

BAB I

PENDAHULUAN

1.1 Latar belakang

Keamanan merupakan salah satu faktor penting dalam penyimpanan dan pengiriman gambar. Keamanan dapat diartikan sekelompok langkah, prosedur, dan strategi yang digunakan untuk menghentikan dan mengamati akses ilegal, pemecahan masalah, pengungkapan, gangguan dan penyesuaian sumber yang didapat (Saputro, Hidayati & H. Ujianto, 2020). Keamanan pertukaran gambar banyak dilakukan menggunakan media internet, salah satunya adalah menggunakan berbagai macam aplikasi yaitu WhatsApp, Instagram, Telegram, dan yang lain. Maka pesan gambar lebih cepat tersampaikan bahkan hanya dalam hitungan detik serta tidak memakan banyak waktu (Deskiva, 2018).

Ada kalanya gambar digunakan dalam berbagai banyak bidang seperti keamanan, medis, ilmu, teknik, seni, hiburan, iklan, pendidikan serta pelatihan. Dengan bertambahnya penggunaan teknik digital bagi transmisi dan penyimpanan gambar, masalah mendasar untuk melindungi kerahasiaan, kebutuhan dan keaslian gambar memang perlu diperhatikan (Christian, Sitorus & Nirmala, 2023). Hal ini dikarenakan kerahasiaan suatu informasi sangatlah penting dan bersifat pribadi. Gambar dapat didefinisikan sebagai hasil buatan dari manusia, hewan, tanaman, dan lain-lain yang dihasil media gambar tersebut. Terdapat aktifitas manusia khususnya pertukaran gambar (Yudanto & Suartana, 2022). Citra memiliki elemen terkecil yaitu piksel yang merupakan komponen gambar terkecil, memiliki nilai numerik intensitas piksel yang berkisaran warna-warna tertentu (Hendrawaty, TB & Munawir, 2022). Pada gambar RGB, setiap piksel pada gambar memuat tiga warna utama yaitu merah, hijau, dan biru. Masing-masing warna tersebut nantinya diproses menjadi sebuah matriks yang kemudian dimanipulasi isinya sehingga menjadi *chipper image* (gambar yang sudah dienkripsi) (Fakhrizal *et al.*, 2023).

Salah satu cara menjaga kerahasiaan data berupa citra adalah dengan cara menyembunyikan bentuk dari citra. Menyembunyikan bentuk citra dapat dilakukan dengan menggunakan Algoritma kriptografi. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu enkripsi, dekripsi, dan kunci. Enkripsi adalah mengubah pesan atau data menjadi kode-kode yang tidak dimengerti. Keamanan dari kriptografi didapat dengan merahasiakan kunci yang dimiliki dari orang lain, tanpa harus merahasiakan algoritma itu sendiri (Sutejo, 2021).

Algoritma RSA adalah salah satu kriptografi asimetri yang sangat populer dipakai dan bahkan masih banyak hingga saat ini, algoritma RSA ini merupakan jenis kriptografi yang menggunakan dua kunci yang berbeda: kunci public (*public key*) dan kunci pribadi (*private key*). Dengan demikian, maka terdapat satu kunci, yakni kunci publik, yang dapat dikirimkan melalui saluran yang bebas, tanpa adanya suatu keamanan tertentu (Safarina & Shamir, 2017). Keamanan pada algoritma RSA ini bisa dilihat dari hasil factor-faktor prima dari bilangan besar. Hasil pemfaktoran itulah yang digunakan untuk memperoleh kunci privat. Hal ini bertolak belakang dengan kriptografi simetri yang hanya menggunakan satu jenis kunci dan kunci tersebut harus terus terjaga keamanan serta kerahasiaannya. Dalam kriptografi asimetri, dua kunci tersebut diatur sedemikian sehingga memiliki hubungan dalam suatu persamaan aritmatika modulo (Trisnawati *et al.*, 2023).

Beberapa penelitian terdahulu terkait melakukan Kriptografi RSA, diantaranya, (Nazir, Arnellis & Dewi, 2019), melakukan penelitian tentang “Penerapan Algoritma RSA untuk File Citra Menggunakan Visual Basic” bertujuan agar file citra menjadi rahasia dan menjadi terjaga secara aman (Harbani & Fahreza, 2019), melakukan penelitian tentang “Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman) Berbasis Desktop” bertujuan agar mengamankan kerahasiaan

file gambar dengan menggunakan kunci, dan menerapkan algoritma RSA dalam aplikasi pengamanan file gambar. (Azhar & Yuliany, 2019), melakukan penelitian tentang “Implementasi Algoritma RSA Untuk Enkripsi dan Dekripsi File” bertujuan agar meningkatkan dalam keamanan data atau dokumen. (Khamsyar & Basri, 2022), melakukan penelitian tentang “Aplikasi Enkripsi Menggunakan Metode (Rivest Shamir Adleman) RSA”, bertujuan untuk mengamankan gambar menggunakan aplikasi enkripsi metode RSA agar bersifat aman. (Baharsyah, Bandung & Bandung, 2023), melakukan penelitian tentang “Implementasi Algoritma RSA dalam Enkripsi dan Dekripsi File Teks”, bertujuan agar file teks yang dikirimkan tidak terjadi kebobolan data.

Pada penelitian sebelumnya terdapat penelitian (Alfaozi, 2021), melakukan penelitian tentang “Aplikasi Algoritma RSA dalam Enkripsi dan Dekripsi Gambar”. Pada penelitian ini hanya melihat keamanan aplikasinya, akan tetapi pada pola gambar aslinya masih terlihat, enkripsi yang dilakukan pada setiap pixel masih menggunakan metode dan kunci yang sama sehingga gambar aslinya masih terlihat. Kekurangan pada program tersebut yang di buat dibutuhkan waktu untuk menjalankan karena program sangat lambat karena menggunakan operasi yang tidak tepat. Berdasarkan penelitian sebelumnya maka perbedaannya adalah bertujuan untuk lebih meningkatkan kualitas citra, menerapkan Algoritma RSA dalam mengenkripsi gambar, maka penulis mencoba untuk melihat algoritma RSA pada file citra digital dengan menganalisa algoritma RSA terhadap proses pengiriman. Dapat meningkatkan tingkat keamanan gambar yang telah dikirimkan, melalui proses enkripsi dan dekripsi yang menggunakan kunci dan password agar informasi yang terdapat pada gambar tetap terjaga kerahasiannya. Dan lebih mengutamakan keamanan setiap kunci dan memakai kunci yang berbeda.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka penulis dapat merumuskan permasalahan yaitu (i) Bagaimana mengimplementasikan enkripsi gambar menggunakan algoritma RSA secara baik dan benar untuk meningkatkan keamanan pada gambar? (ii) Bagaimana pengujian penerapan algoritma RSA pada citra digital?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini yaitu (i) Meningkatkan keamanan gambar dan melindungi gambar dari akses orang yang tidak bertanggung jawab. Dan menerapkan algoritma RSA dalam mengamankan gambar dalam proses pengiriman dan membangun sistem pengamanan gambar agar gambar dapat ditingkatkan secara aman dengan melakukan enkripsi dan disimpan pada media lain berupa citra digital. (ii) Mengetahui keakuratan algoritma RSA melalui pengujian dengan mengenkripsi gambar

1.4 Manfaat Penelitian

Manfaat dari penelitian ini yaitu (i) Menambah pengetahuan mengenai penerapan kriptografi, khususnya pada algoritma RSA pada citra digital. Selama pengiriman, keaslian citra digital tetap terjaga dan resiko akses yang tidak sah dapat diminimalkan. (ii) Keamanan informasi dalam citra digital menjadi lebih terjamin, dengan menggunakan enkripsi RSA, citra dapat terlindung dari ancaman pemalsuan.