BAB III

HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Penelitian ini berjudul penerapan algoritma RSA pada citra digital. Berdasarkan hasil penelitian jurnal sebelumnya penulis melakukan penelitian tentang penerapan algoritma RSA pada citra digital. Fokus utama adalah pada evaluasi terlebih dahulu untuk mengetahui efektivitas algoritma yang digunakan. Penerapan pada algoritma RSA untuk enkripsi pada gambar serta mentransformasi entropi yang digunakan untuk evaluasi kualitas keamanan gambar. Pengujian ini dilakukan untuk melihat entropi pada gambar yang melalui beberapa tahap proses seperti, pengacakan (s*crambling*), enkripsi, dekripsi, dan pengembalian gambar (*unscrambling*). Hasil pengujian ini dilakukan dengan menggunggah gambar, kemudian gambar tersebut diproses melalui beberapa beberpa langkah: pengacakan, enkripsi, dekripsi, dan pengembalian. Pada setiap langkah, hasil entropi gambar dari setelah dihitung untuk mengukur perubahan tingkat acak.

3.1.1 Gambar Asli

Pada tahap ini gambar 3.1 merupakan gambar asli ini sebelum melakukan proses enkripisi. Gambar asli ini berfungsi sebagai input awal dalam proses enkripsi dan dekripsi agar mengetahui nilai piksel dalam gambar asli nantinya.

Gambar 3. 1 Gambar asli.

3.1.2 Ekstraksi Data

Pada ekstraksi data ini merupakan langkah sebelum melakukan dalam proses enkrispi dan dekripsi pada citra digital. Proses ini melibatkan nilai-nilai numerik yang mewakili ukuran, warna, dan format file dari setiap pixel dalam gamba. Hasil ekstraksi data dapat dilihat pada tabel 3.1.

Tabel 3.1 Hasil Ekstraksi Gambar Asli

Ukuran (Dimensi)	Tipe Warna	Format
225 x 225	RGB	JPEG

3.1.3 Enkripsi

Gambar yang telah di *scrambling* dienkripsi menggunakan algoritma RSA dengan fungsi *encrypt_image()*. Kunci publik digunakan untuk mengenkripsi data gambar, menghasilkan data terenkripsi yang tidak dapat dikenali. Berikut ini adalah hasil gambar yang telah di *enkripsi* bisa dilihat pada gambar 3.2.

Gambar 3. 2 Gambar Asli Sebelum Proses Enkripsi

Gambar 3. 3 Hasil Gambar Enkripsi.

Hasil gambar yang telah di enkripsi ditampilkan dalam bentuk noise acak menunjukkan bahwa gambar asli telah diacak.

3.1.4 Dekripsi

Setelah proses yang telah di enkripsi kemudian didekripsi menggunakan kunci privat dengan fungsi *decrypt_image()*. Proses ini mengembalikan gambar ke bentuk scrambled sebelum enkripsi. Pada dekripsi ini menggunakan algoritma RSA yang sama seperti yang digunakan pada proses enkripsi. Setelah proses dekripsi selesai, gambar yang telah didekripsi ditampilkan dan dibandingkan dengan gambar asli sebelum proses enkripsi.

Gambar 3. 4 Gambar Enkripsi Yang Akan Dekripsi

Gambar 3. 5 Hasil gambar Dekripsi.

3.2 Algoritma RSA Termodifikasi (*Scrambling* dan *Unscrambling*)

Modifikasi algoritma RSA dengan teknik scramble dan unscramble bertujuan untuk meningkatkan lagi keamanan data visual seperti gambar yang dienkripsi. Proses dimulai dengan *scrambling* gambar, di mana distribusi piksel pada gambar diacak untuk menghilangkan pola atau struktur visual yang ada. Dengan ini dilakukan menambahkan offset acak pada nilai komponen warna piksel, sehingga membuat gambar lebih sulit dikenali dan meningkatkan keamanan. Setelah gambar diacak, langkah berikutnya adalah enkripsi RSA, di mana nilai-nilai piksel yang telah diacak dienkripsi menggunakan kunci publik RSA. Proses enkripsi RSA mengubah setiap nilai piksel menjadi cipher menggunakan eksponen enkripsi dan modulus.

Setelah gambar dienkripsi dan didekripsi dengan RSA, dilakukanlah pada nilai-nilai piksel yang terenkripsi, menggunakan kunci privat RSA untuk mengembalikan nilai piksel ke bentuk aslinya. Terakhir, gambar yang telah didekripsi menjalani proses *unscrambling* untuk mengembalikan distribusi piksel ke posisi semula. *Unscrambling* ini memastikan bahwa gambar yang didekripsi dapat ditampilkan dalam format yang dapat dikenali seperti sebelum enkripsi dilakukan. Dengan cara ini, modifikasi RSA yang melibatkan *scrambling* dan *unscrambling* tidak hanya meningkatkan keamanan dengan mengacak data visual sebelum enkripsi, tetapi juga memastikan integritas dan keaslian gambar setelah proses enkripsi dan dekripsi.

3.2.1 Gambar Asli Termodifikasi

Pada tahap ini, dilakukan analisis terhadap gambar asli yang di unggah sebagai dataset, sama seperti pada algoritma RSA asli. Gambar ini berfungsi sebagai input awal dalam proses enkripsi dan dekripsi. Nilai piksel dalam gambar asli akan menjadi dasar untuk penerapan teknik *scrambling*, enkripsi RSA, dekripsi, dan *unscrambling*. Gambar asli disimpan dalam format yang memungkinkan analisis lebih lanjut dan mempermudah pemantauan perubahan selama proses.

Gambar 3. 6 Gambar Asli Sebelum Proses Enkripsi Termodifikasi

3.2.2 Ekstraksi Data Termodifikasi

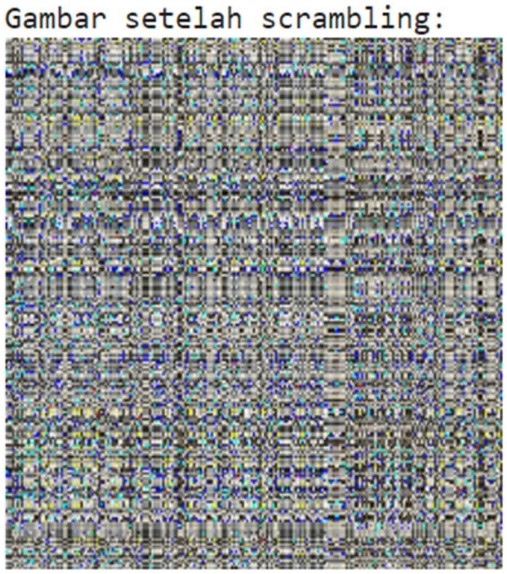
Pada proses ekstraksi data merupakan tahap awal dalam pengelolaan gambar dimana informasi gambar asli diambil dan dianalisis. Informasi ini melingkupi ukuran, warna, dan format file. Hasil ekstraksi data dapat dilihat pada Tabel 3.2.

Tabel 3. 2 Hasil Ekstraksi Data Gambar Asli termodifikasi

Ukuran (Dimensi)	Tipe Warna	Format
225 x 225	RGB	JPEG

3.2.3 *Scrambling* dengan *Caesar Cihper*

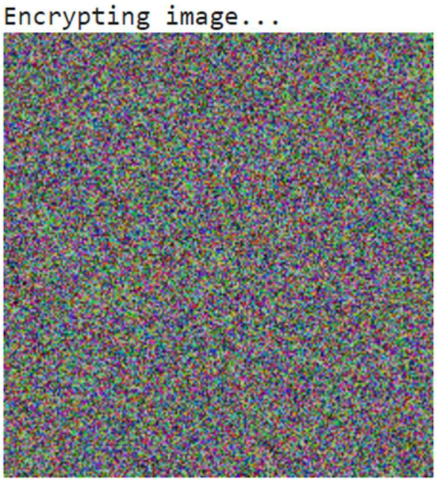
Tujuan dari pengacakan pada gambar yaitu untuk mengubah struktur spasial dari pixel dalam gambar, namun secara visual, gambar yang teracak tetap mempertahankan komposisi warna yang mirip dengan gambar asli. Gambar asli kemudian diacak menggunakan fungsi *scramble_image()*. Proses ini melibatkan dua langkah utama yaitu *Caesar cipher* mengubah nilai pixel gambar berdasarkan pergeseran yang ditentukan lalu dengan adanya permutasi menukar baris dan kolom gambar secara acak. Setiap piksel gambar digeser nilainya berdasarkan posisi piksel tersebut. Fungsi *caesar_cipher* menambahkan nilai shift yang dihitung dari koordinat piksel (x dan y) ke nilai piksel RGB (*Red, Green, Blue*). Proses ini menciptakan kerandoman tambahan pada gambar sehingga gambar menjadi lebih sulit dikenali.



Gambar 3.7 Hasil Gambar Setelah Discrambling.

3.2.4 Enkripsi Termodifikasi

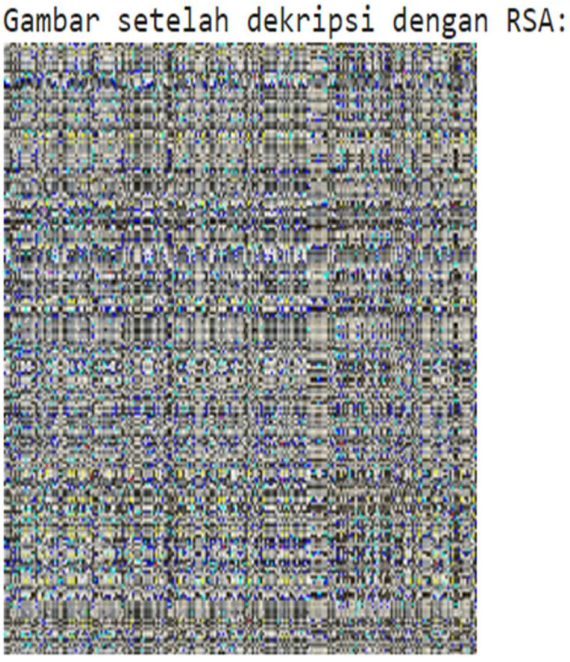
Pada gambar yang sudah diacak kemudian dienkripsi menggunakan Algoritma RSA dengan kunvi publik. Enkripsi ini mengubah gambar menjadi bentuk yang tidak dapat dikenal, dan meningkatkan keamanan dengan menjadikan gambar sulit untuk difahami atau dimengerti.



Gambar 3.8 Setelah dilakukan Enkripsi

3.2.5 Dekripsi Termodifikasi

Setelah proses yang telah di enkripsi kemudian dekripsi menggunakan kunci privat RSA yang sesuai, ini menunjukkan bahwa proses dekripsi mengembalikan gambar keadaan yang sangat mirip dengan keadaan setelah enkripsi.

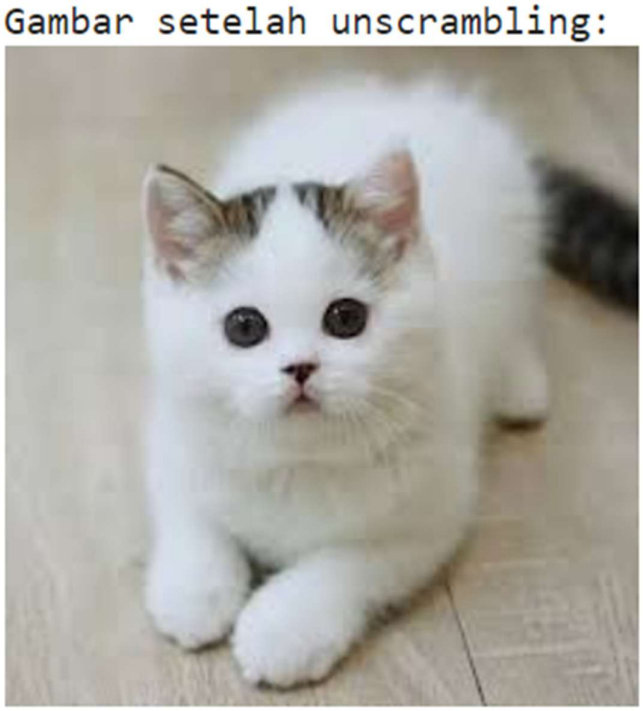


\

Gambar 3.9 Hasil Gambar Setelah Dekripsi.

3.2.6 *Unscrambling*

Langkah terakhir dalam melakukan proses unscrambling yaitu mengembalikan gambar yang telah didekripsi ke bentuk gambar aslinya dengan menggunakan algoritma *unscrambling*. Pada proses ini mengembalikan efek dari *scrambling* yang dilakukan sebelumnya sehingga piksel pada gambar kembali possisi semula.



Gambar 3.10 Gambar Setelah *Unscrambling*

3.2.7 Analisis Entropi

Analisis entropi digunakan untuk mengukur tingkat keacakan dalam sebuah gambar yang telah melalui proses enkripsi dan deksripsi. Nilai entropi yang tinggi menunjukkan tingkat keacakan pada gambar, yang berarti data menjadi lebih sulit untuk diprediksi da lebih aman. Berikut adalah hasil pengujian entropi secara menyeluruh, yang diperoleh dapat dilihat pada tabel 3.1.

Tabel 3 3 Hasil Perhitungan Entropi Gambar

Proses	Hasil Entropy(bits/pixel)	Hasil Entropi Termodifikasi
Gambar Asli	7.09	7.09
Gambar Setelah *Scrambling*	-	8.00
Data Terenkripsi	7.76	7.95
Gambar Setelah Dekripsi	7.69	7.72
Gambar Setelah *Unscrambling*	-	7.21

Secara keseluruhan, hasil yang menunjukkan bahwa operasi Gambar asli memiliki entropi yang memberikan baseline untuk kerandoman gambar. Gambar setelah scrambling menunjukkan peningkatan

entropi yang mengindikasikan kerandoman lebih tinggi setelah aplikasi Caesar cipher dan permutasi. Data terenkripsi dengan RSA menunjukkan entropi yang lebih tinggi, menandakan kerandoman yang signifikan dalam data terenkripsi. Gambar setelah dekripsi Menunjukkan bahwa meskipun data telah kembali ke bentuk yang dapat diinterpretasi, tingkat keragamannya masih tinggi, mendekati gambar asli tetapi dengan sedikit perbedaan dan *unscrambling* menunjukkan bahwa proses pembalikan pengacakan berhasil mengembalikan sebagian besar informasi ke bentuk semula, meskipun ada sedikit penurunan keragaman informasi dibandingkan dengan gambar asli.

3.3 Pembahasan

Penelitian ini menggunakan penerapan algoritma RSA ***(****Rivest-Shamir-Adleman)* dalam pengamanan citra digital. Algoritma RSA adalah sebuah algoritma kriptografi yang menggunakan metode enkripsi dan dekripsi asimetris. Asimetris berarti bahwa ada dua kunci yang berbeda digunakan untuk enkripsi dan dekripsi data: kunci publik dan kunci privat.

a. ***Scrambling* dengan *Ceasar Cipher*:** *Scrambling* ini dilakukan dengan menggeser nilai piksel berdasarkan pola baris dan kolom, mirip dengan metode Caesar cipher pada teks. Dalam metode ini, setiap piksel gambar diacak dengan menambahkan nilai acak berdasarkan posisi baris dan kolomnya, menghasilkan pengacakan yang deterministik namun kompleks. Setelah citra diacak, proses enkripsi RSA dilakukan pada citra yang telah diacak. Pengacakan ini menambah lapisan tambahan keamanan dengan mengaburkan pola gambar asli sebelum enkripsi dilakukan.

b. **Enkripsi dan Dekripsi:** Algoritma RSA terbukti efektif dalam mengamankan citra digital melalui proses enkripsi dan dekripsi. Hasil penelitian menunjukkan bahwa citra yang telah terenkripsi tidak dapat dikenali tanpa kunci dekripsi yang benar, yang membuktikan bahwa algoritma ini berhasil dalam menjaga kerahasiaan citra digital. Pada langkah ini, kunci publik dan privat RSA dihasilkan menggunakan RSA.generate(2048) yang menghasilkan kunci dengan panjang 2048 bit. Pada tahap dekripsi, citra berhasil dikembalikan ke bentuk aslinya, yang menunjukkan bahwa proses dekripsi menggunakan kunci privat yang benar dapat mengembalikan citra yang terenkripsi ke bentuk semula tanpa kehilangan kualitas.

***c. Unscrambling*:** Unscrambling ini menggunakan dengan membalik proses scrambling yang telah dilakukan sebelumnya. Permutasi dibalik menggunakan urutan permutasi terbalik dan nilai-nilai piksel diubah kembali menggunakan fungsi reverse_caesar_cipher. Proses unscrambling ini memastikan gambar kembali ke susunan baris dan kolom semula dan nilai piksel yang sesuai dengan gambar asli sebelum di-scramble.