Impelementasi Kriptografi RSA dan XOR Cipher untuk Enkripsi Citra Digital KTP

Gede Krisna Surya Artajaya[a1], Agus Muliantara[a2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]krisnasurya09@gmail.com
[2]muliantara@unud.ac.id

Abstract

The advancement of technology has led to innovative solutions in administrative sectors, exemplified by the introduction of "KTP Digital". However, not everyone has adopted "KTP Digital" and is still relying on scanned copies of identity cards that can expose digital image data to security vulnerabilities. This study addresses these vulnerabilities by proposing encryption techniques. Utilizing RSA and XOR Cipher algorithms, this research demonstrates effective encryption and decryption of digital image data. Evaluation metrics, including Peak Signal-to-Noise Ratio (PSNR), confirm minimal similarity between plain and cipher images, indicating robust encryption. Specifically, PSNR values for plain vs. cipher images range from 7 to 8 dB, well below 10 dB, indicating a very significant difference. Additionally, high PSNR values between original and decrypted plain images, which is 100 dB, suggest negligible data alteration post decryption confirming that the decryption process successfully restores the image to its original state.

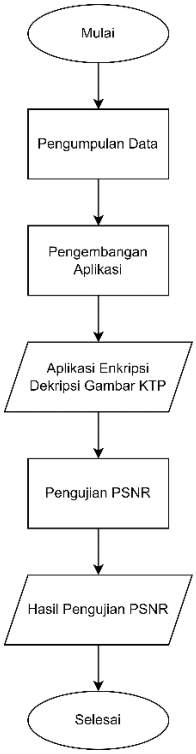
Keywords: *Cryptography, Encrypting, Decrypting, RSA, XOR Cipher*

1. Pendahuluan

Dewasa ini perkembangan teknologi telah membantu dalam segala aspek kehidupan, termasuk dalam keperluan administratif. Hadirnya KTP digital sebagai inovasi pemerintah dalam upaya mempermudah dan mempercepat proses administrasi sekaligus memberikan keamanan dalam mencegah pemalsuan atau penyalahgunaan data kependudukan. KTP digital adalah kartu tanda penduduk dalam bentuk aplikasi di *smartphone* (ponsel pintar) yang dilengkapi QR Code [1]. Meskipun demikian, penggunaan KTP digital masih belum sepenuhnya umum di masyarakat. Banyak orang masih mengandalkan KTP fisik, yang sering kali memerlukan pemindaian (*scan*) untuk berbagai keperluan, seperti saat melamar pekerjaan. Tentunya cara ini memiliki risiko yang lebih, di mana hasil pemindaian yang berupa citra digital lebih rentan dengan ancaman keamanan seperti pencurian data sensitif dari KTP sehingga diperlukan teknik untuk melindungi data tersebut. Salah satu teknik dalam penanganan ancaman keamanan pada citra digital adalah dengan mengenkripsi data citra sehingga tidak terbaca oleh pihak yang tidak bertanggung jawab. Teknik enkripsi pada gambar merupakan teknik enkripsi yang mengubah informasi atau format pada gambar ke dalam bentuk informasi atau format gambar lain yang sulit dimengerti atau dibaca oleh pihak lain [2]. Pada penelitian ini penulis menggabungkan algoritma RSA dengan algoritma XOR Cipher dalam melakukan enkripsi data pada citra. Algoritma RSA merupakan algoritma kriptografi asimetris, yang artinya kunci untuk mengenkripsi dan mendekripsi file berbeda. Sementara XOR Cipher merupakan algoritma kriptografi simetris, di mana kunci untuk mengenkripsi dan mendekripsi file adalah sama. Penggabungan kedua algortima ini bertujuan untuk mendapatkan keamanan yang lebih tinggi lagi. Kemudian untuk menguji efektivitas enkripsi dari penggabungan algoritma RS dengan algoritma XOR Cipher digunakan pengujian PSNR, yakni dengan membandingkan citra asli dengan citra terenkripsi. Penelitian terkait enkripsi citra yang pernah dilakukan salah satunya adalah penelitian enkripsi gambar yang menggunakan algoritma RSA yakni Aplikasi Algoritma RSA dalam Enkripsi dan Dekripsi Gambar [2]. Penelitian tersebut dilakukan dengan mengaplikasikan enkripsi RSA pada tiap bit warna dalam bit R, G, B sebuah gambar. Hasil dari penelitian tersebut adalah gambar yang dienkripsi menggunakan RSA

sangat berbeda dengan gambar aslinya. Jurnal selanjutnya adalah Implementasi Algoritma XOR Pada Citra Sebagai Pengamanan Pengajuan Hak Merek [3]. Di mana pada penelitian ini dilakukan enkripsi pada gambar menggunakan algoritma XOR, dengan hasil algoritma XOR dapat digunakan untuk enkripsi dan dekripsi gambar dengan baik.

2. Metode Penelitian



Gambar 1. Diagram Alur Metode Penelitian

Penelitian ini dilakukan menggunakan metode eksperimental dengan mengembangkan program kriptografi dengan tujuan untuk mengenkripsi data pada citra digital menggunakan algoritma RSA dan XOR Cipher. Alur dalam penelitian ini dimulai dari pengumpulan data terkait penelitian, kemudian melakukan pengembangan aplikasi, di mana setelah aplikasi telah dibuat maka dilakukan pengujian PSNR untuk menguji hasil dari enkripsi dan dekripsi gambar KTP dari aplikasi.

2.1. Kajian Pustaka

a. Kriptografi

Secara etimologi kriptografi berasal dari bahasa Yunani yakni *crypto* yang berarti tersembunyi dan *graphien* yang berarti menulis. Kriptografi merupakan ilmu yang mempelajarinya metode untuk mengirim pesan secara rahasia atau disamarkan sehingga hanya penerima yang dituju yang dapat menghapus penyamaran dan membaca pesan yang dikirim [4]. Dalam kriptografi pesan (data atau informasi) yang dapat dibaca dan dipahami disebut dengan *plaintext sedangkan* pesan yang telah disandikan sehingga tidak bermakna lagi disebut dengan *ciphertext*. Proses penyandian *plaintext* menjadi *ciphertext* disebut dengan enkripsi sedangkan untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dengan dekripsi [5]. Secara umum kriptografi diklasifikasikan menjadi dua, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris adalah algoritma kriptografi yang menggunakan satu kunci untuk mengenkripsi dan mendekripsi pesan. Kriptografi asimetris adalah algoritma kriptografi yang menggunakan dua kunci, yakni kunci publik untuk mengenkripsi dan kunci privat untuk mendekripsi pesan.

b. Algoritma RSA

Algoritma RSA (Rivest, Shamir, Adleman) adalah algoritma kriptografi asimetris. Proses enkripsi dan dekripsi dari algoritma RSA ini didasari pada proses matematika khususnya pada konsep bilangan prima dan aritmatika modulo untuk menghasilkan kunci rahasia untuk melakukan proses enkripsi dan dekripsi [6]. Berikut ini merupakan cara kerja dari algoritma RSA:

a. Pilih dua bilangan prima p dan q
b. Hitung nilai n, di mana $n = p * q$ (1)
c. Hitung nilai ϕ(n), di mana $\phi(n) = (p - 1) * (q - 1)$ (2)
d. Pilih sebuah bilangan bulat e sebagai kunci publik dengan syarat e harus relatif prima terhadap ϕ(n)
e. Hitung kunci dekripsi d menggunakan persamaan $ed \equiv 1 \ (mod \ \phi(n))$ atau $d \equiv e - 1 \ mod \ (\phi(n))$ (3)
f. Kunci publik dan kunci privat dari perhitungan tersebut adalah sebagai berikut:
   - Kunci publik adalah pasangan (e, n)
   - Kunci privat adalah pasangan (d, n)
g. Untuk melakukan enkripsi hitung blok *ciphertext* dengan menggunakan persamaan $c = me \ mod \ n$, di mana c adalah *ciphertext* dan m adalah *plaintext* (4)
h. Untuk melakukan dekripsi hitung blok *plaintext* dengan menggunakan persamaan $m = cd \ mod \ n$ (5)

c. Algoritma XOR Cipher

Algoritma XOR Cipher adalah algoritma kriptografi simetris. Proses dari enkripsi XOR Cipher adalah dengan melakukan operasi XOR *plaintext* dengan kunci sehingga menghasilkan *ciphertext*. Sedangkan proses dari dekripsi XOR Cipher adalah dengan melakukan operasi XOR *ciphertext* dengan kunci sehingga menghasilkan *plaintext* [7]. Operasi dari XOR mengikuti aturan sebagai berikut:

Tabel 1. Aturan Operasi XOR

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

d. PSNR

Peak Signal to Noise Ratio (PSNR) merupakan sebuah metode perbandigan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut [8]. Nilai pada PSNR dinyatakan dalam satuan desibel (dB). Dalam PSNR semakin besar nilai yang dihasilkan dari perbandingan PSNR maka semakin mirip dengan citra aslinya. Berikut ini merupakan persamaan yang digunakan untuk menentukan nilai PSNR:

$$PSNR = 20log10(\frac{MAX_i}{\sqrt{MSE}}) \quad (6)$$

$$MSE = \frac{1}{mn}\sum_i^m \sum_j^n \left| I_{(i,j)} - K_{(i,j)} \right|^2 \quad (7)$$

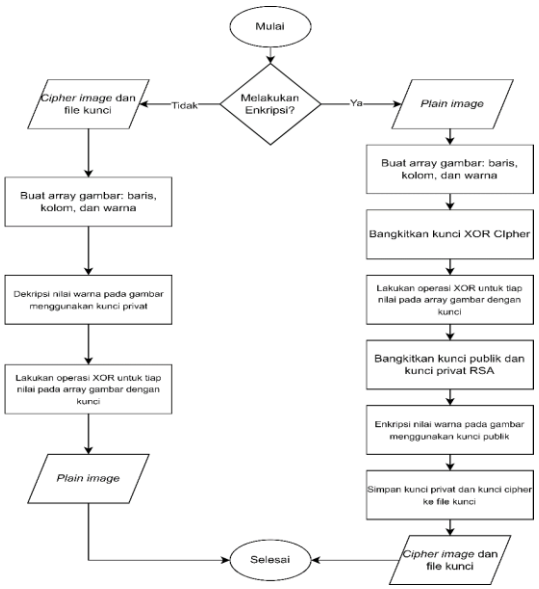
Keterangan:

MAXi = Nilai maksimum piksel pada citra
m = panjang citra (dalam piksel)
n = panjang citra (dalam piksel)

i,j = koordinat masing-masing piksel
I = nilai intensitas citra asli
K = nilai intensitas citra terenkripsi

Dari persamaan di atas, untuk mendapatkan nilai PSNR diperlukan nilai MSE sebagai pembagi nilai maksimum pada citra. Nilai MSE ini merupakan nilai eror kuadrat rata-rata antara citra asli (*plain image*) dengan citra yang terenkripsi (*cipher image*). Nilai MSE ini dapat bernilai nol jika tidak ada error atau perbedaan antara kedua citra tersebut yang mengakibatkan nilai PSNR mencapai tak terhingga, sehingga nilai PSNR dibatasi hanya sampai dengan 100 dB [9].

2.2. Alur Program



Gambar 2. Flowchart Sistem

Pertama, pengguna diminta untuk memilih apakah akan melakukan enkripsi atau dekripsi gambar. Pada proses enkripsi alur proses pengenkripsian gambar adalah sebagai berikut:

a. Pengguna diminta untuk memasukkan gambar (*plain image)* yang akan dienkripsi.
b. Program akan membuat array gambar dari *plain image* yang dimasukkan. Array tersebut berisi data baris, kolom, dan warna *plain image*.
c. Program akan membangkitkan kunci XOR Cipher.
d. Program melakukan operasi XOR pada setiap nilai dalam array *plain image* dengan kunci XOR Cipher.
e. Program akan membangkitkan kunci publik dan kunci privat RSA.
f. Program melakukan prosees enkripsi nilai warna menggunakan RSA dengan kunci publik.
g. Menyimpan *cipher image* dan file kunci untuk keperluan dekripsi.

Sedangkan alur pada proses dekripsi adalah sebagai berikut:

a. Pengguna diminta untuk memasukkan *cipher image* dan juga file kunci.
b. Program membuat array gambar dari *cipher image* yang berisi data baris, kolom, dan warna.
c. Program akan melakukan dekripsi nilai warna menggunakan RSA menggunakan kunci privat dari file kunci.
d. Program akan melakukan operasi XOR kunci cipher dari file kunci dengan data pada array *cipher image*
e. Program akan menyimpan gambar (*plain image)* dari hasil dekripsi.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

2.3. Pengujian Sistem

Pada penelitian ini, pengujian sistem dilakukan dengan mengenkripsi dan mendekripsi citra digital *dummy* sebagai representasi dari hasil *scan* KTP. Kemudian dilakukan pengujian menggunakan PSNR untuk mendapatkan nilai PSNR dari perbandingan *plain image* dengan *cipher image* dan nilai PSNR dari perbandingan *plain image* dengan *plain image* hasil dekripsi. Dalam pengujian PSNR kualitas nilai PSNR akan dianalisis mengikuti nilai pada tabel berikut:

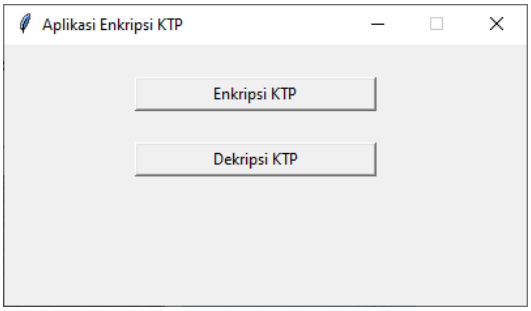
Tabel 2. Tingkat Nilai PSNR

Nilai PSNR (dB)	Kualitas Sinyal
> 30	Sangat baik
25 – 30	Baik
20 – 24	Cukup
11 - 19	Buruk
< 10	Sangat buruk

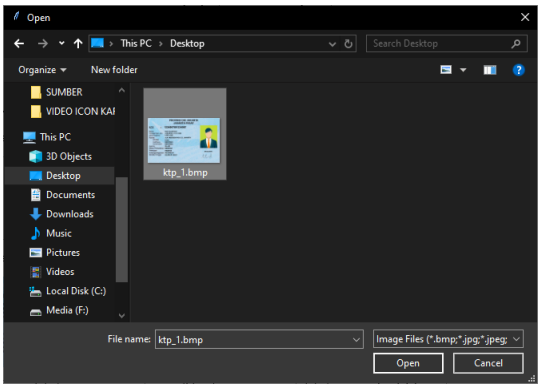
3. Hasil dan Diskusi

3.1. Enkripsi Gambar KTP

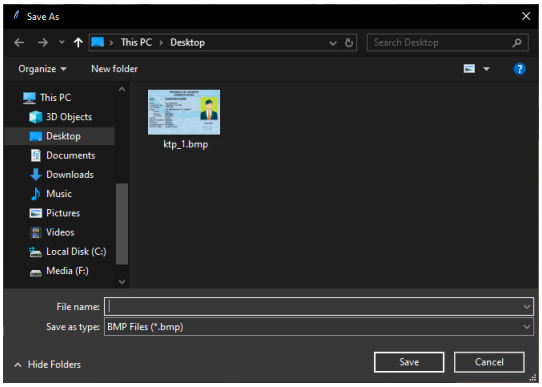
Berikut merupakan penggunaan aplikasi untuk enkripsi gambar KTP:



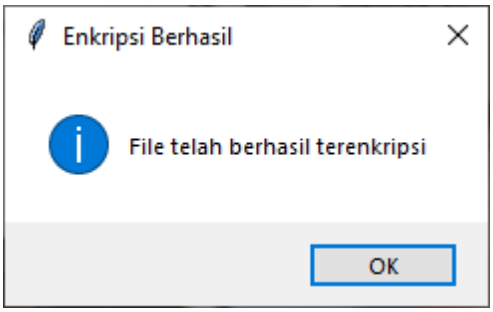
(a) *halaman utama aplikasi*



(b) *membuka gambar KTP untuk dienkripsi*



(c) *menentukan lokasi menyimpan gambar KTP hasil enkripsi*



(d) *notifikasi enkripsi berhasil*

Gambar 3. Penggunaan Aplikasi Untuk Mengenkripsi Gambar KTP

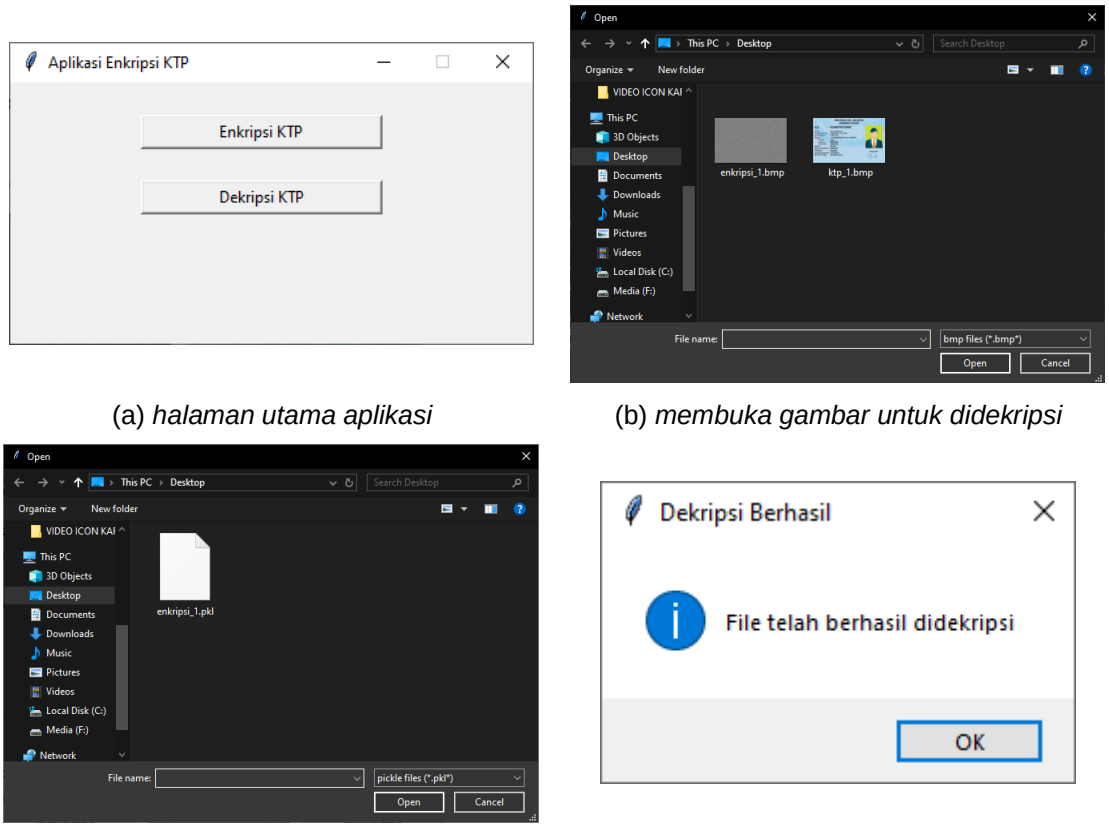
p-ISSN: 2986-3929
e-ISSN: 3032-1948

Penggunaan aplikasi untuk mengenkripsi gambar dilakukan dengan beberapa tahap sebagai berikut:

a. Pengguna menjalankan aplikasi kemudian menekan tombol Enkripsi KTP
b. Pengguna diminta untuk memilih gambar KTP yang ingin dienkripsi
c. Pengguna diminta untuk menentukan lokasi penyimpanan gambar KTP hasil enkripsi dan kunci untuk keperluan dekripsi
d. Setelah proses enkripsi selesai maka akan ada notifikasi bahwa enkripsi telah berhasil

3.2. Dekripsi Gambar KTP

Berikut merupakan penggunaan aplikasi untuk dekripsi gambar KTP:



(a) *halaman utama aplikasi* (b) *membuka gambar untuk didekripsi*

(c) *membuka kunci untuk dekripsi* (d) *notifikasi dekripsi berhasil*

Gambar 4. Penggunaan Aplikasi Untuk Mendekripsi Gambar KTP

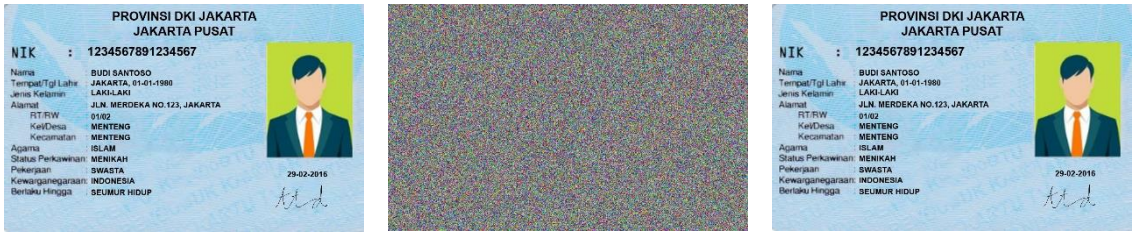
Penggunaan aplikasi untuk mengenkripsi gambar dilakukan dengan beberapa tahap sebagai berikut:

a. Pengguna menjalankan aplikasi kemudian menekan tombol Dekripsi KTP
b. Pengguna diminta untuk memilih gambar yang ingin dekripsi
c. Pengguna diminta untuk memilih kunci untuk keperluan dekripsi
d. Setelah proses dekripsi selesai maka akan ada notifikasi bahwa dekripsi telah berhasil

p-ISSN: 2986-3929
e-ISSN: 3032-1948

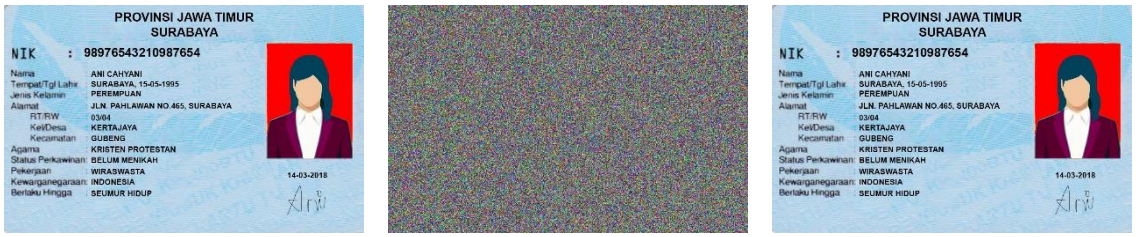
3.3. Hasil Enkripsi, Dekripsi, dan Pengujian PSNR

Berikut merpakan hasil dari enkripsi dan dekripsi menggunakan algoritma XOR Chiper dan RSA:



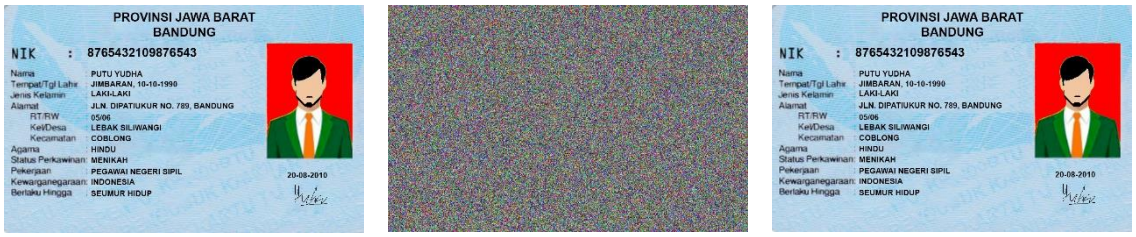
(a) *plain image* (b) *cipher image* (c) *plain image* hasil dekripsi

Gambar 5. Hasil Enkripsi dan Dekripsi Eksperimen 1



(a) *plain image* (b) *cipher image* (c) *plain image* hasil dekripsi

Gambar 6. Hasil Enkripsi dan Dekripsi Eksperimen 2



(a) *plain image* (b) *cipher image* (c) *plain image* hasil dekripsi

Gambar 7. Hasil Enkripsi dan Dekripsi Eksperimen 3

Dari eksperimen yang telah dilakukan, dapat dilihat bahwa secara visual tidak ada perubahan antara *plain image* asli dan *plain image* hasil dekripsi. *Cipher image* yang dihasilkan dari proses enkripsi juga tidak dapat dipahami karena hanya berupa *noise* warna sehingga sangat berbeda dengan gambar aslinya. Kemudian dalam pengujian dengan PSNR didapatkan hasil sebagai berikut:

Tabel 3. Tingkat Nilai PSNR *Plain Image VS Cipher Image*

Nama Image	Nilai PSNR (dB)
Ktp_dummy_1.bmp	8.499
Ktp_dummy_2.bmp	7.613
Ktp_dummy_3.bmp	7.588

Tabel 4. Tingkat Nilai PSNR *Plain Image VS Plain Image* Hasil Dekripsi

Nama Image	Nilai PSNR (dB)
Ktp_dummy_1.bmp	100
Ktp_dummy_2.bmp	100
Ktp_dummy_3.bmp	100

Dari tabel 3 didapat hasil dari tingkat nilai psnr *plain image vs cipher image* di mana nilai psnr yang didapat sangat buruk. Dalam hal ini nilai yang sangat buruk berarti hasil enkripsi dari algoritma RSA dan algoritma XOR sangat baik, karena *plain image* dan *cipher image* sangat berbeda. Sedangkan, pada tabel 4 didapat hasil nilai psnr *plain image vs plain image* hasil dekripsi yang sangat baik yang menandakan tidak ada perubahan antara *plain image* dengan *plain image* hasil dekripsi.

4. Kesimpulan

Kesimpulan yang dapat ditarik dari penelitian ini adalah algoritma RSA dan XOR Cipher sangat baik digunakan dalam enkripsi citra digital ktp di mana dari proses enkripsi *plain image* menjadi *cipher image* menghasilkan citra digital yang sangat berbeda yang tidak dapat dipahami karena hanya berupa *noise* warna. Dan dari proses dekripsi *cipher image* kembali ke *plain image* menghasilkan citra digital yang sama sesuai dengan *plain image* sebelum enkripsi. Kemudian dari hasil pengujian PSNR didapat nilai PSNR *plain image* dan *cipher image* di bawah 10 dB atau sangat buruk yang artinya *plain image* dan *cipher image* sangatlah berbeda. Sedangkan dari hasil pengujian PSNR *plain image* dan *plain image* hasil dekripsi mendapatkan nilai yang sangat baik yang berarti tidak ada perubahan saat mendekripsi citra digital. Implementasi algoritma RSA dan algoritma XOR Cipher perlu dikembangkan lagi agar dapat diintregasikan ke dalam berbagai *platform* untuk mengenkripsi citra digital ktp sehingga data sensitif dalam citra digital ktp dapat dijaga dari ancaman keamanan.

Daftar Pustaka

[1] "Cara Memperoleh KTP Digital." Accessed: May 23, 2024. [Online]. Available: https://www.kominfo.go.id/content/detail/53836/cara-memperoleh-ktp-digital/0/artikel
[2] I. Alfaozi, "Aplikasi Algoritma RSA dalam Enkripsi dan Dekripsi Gambar," 2021.
[3] M. F. Gunawan, "Implementasi Algoritma XOR Pada Citra Sebagai Pengamanan Pengajuan Hak Merek," 2022.
[4] Jamaludin *et al.*, "Kriptografi Teknik Keamanan Data".
[5] S. I. Lestariningati, "Rekayasa Internet."
[6] J. K. Azhar and S. Yuliany, "Implementasi Algoritma RSA (Rivest, Shamir dan Adleman) untuk Enkripsi dan Dekripsi File .pdf."
[7] Suhardi, "Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-Or (Xor)," 2016.
[8] E. Yudi Hidayat and K. Hastuti, "Analisis Steganografi Metode Least Significant Bit (Lsb) Dengan Penyisipan Sekuensial Dan Acak Secara Kuantitatif Dan Visual," 2013.
[9] J. Elektronik and I. Komputer Udayana, "Enkripsi Gambar Berdasarkan Modifikasi Bit Piksel Dengan Menggunakan Perpaduan Logistic Map Dan Henon Map".