IMPLEMENTASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

Oleh:
Delvira Salsabilla Milania
NIM. 18610042

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2024

IMPLEMENTASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan
dalam Memperoleh Gelar Sarjana Matematika (S.Mat.)

Oleh:
Delvira Salsabilla Milania
NIM. 18610042

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2024

IMPLEMENTASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

Oleh:
Delvira Salsabilla Milania
NIM. 18610042

Telah Disetujui Untuk Diuji
Malang, 18 Desember 2024

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Nafie Jauhari, M.Si	Ach. Nashichuddin, MA
NIPPPK. 19870218 202321 1 018	NIP.19730705 200003 1 002

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

IMPLEMENTASI KRIPTOGRAFI RSA DAN STEGANOGRAFI LSB DALAM PENYISIPAN PESAN PADA CITRA DIGITAL

SKRIPSI

Oleh
Delvira Salsabilla Milania
NIM. 18610042

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 23 Desember 2024

Ketua Penguji	: Prof. Dr. H. Turmudi, M.Si, Ph.D.,	.....
Anggota Penguji 1	: Muhammad Khudzaifah, M.Si.,	.....
Anggota Penguji 2	: Muhammad Nafie Jauhari, M.Si.,	.....
Anggota Penguji 3	: Ach. Nashichuddin, MA	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini

Nama : Delvira Salsabilla Milania

NIM : 18610042

Program Studi : Matematika

Fakultas : Sains dan Teknologi

Judul Skripsi : Implementasi Kriptografi RSA dan Steganografi LSB dalam Penyipan Pesan pada Citra Digital

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini merupakan hasil karya saya sendiri, bukan pengambilan tulisan atau pemikiran orang lain yang saya akui sebagai pemikiran saya, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka di halaman terakhir. Apabila dikemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 23 Desember 2024

Yang membuat pernyataan,

Delvira Salsabilla Milania

NIM. 18610042

HALAMAN MOTO

“Sampaikan amanah dengan penuh keadilan, karena Allah Maha Melihat dan Maha Mendengar”

HALAMAN PERSEMBAHAN

Bismillahirrahmanirrahim

Skripsi ini penulis persembahkan kepada:

Seluruh keluarga penulis, terkhusus kepada kedua orang tua penulis, Bapak Eko Widarto dan Ibu Nurvita yang mempercayai penulis dalam setiap proses demi proses yang penulis lewati serta senantiasa menemani penulis melalui doa yang tidak pernah lelah dipanjatkan di sepertiga malam. Tidak lupa atas besarnya pengorbanan dukungan material yang diberikan keduanya untuk kelancaran penulis dalam menyelesaikan tugas akhir ini. Serta kepada seluruh teman-teman, yang selalu bersedia menjadi pendengar keluh kesah penulis dan tak lupa memberi nasihat agar penulis semangat mengerjakan skripsi. *Last but not least,* kepada diri saya sendiri yang telah berjuang hingga sejauh ini, dan memilih untuk membersamai Allah di setiap prosesnya, serta percaya atas segala ketetapan-Nya.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Alhamdulillah Wa Syukurillah, Segala puji hanya bagi Allah SWT, penulis merasa bersyukur karena dengan rahmat dan pertolongan-Nya, penulisan skripsi berjudul "Implementasi Kriptografi RSA dan Steganografi LSB dalam Penyipisan Pesan Pada Citra Digital" dapat diselesaikan. Skripsi ini merupakan syarat untuk memperoleh gelar sarjana dalam bidang Matematika di Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Shalawat dan salam senantiasa disampaikan kepada Nabi besar Muhammad SAW, yang telah memberikan petunjuk kepada umat manusia dari masa kebodohan (jahiliyah) menuju masa yang penuh cahaya, yaitu era agama Islam. Semoga kita semua nantinya mendapatkan syafaatnya di hari kiamat. *Aamiin, yaa rabbal, alamiin.*

Dalam proses penulisan skripsi ini, tidak dapat dipisahkan dari kontribusi dan dukungan berbagai pihak. Oleh karena itu, penulis ingin mengungkapkan rasa terima kasih yang sangat besar kepada semua pihak terkait:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. Sri Harini, M.Si, selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc, selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Nafie Jauhari, M.Si., selaku dosen pembimbing I yang telah bersedia memberikan ilmu dan arahan serta masukan kepada penulis sehingga penulis bisa menyelesaikan skripsi.
5. Ach. Nashichuddin,MA., selaku dosen pembimbing II yang telah memberikan arahan, masukan dalam bidang keagamaan kepada penulis dalam menentukan integrasi pada skripsi ini.
6. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim yang telah membantu, mendoakan dan memotivasi penulis dalam menyelesaikan skripsi.

7. Kedua orang tua tercinta, Ibu Nurvita dan Bapak Eko Widarto yang telah mendukung, mendoakan dan memotivasi sepanjang waktu, kedua orang tua yang terus memberikan kekuatan mental dan dorongan spiritual untuk penulis dalam menyelesaikan skripsi.
8. Seluruh teman-teman dari segala angkatan yang telah meluangkan waktu membantu penulis dalam menyelesaikan skripsi,
9. Pihak-pihak di luar yang tidak dapat disebutkan satu-persatu, yang telah ikut serta berperan dalam membantu penulis menyelesaikan skripsi.

Semoga Allah SWT melimpahkan rahmat dan karunia-Nya kepada kita semua. Saat menyusun skripsi ini, penulis menyadari bahwa masih terdapat kekurangan yang perlu diperbaiki. Meskipun demikian, harapannya adalah agar skripsi ini dapat memberikan manfaat dan nilai positif, terutama bagi penulis dan pembaca. *Aamiin ya rabbal aalamiin.*

Wassalamualaikum Warahmatullahi Wabarakatuh.

Malang, 23 Desember 2024

Penulis

DAFTAR ISI

DAFTAR SIMBOL

p, q	:	Bilangan prima yang besar
n	:	Modulus
$\varphi(n)$	:	Fungsi Euler
e	:	Eksponen publik
d	:	Eksponen privat
C	:	Cipherteks
M	:	Plaintext
(e,n)	:	Kunci publik (public key)
(d,n)	:	Kunci privat (private key)

ABSTRAK

Milania, Delvira Salsabilla. 2024. **Implementasi Kriptografi RSA dan Steganografi LSB dalam Penyisipan Pesan Pada Citra Digital**. Skripsi. Program Studi Matematika Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing: (I) Muhammad Nafie Jauhari, M.Si. (II) Ach. Nashicuddin, MA.

Kata kunci: Kriptografi RSA, Steganografi LSB, Penyisipan Pesan dan Citra Digital.

Keamanan data menjadi salah satu tantangan utama di era digital, terutama dalam menjaga kerahasiaan informasi sensitif yang ditransmisikan melalui jaringan. Data yang tidak dilindungi dengan baik berisiko menjadi sasaran serangan seperti pencurian, manipulasi, atau akses tidak sah. Kriptografi dan steganografi adalah dua teknologi yang secara luas digunakan untuk meningkatkan keamanan data. Penelitian ini mengusulkan kombinasi algoritma kriptografi RSA dengan teknik steganografi Least Significant Bit (LSB) untuk menyisipkan pesan rahasia ke dalam citra digital. Kriptografi RSA dipilih karena tingkat keamanan yang tinggi dengan menggunakan pasangan kunci publik dan privat, sedangkan metode LSB memungkinkan penyisipan pesan secara tersembunyi tanpa memengaruhi kualitas visual citra secara signifikan. Kombinasi kedua metode ini dirancang untuk menciptakan perlindungan ganda, sehingga meningkatkan tingkat keamanan pesan dari ancaman pihak yang tidak berwenang.

Penelitian ini bertujuan untuk mengembangkan dan mengevaluasi sistem keamanan data yang menggabungkan RSA dan LSB. Proses penelitian dimulai dengan enkripsi pesan menggunakan kunci publik RSA untuk menghasilkan chipertek, yang kemudian dikonversi menjadi format biner dan disisipkan ke dalam citra digital menggunakan teknik LSB. Pada tahap dekripsi, pesan yang telah disisipkan diekstraksi dari citra dan diubah kembali menjadi plaintext menggunakan kunci privat RSA. Metode penelitian meliputi simulasi proses enkripsi, penyisipan, dan dekripsi, serta pengukuran efektivitas sistem melalui perhitungan Mean Squared Error (MSE) untuk membandingkan perbedaan antara citra asli dan citra hasil penyisipan. Selain itu, penelitian ini mengintegrasikan nilai-nilai Islam dalam menjaga amanah berdasarkan Al-Qur'an untuk memperkuat landasan etis dari solusi yang diusulkan.

Hasil penelitian menunjukkan bahwa kombinasi RSA dan LSB mampu memberikan perlindungan data yang optimal. Proses enkripsi dan dekripsi RSA memastikan keamanan data dengan menjaga integritas pesan, sementara metode LSB menyembunyikan pesan secara efektif dalam citra tanpa memengaruhi kualitas visual secara signifikan, yang dibuktikan dengan nilai MSE yang rendah. Selain aspek teknis, pendekatan ini juga sejalan dengan nilai moral dan keagamaan dalam menjaga amanah dan kerahasiaan informasi. Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam keamanan data digital, tidak hanya menawarkan solusi yang inovatif secara teknis tetapi juga memperhatikan nilai-nilai etis yang relevan. Sistem ini dapat menjadi model yang efektif untuk diterapkan dalam berbagai kebutuhan keamanan informasi di era digital.

ABSTRACT

Milania, Delvira Salsabilla. 2024. Implementation of RSA Cryptography and LSB Steganography for Embedding Messages in Digital Images. Thesis. Mathematics Study Program, Faculty of Science and Technology, Universitas Negeri Maulana Malik Ibrahim Malang. Advisors: (I) Muhammad Nafie Jauhari, M.Si., (II) Ach. Nashicuddin, MA.

Keywords: Keywords: RSA Cryptography, LSB Steganography, Message Insertion and Digital Images.

Data security is one of the main challenges in the digital era, especially in maintaining the confidentiality of sensitive information transmitted over the network. Data that is not properly protected is at risk of being the target of attacks such as theft, manipulation, or unauthorized access. Cryptography and steganography are two technologies that are widely used to improve data security. This study proposes a combination of the RSA cryptography algorithm with the Least Significant Bit (LSB) steganography technique to insert secret messages into digital images. RSA cryptography was chosen because of its high level of security using a pair of public and private keys, while the LSB method allows hidden message insertion without significantly affecting the visual quality of the image. The combination of these two methods is designed to create double protection, thereby increasing the level of message security from threats from unauthorized parties.

This study aims to develop and evaluate a data security system that combines RSA and LSB. The research process begins with message encryption using the RSA public key to produce ciphertext, which is then converted into binary format and inserted into the digital image using the LSB technique. At the decryption stage, the inserted message is extracted from the image and converted back into plaintext using the RSA private key. The research method includes simulation of the encryption, insertion, and decryption processes, as well as measuring the effectiveness of the system through the calculation of Mean Squared Error (MSE) to compare the differences between the original image and the embedded image. In addition, this study integrates Islamic values in maintaining trust based on the Qur'an to strengthen the ethical foundation of the proposed solution.

The results show that the combination of RSA and LSB is able to provide optimal data protection. The RSA encryption and decryption process ensures data security by maintaining message integrity, while the LSB method effectively hides messages in images without significantly affecting visual quality, as evidenced by the low MSE value. In addition to technical aspects, this approach is also in line with moral and religious values in maintaining the trust and confidentiality of information. Thus, this research makes a significant contribution to digital data security, not only offering technically innovative solutions but also considering relevant ethical values. This system can be an effective model to be applied in various information security needs in the digital era.

مستخلص البحث

ميلانيا، دلفيرا سلسبيلا. ٢٠٢٤ . **تنفيذ تشفير *RSA* وإخفاء المعلومات *LSB* في إدراج الرسائل في الصور الرقمية. البحثالجامعي** . برنامج دراسة الرياضيات، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية، مالانج. المشرف: (١) محمد نافع جوهري، M.Si. (٢) أحمد نا صح الدين .M.A

الكلمات المفتاحية: تشفير *RSA*، إخفاء المعلومات *LSB*، إخفاء الرسائل والصورة الرقمية.

يعد أمن البيانات في العصر الرقمي من التحديات الرئيسية ، خاصة في الحفاظ على سرية المعلومات الحساسة المنقولة عبر الشبكة. البيانات التي لم تتم حمايتها بشكل صحيح معرضة لخطر التعرض لهجمات مثل السرقة أو التلاعب أو الوصول غير المصرح به. التشفير وإخفاء المعلومات هما تقنيتان تستخدمان على نطاق واسع لتحسين أمان البيانات. يقترح هذا البحث مزيجًا من خوارزمية التشفير *RSA* وتقنية إخفاء المعلومات ذات البت الأقل أهمية (*LSB*) لإدراج رسائل سرية في الصور الرقمية. تم اختيار تشفير RSA بسبب مستوى الأمان العالي الذي يوفره باستخدام أزواج المفاتيح العامة والخاصة، بينما تسمح طريقة LSB بإدخال رسالة مخفية دون التأثير بشكل كبير على الجودة المرئية للصورة. تم تصميم الجمع بين هاتين الطريقتين لإنشاء حماية مزدوجة، وبالتالي زيادة مستوى أمان الرسالة من التهديدات الصادرة عن أطراف غير مصرح لها.

يهدف هذا البحث إلى تطوير وتقييم نظام أمن البيانات الذي يجمع بين *RSA* و*LSB*. تبدأ عملية البحث بتشفير الرسائل باستخدام مفتاح *RSA* العام لإنتاج نص مشفر، والذي يتم بعد ذلك تحويله إلى تنسيق ثنائي وإدراجه في صورة رقمية باستخدام تقنية *LSB*. في مرحلة فك التشفير، ثم استخراج الرسالة المضمنة من الصورة وتحويلها مرة أخرى إلى نص عادي باستخدام مفتاح *RSA* الخاص. تتضمن طرق البحث محاكاة عمليات التشفير والإدراج وفك التشفير، بالإضافة إلى قياس فعالية النظام من خلال حسابات متوسط الخطأ التربيعي (*MSE*) لمقارنة الاختلافات بين الصورة الأصلية والصورة المدرجة. بالإضافة إلى ذلك، يدمج هذا البحث القيم الإسلامية في الحفاظ على الثقة المبنية على القرآن لتعزيز الأساس الأخلاقي للحل المقترح.

تظهر نتائج البحث أن الجمع بين *RSA* و*LSB* قادر على توفير الحماية المثلى للبيانات. تضمن عملية التشفير وفك التشفير *RSA* أمان البيانات من خلال الحفاظ على سلامة الرسالة، بينما تقوم طريقة LSB بإخفاء الرسائل في الصور بشكل فعال دون التأثير بشكل كبير على الجودة المرئية، كما يتضح من انخفاض قيم *MSE*. وبصرف النظر عن الجوانب الفنية، فإن هذا النهج يتماشى أيضًا مع القيم الأخلاقية والدينية في الحفاظ على مصداقية وسرية المعلومات. وبالتالي، فإن هذا البحث يقدم مساهمة كبيرة في أمن البيانات الرقمية، ليس من خلال تقديم حل مبتكر تقنيًا فقط ولكن أيضًا مع مراعاة القيم الأخلاقية ذات الصلة أيضا. يمكن أن يكون هذا النظام نموذجًا فعالاً يمكن تطبيقه في مختلف احتياجات أمن المعلومات في العصر الرقمي.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini, penyampaian pesan melalui sejumlah saluran perantara, termasuk internet, media cetak, dan media sosial, jauh lebih mudah dari sebelumnya. Namun, tidak semua komunikasi terbuka untuk umum karena mengandung informasi sensitif. Kriptografi adalah metode untuk memastikan kerahasiaan pesan yang dikirim dengan mengodekan pesan rahasia ke dalam kode yang membuatnya tampak berbeda satu sama lain, sehingga pihak yang tidak berwenang dapat menguraikan pesan asli.

Kriptografi adalah salah satu cabang matematika yang mengamankan dan menjaga kerahasiaan pesan melalui sistem enkripsi dekripsi. Dekripsi mengubah komunikasi terenkripsi kembali ke bentuk aslinya, sementara enkripsi mengubahnya menjadi kode yang mudah dipecahkan. Dalam Yunani kuno kriptografi berarti "tulisan tersembunyi" dan memiliki sejarah penggunaan yang panjang. Kriptografi asimetris adalah metode enkripsi yang menggunakan sepasang kunci, yaitu kunci publik (public key) dan kunci privat (private key) salah satu contoh algoritma adalah RSA. Dengan penggunaan kunci enkripsi dan dekripsi yang terpisah dan sangat rahasia. RSA ditemukan oleh Rivest, Shamir, dan Adleman. Metode RSA sering digunakan karena sulitnya memfaktorkan bilangan besar. Metode ini penting untuk melindungi informasi sensitif dalam organisasi atau instansi.

Steganografi adalah seni dan ilmu menyembunyikan informasi dalam media lain, seperti teknik memasukkan pesan tersembunyi ke dalam gambar sehingga orang awam tidak akan menduga bahwa gambar tersebut menyimpan informasi rahasia. Dalam penelitian ini, metode steganografi yang digunakan adalah metode LSB (*Least Significant Bit*). Metode LSB bekerja dengan mengubah bit terakhir pada citra. Diharapkan, metode yang diterapkan dalam penelitian ini dapat menjaga kerahasiaan isi pesan dari pihak-pihak yang tidak berwenang dengan menggabungkan teknik kriptografi dan steganografi.

Berdasarkan penelitian sebelumnya yang dilakukan oleh (Hani, 2020) membahas tentang Algoritma Kriptografi dan Steganografi untuk Pengamanan Pesan ke dalam Citra. Namun, dalam penelitian tersebut, nilai p dan q yang digunakan dalam RSA relatif kecil, sehingga memungkinkan untuk ditebak dengan mudah. Fokus utama dalam penelitian ini adalah menggunakan nilai p dan q yang dapat berupa angka besar agar RSA sulit dipecahkan.

Berdasarkan paparan di atas, penelitian ini mengambil judul "Implementasi Kriptografi RSA dan Steganografi LSB dalam Penyisipan Pesan Pada Citra Digital".

Al-Qur'an menganjurkan manusia untuk menjaga rahasia yang diketahui dan harus menyimpan rahasia tersebut dengan baik, karena dalam surat An-Nisa ayat:

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat."

Menurut tafsir tahlili yang berisi Amanat Allah terhadap hamba-Nya yang harus dilaksanakan antara lain : melaksanakan apa yang diperintahkan-Nya dan menjauhi larangan-Nya Semua nikmat Allah berupa apa saja hendaklah kita manfaatkan untuk taqqarrub (mendekatkan diri) kepada-Nya. Pada tafsir tersebut, kita dianjurkan untuk memelihara dan menyampaikan amanah kepada pihak yang berhak, serupa dengan cara kita mengomunikasikan pesan secara utuh tanpa mengurangi atau menambah isinya, serta memastikan bahwa pesan tersebut sampai kepada penerima yang tepat. Untuk menjamin kerahasiaan pesan yang disampaikan, penerapan teknik kriptografi RSA sangat dianjurkan, karena diharapkan mampu menjaga privasi pesan secara optimal. Selain itu, untuk meningkatkan tingkat kerahasiaan pesan lebih lanjut, digunakan pula teknik steganografi dengan metode LSB pada gambar, sehingga pesan dapat disembunyikan dalam media citra dengan lebih efektif dan aman.

1.2 Rumusan Masalah

Dengan memperhatikan konteks yang telah dijelaskan sebelumnya, maka permasalahan yang dibahas dalam penelitian ini adalah:

1. Bagaimana proses enkripsi kode pesan dengan kriptografi RSA dan menyisipkan kode cipherteks ke dalam citra dengan steganografi LSB?
2. Bagaimana proses ekstraksi *stego image* dengan steganografi LSB serta proses dekripsi kode ciphertks dengan kriptografi RSA?

1.3 Tujuan Penelitian

Dengan merujuk pada rumusan masalah diatas, maka tujuan dari penelitian ini adalah:

1. Untuk mengetahui proses enkripsi kode pesan dengan kriptografi RSA dan proses menyisipkan kode cipherteks ke dalam citra dengan steganografi LSB.
2. Untuk mengetahui proses ekstraksi *stego image* dengan steganografi LSB serta proses dekripsi kode cipherteks dengan kriptografi RSA.

1.4 Manfaat Penelitian

Diharapkan penelitian ini dapat bermanfaat untuk peneliti maupun pembaca. Berikut manfaat yang diharapan dari penelitian ini adalah sebagai berikut:

1. Bagi peneliti

   Kriptografi dasar, matematika kriptografi (termasuk teori bilangan dan aritmatika modulo), teorema Euler, dan implementasi pemrograman semuanya dibahas secara lebih mendalam dalam materi kursus yang dapat digunakan peneliti untuk mendukung pekerjaan mereka.
2. Bagi Instansi

   Mengingat minat peserta program studi matematika terhadap aljabar tergolong jarang, penelitian ini akan menjadi tambahan yang berharga bagi pengetahuan yang ada dalam subjek tersebut.
3. Bagi pembaca

   Kriptografi dan steganografi dapat dipahami dengan lebih baik dengan bantuan referensi tambahan yang disediakan oleh penelitian ini.

1.5 Batasan Masalah

Berdasarkan pernyataan masalah dan tujuannya, penelitian ini dibatasi pada batasan-batasan berikut:

1. Pesan berupa teks.
2. Menggunakan citra RGB.
3. Metode Kriptografi yang digunakan adalah RSA, sedangkan metode Steganografi yang digunakan adalah LSB.

BAB II

KAJIAN TEORI

2.1 Teori Pendukung

Untuk menyiapkan bab pembahasan, kita akan membahas beberapa sumber tambahan yang mencakup teorema dan definisi yang relevan dengan masalah yang sedang dibahas.

2.1.1 Bilangan Prima

Bilangan prima adalah konsep dasar dalam matematika yang merujuk pada bilangan bulat positif yang lebih besar dari 1 dan hanya dapat dibagi oleh 1 dan dirinya sendiri. Dengan kata lain, bilangan prima memiliki tepat dua faktor pembagi. Contoh bilangan prima termasuk 2, 3, 5, 7, 11, dan seterusnya.. Ciri-ciri bilangan prima adalah:

1. Jika ada sesuatu yang dua faktor, maka hanya ada dua variabel yang terlibat 1 dan angka itu sendiri.
2. Lebih Besar dari satu yaitu bilangan prima harus lebih besar dari 1. Angka 1 tidak dianggap sebagai bilangan prima.
3. Tidak Genap yaitu semua bilangan prima kecuali 2 adalah bilangan ganjil. Bilangan genap lainnya dapat dibagi oleh 2, sehingga memiliki lebih dari dua faktor.

2.1.2 Faktor Persekuatuan Terbesar

Menurut definisi, Faktor Persekutuan Terbesar (FPB) adalah bilangan terbesar yang, jika dibagi oleh dua atau lebih bilangan bulat, tidak meninggalkan

sisa. Dalam matematika, FPB sering digunakan dalam berbagai konteks seperti penyederhanaan pecahan atau pemecahan masalah bilangan di dalam Kriptografi.

Definisi 2.2

Dengan asumsi $d|a$ dan $d|b$, faktor persekutuan dua bilangan bulat a dan b adalah bilangan bulat d yang sama dengan a dan b. Karena 1 adalah pembagi (faktor) semua bilangan bulat, setiap pasangan bilangan a dan b memiliki faktor persekutuan 1.

Karena semua bilangan bulat membagi nol, setiap bilangan bulat bukan nol adalah faktor persekutuan a dan b jika a dan b sama dengan nol. Ada himpunan bilangan bulat positif tak terhingga yang merupakan faktor persekutuan a dan b, sebagaimana dinyatakan oleh (Nurjamil, Amarulloh, & Apriliani, 2023).

Kita nyatakan bahwa jika a dan b adalah bilangan bulat positif dan tidak ada satu pun yang nol, maka himpunan semua faktor persekutuan bilangan bulat positif a dan b adalah terhingga. Oleh karena itu, elemen terbesar dalam himpunan tersebut, yang merupakan FPB dari a dan b, harus ada. Berikut definisi formalnya:

Definisi 2.3

Untuk bilangan apa pun a dan b yang paling sedikit satu di antaranya bukan nol, fungsi penghitungan umum (FPB) dari kedua variabel tersebut jika diberi simbol (a, b) adalah bilangan bulat positif, misal d, yang memenuhi kondisi berikut:

1. $d|a$ dan $d|b$, serta
2. jika $e|a$ dan $e|b$, maka $e \leq d$

Jelas dari pernyataan ini bahwa $d = 1$ jika dan hanya jika $(a, b) = d$. Dengan cara yang sama, jika e adalah komponen umum lainnya, maka $e = d$ (Nurjamil, Amarulloh, & Apriliani, 2023).

2.1.3 Fungsi Euler (Totient Euler)

Fungsi *Euler* (*Totient Euler*) biasanya dilambangkan dengan $\varphi(n)$, adalah sebuah fungsi yang penting dalam teori bilangan, terutama dalam konteks aritmetika modular dan kriptografi. Fungsi ini berfungsi untuk menemukan semua bilangan bulat positif yang secara substansial prima terhadap n dan lebih kecil dari nnn. Kita mengatakan bahwa dua bilangan relatif prima ketika Faktor Persekutuan Terbesar FPB adalah 1.

2.1.4 Invers Modular

Invers Modular adalah bilangan bulat b^{-1} yang memenuhi persamaan berikut dalam aritmatika modular:

$$a \cdot b^{-1} \equiv 1 \ (mod\ n)$$

Ini berarti bahwa ketika a dikalikan dengan invers modular b^{-1} dan hasilnya dibagi oleh n, sisa dari pembagi tersebut adalah 1. Dalam kata lain, b^{-1} adalah bilangan yang ketika dikalikan dengan a menghasilkan kelipatan dari n ditambah 1.

2.1.5 Kriptografi

Berasal dari bahasa Yunani, kata "*crypto*" dan "*graphia*" menjadi dasar kriptografi modern. *Graphia* berarti tulisan dan crypto berarti rahasia. Saat

komunikasi dikirim dari satu lokasi ke lokasi lain, kriptografi memastikan bahwa komunikasi tersebut tetap aman dengan menggunakan metode ilmiah dan artistik (Ariyus, 2008).

2.1.6 RSA (Rivest, Shamir, dan Adleman).

RSA (Rivest Shamir Adleman) adalah algoritma kriptografi yang menggunakan sistem enkripsi kunci publik. Dikenal sebagai salah satu algoritma kriptografi asimetris pertama, RSA diciptakan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1977 di Massachusetts Institute of Technology (MIT).

Algoritma kunci asimetris, yang mana algoritma RSA menggunakan dua kunci, yakni kunci public dan privat. Algoritma RSA enkripsi teks asli menggunakan kunci publik untuk membuat cipherteks, kemudian mendekripsi cipherteks dengan kunci pribadi untuk memulihkan teks atau pesan asli. Besaran yang digunakan pada algoritma RSA.

Tabel 2.1 Tabel besaran algoritma RSA

Besaran	Sifat
p dan q (bilangan prima)	Rahasia
$n = p\,x\,q$	Tidak Rahasia
$\varphi(n) = (p-1)(q-1)$	Rahasia
e (Kunci Enkripsi)	Tidak Rahasia
d (Kunci Dekripsi)	Rahasia

Algoritma RSA menggunakan pernyataan berikut dari teorema Euler:

$$a\phi(n) \equiv 1(mod\ n) \tag{2.1}$$

yang harus memenuhi syarat:

1. a harus relatif prima dengan n
2. $\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_n)$,

yang dalam hal ini $p1, p2, \dots p_n$ adalah faktor prima dari n.

$\phi(n)$ adalah jumlah bilangan bulat prima yang dimulai dengan n menggunakan fungsi Totient Euler.

Kita dapat menulis ulang persamaan (2.1) sebagai berikut dengan asumsi bahwa untuk bilangan bulat apa pun k lebih besar dari 1, $ak \equiv bk \ (mod\ n)$.

$ak\phi(n) \equiv 1k(mod\ n)$,

Atau

$$ak\phi(n) \equiv 1(mod\ n) \tag{2.2}$$

Jika a diganti dengan m maka persamaan (2.2) menjadi

$$mk\phi(n) \equiv 1(mod\ n) \tag{2.3}$$

Berdasarkan sifat $ac \equiv bc(mod\ n)$, maka persamaan (2.3), jika dikali dengan m menjadi :

$$mk\phi(n) + 1 \equiv m(mod\ n) \tag{2.4}$$

dalam hal ini m relatif prima terhadap n.

Misalkan e dan d dipilih sedemikian sehingga

$$e \cdot d \equiv 1(mod\ \phi(n)) \tag{2.5}$$

atau

$$e \cdot d \equiv k\phi(n) + 1 \tag{2.6}$$

Substitusikan (2.6) ke (2.4) menjadi:

$$me \cdot d \equiv m(mod\ n) \tag{2.7}$$

Persamaan (2.7) dapat ditulis menjadi :

$$(me)d \equiv m(mod\, n) \tag{2.8}$$

Berikut ini adalah definisi enkripsi dan dekripsi menggunakan persamaan (2.9):

$$Ee(m) = c = m^e \, mod\, n \tag{2.9}$$

$$Dd(m) = c = m^d \, mod\, n \tag{2.10}$$

Karena $e.d = d.e$, maka enkripsi diikuti dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi:

$$Dd(Ee(m)) = Ee(Dd(m) \equiv md \, mod\, n \tag{2.11}$$

Oleh karena $mdmod\, n \equiv (m + jn)dmod\, n$ untuk sebarang bilangan bulat j, maka setiap plaintext $m, m + n, m + 2n, \ldots$ menghasilkan cipherteks yang sama. (Ariyus, 2008)

Untuk mendapatkan kunci publik dan kunci privat yang dibutuhkan untuk algoritma RSA, seseorang dapat mengikuti langkah-langkah berikut:

1. Pilih p dan q yaitu sebarang dua bilangan prima acak dengan $p \neq q$
2. Hitung $n = p \times q$
3. Hitung $\phi(n) = (p - 1) \times (q - 1)$
4. Pilih satu bilangan bulat e untuk kunci publik, dimana e relatif prima terhadap $\phi(n)$
5. Bangkitkan kunci privat dengan menggunakan persamaan :

$$d \equiv e - 1 \, mod\, (\phi(n))$$

Hasil dari algoritma di atas adalah :

1. Kunci publik (e, n)
2. Kunci privat (d, n)

2.1.7 Steganografi

Steganografi adalah seni dan ilmu yang berkaitan dengan penyembunyian pesan rahasia dalam media lain (gambar, audio, video, atau teks) sehigga keberadaan pesan tersebut tidak terdeteksi oleh pihak yang tidak berwenang.. Steganografi berfokus pada penyembunyian fakta bahwa ada pesan yang terkandung dalam media. Berasal dari bahasa Yunani, kata "steganografi" terdiri dari *steganos* yang berarti "tersembunyi" dan *graphein* yang berarti "menulis" Karakteristik utama steganografi:

1. Penyembunyian Data : Informasi rahasia disisipkan dalam media digital (misalnya, menyembunyikan pesan teks di dalam gambar atau video).
2. Media Penyamaran : Media yang digunakan sebagai "penyamaran" dapat berupa gambar, audio, video, atau dokumen teks biasa.
3. Keamanan Ganda : Steganografi sering digunakan bersama kriptografi untuk meningkatkan keamanan, di mana data yang disembunyikan sudah dienkripsi terlebih dahulu sebelum disisipkan.

2.1.8 *Least Significant Bit* (LSB)

Salah satu teknik dalam steganografi digital adalah metode *Least Significant Bit* (LSB), yang digunakan untuk menyembunyikan data dalam media digital seperti foto, musik, dan film. Metode ini mengenkripsi data dengan memanfaatkan bit terkecil yang ada di setiap piksel atau sampel. Karena perubahan pada bit paling tidak signifikan ini tidak banyak mempengaruhi kualitas keseluruhan dari media tersebut, metode LSB sangat efektif untuk menyembunyikan data dengan cara yang hampir tidak terdeteksi.

Cara Kerja Metode LSB dalam konteks gambar digital, setiap piksel biasanya diwakili oleh nilai RGB (merah, hijau, biru). Setiap warna dalam RGB memiliki nilai antara 0 dan 255, yang dapat direpresentasikan dalam bentuk biner sebagai 8 bit. Metode LSB akan menyembunyikan data rahasia dengan menggantikan bit paling tidak signifikan (bit ke-8) dari setiap komponen warna (merah, hijau, biru) dalam piksel gambar.

Langkah-langkahnya:

1. Ambil data yang akan disembunyikan: Kami mengubah data rahasia yang harus diintegrasikan ke dalam bentuk biner.
2. Ambil gambar penampung: Gunakan gambar Untuk menyembunyikan informasi.
3. Sisipkan data: Gantilah bit paling tidak signifikan dari setiap piksel gambar penampung dengan bit data rahasia secara berurutan.

Contoh Perhitungan Manual Sederhana

Misalkan kita ingin menyembunyikan data rahasia "A" (dalam ASCII, huruf "A" adalah 65 atau 01000001 dalam biner) ke dalam tiga piksel gambar.

Langkah 1: Konversi data rahasia ke biner

Data rahasia: "A"

Biner dari "A": 01000001

Langkah 2: Ambil nilai RGB dari tiga piksel gambar penampung

Misalkan kita punya tiga piksel dengan nilai RGB sebagai berikut:

Piksel 1: (10101010, 11001100, 11110000)

Piksel 2: (01100110, 10101010, 11001100)

Piksel 3: (11100011, 00011100, 01010101)

Langkah 3: Sisipkan data rahasia ke dalam bit paling tidak signifikan dari setiap komponen warna

Piksel 1:

R: 10101010 → 10101010 (tidak berubah)

G: 11001100 → 11001101 (ubah bit LSB menjadi 1)

B: 11110000 → 11110000 (tidak berubah)

Piksel 2:

R: 01100110 → 01100110 (tidak berubah)

G: 10101010 → 10101010 (tidak berubah)

B: 11001100 → 11001100 (tidak berubah)

Piksel 3:

R: 11100011 → 11100010 (ubah bit LSB menjadi 0)

G: 00011100 → 00011101 (ubah bit LSB menjadi 1)

B: 01010101 → 01010101 (tidak berubah)

Hasil Setelah Penyisipan Data

Piksel 1: (10101010, 11001101, 11110000)

Piksel 2: (01100110, 10101010, 11001100)

Piksel 3: (11100010, 00011100, 01010101)

Metode LSB adalah teknik yang sederhana namun efektif untuk menyembunyikan data dalam media digital. Dengan memodifikasi bit paling tidak signifikan, informasi rahasia dapat disisipkan tanpa merusak kualitas visual atau audio dari media penampung. Contoh perhitungan di atas menunjukkan bagaimana data biner dari huruf "A" dapat disisipkan ke dalam bit LSB dari piksel gambar secara manual.

2.1.9 Citra Digital

Citra digital adalah representasi visual dari objek atau adegan yang ditangkap dan disimpan dalam format digital. Citra ini terdiri dari piksel-piksel yang diatur dalam grid dua dimensi, di mana setiap piksel memiliki nilai tertentu yang menunjukkan intensitas warna atau kecerahan.

1. Struktur dan Komponen Citra Digital

   a) Piksel

      Piksel adalah elemen terkecil dari citra digital yang menyimpan informasi warna. Setiap piksel memiliki koordinat (x, y) yang menunjukkan posisinya dalam grid dua dimensi. Piksel dapat berupa grayscale (hanya memiliki satu nilai intensitas) atau berwarna (memiliki beberapa komponen warna, seperti RGB).

   b) Resolusi

      Resolusi citra digital ditentukan oleh jumlah piksel dalam citra tersebut, biasanya dinyatakan sebagai lebar × tinggi (misalnya, 1920×1080 piksel). Gambar dengan resolusi lebih tinggi lebih tajam dan lebih detail karena ada lebih banyak piksel untuk digunakan.

   c) Kedalaman Warna (Color Depth)

      Kedalaman warna merujuk pada jumlah bit yang digunakan untuk mewakili warna setiap piksel. Misalnya, citra 8-bit grayscale memiliki 256 tingkat keabuan, sementara citra 24-bit RGB memiliki sekitar 16,7 juta warna (8 bit untuk masing-masing komponen merah, hijau, dan biru).

2. Proses Digitalisasi citra melibatkan beberapa langkah, termasuk penangkapan gambar, pengolahan, dan penyimpanan:

   a) Penangkapan Gambar

      Gambar ditangkap menggunakan sensor gambar (misalnya, kamera digital) yang mengkonversi cahaya menjadi sinyal listrik. Langkah berikutnya, yang dikenal sebagai digitalisasi, adalah mengubah impuls listrik ini menjadi data digital.

   b) Pengolahan Citra

      Citra digital dapat mengalami berbagai macam pengolahan, seperti peningkatan kualitas gambar (enhancement), kompresi, segmentasi, dan deteksi fitur. Pengolahan citra bertujuan untuk memperbaiki, menganalisis, atau mengekstraksi informasi yang relevan dari citra.

   c) Penyimpanan dan Format File

      Citra digital disimpan dalam berbagai format file, seperti JPEG, PNG, BMP, dan TIFF, masing-masing dengan karakteristik kompresi dan kualitas yang berbeda. Format file yang dipilih bergantung pada kebutuhan aplikasi, seperti kompresi lossy untuk menghemat ruang penyimpanan atau kompresi lossless untuk menjaga kualitas gambar.

Citra digital adalah dasar dari banyak teknologi modern yang memanfaatkan kemampuan komputer untuk menangkap, menyimpan, mengolah, dan menganalisis gambar. Pemahaman yang mendalam tentang struktur dan sifat citra digital, serta teknik pengolahan dan penyimpanan yang digunakan, sangat penting dalam penelitian yang melibatkan citra digital. Pengetahuan ini memungkinkan

pengembangan aplikasi baru dan peningkatan teknologi yang ada untuk berbagai tujuan praktis dan ilmiah.

Untuk memahami konsep piksel dalam citra digital, mari kita lihat contoh konkret bagaimana piksel bekerja dalam gambar digital. Misalkan kita memiliki citra digital berukuran 3×3 piksel, yang berarti citra ini terdiri dari 9 piksel yang disusun dalam grid 3 baris dan 3 kolom. Kita akan melihat contoh untuk citra grayscale dan citra berwarna.

1. Citra Berwarna (RGB)

   Citra berwarna memiliki tiga komponen warna untuk setiap piksel yakni Merah (R), Hijau (G), dan Biru (B). Nilai setiap komponen berkisar antara 0 hingga 255. Misalkan kita memiliki citra berwarna 3x3 sebagai berikut:

   Piksel 1: [R, G, B] = [255, 0, 0]

   Piksel 2: [R, G, B] = [0, 255, 0]

   Piksel 3: [R, G, B] = [0, 0, 255]

   Dalam citra RGB di atas:

   a) Piksel 1 pada kolom pertama memiliki nilai (R: 255, G: 0, B: 0), yang berarti warnanya sangat merah.
   b) Piksel 2 pada kolom kedua memiliki nilai (R: 0, G: 255, B: 0), yang berarti warnanya sangat hijau.
   c) Piksel 3 pada kolom ketiga memiliki nilai (R: 255, G: 0, B: 0), yang berarti warnanya sangat biru.

Setiap piksel disimpan dalam memori komputer sebagai nilai numerik. Jika menyangkut gambar merah, hijau, dan biru, setiap piksel dalam gambar RGB menyimpan tiga nilai yang berbeda.

Misalnya, saat menyimpan gambar dalam format RGB 24-bit, setiap piksel memerlukan 24 bit-8 bit untuk merah, 8 bit untuk hijau, dan 8 bit untuk biru.

2.1.10 MSE (Mean Squared Error)

Mean Squared Error (MSE) adalah salah satu metrik evaluasi yang digunakan untuk mengukur tingkat kesalahan dalam sebuah model prediksi, terutama pada kasus regresi. MSE menghitung rata-rata kuadrat dari selisih antara nilai yang diprediksi dan nilai aktual . Semakin kecil nilai MSE, semakin baik performa model karena kesalahan prediksinya semakin kecil.

Secara matematis, MSE dirumuskan sebagai:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - Y(i,j))^2$$

di mana:

- M adalah jumlah baris piksel dalam citra.
- N adalah jumlah kolom piksel dalam citra.
- $X(i,j)$ adalah nilai intensitas piksel pada posisi (i,j) dalam citra asli.
- $Y(i,j)$ adalah nilai intensitas piksel pada posisi (i,j) dalam citra hasil modifikasi setelah penyisipan atau setelah modifikasi.
- $\sum_{i=1}^{M} \sum_{j=1}^{N}$ adalah penjumlahan dua dimensi untuk seluruh piksel.

2.2 Penyampaian Amanah dalam Al-Qur'an

Penelitian ini mengajarkan tentang sebuah tanggungjawab seseorang agar selalu menjalankan kewajiban sesuai dengan apa yang dikerjakannya atau dapat diartikan sebagai seseorang harus menjaga amanah dalam menjalani kehidupan. Berikut adalah firman Allah SWT yang membahas tentang amanah pada Surat Al-Mu'minum ayat 8-ll yang artinya sebagai berikut:

"Dan (sungguh beruntung) orang yang memelihara amanat-amanat (yang dipikulnya) dan janjinya, serta orang yang memelihara shalatnya, mereka itulah orang yang akan mewarisi (yakni) yang akan mewarisi (surga) Firdaus. Mereka kekal didalamnya" (QS. Al-Mu'minum)

Dalam kitab tafsir al-Misbah, Menjaga amanah yang baik, baik kepada Allah maupun kepada manusia (seperti menitipkan sesuatu kepada orang lain) merupakan ciri keenam orang mukmin yang beruntung. Atau dana yang wajib ditransfer kepada pihak lain dengan cara yang sah dan tepat waktu tanpa mengurangi ketentuan perjanjian (Shihab, Tafsir Al Mishbah, 2002).

Demikian pula ketika mereka melakukan perjanjian mereka menepati janjinya dengan sempurna. Menurut sebuah hadis yang terkenal, orang munafik memiliki tiga ciri: sering berbohong, sering mengingkari janji, dan suka mengkhianati amanah. Orang-orang munafik menghindari orang munafik karena hal ini.

Tetap melaksanakan shalat lima waktu setiap hari. Orang yang bahagia cenderung beriman dan taat beribadah, memperhatikan shalat lima waktu, tepat waktu, dan menyempurnakan rukun Islam, sesuai dengan firman Allah yang menjelaskan sifat ketujuh dalam ayat ini.

Surga adalah surga yang paling utama, tempat tinggal Arsy Allah Yang Maha Tinggi, dan orang-orang yang memiliki sifat-sifat mulia yang telah melakukan

perbuatan baik di dunia akan mewarisinya (Shihab, Tafsir Al Mishbah, 2002). Menurut tafsir Umar dari sebuah hadis, Rasulullah bersabda:

"Telah diturunkan kepadaku sepuluh ayat: Barang siapa yang menegakkannya akan masuk surga, lalu ia membaca sepuluh ayat ini dari permulaan Surah al-Mu`minun." (Riwayat at-Tirmizi)

Segala sesuatu yang seharusnya dilestarikan dan diwariskan kepada penerima yang sah termasuk dalam amanah, kata Ahmad Musthafa Al-Maraghi (Shihab, 2002). Pada dasarnya ada tiga jenis amanah:

1. Amanah Manusia kepada Allah

   Kewajiban manusia terhadap Allah adalah mengikuti perintah-Nya dan menjauhi larangan-Nya. Selain itu, perintah ini juga menyatakan bahwa kita harus memanfaatkan bakat yang telah diberikan Allah kepada kita dengan baik.

2. Amanah kepada Sesama Manusia

   Tidak mudah untuk mengemban amanah kepada orang lain, terutama jika menyangkut uang atau harta benda. Daya tarik harta benda merupakan kelemahan manusia yang umum. Mengembalikan barang titipan kepada pemilik aslinya setelah menjaganya tanpa mengurangi isinya merupakan contoh amanah terhadap manusia lain.

3. Amanah Manusia kepada Diri Sendiri

   Beriman pada diri sendiri dikaitkan dengan berbudi luhur dalam kegiatan keagamaan dan duniawi. Ini mencakup upaya untuk menghindari tindakan yang merugikan, baik di dunia maupun di akhirat.

Dengan kata lain, amanah adalah tanggung jawab yang harus dipenuhi dengan integritas dan kejujuran, baik kepada Allah, sesama manusia, maupun kepada diri sendiri.

2.3 Kajian Topik dengan Teori Pendukung

Ada banyak aspek positif bagi keberadaan manusia yang dihasilkan dari kemajuan teknologi. Meskipun teknologi memiliki banyak efek baik, teknologi juga memiliki banyak konsekuensi buruk, seperti meningkatnya kejahatan dunia maya (termasuk penipuan, pemerasan, pencurian, dan persaingan), dan lain-lain. Pemilik data akan mengalami kerugian jika data tersebut jatuh ke tangan yang salah. Misalnya, jika menyangkut perusahaan A, hanya beberapa orang terpilih yang boleh memiliki akses ke informasi sensitif. Algoritma dan metode yang efektif diperlukan untuk mengamankan data guna menjaga kerahasiaannya.

Dalam penelitian ini, diterapkan ilmu kriptografi dan steganografi yang berfungsi untuk mengamankan data. Algoritma RSA dan LSB digunakan untuk meningkatkan tingkat keamanan pesan asli yang telah dienkripsi dan disembunyikan dalam piksel, sehingga sulit terdeteksi oleh pihak lain. Konsep yang diterapkan dalam kriptografi mencakup bilangan prima, FPB, totient Euler, dan invers modular yang semuanya relevan dengan algoritma RSA. Di sisi lain, LSB menggunakan sistem kode ASCII dan bit string. Dalam penelitian ini, peneliti akan menganalisis perlindungan pesan menggunakan RSA dan LSB, dengan memanfaatkan ilmu matematika dalam proses pengembangan kunci, enkripsi, dan dekripsi. Oleh karena itu, terdapat hubungan antara penelitian ini dan teori-teori pendukung yang ada dalam bidang matematika.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian yang dilakukan termasuk dalam kategori penelitian kualitatif, yang berupaya untuk mengatasi isu-isu terkini dengan menggunakan ide-ide yang sudah mapan. Penelitian ini dimulai dengan mendefinisikan secara teoritis prinsip-prinsip yang terkait dengan steganografi dan kriptografi.

3.2 Pra Penelitian

Untuk memperoleh tingkat keamanan terbaik dalam metode kriptografi RSA dan steganografi LSB, para peneliti menemukan, meneliti, dan menguji banyak teori yang mendukung proses enkripsi dan dekripsi.

1. Cari literatur utama yang akan menjadi dasar penelitian.
2. Kumpulkan literatur yang mendukung penelitian.
3. Saran berikutnya adalah mempelajari teknik steganografi dan kriptografi LSB.
4. Dapatkan pengetahuan tentang kriptografi algoritma RSA.

3.3 Tahapan Penelitian

Tahapan yang perlu dilakukan untuk melakukan penelitian ini yaitu sebagai berikut:

3.3.1 Proses Enkripsi Menggunakan Metode RSA dan LSB

1. **Enkripsi**

   a. **Pembentukan Kunci RSA**

   1) Menentukan nilai p dan q yang merupakan dua bilangan prima besar yang dipilih oleh penulis. Sebaiknya dalam memilih p dan q adalah $p \neq q$, sebab apabila $p = q$ maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari (n). Kedua bilangan tersebut bersifat rahasia, sehingga hanya penerima yang mengetahui bilangan tersebut.
   2) Mengkalikan dua bilangan prima besar atau p dan q untuk memperoleh nilai n atau $n = p \cdot q$ dengan n adalah salah satu parameter untuk proses enkripsi dan dekripsi dan sifatnya tidak rahasia dapat disebarluaskan.
   3) Mencari nilai Totient Eular atau $\phi(n) = (p - 1)(q - 1)$, $\phi(n)$ digunakan untuk mendapatkan kunci publik dan kunci privat dan sifatnya rahasia hanya penerima yang dapat mengetahui.
   4) e (salah satu kunci publik), dengan $(e, \phi(n)) = 1$ atau FPB dan $\phi(n) = 1$ Karena sebagai salah satu kunci publik maka dapat disebarluaskan.
   5) d (salah satu kunci privat), dengan $d = 1 + k\,\phi(n)$. Karena sebagai salah satu e kunci privat maka sifatnya rahasia hanya penerima yang dapat mengetahui.
   6) Pasangan kunci publik adalah e dan n sedangkan pasangan kunci privat adalah d dan n.

b. Enkripsi Pesan

1) Konversi pesan ke bilangan bulat, pesan asli yang akan dienkripsi, harus terlebih dahulu diubah menjadi sebuah bilangan bulat. Menggunakan ASCII (*American Standard Code for Information Interchang*e).
2) Penggunaan kunci publik, gunakan kunci publik (n, e) yang telah dihasilkan sebelumnya.
3) Rumus enkripsi : $c = m^e \ (mod\ n)$

   di mana m adalah kode ASCII, e adalah kunci publik, dan n adalah modulus.
4) Enkripsi masing-masing karakter, misalnya menggunakan 3 karakter:

$$c_1 = {m_1}^e \ (mod\ n)$$

$$c_2 = {m_2}^e \ (mod\ n)$$

$$c_3 = {m_3}^e \ (mod\ n)$$

   Gabungkan hasil enkripsi karakter menjadi satu blok data menjadi cipherteks gabungan: [c_1, c_2, c_3].
5) Ubah cipherteks menjadi representasi biner (8 bit), dan susun representasi biner menjadi satu rangkaian panjang.

2. Steganografi

a) Pilih citra RGB yang akan digunakan sebagai media penyisipan pesan rahasia.
b) Konversi citra menjadi matriks piksel dengan nilai desimal untuk setiap komponen warna RGB.

c) Konversi desimal ke biner, konversi setiap nilai komponen warna (Red, Green, Blue) dari desimal ke biner 8-bit.

d) Penyisipan dalam LSB, gantikan bit terakhir (*Least Significant Bit*) dari setiap komponen RGB dengan bit-bit dari cipherteks yang sudah direpresentasikan sebelumnya secara berurutan.

e) Menentukan Jumlah Piksel yang Diperlukan, setiap piksel memiliki 3 komponen (R, G, B), sehingga setiap piksel dapat menyimpan 3 bit informasi.

f) Ubah kembali bentuk *binner* pada komponen RGB kedalam bentuk desimal.

g) Simpan citra RGB yang baru dengan nama image_encode.png

3.3.2 Proses Dekripsi Menggunakan Metode RSA dan LSB

1. **Ekstraksi**

a) Ambil Citra RGB yang digunakan untuk menyisipkan data diambil dari sumbernya dan ubah setiap pixel RGM menjadi matrix desimal.

b) Ekstraksi bit LSB, setiap piksel desimal diruubah kedalam bentuk biner (8bit) dalam citra RGB terdiri dari tiga komponen warna: merah (R), hijau (G), dan biru (B). Untuk mengekstrak data, lihat bit terkecil (*Least Significant Bit)* dari setiap pixel biner pada komponen RGB.

c) Kumpulkan bit-bit yang diekstraksi dari bit terkecil dari setiap komponen RGB hingga semua data yang disisipkan berhasil dikumpulkan.

d) Rekonstruksi data, bit-bit yang telah dikumpulkan digabungkan kembali menjadi bentuk biner panjang dan rubah kedalam bentuk decimal untuk setiap 8bit nya. Data yang diekstraksi masih dalam bentuk terenkripsi.

2. Dekripsi

a) Ambil kunci privat, dekripsi RSA membutuhkan kunci privat yang pasangannya adalah kunci publik yang digunakan saat enkripsi.

b) Ambil data terenkripsi, data yang telah diekstraksi dari citra RGB diambil untuk diproses lebih lanjut.

c) Dekripsi dilakukan dengan rumus $M = C^d \ mod \ n$, di mana C adalah cipherteks (data terenkripsi), d adalah eksponen dekripsi (bagian dari kunci privat), dan n adalah modulus (bagian dari kunci publik dan privat). Hasil dekripsi M adalah plainteks asli.

3.3.3 Proses Menghitung MSE dari Citra Sebelum dan Sesudah Encoding

1. Input Citra

Ambil dua citra dengan dimensi yang sama, misalnya $m \times n$ piksel. Masukan, citra asli sebelum *encoding* (I) dan citra sesudah *encoding* yang ingin dibandingkan (I').

2. Menghitung MSE

a. Untuk setiap piksel pada citra, hitung selisih nilai intensitas antara piksel pada citra asli dan citra hasil.

b. Kuadratkan selisih tersebut untuk memastikan semua perbedaan dihitung sebagai nilai positif.

c. Jumlahkan semua hasil kuadrat dari selisih intensitas piksel. Bagi total nilai kuadrat selisih dengan jumlah total piksel $m \times n$ untuk mendapatkan rata-rata kuadrat dari perbedaan intensitas.

3. Hasil Akhir

a) Menampilkan output citra

b) Nilai MSE yang diperoleh merupakan angka yang menunjukkan rata-rata kesalahan kuadrat antara dua citra. Semakin kecil nilai MSE, semakin mirip kedua citra tersebut.

BAB IV

HASIL DAN PEMBAHASAN

Setelah menyelesaikan tahap perancangan yang dijabarkan dalam Bab III, langkah selanjutnya adalah melakukan pembahasan serta analisis terhadap data yang berkaitan dengan kebutuhan sistem untuk menerapkan kombinasi metode kriptografi dan steganografi. Dengan adanya hasil dari pembahasan tersebut, dapat diketahui apakah terdapat perbedaan antara hasil yang diperoleh secara manual dengan hasil yang diperoleh melalui sistem yang terkomputerisasi.

4.1 Proses Enkripsi Metode RSA dan LSB

4.1.1 Simulasi Algoritma Enkripsi Metode RSA dan LSB

1. Enkripsi

a. Pembentukan Kunci RSA

Pilih dua bilangan (*integer*) prima p dan q sembarang, dimana $p \neq q$.

Misalnya: $p = 193$ dan $q = 191$ (nilai yang ditentukan penulis)

Hitung nilai $n = p \times q$, $(p \neq q)$, bilangan n merupakan parameter keamanan, dimana panjang nilai *n* nya maka semakin sukar di pecahkan.

$$n = 193 \times 191 = 36863.$$

1) $Hitung\ \varphi(n) = (p - 1)(q - 1)$

$$= (193 - 1)(191 - 1)$$

$$= 36480$$

2) Bangkitkam secara acak kunci e dengan syarat:

$$1 < e < \varphi(n)$$

$$FPB(e.\varphi(n)) = 1$$

e relatif prima (yang tidak merupakan faktor dari nilai $\varphi(n)$).

Misalnya e = 7 (angka yang ditentukan penulis)

$FPB(\mathrm{e}.\varphi(n)) = gcd\ (7, 36480) = 1$ (memenuhi)

3) Hitung nilai d kebalikan dari modulo

$$\varphi(n) : (\mathrm{e}, d)\ mod\ \varphi(n) = 1$$

Dengan mencoba nilai $k = 1, 2, 3, 4, .n$ sehingga memenuhi persamaan tersebut.

$$d = \frac{1 + K\varphi(n)}{e}$$

$$= \frac{1 + K.36480}{7}\ (dimana\ K = 2)$$

$$= \frac{1 + (2.36480)}{7}$$

$$= 10423$$

Keterangan: K = bilangan bulat positif dengan tujuan hasil nilai qInv adalah bilangan bulat positif ketika dibagi dengan nilai q

4) Pasangan kunci publik adalah (e, n) yaitu $(7, 36863)$ sedangkan pasangan kunci privat adalah (d, n) yaitu $(10423, 36863)$.

b. Enkripsi Pesan

1) Pesan yang akan disampaikan adalah M = UIN, dengan menggunakan kode ASCII.

U = 85

I = 73

N = 78

2) Gunakan kunci publik $(e, n) = (7, 36863)$ yang telah dihasilkan sebelumnya.

3) Rumus enkripsi : $c = m^e \ (mod\ n)$

4) Enkripsi masing-masing karakter, karakter yang digunakan adalah UIN:

   Plaintext P1 = 85, perhitungan:

   $$c_U = m_U{}^e \ (mod\ n)$$

   $= 85^7 \bmod 36863$

   $= 12051$

   Plaintext P2 = 73, perhitungan:

   $$c_I = m_I{}^e \ (mod\ n)$$

   $= 73^7 \bmod 36863$

   $= 33138$

   Plaintext P3 = 72, perhitungan:

   $$c_N = m_N{}^e \ (mod\ n)$$

   $= 78^7 \bmod 36863$

   $= 4261$

   Gabungkan hasil enkripsi karakter menjadi satu blok data menjadi cipherteks gabungan: [12051, 33138, 4261].

5) Untuk mengubah setiap digit pada cipherteks ke dalam bentuk biner 8-bit, kita perlu mengonversi setiap digit satu per satu. Langkah ini memastikan bahwa setiap digit dari cipherteks akan direpresentasikan dalam bentuk biner. Pisahkan setiap digit dari cipherteks.

12051 terdiri dari [1,2,0,5,1]

33138 terdiri dari [3,3,1,3,8]

4261 terdiri dari [4,2,6,1]

Berikut konversi setiap digit dari cipherteks ke dalam biner 8-bit:

- 12051:

1 → '00000001'

2 → '00000010'

0 → '00000000'

5 → '00000101'

1 → '00000001'

Jadi, 12051 dalam biner 8-bit = ['00000001', '00000010', '00000000', '00000101', '00000001'] disertakan biner koma (ASCII) [00101100]

- 33138:

3 → '00000011'

3 → '00000011'

1 → '00000001'

3 → '00000011'

8 → '00001000'

Jadi, 33138 dalam biner 8-bit = ['00000011', '00000011', '00000001', '00000011', '00001000'] disertakan biner koma (ASCII) [00101100]

- 4261:

4 → '00000100'

2 → '00000010'

6 → '00000110'

1 → '00000001'

Jadi, 4261 dalam biner 8-bit = ['00000100', '00000010', '00000110', '00000001'] disertakan biner koma (ASCII) [00101100]

Ringkasan Hasil Konversi:

- Cipherteks 12051+(koma) dalam biner 8-bit: ['00000001', '00000010', '00000000', '00000101', '00000001', '00101100']
- Cipherteks 33138+(koma) dalam biner 8-bit: ['00000011', '00000011', '00000001', '00000011', '00001000', '00101100']
- Cipherteks 4261+(koma) dalam biner 8-bit: ['00000100', '00000010', '00000110', '00000001', '00101100']

Setiap karakter dalam cipherteks dikonversi menjadi 8-bit biner sesuai dengan nilai ASCII, menghasilkan sebuah rangkaian panjang dari kode biner. Di antara setiap blok biner 8-bit, kita menambahkan tanda koma sebagai pemisah. Dengan memisahkan setiap blok biner 8-bit menggunakan tanda koma ASCII, kita dapat menandai batas antara blok data secara jelas. Ini menjaga struktur data tetap sederhana dan mudah dipahami. Saat data dibaca kembali, tanda koma ASCII memudahkan pemisahan dan interpretasi blok-blok biner yang merepresentasikan karakter asli dari cipherteks.

2. Steganografi

a) Citra RGB yang digunakan adalah logo dari Universitas Islam Negeri Maulana Malik Ibrahim Malang. Berikut adalah citra RGB yang ditunjukkan pada gambar 4.1

Gambar 4.1 Logo UIN

b) Konversi citra menjadi matriks piksel dengan nilai desimal untuk setiap komponen warna RGB. Disini peneliti akan menggunakan ukuran piksel 150x150 yang diambil sebagian dari citra RGB yang digunakan.

c) Konversi desimal ke biner, konversi setiap nilai komponen warna (Red, Green, Blue) dari pixel yang terdapat pada citra yang berupa nilai desimal dan dirubah menjadi biner 8-bit.

d) Proses Penyisipan Bit cipherteks ke Piksel. Kita akan mulai menyisipkan bit terakhir dari cipherteks ke dalam LSB (Least Significant Bit) dari setiap komponen warna (R, G, B) dari piksel.

e) Menentukan Jumlah Piksel yang Diperlukan:

Setiap piksel memiliki 3 komponen (R, G, B), sehingga setiap piksel dapat menyimpan 3 bit informasi.

Dengan total 136 bit cipherteks yang ingin disisipkan, kita memerlukan:

$$= \frac{136\ bit}{3\ bit\ per\ pixel} = 45.33\ (Dibulatkan\ keatas\ menjadi\ 46)$$

Jadi, kita hanya membutuhkan 46 piksel untuk menyimpan seluruh cipherteks.

6. Ubah kembali bentuk binner pada komponen RGB kedalam bentuk decimal. Proses ini bertujuan untuk mengembalikan nilai warna yang

sebelumnya telah dimodifikasi atau dienkripsi dalam bentuk biner sehingga bisa kembali dikenali sebagai informasi warna yang sesuai dalam citra.

Total biner dari cipherteks:

'00000001', '00000010', '00000000', '00000101', '00000001', '00101100', '00000011', '00000011', '00000001', '00000011', '00001000', '00101100', '00000100', '00000010', '00000110', '00000001', '00101100'

Total panjang: 136 bit. Berikut penyisipan ke dalam piksel awal:

Penyisipan ke Piksel:

a) Piksel 1 (RGB awal: 255, 255, 255):

Cipherteks (3 bit pertama): 000

R = 11111111 → LSB diubah menjadi 11111110 (0)

G = 11111111 → LSB diubah menjadi 11111110 (0)

B = 11111111 → LSB diubah menjadi 11111110 (0)

Piksel 1 sekarang menjadi (254, 254, 254).

b) Piksel 2 (RGB awal: 255, 255, 255):

Cipherteks (3 bit berikutnya): 000

R = 11111111 → LSB diubah menjadi 11111110 (0)

G = 11111111 → LSB diubah menjadi 11111110 (0)

B = 11111111 → LSB diubah menjadi 11111110 (0)

Piksel 2 sekarang menjadi (254, 254, 254).

c) Piksel 3 (RGB awal: 255, 255, 255):

Cipherteks (3 bit berikutnya): 010

R = 11111111 → LSB diubah menjadi 11111110 (0)

G = 11111111 → LSB diubah menjadi 11111111 (1)

B = 11111111 → LSB diubah menjadi 11111110 (0)

Piksel 3 sekarang menjadi (254, 255, 254).

d) Piksel 4 (RGB awal: 255, 255, 255):

Cipherteks (3 bit berikutnya): 000

R = 11111111 → LSB diubah menjadi 11111110 (0)

G = 11111111 → LSB diubah menjadi 11111110 (0)

B = 11111111 → LSB diubah menjadi 11111110 (0)

Piksel 4 sekarang menjadi (254, 254, 255).

e) Piksel 5 (RGB awal: 255, 255, 255):

Cipherteks (3 bit berikutnya): 000

R = 11111111 → LSB diubah menjadi 11111110 (0)

G = 11111111 → LSB diubah menjadi 11111110 (0)

B = 11111111 → LSB diubah menjadi 11111110 (0)

Piksel 5 sekarang menjadi (254, 254, 254).

Lanjutkan proses ini sampai 32 piksel pertama telah digunakan untuk menyimpan seluruh 96 bit dari cipherteks.

7. Menyimpan citra RGB baru dengan nama image_encode.png, setelah komponen warna RGB dikonversi kembali ke bentuk desimal, langkah berikutnya adalah menyimpan citra tersebut dalam format yang dapat diakses, yaitu PNG. Penyimpanan ini bertujuan untuk menghasilkan output citra dengan nama image_encode.png, yang merupakan citra baru yang berisi perubahan yang dilakukan pada komponen RGB.

Format PNG dipilih karena memiliki kualitas gambar yang tinggi tanpa kompresi, sehingga hasil perubahan atau enkripsi tetap tersimpan dengan baik tanpa kehilangan kualitas atau informasi visual.

4.2 Proses Menggunakan Metode RSA dan LSB

4.2.1 Simulasi Dekripsi Metode RSA dan LSB

1. Ekstraksi

1. Ambil Citra RGB yang digunakan untuk menyisipkan data diambil dari sumbernya dan ubah setiap piksel RGB menjadi matrik desimal.
2. Ekstraksi bit LSB, setiap piksel desimal diruubah kedalam bentuk biner (8bit) dalam citra RGB terdiri dari tiga komponen warna: merah (R), hijau (G), dan biru (B). Untuk mengekstrak data, lihat bit terkecil (*Least Significant Bit)* dari setiap pixel biner pada komponen RGB.
3. Kumpulkan bit-bit yang diekstraksi dari bit terkecil dari setiap komponen RGB hingga semua data yang disisipkan berhasil dikumpulkan. Rekonstruksi data, bit-bit yang telah dikumpulkan dan dipilah dengan pemisah biner koma (ASCII), kemudian digabungkan kembali menjadi bentuk biner panjang.

   ekstraksi bit: '00000001', '00000010', '00000000', '00000101', '00000001', **'00101100'** (koma), '00000011', '00000011', '00000001', '00000011', '00001000', **'00101100'** (koma), '00000100', '00000010', '00000110', '00000001', **'00101100'** (koma)

4. Cipherteks yang dihasilkan:
    1. 12051
    2. 33138
    3. 4261
5. Data yang diekstraksi masih dalam bentuk terenkripsi.

2. Dekripsi

a) Gunakan kunci privat $(d, n) = (10423, 36863)$.

b) Ambil data yang telah diekstraksi dari citra RGB sebelumnya. Ubah kedalam bentuk desimal.

c) Dekripsi dilakukan dengan rumus $M = C^d \ mod \ n$

d) $M_1 = C^d \ mod \ n$

$= 1205110423 \ mod \ 36863$

$= 85$

$M_2 = C^d \ mod \ n$

$= 3313810423 \ mod \ 36863$

$= 73$

$M_3 = C^d \ mod \ n$

$= 426110423 \ mod \ 36863$

$= 78$

Ubah kembali ke karakter ASCII:

85 = 'U'

73 = 'I'

78 = 'N'

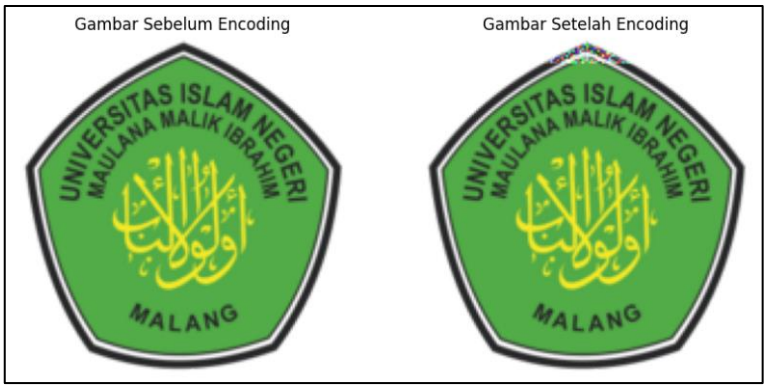
Jadi pesan asli yang tersembunyi pada citra RGB adalah “UIN”

4.3 Proses Menghitung MSE dari Citra Sebelum dan Sesudah Encoding

4.3.1 Simulasi Menghitung MSE dari Citra Sebelum dan Sesudah Encoding

1. Input Citra

a. Input Citra: Dua citra RGB dengan ukuran piksel yang sama:



Gambar 4. Citra sebelum dan sesudah encoding

2. Menghitung MSE

a. Iterasi setiap piksel (i,j). Untuk setiap piksel pada citra, hitung selisih nilai intensitas antara piksel pada citra asli dan citra hasil.

b. Kuadratkan selisih tersebut untuk memastikan semua perbedaan dihitung sebagai nilai positif.

c. Hitung kuadrat selisih intensitas piksel antara $image$ dan $image\_encode$ dan hitung rata-rata dari seluruh selisih kuadrat.

Menggunakan Rumus:

$$MSE = \frac{1}{m.n}\sum_{i=1}\sum_{j=1}(image\ \ [i,j] - image_{encode}\ \ [i,j])^2$$

Di mana:

m dan n : Dimensi tinggi dan lebar.

3. Hasil Akhir

a. Ouput Nilai MSE untuk pesan rahasia “UIN MALIKI MALANG”.

Gambar 4 Hasil Output Nilai MSE

b. Nilai MSE dihitung untuk setiap saluran warna (R, G, B), kombinasi saluran (RG dan GB), serta keseluruhan citra RGB. Hasil perhitungan MSE adalah sebagai berikut:

Komponen	Nilai MSE
Saluran R	0.0517
Saluran G	0.0502
Saluran B	0.0506
Saluran RG	4.1861
Saluran GB	4.3731
Keseluruhan RGB	0.0508

4.4 Implementasi Penyampaian pesan dalam pandangan Islam

Dengan pesatnya kemajuan teknologi, penggunaan penyandian pesan menjadi sangat penting untuk mengurangi risiko pesan diakses atau diketahui oleh pihak yang tidak berwenang. Dalam Islam menjaga amanah kepada orang yang berhak menerimanya sangatlah penting karena merupakan tanggung jawab moral seperti halnya Islam tentang keharusan menjaga amanah yang diberikan kepadanya amanah bisa berupa harta, kepercayaan, informasi. Menjaga amanah kepada Allah juga merupakan suatu kewajiban yang harus dilaksanakan dan merupakan ketakwaan kepada Allah SWT dijelaskan dalam Al-Qur'an Surat An-Nisa' ayat 58 yang artinya :

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan apabila kamu menetapkan hukum di antara manusia supaya kamu menetapkanya dengan adil. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat"

Ayat ini menunjukkan bahwa Allah menegaskan pentingnya menyampaikan amanah kepada yang berhak menerimanya dengan adil dan jujur. Islam juga menekankan agar umatnya menjauhi pengkhianatan terhadap amanah yang diberikan kepadanya. (Shihab, Tafsir Al Mishbah, 2002)

Pengkhiantan terhadap amanah merupakan perbuatan yang sangat tidak diterima dalam Islam karena dapat merusak perbuatan yang sangat tidak diterima dalam Islam karena dapat merusak hubungan sosial, ekonomi dan moral. Dengan demikian, dalam pandangan Islam, menjaga amanah kepada orang yang berhak merupakan bagian dari ketaatan spiritual dan moral kepada Allah SWT. Amanah harus dijaga dengan penuh kejujuran, keadilan, dan keikhlasan, tanpa memandang

amanah kecil ataupun besar, karena setiap amanah memiliki nilai penting dalam Islam untuk menjaga keadilan dan keharmonisan dalam masyarakat.

Mengimplementasikan Kriptografi dan Steganografi dalam penyampaian pesan merupakan cara efektif untuk menjaga amanah karena kriptografi memungkinkan pesan yang dikirimkan tetap rahasia dan tidak dapat dibaca oleh pihak yang tidak berhak karena penerima pesan hanya dapat membuka dan membaca pesan tersebut menggunakan kunci yang sesuai. Menjaga pesan lewat steganografi yang disisipakan ke dalam media lain tanpa menimbulkan kecurigaan. Menggabungkan kriptografi dan steganografi pengguna dapat meningkatkan keamanan dan privasi dan komunikasi dan penyampaian pesan. Pesan yang dikirimkan tidak hanya terenkripsi secara matematis, tetapi juga disembunyikan dengan baik sehingga tidak mudah menjaga amanah dan memenuhi tanggung jawab moral dan berkomunikasi, terutama dalam situasi di mana privasi dan keamanan informasi menjadi sangat penting.

Implementasi steganografi dan kriptografi memiliki berbagai kelebihan yang menjadikannya solusi yang efektif untuk menjaga keamanan dan privasi dalam berbagai konteks komunikasi dan penyimpanan data seperti halnya kriptografi dapat menjaga keamanan data, integritas data, otorisasi, kepatuhan privasi dengan dilengkapi steganografi yang tidak terdeteksi, mendapatkan keamanan tambahan, fleksibilitas dan resistensi terhadap serangan. Dengan memadukan kriptografi dan steganografi, pengguna dapat mencapai tingkat keamanan yang tinggi dalam komunikasi dan penyimpanan data, sambil mempertahankan kerahasiaan dan integritas informasi yang dikirimkan atau disimpan. Keduanya memiliki peran yang

penting dalam memenuhi kebutuhan keamanan digital dalam berbagai lingkungan dan skenario penggunaan.

BAB V

KESIMPULAN

5.1 Kesimpulan

Setelah melakukan keselurahan tahapan dalam penelitian "Implementasi Kriptografi RSA dan Steganografi LSB dalam penyisipan pesan pada citra digital". Dalam proses enkripsi kode pesan dengan kriptografi RSA berjalan efektif di mana pesan yang akan disampaikan dienkripsi terlebih dahulu menggunakan kunci publik RSA dengan menggunakan $p\ dan\ q$ dengan angka yang besar. Setelah pesan terenkripsi menjadi cipherteks, kode cipherteks tersebut disisipkan ke dalam citra menggunakan teknik steganografi LSB (Least Significant Bit). Dalam proses ini memungkinkan pesan terenkripsi disembunyikan secara aman dalam sebuah citra tanpa mengubah tampilan citra secara kasat mata. Teknik LSB memberikan hasil yang cukup baik dalam menyembunyikan informasi tanpa mengurangi kualitas visual dari citra yang digunakan.

Proses ekstraksi stego image yang telah disisipi pesan menggunakan teknik LSB dilakukan untuk mengambil kembali kode cipherteks dari citra tersebut. Setelah kode cipherteks berhasil diekstraksi, proses dekripsi dilakukan dengan menggunakan kunci privat RSA. Hasil dekripsi memungkinkan penerima untuk mengembalikan pesan asli yang telah dienkripsi. Keseluruhan proses ini menunjukkan bahwa metode kombinasi kriptografi RSA dengan menggunakan metode yang semestinya harus menggunakan $p\ dan\ q$ yang besar agar sulit ditebak dan steganografi LSB dapat menjaga kerahasiaan dan keamanan pesan, dengan ketahanan yang baik terhadap deteksi visual maupun serangan pihak ketiga.

Secara keseluruhan, penelitian ini membuktikan bahwa gabungan metode kriptografi RSA dan steganografi LSB dapat digunakan sebagai solusi efektif untuk menyembunyikan dan melindungi pesan digital dalam citra, sehingga meningkatkan keamanan dan privasi komunikasi digital.

5.2 Saran

Berdasarkan hasil penelitian "Implementasi Kriptografi RSA dan Steganografi LSB dalam Penyisipan Pesan pada Citra Digital", terdapat beberapa saran yang dapat dikembangkan untuk penelitian selanjutnya agar metode ini semakin efektif dan optimal dalam menjamin keamanan pesan digital, di antaranya:

1. **Peningkatan Kapasitas Penyisipan Pesan:** Penelitian selanjutnya dapat mengembangkan metode steganografi LSB yang lebih canggih atau menggabungkan teknik steganografi lainnya untuk meningkatkan kapasitas penyisipan pesan dalam citra tanpa memengaruhi kualitas visual. Hal ini penting untuk mengatasi keterbatasan kapasitas pada metode LSB standar.
2. **Penggunaan Algoritma Kriptografi Lain:** Selain RSA, algoritma kriptografi lain seperti AES atau ECC dapat dipertimbangkan untuk penelitian lebih lanjut. Algoritma ini mungkin menawarkan performa yang lebih cepat atau tingkat keamanan yang lebih tinggi, tergantung pada kebutuhan sistem.
3. **Implementasi pada Format Media Lain:** Sebagai perluasan dari penelitian ini, steganografi LSB dapat diterapkan pada format media lain, seperti audio atau video, untuk memperluas pilihan media penyimpanan pesan yang lebih beragam dan memiliki kapasitas lebih besar.

4. **Peningkatan Keamanan terhadap Deteksi dan Serangan:** Penelitian lanjutan dapat menguji ketahanan metode ini terhadap berbagai serangan atau teknik deteksi steganalisis. Dengan demikian, sistem dapat dirancang agar lebih tangguh terhadap upaya pihak ketiga dalam mendeteksi atau merusak pesan yang disisipkan.

Dengan pengembangan lebih lanjut, diharapkan metode ini dapat memberikan solusi yang lebih kuat dan luas penggunaannya untuk menjaga privasi dan keamanan pesan digital.

DAFTAR PUSTAKA

Ariyus, Dony. 2006. *Kriptografi: Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

Ariyus, Dony. 2006. *Pengantar Ilmu Kriptografi, Teori, Analisis dan Implementasi*. Yogyakarta: Andi.

Azlansyah, Muhammad, dkk. 2019. *Penyisipan Pesan pada Citra Digital menggunakan Metode Least Significant Bit.* ITS. Jurnal Sains dan Seni. Vol.8, No.1.

Benny, Leo. 2017. *Analisis dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks dengan Menggunakan Metode RSA*. Medan. Riset dan E-Jurnal Manajemen Informatika Komputer. Vol.1 No 2.

Handoyo, Antonius Erick, dkk. 2018. *Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA*. Universitas Dian Nuswantoro. Jurnal Teknologi dan Sistem Komputer. 6(1).

Ibrahim, Rohmat Nur, Ilham M.S. 2017. *Perancangan Aplikasi Stegakrip dengan Metode LSB dan Algoritma RSA Berbasis WEB*. STMIK Mardira Indonesia. Jurnal Computech & Bisnis. Vol.11 No 1.

Jatmoko, dkk. 2018. *Uji Performa Penyisipan Pesan dengan Metode LSB dan MSB pada Citra Digital untuk Keamanan Komunikasi.* Universitas Dian Nuswantoro. Semarang. Jurnal Dinamika Rekayasa. Vol. 14 No. 1.

Kromodimoeljo, Sentot. 2009. *Teori dan aplikasi Kriptografi.* SPK IT Consulting.

Kusumanto, RD, dkk. 2011. *Pengolahan Citra Digital untuk Mendeteksi Obyek menggunakan Pengolahan Warna Model Normalisasi RGB.* Politeknik Negeri Sriwijaya, Palembang. Seminar Nasional Teknologi Informasi & Komunikasi Terapan.

Manalu, Harry S. 2013. *Penerapan Metode Most Significant Bit untuk Penyisispan Pesan Teks Pada Citra Digital*. STMIK Budidarma. Medan. Pelita Informatika Budi Darma. Vol IV, No 1.

Munir, Rinaldi. 2004. *Kriptografi.* Bandung: Institut Teknologi Bandung.

Munir, Rinaldi. 2019. *Kriptografi Edisi 2* .Bandung: Institut Teknologi Bandung.

Munir, Rinaldi. 2004. *Steganografi dan Watermarking.* Bandung: Institut Teknologi Bandung.

Munir, Rinaldi. 2004. *Pengantar Pengolahan Citra.* Bandung: Institut Teknologi Bandung.

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan dan Jaringan dan Implementasinya dalam Bahasa Java*. Yogykarta: Andi.

Saputra, Ragil, dkk. 2016. *Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging.* Semarang. Universitas Diponegoro. *Scientific journal of informatics*. Vol.3 No.1.

Syawal, Muhamad Fitra, dkk. 2016. *Implementasi Teknik Steganografi menggunakan Algoritma Vignere Cipher dan Metode LSB.* Universitas Budi Luhur. Jurnal TICOM Vol.4 No.3.

Utomo, Tri Prasetyo. 2017. *Steganografi Gambar dengan Metode Least Significant Bit untuk Proteksi Komunikasi Media Online.* UIN Sunan Gunung Djati Bandung.

Shihab, M. Quraish. 2002. *Tafsir Al Misbah*. Lentera Hati

Kementrian Agama RI. (2019). *Qur'an Kemenag*. Lajnah Penthasihan Mushaf Al-Qur'an

LAMPIRAN

A. Source Code

```
# Import library yang dibutuhkan
import numpy as np
from PIL import Image
import binascii
import random
import sympy as sp
import matplotlib.pyplot as plt
import cv2

    # 4.1.1 Proses Enkripsi Kriptografi dan Steganografi Menggunakan Metode RSA dan LSB
    # Fungsi untuk menghasilkan bilangan prima untuk pembentukan kunci RSA
    def generate_prima(bits):
        return sp.randprime(2**(bits-1), 2**bits)

    # Fungsi untuk menghitung kunci publik dan kunci privat RSA
    bits = 512
    def generate_rsa_keys():
        # Pilih dua bilangan prima p dan q secara acak
        p = generate_prima(bits)
        q = generate_prima(bits)
        while q == p:
            q = generate_prima(bits)
        # p = 193
        # q = 191
        # Hitung n sebagai hasil perkalian p dan q
        n = p * q
        phi = (p - 1) * (q - 1)

        # Pilih e yang relatif prima terhadap phi
        e = random.randint(2, phi - 1)
        # e = 7
        while np.gcd(e, phi) != 1:
            e = random.randint(2, phi - 1)

        # Hitung d sebagai kebalikan dari e modulo phi
        d = pow(e, -1, phi)

        # Pasangan kunci publik (e, n) dan kunci privat (d, n)
        return (e, n), (d, n)

    # Fungsi enkripsi dengan RSA
```

```
    def rsa_encrypt(plaintext, public_key):
        e, n = public_key
        encrypted_message = [pow(ord(char), e, n) for char in
plaintext]
        return encrypted_message

    # Enkripsi pesan Rahasia menjadi ciphertext
    public_key, private_key = generate_rsa_keys()
    pesan_rahasia = "UIN MALIKI MALANG"
    ciphertext = rsa_encrypt(pesan_rahasia, public_key)

    # Fungsi untuk mengonversi setiap elemen ciphertext menjadi
biner 8-bit dengan pemisah koma
    def to_binary(data):
        binary_data = []
        for num in data:
            # Konversi ke biner dan tambahkan koma setelah
setiap blok data
            binary_data.extend([format(int(digit), '08b') for
digit in str(num)])
            binary_data.append('00101100')  # ASCII untuk koma
        return binary_data

    binary_ciphertext = to_binary(ciphertext)

    # Steganografi: Menyisipkan biner ciphertext ke dalam gambar
RGB
    # Load gambar dan ubah ukuran ke 150x150
    image = Image.open("image.png")
    image = image.resize((150, 150))
    pixels = np.array(image)

    # Sisipkan biner ciphertext ke dalam LSB gambar
    def embed_data(pixels, data):
        data_index = 0
        for i in range(pixels.shape[0]):
            for j in range(pixels.shape[1]):
                for k in range(3): # R, G, B
                    if data_index < len(data):
                        # Sisipkan bit terakhir dari ciphertext
ke dalam LSB komponen warna
                        pixels[i][j][k] = (pixels[i][j][k] &
0xFE) | int(data[data_index])
                        data_index += 1
        return pixels

```

```
    encoded_pixels = embed_data(pixels.copy(),
binary_ciphertext)
    encoded_image = Image.fromarray(encoded_pixels)
    encoded_image.save("image_encode.png")

    # 4.1.2 Proses Dekripsi Kriptografi dan Steganografi
Menggunakan Metode RSA dan LSB
    # Ekstraksi data dari LSB gambar yang disisipkan
    def extract_data(pixels, length):
        binary_data = []
        data_index = 0
        for i in range(pixels.shape[0]):
            for j in range(pixels.shape[1]):
                for k in range(3): # R, G, B
                    if data_index < length:
                        binary_data.append(str(pixels[i][j][k] &
1))
                        data_index += 1
        return binary_data

    # Menggabungkan biner menjadi teks dan memfilter tanda koma
    def binary_to_text(binary_data):
        message = ''
        i = 0
        while i < len(binary_data):
            # Ambil blok 8-bit
            byte = ''.join(binary_data[i:i+8])
            if byte == '00101100':  # Cek apakah blok ini adalah
tanda koma (ASCII untuk ',')
                i += 8  # Lewati tanda koma
                continue
            # Ubah dari biner ke karakter ASCII
            message += chr(int(byte, 2))
            i += 8  # Lanjut ke blok 8-bit berikutnya
        return message

    # Ekstraksi ciphertext dari gambar
    extracted_binary_data = extract_data(encoded_pixels,
len(binary_ciphertext))
    extracted_text = binary_to_text(extracted_binary_data)

    # Deskripsi pesan dengan RSA
    def rsa_decrypt(encrypted_message, private_key):
        d, n = private_key
        decrypted_message = ''.join([chr(pow(char, d, n)) for
char in encrypted_message])
        return decrypted_message
```

```
122.
123.   # Deskripsi ciphertext menjadi pesan asli
124.   decrypted_message = rsa_decrypt(ciphertext, private_key)
125.
126.   # Menampilkan gambar asli (sebelum encoding)
127.   original_image = Image.open("image.png")  # Ganti dengan
   path gambar asli
128.   plt.figure(figsize=(10, 5))
129.   plt.subplot(1, 2, 1)
130.   plt.imshow(original_image)
131.   plt.title("Gambar Sebelum Encoding")
132.   plt.axis("off")
133.
134.   # Menampilkan gambar setelah encoding
135.   encoded_image = Image.open("image_encode.png")
136.   plt.subplot(1, 2, 2)
137.   plt.imshow(encoded_image)
138.   plt.title("Gambar Setelah Encoding")
139.   plt.axis("off")
140.
141.   plt.show()
142.
143.   # Cetak hasil
144.   print("Hasil:")
145.   print("Ciphertext:", ciphertext)
146.   print("Pesan Terenkripsi (Biner):", binary_ciphertext)
147.   print("Pesan Asli (Dekripsi):", decrypted_message)
148.
149.   # 4.1.3 Menghitung Nilai MSE dari Citra Sebelum dan Sesudah
   Enkripsi
150.   # Fungsi untuk menghitung MSE
151.   def calculate_mse(image1, image2):
152.       # Pastikan dimensi kedua citra sama
153.       if image1.shape != image2.shape:
154.           raise ValueError("Dimensi kedua citra harus sama
   untuk menghitung MSE.")
155.
156.       # Hitung MSE
157.       mse = np.mean((image1 - image2) ** 2)
158.       return mse
159.
160.   # Fungsi untuk menampilkan citra dan MSE
161.   def display_images_and_mse(image1_path, image2_path):
162.       # Membaca citra
163.       image1 = cv2.imread(image1_path, cv2.IMREAD_GRAYSCALE)
164.       image2 = cv2.imread(image2_path, cv2.IMREAD_GRAYSCALE)
165.
```

```
166.        if image1 is None or image2 is None:
167.            raise FileNotFoundError("Pastikan path citra benar
    dan file dapat diakses.")
168.
169.        # Hitung MSE
170.        mse = calculate_mse(image1, image2)
171.
172.        # Tampilkan citra
173.        plt.figure(figsize=(10, 5))
174.        plt.subplot(1, 2, 1)
175.        plt.imshow(image1, cmap='gray')
176.        plt.title("Citra Sebelum Encoding")
177.        plt.axis("off")
178.
179.        plt.subplot(1, 2, 2)
180.        plt.imshow(image2, cmap='gray')
181.        plt.title("Citra Setelah Encoding")
182.        plt.axis("off")
183.
184.        plt.suptitle(f"Mean Squared Error (MSE): {mse:.2f}",
    fontsize=16)
185.        plt.show()
186.
187.    display_images_and_mse('image.png', 'image_encode.png')
```

RIWAYAT HIDUP

Delvira Salsabilla Milana, lahir di Blitar pada tanggal 1 Januari 2000. Putri tunggal dari Eko Widarto dan Ibu Nurvita. Ia dibesarkan di rumah sederhana yang terletak di JL.Semeru Barat No. 128 RT 02 RW O6 Kelurahan Kauman Kecamatan Kepanjen Kidul Kota Blitar. Lahir dan besar tinggal di Blitar,

Perempuan dengan sapaan Delvi ataupun Vira ini telah menempuh pendidikan formal mulai dari TK Al Hidayah Kauman, kemudian menempuh pendidikan sekolah dasar di SD Kepanjenlor 2 lulus tahun 2012. Setelah itu, penulis melanjutkan ke jenjang pendidikan menengah pertama di SMPN 1 Blitar dan berhasil lulus pada tahun 2015. Selanjutnya, pendidikan menengah atas ditempuh di SMAN 3 Blitar dan diselesaikan pada tahun 2018. Setelah menyelesaikan pendidikan tersebut, penulis melanjutkan studi ke jenjang perguruan tinggi di Universitas Islam Negeri Maulana Malik Ibrahim Malang dengan memilih Program Studi Matematika pada Fakultas Sains dan Teknologi. Selama menjadi mahasiswa di Universitas Islam Negeri Maulana Malik Ibrahim Malang, penulis bergabung dalam Ikatan Mahasiswa Blitar.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Delvira Salsabilla Milania
NIM : 18610042
Fakultas / Jurusan : Sains dan Teknologi / Matematika
Judul Skripsi : Implementasi Kriptografi RSA dan Steganografi LSB dalam Penyisipan Pesan Pada Citra Digital
Pembimbing I : Muhammad Nafie Jauhari, M.Si
Pembimbing II : Ach. Nashichuddin, MA

No	Tanggal	Hal	Tanda Tangan
1.	24 Januari 2024	Konsultasi Topik dan Data	1.
2.	2 Februari 2024	Konsultasi Bab I, II, dan III	2.
3.	27 Februari 2024	Konsultasi Bab I, II, dan III	3.
4.	5 Maret 2024	Konsultasi Bab I, II, dan III	4.
5.	13 Maret 2024	Konsultasi Kajian Agama Bab I dan II	5.
6.	27 Maret 2024	ACC Bab I, II, dan III	6.
7.	1 April 2024	ACC Kajian Agama Bab I dan II	7.
8.	12 April 2024	ACC Seminar Proposal	8.
9.	1 Mei 2024	Konsultasi Revisi Seminar Proposal	9.
10.	26 September 2024	Konsultasi Bab IV dan V	10.
11.	3 Oktober 2024	Konsultasi Bab IV dan V	11.
12.	10 Oktober 2024	Konsultasi Bab IV dan V	12.
13.	17 Oktober 2024	Konsultasi Kajian Agama Bab IV	13.
14.	24 Oktober 2024	ACC Bab IV dan V	14.
15.	31 Oktober 2024	ACC Kajian Agama Bab IV	15.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

16.	7 November 2024	ACC Seminar Hasil	16.
17.	26 November 2024	Konsultasi Revisi Seminar Hasil	17.
18.	28 November 2024	Konsultasi Revisi Seminar Hasil	18.
19.	18 Desember 2024	ACC Sidang Skripsi	19.
20.	23 Desember 2024	ACC Keseluruhan	20.

Malang, 23 Desember 2024
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc.
NIP. 19741129 200012 2 005