are getting better and faster at breaking it down. As a result, they devised a technique known as steganography.

Encryption is a form of cryptography that converting an original representation of data known as plaintext into an unreadable alternative known as cyphertext. Asymmetric and symmetric cryptography are the two types of encryptions. Rivest–Shamir–Adleman (RSA) is the most popular asymmetric algorithm [1], while Data Encryption Standard (DES) is a symmetric algorithm (DES). Steganography, on the other hand, is much more unique because it employs the science and art of concealing the existence of messages through another medium, such as an image file, an audio file, or even a video file. Each type of file into which it can be hidden employs a different algorithm. Although both cryptography and steganography methods provide security, combining cryptography and steganography into a single system provides greater security and confidentiality [2].

This project is focused on how cryptography, encryption, and may be used to help protect messages from sender to recipient by offering a high level of security. The reason for not using encryption alone is that steganography can mask the existence of the message, reducing the risk by lowering its susceptibility to being an important message. The messages to be sent are practically safe because they arrived in an unobtrusive format such as a picture or video, and if the steganography is discovered and decrypted, the second layer of encryption is available to prevent or slow down the decryption. Fig.1 shows the combination of cryptography and steganography.

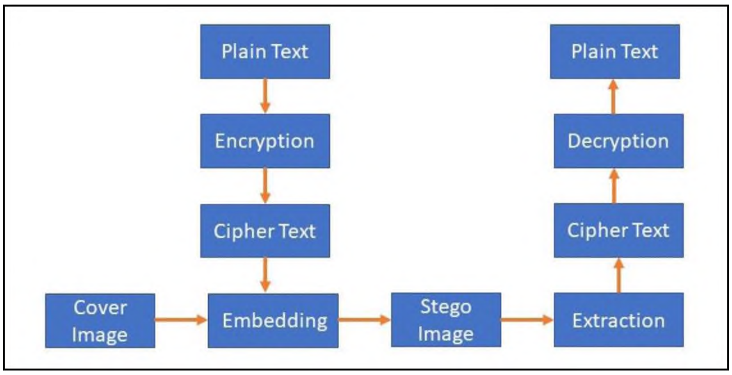


Fig. 1. Cryptography and Steganography

II. LITERATURE REVIEW

A literature review is discussed in this research to identify sources and gaps in the current knowledge. These include, review the existing system, procedures and techniques which can be used in this project development

A. *Image Steganography Technique*

Image steganography is one of the techniques in steganography which the information is hidden inside an image files either in a form of JPEG, BMP or any other forms. Steganography is the combination of science and art used to write secret messages so that only the intended recipient is aware of their existence [3] [4]. The original image, before any message is hidden in it, is referred to as the cover image. After hiding the message in it, it is referred to as the stego image [5] . Image steganography is the most frequently used especially for creating a project as it can be considered as the easiest to make.

B. *LSB – Steganography Algorithm*

LSB (Least Significant Bit) is the most common algorithm used for image-based steganography due to its simplicity and better for a beginner to use. However, it is the most easily to be detected because the noise it is created are a lot In the LSB method the 8th bit of every byte of the carrier file is substituted by one bit of the secret information. Instead of hiding a fixed number of bits in the LSBs of each pixel, one can also embed different number of bits in LSBs of different pixels based on pixel value range calculation [6].

C. *RSA- Encryption Algorithm*

RSA encryption is an asymmetric cryptographic algorithm which used to encrypt and decrypt message. It features public key and private key which the public key is used to encrypt message while the private key is used to decrypt message. This is the most commonly used public key cryptographic algorithm [7] , and it is considered secure when sufficiently long keys are used. The security of RSA depends on the difficulty of factoring large integers. Difficulty of factoring n to find the original primes p,q defines the strength of RSA [8].

D. *Related Work*

Al-Shabby and Al-Kharobi [9] proposed a method that encrypts the message with the AES algorithm and hashes the key with the SHA-12 algorithm. Following that, the encrypted message will be embedded into an image, video, or audio using a modified LSB technique. Because of the skimming mechanism used in the process, the percentage of concealment in this method is lower than in traditional techniques of space left without hiding. As a result, it is recommended to utilise an image with a lot of details.

Sathiaraj et al. [10], proposed a method that involves first transcribing text written in handwritten documents into digital text, which can be accomplished using a neural network deep learning approach. The proposed model employs a key that encrypts the key and is padded with extra bits to create a 256-bit unique key. After obtaining the text, it will be converted to unintelligible or ciphertext using the pad cypher technique. The encrypted text will then be tainted with LSB steganography. Because each encryption uses a unique 256-bit key, the proposed method is resistant to brute force attacks.

The proposed method in [11], combines Double-Stegging and RSA encryption. The secret data is encrypted in the first stage using the public key in the RSA algorithm to generate the cypher key as well as the public and private encryption keys. Using Haar's wavelet steganography, this text will be converted into 8-bit binary codes and embedded in the 2-Dimensional Discrete Wavelet Transform (2-DWT). Because it can transmit confidential data with minimal distortion to the cover image, double-stegging produces the best peak signal-to-noise ratio (PSNR) value.

According to [12], the proposed method employs double-layered encryption in conjunction with LSB steganography. First, the intended text will be encrypted with the DES algorithm and a key. The key is then concealed using the RSA technique, which encrypts the key before sending it separately. Using the LSB algorithm, the encrypted text is then embedded in an image. Because LSB is easily decoded, this proposed algorithm adds an extra layer of security.

III. METHODS

Iterative waterfall model has been chosen for this project methodology. In this model, each stage need to be completed before the next phase begin. This method is improvised version of normal waterfall method that more suitable for this case.

The design of system as shown in Fig. 2 involves the process of the front end and the back end of the system. It depicted the user uploading the image into the system. Then, the user will input the message and confirm to be encrypted. The process however will be done in the Google Drive. After it is done, the output will be located at the same Google Drive. The other party who wants the message will download the encrypted image located in the Google Drive and with the same system, decryption is available. The decryption process will be done in the Google Drive too.

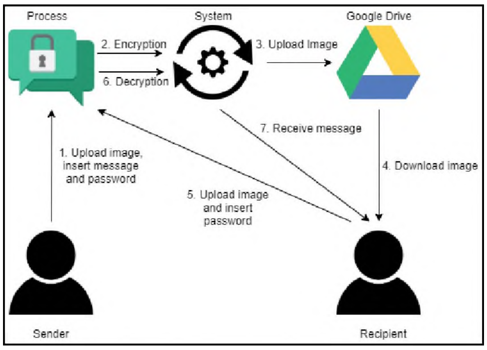


Fig. 2. System Design

The project's implementation is divided into six stages, which are as follows; (1) Upload the image file (.png), (2) Encrypt the text data using RSA and generate the encryption keys, (3) Encrypt the Public key and message with AES, (4) Embed the private key and encrypted message into the image using the LSB algorithm, (5) Extract the encrypted data from the Image files, (6) Decrypt the text data using the decryption key.

IV. RESULTS AND FINDINGS

The analysis of the result from the steganography with LSB algorithm and hybrid encryption will be recorded and checked whether it managed to achieve all the objectives aforementioned while having a perfect effectiveness in its functionality.

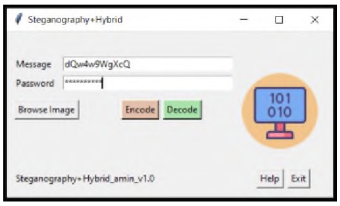
A. Encode The Message Into The Image

For the encode part which is encrypted the user's message and then embedded it into the image previously uploaded, the user is required to input the message they desired and the password for the verification when decoding later as shown in Fig. 3. Below are the following steps and flow of the system:

1) The user is required to upload a PNG file, or it will prompt an error showing that it will only receive a PNG file and none other.

2) The user is required to input the message they desired and the password for the verification when decoding later.

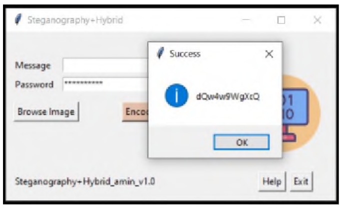
3) After the successfully encode the message into the image as well as clicked on OK button, the system will then automatically try to upload the image into the Google Drive that the path has been set beforehand.


Steganography+Hybrid

Message dQw4w9WgXcQ

Password **********

Fig. 3. Encode the Message into the Image


Steganography+Hybrid

Message

Password **********

Success

dQw4w9WgXcQ

Fig. 4. Encode the Message into the Image

B. Decode The Message From The Image

The intended flow of the system is that the second party will download the encrypted image in the Google Drive to decode it. That second party then, supposedly will run the system and to decode it, it will be required only uploading that particular image and input the password for verification as shown in Fig. 4. Below are the following steps and flow of the system

1) The intended flow of the system is that the second party will download the encrypted image in the Google Drive to decode it.

2) The user now only required to upload that particular image and input the password for verification

The steganography used a simple algorithm which can be easily detected and decoded. It is so simple to the point that it can be done through uploading the encrypted image to any steganography decode software or website. However, the hybrid encryption became the second layer of security that protected the image to be easily decoded.

A testing has been conducted on other application with similar method which steganography. One of the applications only managed to read a long string of unreadable characters because the tools does not able to decrypt through the hybrid encryption.

Another application has been chosen for the test and this time, the tools itself unable to find the existence of the encrypted message. So, it prompts a message that there is no hidden message at all found in the image. Similar result has been found to yet another application which result in unable to find the existence of encrypted message from the image uploaded.

V. CONCLUSIONS

This web application system was successfully developed and managed to meet the aim and objectives of the project by providing back-end security using LSB algorithm for steganography and hybrid type of encryption. The objective of this project is that the project is design and develop for the security purpose. While the aim of this project is that the user is able to embed a message into the image chosen and upload it to the Google Drive whilst the second party or the receiver will then download the image and able to extract the message back into the original plain text.

ACKNOWLEDGMENT

We would like to give our special thanks to Universiti Teknologi MARA's Student Development Fund (TAPA) as the sponsor to this paper publication.

REFERENCES

[1] Rivest R L, Shamir A and Adleman L 1983 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM

[2] Saraireh S. S., Saraireh M. S., Saraireh S. S., and Saraireh M. S. (2017, Feb), "Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange," Int. J. Commun. Antenna Propag., vol. 7, no. 1, p. 1.

[3] Şahin, F., Çevik, T., & Takaoğlu, M. Review of the Literature on the Steganography Concept. International Journal of Computer Applications, 975, 8887.

[4] S. Natanj, and S. R. Taghizadeh, "Current Steganography Approaches: A survey." International Journal of Advanced Research in Computer Science and Software Engineering, IJARCSSE, 1(1), 1-8, 2011.

[5] Munikar, M. (2019). Image Steganography : Basic Concepts and Proposed Algorithm Image Steganography : Basic Concepts and Proposed Algorithm. September.

[6] Kumar, R., & Bhatia, R. K. (2012). Global Trends in Information Systems and Software Applications. Communications in Computer and Information Science, 270(PART II), 202–211. https://doi.org/10.1007/978-3-642-29216-3A. A. Chincholkar, and D. A. Urkude "Design and Implementation of Image Steganography." Journal of Signal and Image Processing, 3(3), 111-113, 2012.

[7] Rivest R L, Shamir A and Adleman L 1983 A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications of the ACM

[8] Tahir, A. S. (2015). Design and Implementation of RSA Algorithm using FPGA. International Journal of Computers & Technology, 14(12), 6361–6367. https://doi.org/10.24297/ijct.v14i12.1737

[9] AL-Shaaby, A. A., & AlKharobi, T. (2017). Cryptography and Steganography: New Approach. Transactions on Networks and Communications, 5(6). https://doi.org/10.14738/tnc.56.3914

[10] Sathiaraj, S. J. F. G., Pingale, G. S., Majumdar, S., Shaikh, S. J., & Thakare, B. S. (2019). Secure Transfer of Image-Acquired Text Using a Combination of Cryptography and Steganography. 1st IEEE International Conference on Advances in Information Technology, ICAIT 2019 - Proceedings, July 2019, 146–152. https://doi.org/10.1109/ICAIT47043.2019.8987361

[11] Nadiya, P. V., & Imran, B. M. (2013, February). Image steganography in DWT domain using double-stegging with RSA encryption. In 2013 International Conference on Signal Processing, Image Processing & Pattern Recognition (pp. 283-287). IEEE.

[12] Gowda, S. N. (2017). Dual layered secure algorithm for image steganography. Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, ICATccT 2016, December, 22–24. https://doi.org/10.1109/ICATCCT.2016.7911959