THE REPUBLIC OF INDONESIA DEFENSE UNIVERSITY

COMBINATION DESIGN OF TRIPLE DATA ENCRYPTION STANDARD (3DES) – CRYPTOGRAPHY AND LEAST SIGNIFICANT BIT (LSB) – STEGANOGRAPHY ON ZIPPED INFORMATION PACKAGE (ZIP) EXTENDED CLASSIFIED DOCUMENTS

ADITYAN WISNU YUDA PRASETYA
120220405002

This Thesis was Written for the Fullfillment of the Requirement
to Earn Master's Degree in Defense Science

FACULTY OF DEFENSE SCIENCE AND TECHNOLOGY
CYBER DEFENSE ENGINEERING STUDY PROGRAM

BOGOR
2024

THE REPUBLIC OF INDONESIA DEFENSE UNIVERSITY

COMBINATION DESIGN OF TRIPLE DATA ENCRYPTION STANDARD (3DES) – CRYPTOGRAPHY AND LEAST SIGNIFICANT BIT (LSB) – STEGANOGRAPHY ON ZIPPED INFORMATION PACKAGE (ZIP) EXTENDED CLASSIFIED DOCUMENTS

ADITYAN WISNU YUDA PRASETYA
120220405002

This Thesis was Written for the Fullfillment of the Requirement
to Earn Master's Degree in Defense Science

FACULTY OF DEFENSE SCIENCE AND TECHNOLOGY
CYBER DEFENSE ENGINEERING STUDY PROGRAM

BOGOR
2024

THESIS APPROVAL SHEET

Student Name	:	Adityan Wisnu Yuda Prasetya
Student Identity Number	:	120220405002
Study Program	:	Cyber Defense Engineering
Faculty	:	Defense Science and Technology
Thesis Title	:	Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents

Advisor I,

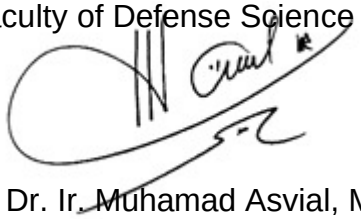
Dr. Bambang Suhardjo, S.Si., M.Si., M.Kom.
Captain NRP 10830/P
Date: 24 Januari 2024

Advisor II,

Dr. Ir. Rinaldi Munir, M.T.

Date: 24 Januari 2024

Acknowledged by,
Dean of The Faculty of Defense Science and Technology,



Prof. Dr. Ir. Muhamad Asvial, M.Eng.
First Class Administrator
Date: 25 Januari 2024

THESIS VALIDATION SHEET

Student Name	:	Adityan Wisnu Yuda Prasetya
Student Identity Number	:	120220405002
Study Program	:	Cyber Defense Engineering
Faculty	:	Defense Science and Technology
Thesis Title	:	Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents

No	Name	Signature	Date
1.	Advisor I: Dr. Bambang Suhardjo, S.Si., M.Si., M.Kom. Captain NRP 10830/P		29-Jan-2024
2.	Advisor II: Dr. Ir. Rinaldi Munir, M.T.		24 Januari 2024
3.	Reviewer I: Dr. H.A. Danang Rimbawa, S.Si., M.T., M.Tr.Opsla., CEH., CSBA., IPM., ASEAN Eng. Captain NRP 10829/P		23/1/2024
4.	Reviewer II: Dr. Hendrana Tjahjadi, S.T., M.Si.		23 Januari 2024
5.	Reviewer III: Dr. Hondor Saragih, S.T., M.Si(Han). Commander NRP 14633/P		23/Jan/2024

DECLARATION OF ORIGINALITY

Hereby I acknowledge that this thesis does not contain some or the whole parts of previously published works that had been submitted to earn any scholarly degree in any University; and to the best of my knowledge and belief, there are no idioms, phrases, sentences, paragraphs, sub-chapters or chapters from any written or published works; except what was written in this thesis and mentioned in the Reference section.

If in the future this thesis is proven to be plagiarizing any previous existing works, I would accept the punishment as stated in the relevant and applicable laws/regulations.

Bogor, January 22th, 2024

Adityan Wisnu Yuda Prasetya

PREFACE

I would like to extend my gratitude to The Almighty God for His blessings and grace, so that this thesis with title “Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents” has finally been completed.

This thesis is written as a requirement to Master’s Degree in Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology, the Republic of Indonesia Defense University.

The completion of this thesis is possible due to the dirrect or indirect help and support from various parties. Therefore, please allow me to extend my gratitude to:

1. Lieutenant General Jonni Mahroza, S.I.P., M.A., M.Sc., CIQnR., CIQaR., Ph.D. as Rector of the Republic of Indonesia Defense University.
2. Brigadier General Andi Tjarwandi, S.E., M.M. as Dirkuad.
3. Brigadier General Dodo Irmanto, S.I.P., M.Si. as Danpoltekad Kodiklatad.
4. Captain Dr. H.A. Danang Rimbawa, S.Si., M.T., M.Tr.Opsla. as Head of Cyber Defense Engineering Study Program, Faculty of Defense Science and Technology, Republic of Indonesia Defense University and Reviewer I.
5. Captain Dr. Bambang Suhardjo, S.Si., M.Si., M.Kom. as Advisor I.
6. Colonel Nanang Pujo Sasongko, S.E. as Kakupus II Ditkuad.
7. Mr. Dr. Ir. Rinaldi Munir, M.T. as Advisor II.
8. Mr. Dr. Hendrana Tjahjadi, S.T., M.Si. as Reviewer II.
9. Commander Dr. Hondor Saragih, S.T., M.Si(Han). as Reviewer III.

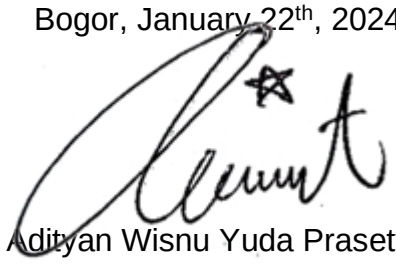
10. All of staff and students of Cyber Defense Engineering Study Program, Republic of Indonesia Defense University.
11. All of staff Ku Poltekad Kupus II Ditkuad
12. All of staff Poltekad Kodiklatad.
13. Father, mother and all of my family.

May God return your kind help and good deeds with a lot of good favor.

I realize that this thesis is far from perfect and thereby look forward to constructive critics and inputs from the readers for a better thesis in the future.

At last, I sincerely hope that this thesis would be beneficial to the development of defense science and useful to all related stakeholders in attempt to cyber defense.

Bogor, January 22th, 2024



Adityan Wisnu Yuda Prasetya

ABSTRACT

COMBINATION DESIGN OF TRIPLE DATA ENCRYPTION STANDARD (3DES) – CRYPTOGRAPHY AND LEAST SIGNIFICANT BIT (LSB) – STEGANOGRAPHY ON ZIP EXTENDED CLASSIFIED DOCUMENTS

ADITYAN WISNU YUDA PRASETYA

Classified documents are very important information that must be protected, especially in transmission through electronic media. Currently, some government agencies have not all implemented security methods in sending classified documents. This research was prepared with the aim of improving security in sending classified documents in a government agency. In this research, several methods are used in combination, namely: Triple Data Encryption Standard (3DES) Cryptography, Least Significant Bit (LSB) Steganography and Zipped Information Package (ZIP) Compression. This combination design uses 50 sample objects (.pdf) ranging in size from 10 KB to 272 KB that are tested against cover images (.png) and videos (.mp4). The test resulted in a PSNR Stego - Video size of about 76.1267 dB and PSNR Stego - Image size of about 69.9054 dB. The PSNR size is quite effective in disguising the existence of a secret message so that there is no difference visually. Overall, the statistical analysis shows that this research fulfills the aspects of integrity, imperceptibility, capacity, recovery and fidelity. Based on the success of this research, it can be concluded that this research can be implemented to improve security in sending classified documents at Ku Poltekad Kupus II Ditkuad.

Keywords: Cryptography, Steganography, Compression, 3DES, LSB and ZIP

ABSTRAK

DESAIN KOMBINASI KRIPTOGRAFI *TRIPLE DATA ENCRYPTION STANDARD (3DES)* DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT (LSB)* PADA DOKUMEN BERKLASIFIKASI BEREKSTENSI *ZIPPED INFORMATION PACKAGE (ZIP)*

ADITYAN WISNU YUDA PRASETYA

Dokumen berklasifikasi adalah sebuah informasi yang sangat penting yang harus dilindungi terutama dalam pengiriman melalui media elektronik. Saat ini, beberapa instansi pemerintahan belum semuanya menerapkan metode keamanan dalam pengiriman dokumen berklasifikasi. Penelitian ini disusun dengan tujuan untuk meningkatkan keamanan dalam pengiriman dokumen berklasifikasi di suatu instansi pemerintahan. Dalam penelitian ini, digunakan beberapa metode yang dikombinasikan, yaitu: Kriptografi *Triple Data Encryption Standard (3DES)*, Steganografi *Least Significant Bit (LSB)* dan Kompresi *Zipped Information Package (ZIP)*. Desain kombinasi ini menggunakan objek sebanyak 50 sampel (.pdf) berukuran antara 10 KB sampai dengan 272 KB yang diujikan terhadap cover gambar (.png) dan video (.mp4). Pengujian tersebut menghasilkan ukuran *PSNR Stego – Video* sekitar 76,1267 dB dan *PSNR Stego – Image* sekitar 69,9054 dB. Ukuran *PSNR* tersebut cukup efektif dalam menyamarkan keberadaan pesan rahasia agar tidak terdapat perbedaan secara visual. Secara keseluruhan, dari analisis statistik yang dilakukan menunjukkan bahwa penelitian ini memenuhi aspek *integrity*, *imperceptibility, capacity, recovery* dan *fidelity*. Berdasarkan keberhasilan penelitian ini, maka dapat disimpulkan bahwa penelitian ini dapat diimplementasikan untuk meningkatkan keamanan dalam pengiriman dokumen berklasifikasi di Ku Poltekad Kupus II Ditkuad.

Kata Kunci: Kriptografi, Steganografi, Kompresi, *3DES, LSB* dan *ZIP*

TABLE OF CONTENTS

LIST OF CHARTS

LIST OF TABLES

LIST OF FIGURES

LIST OF GRAPHS

LIST OF ABBREVIATIONS

3DES	:	Triple Data Encryption Standard
A3DES	:	Anonymization 3DES
AEC	:	Absolute Edge Change
AES	:	Advanced Encryption Standard
APT	:	Advanced Persistent Threat
ASCII	:	American Standard Code for Information Interchange
ATM	:	Automated Teller Machine
AV	:	Audio Video
BSSN	:	Badan Siber dan Sandi Negara (National Cyber and Crypto Agency)
CAST	:	Carlisle Adams and Stafford Tavares
CF	:	Compression Factor
CPU	:	Central Processing Unit
CR	:	Compression Ratio
CVD	:	Cover Value Difference
dB	:	Decibel
DCT	:	Discrete Cosine Transform
DDoS	:	Distributed Denial of Service
DES	:	Data Encyrption Standard
EC	:	Embedding Capacity
ECC	:	Elliptic Curve Cryptography
EDI	:	Electronic Data Interchange
ESDM	:	Energi dan Sumber Daya Mineral (Energy and Mineral Resources)
FEAL	:	Fast Data Encipherment Algorithm
FIPS	:	Federal Information Processing Standard
GUI	:	Graphical User Interface
HH	:	High High
HL	:	High Low
ICT	:	Information and Communication Technology
IDEA	:	International Data Encryption Algorithm
IIV	:	Infrastruktur Informasi Vital (Critical Information Infrastructure)
IP	:	Initial Permutation
ITE	:	Informasi dan Transaksi Elektronik (Electronic Information and Transaction)
IWT	:	Integer Wavelet Transform
KBBI	:	Kamus Besar Bahasa Indonesia (Dictionary of Indonesian Languange)
Ku Poltekad	:	Keuangan Politeknik Angkatan Darat (Finance of Army College)
LH	:	Low High
LSB	:	Least Significant Bit
LZW	:	Lempel-Ziv-Welch
MARS	:	Multiple Algorithm Rijndael Submission

MCT	:	Military Cryptography Technology
MMB	:	Massey, Mills, and Broadcast
MPVD	:	Modified Pixel Value Differencing
MSB	:	Most Significat Bit
MSE	:	Mean Square Error
NIST	:	National Institute of Standards and Technology
NKRI	:	Negara Kesatuan Republik Indonesia (Unitary State of The Republic of Indonesia)
NPCR	:	Number of Pixels Changing Rate
n-RBR	:	n-Rightmost Bit Replacement
OTP	:	One Time Pad
P - Box	:	Permutation Box
Paku	:	Perwira Keuangan (Financial Officer)
PC	:	Permuted Choice
PDH	:	Pixel Difference Histogram
Polri	:	Kepolisian Negara Republik Indonesia (Indonesian National Police)
PSDN	:	Pengelolaan Sumber Daya Nasional (National Resource Management)
PSNR	:	Peak Signal to Noise Ratio
RC4	:	Rivest Cipher 4
RDH	:	Reversible Data Hiding
RDP	:	Remote Desktop Protocol
RGB	:	Red Green Blue
RLE	:	Run-Length Encoding
RSA	:	Rivest, Shamir, and Adleman
S - Box	:	Subtitution Box
SAFER	:	Secure and Fast Encryption Routine
SARA	:	Suku, Agama, Ras dan Antargolongan (Ethnicity, Religion, Race and Intergroup)
Sishankamrata	:	Sistem Pertahanan dan Keamanan Rakyat Semesta (Universal People's Defense and Security System)
SMS	:	Short Message Service
SP	:	Saving Percentage
SSL	:	Secure Socket Layer
TNI	:	Tentara Nasional Indonesia (Indonesian National Military)
TV	:	Television
UACI	:	Unifed Average Changing Intensity
VLC	:	Video LAN Client
ZIP	:	Zipped Information Package

KEMENTERIAN PERTAHANAN RI
UNIVERSITAS PERTAHANAN RI
Terakreditasi BAN-PT "A"

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Yang bertanda tangan di bawah ini, saya :

Nama	:	Adityan Wisnu Yuda Prasetya
NIM	:	120220405002
Program Studi/Fakultas	:	S2 – Rekayasa Pertahanan Siber / Fakultas Sains dan Teknologi Pertahanan
HP/E-mail	:	081222217695 / adityan.wisnu@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada UPA Perpustakaan Universitas Pertahanan Republik Indonesia, Hak Bebas Royalti *Non-Eksklusif* (*Non-exclusive Royalty-Free Right)* atas karya ilmiah yang berjudul:

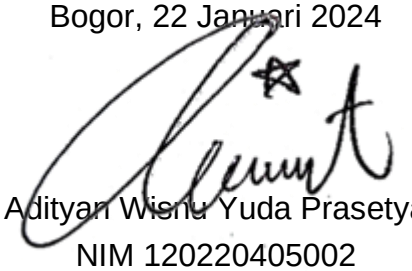
"Combination Design of Triple Data Encryption Standard (3DES) – Cryptography and Least Significant Bit (LSB) – Steganography on Zipped Information Package (ZIP) Extended Classified Documents"

Beserta perangkat yang diperlukan (apabila ada). Dengan Hak Bebas Royalti *Non-Eksklusif* (*Non-exclusive Royalty-Free Right)* ini UPA Perpustakaan Universitas Pertahanan Republik Indonesia berhak menyimpan, mengalih media/formatkan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya, dan menampilkan/mempublikasikannya di internet atau media lain untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencatumkan nama saya sebagai penulis/pencipta.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak UPA Perpustakaan Universitas Pertahanan Republik Indonesia, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini saya buat dengan sebenarnya.

Bogor, 22 Januari 2024



Adityan Wisnu Yuda Prasetya
NIM 120220405002