Analisis Kekuatan Enkripsi Data Pada Citra Digital Menggunakan Metode Rubiks Cube

Yudhistira Satrio Yudanto[1], I Made Suartana[2]

[1,2] Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]yudhistirayudanto16051204045@mhs.unesa.ac.id
[2]imadesuartana@unesa.ac.id

***Abstrak*—Perkembangan teknologi pada saat ini sangatlah pesat, yang dimana dapat memberikan berbagai macam informasi dan berbagai macam - macam pilihan untuk melakukan sebuah penyimpanan dan pengiriman informasi. Citra Digital merupakan salah satu media yang banyak digunakan untuk menyimpan foto, gambar, maupun hasil karya dalam format berbentuk digital dan sedangkan kriptografi merupakan ilmu yang mempelajari suatu teknik matematika dimana teknik tersebut berhungan dengan adanya keamanan pada media informasi seperti gambar, video, audio, dan tulisan. Media tersebut sangatlah penting dan perlu dijaga kerahasiaannya, maka dari itu saat proses pengiriman informasi yang bersifat rahasia atau sensitif, maka sebisa mungkin menjaga informasi tersebut agar tidak rentan terhadap pencurian informasi oleh pihak yang akan mencuri informasi yang dimana tidak akan merugikan pemilik informasi.**

Pada penelitian kali ini penulis akan melakukan suatu penelitian untuk memberikan suatu keamanan pada media gambar (citra digital) yang merupakan suatu keamanan kriptografi yang menggunakan algoritma Rubiks Cube. Citra yang akan digunakan sebagai bahan penelitian ini adalah citra digital yang berformat .jpg dan .bmp. Pada pengujian kali ini, penulis akan melakukan dengan dua tahap yaitu dengan menggunakan indera pengelihatan manusia dan tahap kedua dengan melakukan suatu perhitungan pada gambar yang asli dan dengan gambar hasil. Yang dimana meliputi beberapa aspek yaitu : pengujian enkripsi dan deskripsi, pengujian melalui hasil uji NPCR, dan pengujian dengan melalui hasil histogram. Dengan proses keamanan tersebut, akan diawali dengan pembangkitan pada deret kunci baris dan kolom yang secara acak, lalu akan dilanjutkan dengan pengacakan pada setiap piksel vertikal maupun horizontal sesuai dengan kunci yang sudah dibangkitkan sebelumnya. Gambar(citra digital) yang telah teracak maka akan dilanjutkan dengan implementasi XOR di setiap bagian pixel gambar tersebut. Sehingga dapat menghasilkan gambar(citra digital) yang telah dienkripsi.

Dari hasil penelitian tersebut, penulis mendapatkan kesimpulan bahwa pengujian enkripsi-dekripsi yang telah dilakukan dengan menggunakan metode rubiks cube berhasil pada bahasa pemrograman python dan pada pengujian nilai NPCR hasilnya menunjukan bahwa nilai pada gambar yang telah dienkripsi menghasilkan nilai rata – rata 99.5% . Gambar yang telah di enkripsi pada pengujian histogram mengalami perubahan nilai warna yang dimana keamanan informasi media sangat terjaga kerahasiaannya.

***Kata Kunci*—citra digital, kriptografi, rubiks cube, enkripsi, dekripsi.**

I. PENDAHULUAN

Kriptografi merupakan ilmu yang mempelajari suatu teknik matematika dimana teknik tersebut berhungan dengan adanya keamanan pada informasi, seperti halnya kerahasiaan pada data, integritas data, keabsahan data, dan autentikasi data. Tetapi bukan berarti semua aspek keamanan pada data dapat diselesaikan dengan cara kriptografi. Kriptogarafi sendiri pada umumnya diartikan sebagai ilmu dan seni yang mempelajari tentang untuk menjaga keamanan pada pesan[4].

Citra Digital merupakan salah satu media yang banyak digunakan untuk menyimpan foto, gambar, maupun hasil karya dalam format berbentuk digital[5]. Jika data - data ini tidak diamanakan secara baik maka dapat menimbulkan suatu hal – hal yang tidak diinginkan seperti halnya data tersebut akan diambil oleh pihak yang dimana pihak tersebut tidak akan bertanggung jawab atas apa yang akan dilakukannya dan digunakan sebagai suatu hal yang bersifat negatif. Hal yang perlu di lakukan agar citra dapat aman maka harus menyandikan citra tersebut agar bentuk citra menjadi acak, sehingga jika citra tersebut jatuh ke pihak yang tidak bertanggung jawab maka citra tersebut tidak bisa digunakan. Selain pengacakan citra adapun cara lainnya, yaitu dengan cara menyisipkan pesan pada gambar, agar gambar tersebut tidak dicuri oleh pihak yang akan mencuri informasi kita

Kriptografi memiliki beberapa metode yang bisa digunakan untuk mengamankan sebuah data, salah satunya adalah Rubiks Cube. Rubiks Cube sendiri merupakan permainan puzzle mekanik 3 dimensi yang telah ditemukan oleh professor arsitektur dan pemahat yang berasal dari Hungaria, bernama Erno Rubik[5]. Erno menemukan penemuannya ini pada tahun 1974. Pada awalnya Rubik memberi nama hasil penemuannya ini dengan nama Magic Cube, dan kemudian penemuannya ini diakui di Hungaria dan saat itu pula pertama kalinya mainan ini dijual di toko mainan yang bernama Ideal Toy[9]. Pada sekitar tahun 1980 toko mainan ini merubah nama termuan Erno yang awalnya Magic Cube dirubah menjadi Rubiks Cube. Hingga pada saat ini mainan yang telah ditemukan oleh Erno masih diperjual belikan dan dimainkan oleh seluruh orang yang ada dibelahan dunia. Normalnya pada sebuah mainan Rubiks Cube memiliki 6 permukaan dan memiliki 6 warna yang berbeda, dengan dimensi 3 x 3 x 3 yang terbentuk dari 26 kubus kecil[9]. Algoritma Rubiks Cube berjalan sesuai dengan permainan rubiks cube tersebut. Misal ada suatu gambar dengan n-bit dan memiliki ukuran panjang x lebar, maka nilai dari pixel ada pada gambar tersebut

dipresentasikan dengan sebuah matriks, dan terdapat dua buah kunci yang dimana kunci tersebut akan digunakan sebagaimana kunci yang pertama untuk mengetahui suatu pergeseran pada baris dari kiri lalu dari baris ke-kanan untuk kunci yang kedua digunakan sebagai untuk mengetahui suatu pergeseran pada kolom ke atas lalu kolom ke bawah[5].

Tujuan daripada penelitian adalah peneliti akan melakukan suatu penelitian untuk melakukan pengimplementasian algoritma Rubiks Cube pada proses enkripsi dan dekripsi pada gambar(citra digital) dengan format PNG dan BMP dan juga untuk mengetahui tingkat keamanan dari hasil implementasi algoritma rubiks cube tersebut dengan dilakukannya proses pengujian nilai NPCR dan melakukan proses analisis histogram untuk mengetahui kualitas citra setelah dilakukannya proses enkripsi.

II. DASAR TEORI

A. Konsep Dasar Citra

Gambar atau image merupakan suatu kumpulan dari titik, garis, bidang, dan warna yang menciptakan sebuah objek. Adapun bebrapa jenis gambar yaitu gambar 2 dimensi dan citra 3 dimensi. Contoh untuk gambar 2 dimensi adalah foto dan lukisan, sedangkan contoh untuk gambar 3 dimensi adalah patung dan hologram.[5]

Adapun juga gambar yang dimana gambar tersebut merupakan. gambaryang telah diproses melalui proses digitalisasi. Pada setiap bagian gambar akan direprentasikan dengan satuan piksel, dimana pada setiap tersebut piksel memiliki ukuran dan warna yang berbeda. Contohnya adalah gambar yang berwarna hitam putih, gambar berwarna hitam putih umumnya pada setiap gambar tersebut hanya memilki dari 1 bit saja pada setiap pikselnya. Sehingga pada gambar berwarna hitam dan putih tersebut hanya berwarna 2 warna saja yaitu warna hitam dan putih saja. Adapun juga gambar 24 bit yang berarti pada gambar tersebut 16.777.216 kombinasi warna (2^{24} warna).[4]

B. Citra dengan format PNG

Format PNG merupakan format yang sangatlah populer dan seringkali juga digunakan sebagai penyimpanan file gambar. PNG(Portable Network Graphics) merupakan format file yang memilki kompresi lossless, biasanya PNG digunakan sebagai pilihan umum untuk mengisi gambar di Web. PNG sendiri merupakan format file yang sangat baik sebagai penyimpanan gambar garis, teks, dan grafis ikon yang dimana file tersebut memilki ukuran file yang kecil.[9]

C. Citra dengan format BMP

Format BMP merupakan format yang paling sering digunakan pada website. Format gambar tersebut terdiri atas garis dan persegi yang biasa disebut dengan pixel. Pada setiap pixel membuat informasi warna.

Pixel – pixel tersebut kemudian bergabung membentuk suatu gambar, jika semakin banyak pixel yang dimuat pada suatu gambar maka akan semakin tinggi resolusi gambar tersebut.

Format bitmap biasanya disingkat menjadi BMP. Jadi pada saat kita mengunduh maupun membuat desain dalam format tersebut akan memiliki nama .bmp. Namun file gambar pada bitmap tidak hanya berakhiran bmp saja. File gambar yang memilki format GIF, PNG, TIFF, dan EXIF juga termasuk dalam golongan gambar bitmap.[7]

D. Algotritma Rubiks Cube

Rubiks Cube sendiri merupakan permainan puzzle mekanik 3 dimensi yang telah ditemukan oleh professor arsitektur dan pemahat yang berasal dari Hungaria, bernama Erno Rubik. Erno menemukan penemuannya ini pada tahun 1974[5]

Rubik memberi nama hasil penemuannya ini dengan nama Magic Cube, dan kemudian penemuannya ini diakui di Hungaria. Normalnya pada sebuah mainan Rubiks Cube memiliki 6 permukaan dan memiliki 6 warna yang berbeda, dengan dimensi 3 x 3 x 3 yang terbentuk dari 26 kubus kecil.[9]

Algoritma Rubiks Cube berjalan sesuai dengan permainan rubiks cube tersebut. Misal ada suatu gambar dengan n-bit dan memiliki ukuran panjang x lebar, maka nilai dari pixel ada pada gambar tersebut dipresentasikan dengan sebuah matriks, dan terdapat dua buah kunci yang dimana kunci tersebut akan digunakan sebagaimana kunci yang pertama untuk mengetahui suatu pergeseran pada baris dari kiri lalu dari baris ke-kanan untuk kunci yang kedua digunakan sebagai untuk mengetahui suatu pergeseran pada kolom ke atas lalu kolom ke bawah.

E. NPCR(Number of Pixel Change Rate)

NPCR merupakan suatu teknik yang membandingkan antara posisi pixel gray, plainimage, dan chiperimage. Tujuan dari pengujian NPCR sendiri adalah untuk mengetahui bahwa dimana pada setiap titik matriks terdapat sebuah perubahan elemen warna[6]

F. Histogram

Histogram merupakan sebuah teknik análisis yang digunakan sebagai untuk mengetahui kesesuaian distribusi pada setiap bagian warna pada plainimage dan chiperimage. Bila histogram pada chiperimage menghasilkan keragaman pada distribusi warna dan menunjukkan perbedaan yang signifikan pada plainimage, maka dapat disimpulkan bahwa chiperimage tidak memberikan sama sekali petunjuk untuk melakukan stastical attack pada chiperiamge yang telah dienrkripsi.[6]

III. METODOLOGI PENELITIAN

A. Proses Enkripsi

Pada proses enkripsi ini penulis akan menjelaskan bagaimana proses enkripsi yang didasarkan dengan algoritma Rubiks Cube. Suatu gambar memiliki nilai a-bit akan direpresentasikan dengan I_0 dengan adanya ukuran suatu gambar yaitu maka Panjang x lebarnya suatu gambar adalah M x N. Disini juga I_0 akan memrepretasikan nilai matriks pada

pixel gambar, langkah – Langkah dari proses algoritma Rubiks Cube dapat dijelaskan sebagai berikut ini:

1. Membangkitkan nilai yang acak pada dua buah vektor yaitu, Kr dan Kc yang dimana masing – masing terdiri atas panjang M dan N. Elemen yang ada pada Kr(i) dan Kc(i) masing – masing terdiri dari nilai acak yang dimana nilai tersebut merupakan antara himpunan A = {0,1,2,3,…,2^a,-1}, dengan catatan nilai Kr dan Kc tidak seterusnya memilki nilai yang harus konstan.
2. Memasukan nilai pada iterasi , Imax, dan memasukan inisialisasi pada Imax dengan memasukan nilai 0
3. Inkremen pada setiap bagian iterasi tersebut dengan satu: Iterasi = Iterasi + 1
4. Pada setiap bagian baris yang ada pada baris i dari gambar $I_{0,}$
   a) Menghitung jumlah pada semua elemen yang ada pada baris i, dan penjumlahan ini dapat didefinisikan dengan a(i)
   $$a(i) = \sum_{j=1}^{n} I_0(i,j), i = 1,2,\dots,M$$
   b) Menghitung bagian yang ada pada modulo 2 dari a(i), yang dapat dilambangkan dengan $M_{a(i)}$
   c) Pada baris i merupakan kiri, atau kanan, melingkar dan bergeser oleh posisi pada Kr(i) (piksel gambar tersebut digeserkan dengan posisi yang ada pada Kr(i) kearah kanan maupun kekiri, dan pada bagian piksel yang pertama akan dipindahkan ke bagian piksel yang terakhir), berdasarkan dengan aturan yang ada dibawah ini:
   If $M_{a(i)}$ = 0 then akan pindah melingkar ke kanan dan Else tersebut akan pindah melingkar kekiri.
5. Disetiap kolom yang ada pada j dari gambar $I_{0,}$
   a) Hitung semua jumlah yang ada pada setiap elemen yang dimilki oleh kolom j, pada penjumlahan kali ini dapat dilambangkan dengan
   $$\beta(i) = \sum_{j=1}^{m} I_0(i,j), i = 1,2,\dots,N$$
   b) Menghitung modulo 2 pada bagian β(j), dan pada bagian ini dapat dilambangkan dengan lambang yaitu $M_{\beta(i).}$
   c) Pada kolom ini j merupakan bawah, atas, atau dapat melingkar maupun bergeser pada posisi yang ada pada Kc(i), dengan catatan dapat mengikuti peraturan yang ada pada berikut ini:
   If $M_{\beta(i)}$ = 0 then akan pindah melingkar ke bagian yang ada di atas dan Else akan pindah melingkar ke bagian yang ada di bawah.

   Langkah yang ada dibagian 4 dan 5 merupakan suatu proses dimana dapat membuat gambar menjadi acak dan dapat dilambangkan dengan lambang $I_{ISCR.}$
6. Dengan adanya penggunaan vektor pada Kc, maka operator dibagian XOR dapat diimplementasikan dengan setiap bagian baris yang ada dari gambar I_1 dapat menggunakan fungsi sebagai berikut ini:
   $$I_1(2i-1,j) = I_{SCR}(2i-1j) xor\ K_c(j),$$
   $$I_1(2i-1,j) = I_{SCR}(2i,j) xor\ rot\ 180(K_C(j))$$
7. Dengan adanya penggunaan vektor pada Kr, maka operator dibagian XOR dapat diimplementasikan dengan setiap bagian kolom yang ada dari gambar I dapat menggunakan fungsi sebagai pada berikut ini:
   $$I_{ENG}(2i-1,j) = I_{SCR}(2i-1j) xor\ K_c(j),$$
   $$I_{ENG}(i,2\ j) = I_{SCR}(2i,j) xor\ rot\ 180(K_C(j))$$
8. Jika iterasi = Imax, maka gambar pada I_{ENG} yang sudah berhasil diacak gambarnya dan berhasil pada proses pengenkripsian tersebut, dan jika tidak berhasil maka harus kembali mengulangi lagi langkahnya dan mengulanginya langkahnya dimulai dari langkah ke 3.

Dari vektor Kc, Kr dan jumlah pada iterasi maksimal yang ada di Imax dapat dianggap sebagai kunci kerahasiaan dalam algoritma enkripsi yang telah dipakai. Namun, jika ingin mendapatkan algoritma enkripsi yang lebih cepat maka hal yang dilakukan adalah mengatur pada Imax = 1(Iterasi tunggal). Sebaliknya jika pada bagian Imax >1, maka algoritma akan lebih aman karena ruang bagian pengunciannya lebih besar dibandingkan dengan Imax = 1. Namun pada simulasi yang telah disajikan jumlah pada Imax sudah ditetapkan menjadi satu.

B. *Proses Dekripsi*

Gambar yang sudah dienkripsi maka langkah selanjutnya adalah melakukan dekripsi pada gambar, pada proses dekripsi ini menggunakan suatu kata kunci dari Kr, Kc, dan Imax dengan proses dan langkah – langkah sebagai berikut ini:

1. Inisialisasi Iter=0
2. Inkremen pada setiap bagian yang ada pada nilai iterasi dan dengan satu: Iterasi = Iterasi + 1
3. Bagian operator pada bitwise XOR dapat digunakan dengan vektor Kr dan pada disetiap bagian kolom yang ada pada gambar telah dienkripsi I_{ENG} dengan menggunakan fungsi yang ada dibawah ini:
   $$I_1(2i-1,j) = I_{ENG}(i,2j-1) xor\ K_r(j),$$
   $$I_1(i,2\ j) = I_{ENG}(i,2j) xor\ rot\ 180(K_r(j))$$
4. Langkah selanjutnya, menggunakan bagian Kc, sebagai operasi bitwise XOR dan digunakan pada setiap bagian baris yang ada di gambar I_1 :
   $$I_{SCR}(2i-1,j) = I_1(i,2j-1) xor\ K_c(j),$$
   $$I_{SCR}(2i,j) = I_1(2i,j) xor\ rot\ 180(K_c(j))$$
5. Lalu disetiap kolom bagian j pada gambar acak I_{SCR}
   a) Menghitung semua elemen pada kolom j, dan dapat dilambangkan dengan lambang $\beta_{SCR}^{(j)}$:
   $$\beta_{SCR}^{(i)} = \sum_{i=1}^{M} I_{SCR}(i,j), j = 1,2,\dots,N$$
   b) Menghitung modulo 2 pada bagian $\beta_{SCR}^{(j)}$, dan pada bagian ini dapat dilambangkan dengan lambang $M_{\beta SCR}^{(j)}$
   c) Pada kolom ini j merupakan bawah, atau atas, dan bergerak secara melingkar pada posisi yang ada pada Kc(i) dengan cacatan dapat mengikuti peraturan yang ada pada berikut ini:

If $M_{\beta SCR(j)}$ = 0 maka akan bergerak melingkar ke bagian yang ada di atas dan Else aka bergerak melingkar ke bagian yang ada di bawah

6. Lalu disetiap baris j pada gambar acak I_{SCR}
   a) Menghitung semua elemen pada baris I, dan dapat Dilambangkan dengan lambang a_{SCR} (i):

$$a_{SCR}{}^{(i)} = \sum_{i=1}^{N} I_{SCR}(i,j), j = 1, 2, \ldots, M$$

   b) Menghitung modulo 2 pada bagian $a_{SCR}{}^{(j)}$, dan pada bagian ini dapat dilambangkan dengan lambang $Na_{SCR}{}^{(j)}$
   c) Pada baris ini j merupakan bawah, atau atas, dan bergerak secara melingkar pada posisi yang ada pada Kc(i) dengan catatan dapat mengikuti peraturan yang ada pada berikut ini:

   If $Ma_{SCR(j)}$ = 0 maka akan bergerak melingkar ke bagian yang ada di atas dan Else akan bergerak melingkar ke bagian yang ada di bawah

7. Langkah berikutnya, jika iterasi pada = Imax maka pada sebuah gambar telah berhasil didekripsi dan proses dekripsinya telah selesai. Jika dekripsi belum berhasil maka harus mengulangi kembali lagi langkah – langkah dekripsi dimulai dari langkah ke 2.

IV. HASIL DAN PEMBAHASAN

Pada bagian ini penulis akan melakukan proses pengujian yang dimana untuk mengetahui apakah program atau aplikasi yang sudah dirancang dan dibuat oleh penulis akan dapat berjalan lancer sesuai yang diharapkan oleh penulis. Pada pengujian kali ini akan dilakukan dengan dua tahap yaitu dengan cara yang pertama adalah dengan menggunakan indera pengelihatan manusia dan akan melakukan suatu perhitungan pada gambar yang asli dan dengan gambar hasil. Yang meliputi 1. Pengujian enkripsi dan deskripsi, 2. Pengujian melalui hasil uji NPCR, 3. Pengujian dengan melalui hasil histogram

A. Pengujian enkripsi dan dekripsi

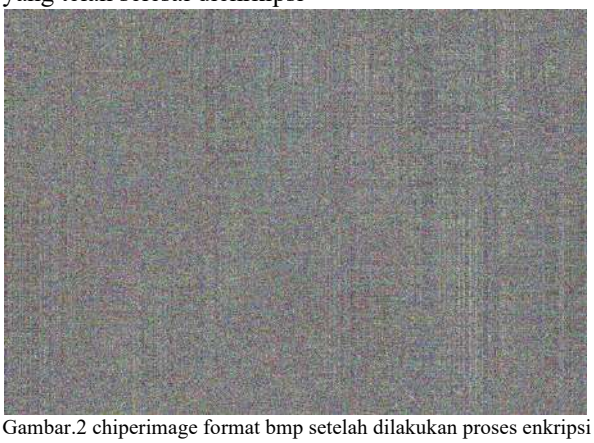
Pada pengujian pertama akan dilakukan dengan cara enkripsi- dekripsi, dimana akan dilakukan pengecekan apakah program yang telah dibangun dapat dijalankan atau tidak, agar dapat melakukan beberapa pengujian lainnya. Pengujian akan dilakukan dengan gambar berformat bmp dan PNG. Gambar yang akan dilakukan sebagai pengujian pertama adalah di bawah ini:

1. Uji enkripsi-dekripsi gambar berformat BMP

   Dibawah ini merupakan plainimage yang berformat BMP yang akan dienkripsi

Gambar.1 plainimage format bmp yang belum dienkripsi

Setelah melalui proses enkripsi maka hasil dari gambar tersebut akan menjadi seperti yang ada dibawah ini:
Dibawah ini merupakan chiperimage yang berformat BMP yang telah selesai dienrkipsi



Gambar.2 chiperimage format bmp setelah dilakukan proses enkripsi

Selanjutnya melakukan proses dekripsi terhdap gambar yang telah dienrkripsi tadi, gambar tersebut akan menjadi seperti yang ada dibawah ini:
Dibawah ini merupakan plainimage berformat BMP hasil dari dekripsi chiperiamge yang sebelumnya terenkripsi dan meghasilkan gambar seperti dibawah ini

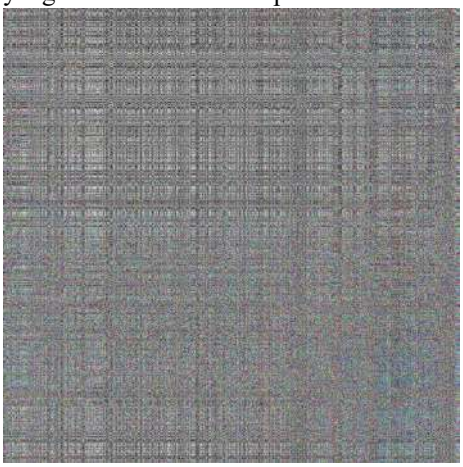
Gambar.3 plainimage format bmp yang telah dilakukan proses dekripsi

2. Gambar dengan format PNG

Dibawah ini merupakan plainimage yang berformat PNG yang akan dienkripsi

Gambar.4 plainimage format png yang belum dienrkipsi

Setelah melakukan proses enrkipsi maka hasil dari gambar tersebut akan menjadi sepertiyang ada dibawah ini:
Dibawah ini merupakan chiperimage yang berformat PNG yang telah selesai dienrkipsi



Gambar.5 plainimage format png yang telah dienkripsi

Selanjutnya melakukan proses dekripsi terhadap gambar yang telah dienkripsi tadi, gambar tersebut akan menjadi seperti yang ada dibawah ini:
Dibawah ini merupakan plainimage berformat PNG hasil dari dekripsi chiperiamge yang sebelumnya terenkripsi dan meghasilkan gambar seperti dibawah ini

Gambar.6 plainimage format png yang telah dilakukan proses dekripsi

B. Pengujian dengan data penyimpanan

Pada pengujian kali ini akan dilakukan dengan membandingkan ukuran file. Tujuan dari pengujian ini adalah untuk mengetahui perbedaan ukuran pada file gambar setelah dan sesudah dilakukannya proses enkripsi dan dekripsi. Gambar yang akan diuji adalah gambar yang berformat jpg dan bmp

Tabel.1 perbandingan ukuran file pada citra

No	Gambar	Ukuran Asli	Ukuran setelah dienkripsi	Ukuran setelah didekripsi
1	 Kopi.bmp	1.48MB	1.48MB	1.48MB
2	 Marbles.bmp	4.06MB	4.06MB	4.06MB
3	 Chugs On Deck.png	750KB	4.12MB	750KB
4	 Laptop.png	516KB	2.10MB	516KB

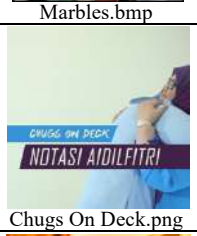
Ada 4 buah gambar yang masing- masing memiliki ukuran yang berbeda. Untuk ukuran file gambar yang telah dienkripsi memiliki ukuran gambar yang berbeda dari ukuran gambar yang asli kecuali pada gambar yang ada di kolom 1 dan 2 gambar tersebut masih tetap sama ukurannya meskipun telah dienkripsi, begitu pula pada saat gambar yang telah dienkripsi lalu dilakukannya proses dekripsi file ukuran gambarnya

berbeda juga, gambar enkripsi yang telah didekripsi file ukuran file gambar tersebut akan kembali seperti semula

C. Pengujian nilai NPCR

Pengujian kali ini akan dilakukan dengan cara mencari nilai NPCR pada gambar. NPCR sendiri adalah *Number Pixel Change Rate* merupakan suatu perbandingan dari posisi pixel antara plainimage dengan chiperimage. Tujuan dari pengujian adalah untuk mengetahui bahwa pada setiap titik yang ada pada matriks terdapat perubahan terhadap elemen warna. Pada pengujian NPCR ini akan menggunakan 4 gambar yang sama dengan pengujian sebelumnya yaitu pengujian dengan data penyimpanan

Tabel.2 Hasil nilai analisis pengujian NPCR

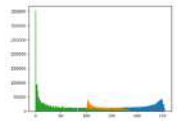
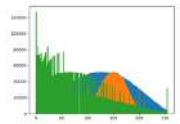
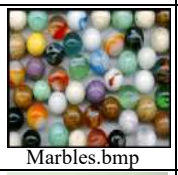
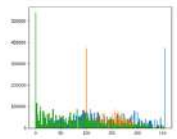
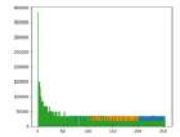
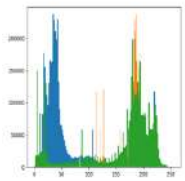
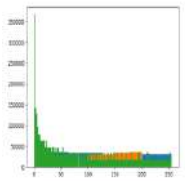
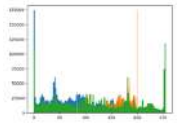
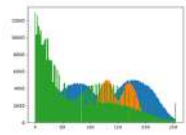
No	Gambar	Ukuran	Hasil Nilai NPCR
1	 Kopi.bmp	1024x508	99.60%
2	 Marbles.bmp	1419x1001	99.59%
3	 Chugs On Deck.png	1200x1200	99.58%
4	 Laptop.png	1050x700	99.58%

Dari tabel diatas terlihat rata – rata nilai yang dihasilkan pada pengujian NPCR hampir mendekati 100% bisa simpulkan bahwa hal tersebut mendekati sempurna. Pada pengujian ini juga mengindikasikan bahwa ada terjadinya perubahan terhadap matriks pixel gambar secara merata atau bisa di indikasikan bahwa adanya perubahan terhadap keseluruhan pixel gambar. Sehingga dapat disimpulkan bahwa tidak adanya kesamaan pada matriks atau posisi pixel antara plainimage dan chiperimage

D. Pengujian analisis Histogram

Pengujian kali ini akan dilakukan dengan cara menganalisis Histogram penyebaran nilai warna pada beberapa gambar. Pengujian ini dilakukan untuk melihat perubahan histogram warna antara plainimage dengan chiperimage.

Tabel.3 Hasil analisis pengujian Histogram

No	Plain Image	Histogram Plain Image	Histogram Chiper Image
1	 Kopi.bmp		
2	 Marbles.bmp		
3	 Chugs On Deck.png		
4	 Laptop.png		

Jika Histogram pada chiperimage memiliki keragaman pada distribusi dan memiliki perbedaan yang signifikan dengan plainimage, maka dapat disimpulkan bahwa chiperimage yang telah dilakukan uji histogram tidak memberikan petunjuk bagi kriptanalis untuk mecari persamaan nilai warna pada gambar atau biasanya disebut dengan Teknik statistical attack. Hasil dari histogram dapat dilihat pada tabel.3

Dari tabel.3 yang ada diatas, terlihat jelas perubahan histogram yang sangat signifikan antara plainimage dan chiperimage. Sehingga dapat disimpulkan bahwa adanya perubahan nilai warna yang menyeluruh pada gambar asli.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil dari pengujian dan pembahasan yang telah dilakukan pada penelitian ini maka dapat disimpulkan, sebagai berikut ini:

1. Pengujian enkripsi-dekripsi yang telah dilakukan dengan menggunakan metode rubiks cube berhasil pada bahasa pemrograman python
2. Pada pengujian nilai NPCR hasilnya menunjukan bahwa nilai pada gambar yang telah dienkripsi menghasilkan nilai rata – rata 99.5%. Dapat dinyatakan bahwa enrkripsi tersebut aman
3. Hasil dari pengujian histogram, menunjukan bahwa gambar yang telah dienkripsi mengalami perubahan nilai warna

Saran dari penulis untuk para penelitian yang serupa dengan penelitian ini, adalah agar memiliki beberapa pengembangan ke dalam bentuk aplikasi yang mempunyai user interface dan melakukan penelitian ke lebih banyak format gambar yang

dimana gambar tidak selalu memiliki format png maupun bmp. Hal itu agar para penelitian kedepan bisa mengetahui perbedaan antara format yang satu dengan yang lainnya.

UCAPAN TERIMA KASIH

Teimakasih kepada Allah S.W.T, orang tua, keluarga, dan para teman – teman yang telah mendukung saya dalam proses pengerjaan artikel ilmiah ini. Terimakasih juga untuk seluruh civitas akademia UNESA, dan seluruh teman – teman Teknik Informatika Angkatan 2016, semoga penelitian yang telah saya selesaikan dan saya lakukan ini dapat digunakan sebagai referensi untuk para peneliti selanjutnya jika memungkinkan membutuhkan sebuah referensi tentang penelitian enkripsi gambar

REFERENSI

[1] Aized Amin Soofi, Irfan Riaz, Umair Rasheed, "An Enhanced Vigenere Cipher For Data Security", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 5, ISSUE 03, MARCH 2016

[2] Lini Abraham, Neenu Daniel, "Secure Image Encryption Algorithms: A Review", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 4, APRIL 2013

[3] Rinaldi Munir, "Security Analysis of Selective Image Encryption Algorithm Based on Chaos and CBC-like Mode", 2012 7th International Conference on Telecommunication Systems, Services, and Applications (TSSA)

[4] A. Satyapratama, Widjianto, and M. Yunus, "Analisis Perbandingan ALgoritma LZW dan Huffman pada Kompresi File Gambar BMP dan PNG," J. Teknol. Inf., vol. Volume 6, pp. 69–81, 2015

[5] Farhan Djiwadukusmah & Rifky Haekal Al-Fadillah, "Implementasi Kriptografi Rubiks Cube Pada Media Gambar PNG", 2019.

[6] Pahrul Irfan., "Aplikasi Enkripsi Citra Menggunakan Algoritma Kriptografi Arnold Cat Map Dan Logistic Map", Jurnal Matrik Vol. 16 No. 1, Nov. 2016.

[7] A. Satyapratama, Widjianto, and M. Yunus, "Analisis Perbandingan ALgoritma LZW dan Huffman pada Kompresi File Gambar BMP dan PNG," J. Teknol. Inf., vol. Volume 6, pp. 69–81, 2015.

[8] Andriyani, Saraswati Yoga, "Implementasi Algoritma Kriptografi Rail Fence Cipher dan Algoritma Myszkowski Transposition dan Algoritma Kompresi Fibonacci Code", 2019

[9] Y. A. Primadhana, R. A. Asmara, and A. R. T. H. Ririd, "Enkripsi Citra Menggunakan Algoritma Kubus Rubik dengan Pembangkit Kunci MD5," J. Inform. Polinema, vol. 3, no. November, pp. 40–46, 2016.

[10] R. Purba, F. Agus, and S. Fatmawati, "Enkripsi Citra Warna Menggunakan Rubik ' S Cube Dan Three Chaotic Logistic Map," vol. 2, no. 1, pp. 76–80, 2016.