TELEKONTRAN: Jurnal Ilmiah Telekomunikasi, Kendali dan Elektronika Terapan
Vol. 12, No. 2, Oktober 2024
DOI : 10.34010/telekontran.v12i2.14167
p-ISSN : 2303 – 2901; e-ISSN : 2654 – 7384

Kombinasi *Cipher* Subtitusi (Beaufort dan Vigenere) Menggunakan Pembangkit Kunci RC4 Pada Kriptogtrafi Video Audio Video Interlaced (AVI)

Combination of Substitution Ciphers (Beaufort and Vigenere) Using RC4 Key Generator in AVI Video Cryptography

Meiton Boru, Akhzan A. Sultani, Arfan Y. Mauko, Sebastianus A. S. Mola, Kornelis Letelay, Dony M. Sihotang
Program Studi Ilmu Komputer, Fakultas Sains dan Teknik, Universitas Nusa Cendana, Indonesia
Jl. Adi Sucipto Penfui, Kupang, Indonesia
Email*: meitonboru@staf.undana.ac.id

Abstrak – Data video merupakan sarana informasi yang paling banyak diakses. Tujuan penelitian ini yaitu mengkombinasikan cipher subsitusi Beaufort dan Vigenere menggunakan pembangkit kunci RC4 untuk menghasilkan video terenkripsi yang tahan terhadap serangan saat transmisi data melalui web. Algoritma kriptografi Vigenere dan Beaufort *chiper* merupakan algoritma kriptografi klasik yang karakter *plaintext* yang sama tidak selalu membentuk karakter cipher yang sama, hal ini berarti *cipher* yang dihasilkan mampu menyamarkan pola *plaintext*. RC4 merupakan sebuah algoritma enkripsi *stream cipher* untuk pembuatan *keystream*. Hasil penelitian terhadap 30 file video AVI diperoleh bahwa proses enkripsi dan dekripsi berhasil. Ukuran file frame video berbanding lurus dengan waktu komputasi enkripsi dan dekripsi. Hasil pengujian terhadap tiga kelompok data video sample uji diperoleh waktu rata-rata yang dibutuhkan untuk enkripsi sebesar 17 menit 17 detik dan dekripsi sebesar 17 menit 40 detik. Kualitas enkripsi acak, dimana untuk audio pada tiga kelompok memberikan rata-rata MSE ± 15883 dan PSNR ± 0,612 dB. Kualitas dekripsi sempurna dibuktikan dengan MSE 0 dan PSNR infinite. Kombinasi Beaufort dan Vigenere Chiper dengan pembangkit kunci RC4 sangat disarankan untuk proses transmisi data melalui web.

Kata kunci *:* Kriptografi Video, AVI, Vigenere, Beaufort, RC4.

Abstract - *Video data is the most widely accessed information medium. The purpose of this study is to combine Beaufort and Vigenere substitution ciphers using the RC4 key generator to produce encrypted video that is resistant to attacks during data transmission over the web. The Vigenere and Beaufort cipher cryptographic algorithms are classical cryptographic algorithms in which the same plaintext characters do not always form the same cipher characters, meaning that the resulting cipher is able to disguise the plaintext pattern. RC4 is a stream cipher encryption algorithm for keystream creation. The results of the study on 30 AVI video files showed that the encryption and decryption processes were successful. The size of the video frame file is directly proportional to the encryption and decryption computation time. The results of testing three groups of test sample video data obtained an average time required for encryption of 17 minutes 17 seconds and decryption of 17 minutes 40 seconds. The quality of random encryption, where for audio in the three groups gave an average MSE of ± 15883 and PSNR of ± 0.612 dB. Perfect decryption quality is evidenced by MSE 0 and infinite PSNR. The combination of Beaufort and Vigenere Cipher with RC4 key generator is highly recommended for data transmission process via the web.*

Keywords *: Video Cryptography, AVI, Vigenere, Beaufort, RC4*

I. PENDAHULUAN

Kriptografi adalah ilmu tentang keamanan informasi yang merupakan isu yang paling mendasar dalam menjamin keamanan transmisi data melalui web [1]. Berdasarkan tekniknya kriptografi dikelompokkan dalam dua jenis yaitu kriptografi klasik dan modern [2]. Kriptografi klasik lebih minim kompleksitas dibandingkan kriptografi modern karenanya lebih unggul dalam segi waktu komputasi. Ada banyak upaya modifikasi algoritma kriptografi klasik untuk menghasilkan cipher yang acak. Misalnya, dalam Beaufort dan Vigenere menggunakan dua kunci acak yaitu citra biner dan bilangan bulat 0-255 sepanjang plaintext pada kriptografi citra, mampu memberikan kualitas cipher yang lebih unggul yaitu jauh dibawah 30 dB dan dengan rata-rata PSNR sebesar 8,87825 sementara MSE sebesar 8489,178675. Menurut Setiadi, dkk. penggunaan algoritma Beaufort dan Vigenere pada citra *grayscale* memberikan kualitas enkripsi yang unggul dibuktikan melalui nilai infinite pada PSNR dan nilai 0 pada MSE [3]. Menurut Diana, dkk. Penggunaan kunci RC4 membuat kunci dari algoritma Beaufort lebih acak [4]. Menurut Siswanto, dkk. enkripsi dan dekripsi video menggunakan algoritma Rivest-Shamir Adleman (RSA) memiliki kekurangan pada waktu komputasi yang relatif lama [5]. Menurut Minarni dkk. Kombinasi algoritma vigenere dan *End of File(EoF)* dapat mengamankan pesan dalam bentuk video [6].
Pola plainteks dikenali sebelum diubah ke citra biner[7].

Penelitian ini berbeda dari penelitian sebelumnya karena menambahkan kunci RC4 pada algoritma Beaufort dan Vigenere sehingga kunci lebih acak dan pastinya chiper video lebih tahan serangan. Jenis data yang digunakan yaitu data tanpa kompresi berupa format video AVI dengan codecs Rawvideo. Tujuan penelitian ini yaitu mengukur performa algoritma kombinasi Beaufort dan Vigenere dengan pembangkit kunci RC4 dan membandingkan apakah kombinasi Beaufort dan Vigenere menggunakan pembangkit kunci RC4 lebih baik dari kombinasi Beaufort dan Vigenere serta beberapa penelitian sebelumnya melalui waktu komputasi, kualitas dan ketahanan cipher.

II. METODOLOGI

Pada Metode Penelitian, algoritma kriptografi yang digunakan yaitu Algoritma Vigenere dan Beufort dengan pembangkit kunci Rivers Chiper 4 (RC4) sedangkan pengujiannya menggunakan nilai rata-rata PNSR dan MSE.
Algoritma kriptografi Vigenere merupakan salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti Caesar *cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama [8]. Rumus dari enkripsi dan dekripsi dengan Vigenere *chiper* dapat dilihat pada persamaan (1).
Enkripsi

$$C_i = (P_i + K_i)\ mod\ 256$$

Dekripsi

$$P_i = (C_i - K_i)\ mod\ 256 \qquad \text{…..(1)}$$

Keterangan :
C_i : Nilai *Ciphertext*
P_i : Nilai *Plaintext*
K_i : Nilai Kunci
Mod 256 : Modulus 256 karakter ASCII

Algoritma kriptografi Beaufort adalah salah satu varian dari Vigenere dimana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada Vigenere. Algoritma kriptografi Beaufort ditemukan oleh Laksamana Sir Francis Beaufort, Royal Navy, yang juga pencipta skala Beaufort, yang merupakan instrumen ahli meteorologi digunakan untuk menunjukkan kecepatan angin. Rumus dari enkripsi dan dekripsi dengan Beaufort *chiper* dapat dilihat pada persamaan (2).
Enkripsi

$$C_i = (K_i - P_i)\ mod\ 256$$

Dekripsi

$$P_i = (K_i - C_i)\ mod\ 256 \qquad \text{….(2)}$$

Keterangan :
C_i : Nilai *Ciphertext*
P_i : Nilai *Plaintext*
K_i : Nilai Kunci
Mod 256 : Modulus 256 karakter ASCII

Dikenal dengan kepanjangan Rivest *Cipher* 4, RC4 merupakan sebuah algoritma enkripsi stream *cipher* yang dirancang oleh Ron Rivest pada tahun 1983. Proses pembuatan *keystream* dari RC4 terbagi atas dua proses yaitu *key-scheduling* dan *pseudo-random generation* [9].

Proses penjadwalan kunci (*key Schedulling*) dilakukan dengan tujuan membangkitkan kunci yang acak sejumlah 256 buah kunci. Penjadwalan kunci melibatkan dua tabel *array* yaitu *array* S dan *array* T. Proses pengacakan dilakukan dengan menukarkan nilai-nilai *array*

S yang sebelumnya dikalkulasikan dengan nilai-nilai *array* T. *Pseudocode* untuk melakukan pembentukan *array* S dan *array* T seperti pada **Gambar 1**.

```
for (i = 0 ; i<=255; i++)
{ ArrayS[i] = i
ArrayT[i] = Kunci[ i mod
panjang_kunci] }
```

Gambar 1. *Pseudocode pembentukan array S dan T*

Pada tahap ini *array* S sepanjang 256 berisi *value* sesuai dengan indeksnya. Sementara, *array* T yang juga panjangnya sama dengan *array* S berisi *value* nilai ASCII dari karakter kunci yang diulang untuk memenuhi 256 indeks *array* T. Oleh karna itu, penggunaan kunci yang hanya mengandung satu jenis karakter akan dianggap sama dengan panjang kunci awal hanya 1 karakter. Selanjutnya dilakukan permutasi *array* S dengan tujuan untuk mengacak *value* dari *array* S. *Pseudocode* untuk melakukan permutasi *array* S seperti pada **Gambar 2**.

```
j = 0
for (i = 0 ; i<=255; i++) {
j = (j + ArrayS[i] +
ArrayT[i]) mod 256
Swap(ArrayS[i], ArrayS[j] )
}
```

Gambar 2. *Pseudocode permutasi array S*

Proses ini dilakukan hingga 256 iterasi (seluruh nilaai *array* S akan teracak). Proses ini memungkinkan nilai *array* tertukar lebih dari sekali.

Proses *pseudo random generation* merupakan proses yang dilakukan untuk membangkitkan kunci sebanyak elemen *plaintext* yang akan dienkripsi. *Pseudocode* untuk melakukan PRGA seperti pada **Gambar 3**.

```
k = 0; j = 0
for (i = 0 ; i < jlh_karakter_plaintext;
i++){
k = (k + 1) mod 256
j = (j + ArrayS[k]) mod 256
Swap( ArrayS[k], ArrayS[j] )
t = (ArrayS[k] + ArrayS[j]) mod 256
Kunci[i] = ArrayS[t] }
```

Gambar 3. *Pseudocode permutasi array S*

Mean Squarred Error (MSE) merupakan salah satu metode yang populer digunakan dalam pengukuran kemiripan antara dua citra. MSE adalah nilai error kuadrat rata-rata antara citra *cover* (citra asli) dengan citra ter-*steganography*. Dalam pengujian citra *steganography*, citra *steganography* dikatakan baik jika MSE yang diperoleh sangat kecil, nilai 0 pada MSE menandakan dua citra yang diukur adalah identik atau persis sama. Hal ini berarti dalam bidang kriptografi MSE diharapkan memberikan nilai yang tinggi. Semakin tinggi nilai MSE yang diperoleh semakin acak *cipher* citra yang dihasilkan. Rumus yang digunakan dalam perhitungan MSE dapat dilihat pada persamaan (3).

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(P_{xy} - C_{xy})^2 \quad \ldots(3)$$

Keterangan :
x,y : koordinat citra
M,N : dimensi citra
P : citra asli
C : citra tersandi atau hasil enkripsi
maxval : nilai pixel tertinggi pada citra

Peak Signal-to-Noise Ratio (PSNR) umumnya digunakan untuk mengukur kualitas dari rekonstruksi pemampatan *(compression)* yang bersifat *lossy* pada citra. Signal yang dimaksud adalah citra asli (sebelum pemampatan) dan *noise* adalah *error* yang disebabkan oleh proses pemampatan. Dua buah citra dikatakan memiliki tingkat kemiripan yang rendah jika nilai PSNR di bawah 30 dB[10]. Untuk menghitung PSNR, diperlukan nilai MSE.

Rumus yang digunakan dalam perhitungan PSNR dapat dilihat pada persamaan (4).

$$PSNR = 10\log_{10}(\frac{maxval^2}{MSE}) \quad \ldots.(4)$$

Dimana: maxval adalah nilai pixel tertinggi pada citra.

Perangkat keras yang diperlukan dalam tahapan pengujian yaitu komputer Lenovo tipe Lenovo MT 80XG BU Idea FM Ideapad 320-14ISK. Video sample dalam penelitian ini diperoleh dari situs berbagi video youtube.com. video yang digunakan merupakan iklan, video pendek dan atau trailer dari beberapa film.

Persiapan yang dilakukan yaitu dengan terlebih melakukan konversi video sample menjadi format file video avi dengan codec rawvideo (uncompressed avi) dengan audio wav dan frame bitmap. Ukuran file dari masing-masing video beragam dan video sample yang digunakan dalam pengujian memiliki durasi 35 detik – 185 detik. Video yang digunakan memiliki kualitas rendah (144p), kualitas standar (360p) dan kualitas HD

(720p). Berikut pengelompokan data video yang digunakan dalam pengujian dapat dilihat pada **Tabel I**.

Tabel I. Pengelompokan Data Video Sample

Kelompok Video	Ukuran	Jumlah video	Kualitas
1	97 MB – 473 MB	10 video	256x144
2	714 MB - 3,029 GB	10 video	640x360
3	714 MB - 3,029 GB	10 video	1280x720

Teknik enkripsi dan dekripsi yang dipergunakan dalam algoritma RC4 adalah operasi XOR pada setiap bit dari karakter kunci dan karakter plaintext, ini memungkinkan serangan dari para kriptanalis karna operasi XOR yang sangat mudah dimanfaatkan untuk menebak kunci. Adapun beberapa penelitian yang telah mencoba memodifikasi operasi XOR yang ada pada proses enkripsi algoritma RC4, seperti menggeser bit-bit ke kiri maupun ke kanan dan atau menukar dua bit awal dengan dua bit akhir pada setiap karakter cipher. Namun operasi ini dirasa cukup memberatkan beban komputasi jika diterapkan pada operasi video.

Teknik yang digunakan dalam mengkombinasikan kedua cipher substitusi (Beaufort dan Vigenere) yaitu dengan menjadikan setiap 1 bit dari kunci awal menjadi rule. Jika bit kunci awal lebih pendek dari plaintext, maka bit-bit kunci awal kemudian diulang hingga panjang rule sama dengan plaintext. Setiap rule berupa nilai boolean (true dan false) atau (1 dan 0). Enkripsi dan dekripsi akan dilakukan dengan formula Beaufort cipher jika rule bernilai 1. Sebaliknya, enkripsi dan dekripsi akan dilakukan dengan formula Vigenere cipher. *Flowchart* enkripsi dan dekripsi dapat dilihat pada **Gambar 4** dan **Gambar 5**.

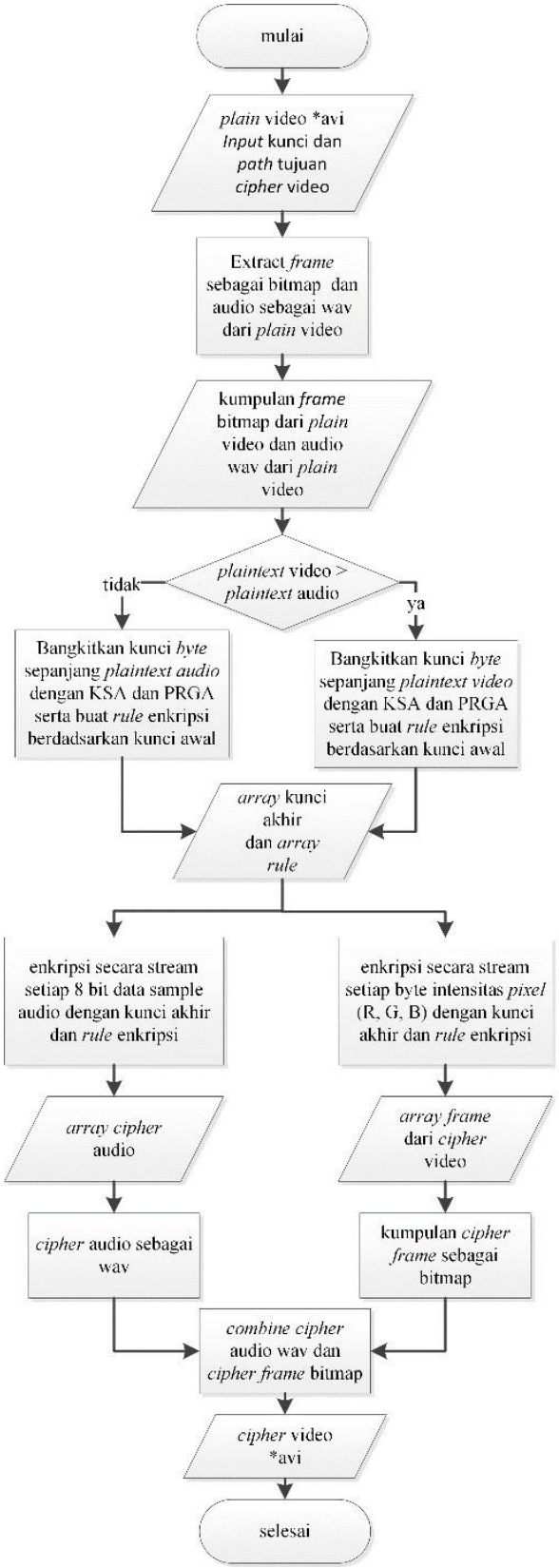
III. HASIL DAN PEMBAHASAN

Adapun waktu komputasi enkripsi dan dekripsi pada file video menggunakan Algoritma Vigenere dan Beufort dengan pembangkit kunci Rivers Chiper 4 (RC4) seperti pada **Tabel II**.

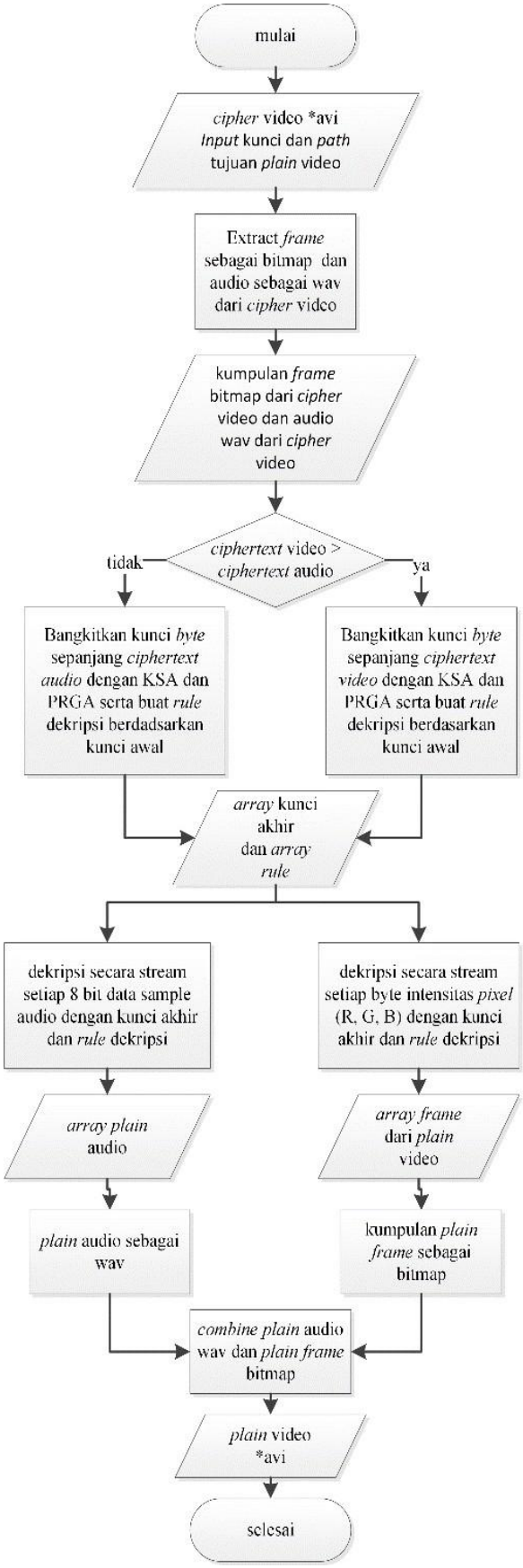
Pada **Tabel II** terlihat bahwa waktu komputasi yang dibutuhkan dalam proses enkripsi maupun dekripsi memiliki selisih waktu rata-rata sebesar 41 detik dengan selisih terkecil adalah 1 detik dan selisih terbesar adalah 3 menit 46 detik. Sementara dari 30 *file* video *sample* memerlukan waktu rata-rata sebesar 17 menit 17 detik pada proses enkripsi dan 17 menit 41 detik pada proses dekripsi. Ukuran *file* video berbanding lurus terhadap waktu komputasi, namun tidak dapat dikatakan waktu enkripsi/dekripsi sepenuhnya dipengaruhi oleh ukuran *file* semata. Sebagian besar waktu komputasi secara keseluruhan didominasi oleh sub proses transformasi *frame* dari *plain* menjadi *cipher* ataupun sebaliknya. Hal ini dikarenakan proses penulisan (*write*) data audio hanya dilakukan sekali, sedangkan data *frame* memerlukan penulisan data citra secara berulang sebanyak *frames* dalam video. Oleh karna itu meskipun ukuran dua *file* video sama persis, ada kemungkinan salah satu dari video tersebut mengandung data *frames* lebih banyak sehingga hal ini akan menjadi menyebabkan waktu komputasi sedikit lebih besar. Hasil pengujian integritas data terlihat pada **Tabel III**.

Tabel II. Waktu Komputasi berdasarkan ukuran *file* video

No. (1)	Nama Video (2)	Ukuran *File* Video (3)	Waktu (jam:menit:detik)		
			Proses Enkripsi (4)	Proses Dekripsi (5)	Selisih (6)
1	Video 1	0,097	0:0:42	0:0:41	0:0:1
2	Video 2	0,180	0:1:9	0:1:8	0:0:1
3	Video 3	0,222	0:1:30	0:1:27	0:0:3
4	Video 4	0,264	0:1:50	0:1:44	0:0:6
5	Video 5	0,305	0:2:47	0:2:52	0:0:5
6	Video 6	0,347	0:4:4	0:3:48	0:0:16
7	Video 7	0,389	0:4:12	0:4:20	0:0:8
8	Video 8	0,447	0:5:13	0:5:20	0:0:7
9	Video 9	0,469	0:5:3	0:5:16	0:0:13
10	Video	0,473	0:5:34	0:5:22	0:0:12
11	Video	0,714	0:4:28	0:4:26	0:0:2
12	Video	1,064	0:6:41	0:7:1	0:0:20
13	Video	1,310	0:7:23	0:8:3	0:0:40
14	Video	1,556	0:9:12	0:9:26	0:0:14
15	Video	1,801	0:10:13	0:11:13	0:1:0
16	Video	2,047	0:11:45	0:12:7	0:0:22
17	Video	2,538	0:15:27	0:15:41	0:0:14
18	Video	2,784	0:16:33	0:17:13	0:0:40
19	Video	2,861	0:16:42	0:18:1	0:1:19
20	Video	3,029	0:17:58	0:18:23	0:0:25
21	Video	3,571	0:26:9	0:26:55	0:0:46
22	Video	3,701	0:27:32	0:28:31	0:0:59
23	Video	4,091	0:31:48	0:31:55	0:0:7
24	Video	4,221	0:32:41	0:34:55	0:2:14
25	Video	5,196	0:37:48	0:38:40	0:0:52
26	Video	5,274	0:36:51	0:40:37	0:3:46
27	Video	5,518	0:41:18	0:39:57	0:1:21
28	Video	6,168	0:43:54	0:43:39	0:0:15
29	Video	6,168	0:45:20	0:46:57	0:1:37
30	Video	6,246	0:46:54	0:44:41	0:2:13
Rata-rata			0:17:17	0:17:40	0:0:41



Gambar 4. *Flowchart* enkripsi



Gambar 5. *Flowchart* dekripsi

Tabel III. Integritas Data

No.	Kelompok Video	MSE = 0	PSNR = *infinite*	Ukuran *file* tdk berubah
1	Kelompok	10	10 video	10 video
2	Kelompok	10	10 video	10 video
3	Kelompok	10	10 video	10 video

Pada **Tabel III** dapat dilihat bahwa kualitas dekripsi yang dihasilkan adalah sempurna dibuktikan dengan nilai MSE 0 dan PSNR *infinite*. Kelemahan yang dapat terlihat jelas yaitu penggunaan format video AVI tanpa kompresi memiliki ukuran *file* yang sangat besar, meskipun begitu tetap cocok digunakan dalam video berdurasi pendek. Nilai rata-rata MSE dan PSNR antara *plain* dan *cipher* dapat dilihat pada **Tabel IV**.

Pada **Tabel IV** dapat dilihat bahwa untuk audio pada tiga kelompok memberikan rata-rata MSE ± 15883 dan PSNR ± 0,612 dB. Sementara untuk *frame* pada tiga kelompok memberikan rata-rata MSE ± 14173 dan PSNR ± 0,674 dB. Nilai MSE dan PSNR tidak jauh berbeda antara tiap-tiap kelompok, hal ini menunjukkan bahwa resolusi video dan ukuran *file* video tidak berpengaruh pada nilai MSE dan PSNR secara signifikan. Perolehan nilai rata-rata PSNR ≤ 30 dB menunjukkan bahwa kualitas enkripsi sangat acak. Nilai rata-rata MSE dan PSNR antara *plain* dan *cipher* pada penggunaan kunci ≤ 2 karakter terlihat pada **Tabel V**.

Pada **Tabel V** dapat dilihat bahwa untuk audio pada tiga kelompok memberikan rata-rata MSE ± 16223 dan PSNR ± 0,603 dB. Sementara untuk *frame* pada tiga kelompok memberikan rata-rata MSE ± 15479 dan PSNR ± 0,633 dB. Sama halnya dengan nilai rata-rata MSE dan PSNR antara *plain* dan *cipher*, nilai yang tidak jauh berbeda juga diperoleh pada kualitas *cipher* dengan ketentuan karakter kunci ≤ 2 karakter. Hal ini menunjukkan bahwa selain resolusi dan ukuran *file* video, panjang kunci awal pun juga tidak mengurangi atau berpengaruh pada nilai MSE dan PSNR secara signifikan. Sehingga, dapat disimpulkan bahwa kualitas *cipher* yang diperoleh juga tetap sangat acak pada kasus enkripsi dengan kunci ≤ 2 karakter.

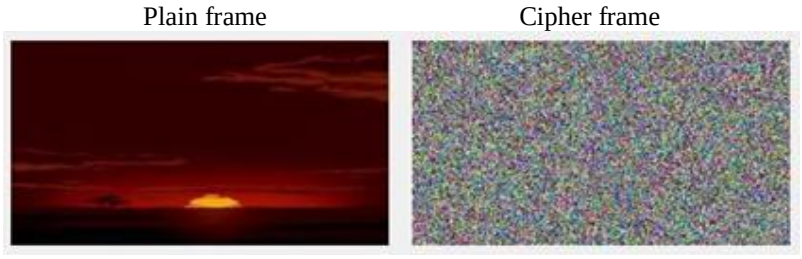
Pengujian histogram tampak pada **Gambar 6,7** diketahui nilai frekuensi tertinggi pada histogram *plain frame* adalah 255 dan frekuensi terendah adalah 0, dengan rata–rata nilai frekuensi kemunculan warnanya adalah 30,667. Sedangkan nilai frekuensi pada histogram *cipher frame* adalah 181 dan frekuensi terendah adalah 115. Secara visual dapat dilihat bahwa secara statistik nilai frekuensi kemunculan warna pada histogram *cipher frame* memiliki *range* nilai yang lebih sempit yaitu 115–181 jika dibandingkan dengan *range* nilai frekuensi kemunculan warna pada histogram *plain frame* yaitu 0–255.

Tabel IV. Nilai rata-rata MSE dan PSNR antara *Plain* dan *Cipher*

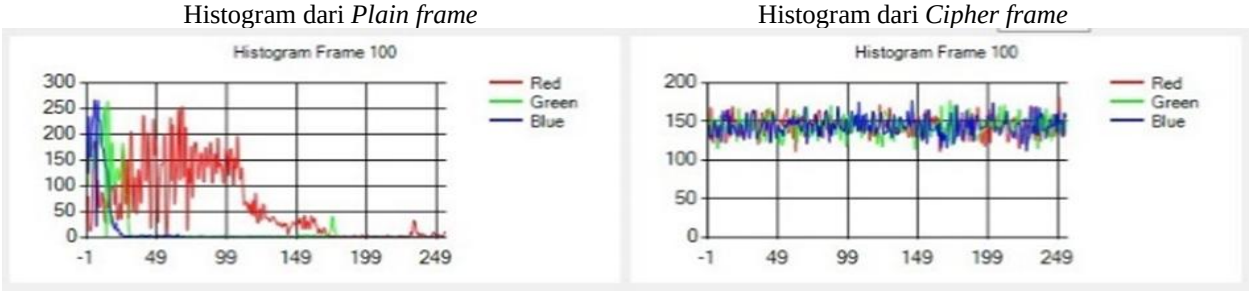
No.	Nama Kelompok	Jumlah video uji	Audio		*Frame*	
			Rata-rata MSE	Rata-rata PSNR (dB)	Rata-rata MSE	Rata-rata PSNR (dB)
1	Kelompok 1	10 video	157,505,654	0,616099489	1,350,346,159	0,699297465
2	Kelompok 2	10 video	1,597,987,742	0,609625142	1,449,754,253	0,665900258
3	Kelompok 3	10 video	1,591,950,048	0,61159729	1,451,976,954	0,659764252
4	Kelompok 1, 2 dan 3	30 video	1,588,331,443	0,61244064	1,417,359,122	0,674987325

Tabel V. Nilai rata-rata MSE dan PSNR antara *Plain* dan *Cipher* pada penggunaan kunci ≤ 2 karakter

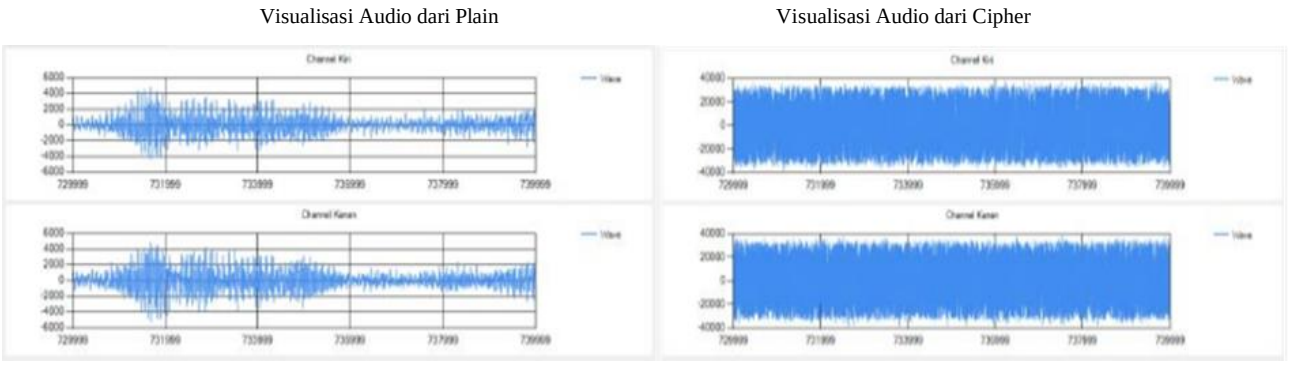
No.	Nama Kelompok	Jumlah video uji	Audio		Frame	
			Rata-rata MSE	Rata-rata PSNR (dB)	Rata-rata MSE	Rata-rata PSNR (dB)
1	Kelompok 1	3 video	16371,55446	0,599207523	15358,6068	0,636271052
2	Kelompok 2	3 video	16257,40889	0,602053361	16830,95811	0,597723493
3	Kelompok 3	3 video	16042,25471	0,608122418	14250,29195	0,665039871
4	Kelompok 1, 2 dan 3	9 video	16223,73935	0,603127767	15479,95229	0,633011472



Gambar 6. Tampak Visual Citra *Frame* ke-100 dari *Plain* dan *Cipher* Video 01



Gambar 7. Histogram Citra Frame ke-100 dari *Plain* dan *Cipher* Video 01



Gambar 8. Visualisasi Audio dari *Plain* dan *Cipher* Video 01

Pada **Gambar 8** dapat dilihat dengan jelas bahwa visualisasi audio dalam *cipher* "Video 01.avi" menunjukkan bahwa gelombang yang terbentuk memiliki amplitudo yang jauh lebih tinggi jika dibandingkan dengan audio dalam *plain* "Video 01.avi" pada Gambar 8, pola gelombang dari audio dalam *plain* "Video 01.avi" sangat tersamarkan. Saat *cipher* "Video 01.avi" dimainkan menggunakan Windows Media Player juga terdengar bunyi yang tidak beraturan. *Cipher* audio yang baik dituntut untuk mampu menyamarkan pola audio sebaik mungkin. Hasil visualisasi audio yang diperoleh dari data *sample* audio dalam "Video 01.avi" sebagai perwakilan dari keseluruhan video *sample* menunjukkan bahwa pola data audio (grafik gelombang bunyi) sangat berbeda antara *plain* dan *cipher*. Gelombang dalam *cipher* audio terhadap satuan waktu bergerak tak beraturan dengan amplitudo *channel* kiri dan *channel* kanan sebesar -32768 juga relatif seragam pada tiap *sample* audio pada *range* level bunyi -32768 sampai 32767, berbeda jauh dari gelombang dalam *plain* audio yang bergerak membentuk pola tertentu dengan amplitudo *channel* kiri sebesar 4781 sementara pada *channel* kanan yaitu -5223 pada *range* level bunyi -32768 sampai 32767.

Pada **Tabel VI** terlihat aspek ketahanan dimana audio pada tiga kelompok memberikan rata-rata MSE ± 16074 dan PSNR ± 0,607 dB. Sementara untuk *frame* pada tiga kelompok memberikan rata-rata MSE ± 15941 dan PSNR ± 0,623 dB. Nilai MSE dan PSNR tersebut merupakan nilai rata-rata yang diperoleh setelah melakukan percobaan dekripsi sebanyak 6 kali pada masing-masing 6 video dari tiap-tiap kelompok video, kemudian menghitung MSE dan PSNR antara *plain* video dan *plain* hasil dekripsi dengan kunci acak dan hampir sama. Perolehan nilai rata-rata MSE dan PSNR setelah serangan dilakukan menunjukkan bahwa *cipher* video tidak berhasil ditransformasikan kembali kedalam bentuk *plain* video dan juga tidak memperkecil nilai MSE ataupun meningkatkan nilai PSNR menjadi lebih besar dari 30 dB.

Tabel VI. Nilai rata-rata MSE dan PSNR antara *Plain* dan *Plain* Hasil Serangan Kunci

No	Jum-lah video uji	Audio		*Frame*	
		Rata-rata MSE	Rata-rata PSNR (dB)	Rata-rata MSE	Rata-rata PSNR (dB)
1	1 video	16968,23865	0,583443609	14800,31509	0,660775206
2	1 video	16033,7217	0,608046035	18402,3034	0,554699428
3	1 video	15220,36336	0,630655361	14622,53796	0,653817009
4	3 video	16074,1079	0,607381668	15941,71882	0,623097214

Kombinasi cipher substitusi (Beaufort dan Vigenere) menggunakan pembangkit kunci RC4 sesuai mendukung penelitian Setiadi, dkk dimana Kombinasi cipher substitusi (Beaufort dan Vigenere) dapat melakukan proses enkripsi dan dekripsi citra grayscale sedangkan penelitian ini juga dapat melakukan proses enkripsi dan dekripsi citra grayscale, citra warna atau RGB dan audio.

Dari sisi waktu komputasi penelitian ini lebih baik dibandingkan penelitian Siswanto dkk dikarenakan nilai PSNR (db) frame gambar video penelitian ini di nilai terbaik 0.65 sedangkan pada penelitian Siswanto dkk. Pada nilai PSNR (db) frame gambar pada 45.18.

IV. KESIMPULAN

Berhasil dibangunnya sebuah aplikasi dengan menerapkan algoritma kombinasi cipher substitusi (Beaufort dan Vigenere) menggunakan pembangkit kunci RC4 yang dapat melakukan proses enkripsi dan dekripsi. Aplikasi ini dapat digunakan untuk melakukan enkripsi dan dekripsi video uncompressed AVI. Pengujian dilakukan dengan menggunakan 30 video sample yang dikelompokkan menjadi tiga kelompok video sample uji berdasarkan ukuran dan resolusi video. Pengujian yang dilakukan adalah untuk mengukur waktu komputasi, kualitas dan ketahanan cipher.

Penelitian ini berakhir pada kesimpulan bahwa waktu komputasi cenderung meningkat seiring ukuran video dan juga diketahui rata-rata waktu yang dibutuhkan untuk enkripsi sebesar 17 menit 17 detik serta dekripsi sebesar 17 menit 41 detik. Kualitas dekripsi sempurna dibuktikan dengan MSE 0 dan PSNR infinite. Kualitas enkripsi acak dimana untuk audio pada tiga kelompok memberikan rata-rata MSE ± 15883 dan PSNR ± 0,612 dB. Sementara untuk frame pada tiga kelompok uji memberikan rata-rata MSE ± 14173 dan PSNR ± 0,674 dB. Resolusi dan ukuran file video maupun panjang kunci awal tidak berpengaruh pada nilai MSE dan PSNR secara signifikan. Secara statistik, range frekuensi kemunculan warna pada histogram cipher frames menjadi lebih sempit dan relatif seragam. Gelombang dalam cipher audio terhadap satuan waktu bergerak tak beraturan dengan amplitudo level bunyi yang berubah dan relatif seragam pada tiap-tiap sample audio. Ketahanan cipher terhadap serangan dibuktikan dengan audio pada tiga kelompok memberikan rata-rata MSE ± 16074 dan PSNR ± 0,607 dB. Sementara untuk frame pada tiga kelompok memberikan rata-rata MSE ± 15941 dan PSNR ± 0,623 dB. Artinya aplikasi ini layak digunakan untuk proses enkripsi dan dekripsi data video.

Dari rata-rata nilai MSE yang bernilai signifikan tinggi baik pada citra maupun audio sejalan dengan tujuan penelitian yang menunjukan bahwa semakin tinggi nilai MSE yang diperoleh semakin acak *cipher* citra yang dihasilkan. Sedangkan hasil PSNR pada penelitian ini ± 0,612 dB yang berarti sesuai dengan tujuan penelitian yaitu dua video (plain dan cipher) dikatakan memiliki tingkat kemiripan yang rendah jika nilai PSNR di bawah 30 dB.

Saran yaitu diperlukan penelitian lebih lanjut seperti evaluasi performance algoritma terkait dengan beberapa algoritma modern yang populer digunakan dalam kriptografi, khususnya dalam kasus kriptografi video. Adapun penelitian lain yang mungkin dapat dilakukan yaitu dengan membangun simulasi kriptografi pada kasus live streaming video, video berbayar (video dengan hak akses) berbasis web ataupun implementasi algoritma ini dalam kriptografi beragam jenis dan format file lainnya.

DAFTAR PUSTAKA

[1] V. B. Savant and R. D. Kasar, "A Review on Network Security and Cryptography," *Research Journal of Engineering and Technology*, pp. 110–114, Dec. 2021, doi: https://doi.org/10.52711/2321-581x.2021.00019.

[2] Q. Shallal and M. Bokhari, "A Review on Symmetric Key Encryption Techniques in Cryptography A Review on Symmetric Key Encryption Techniques in Cryptography," *Article in International Journal of Computer*

Applications, vol. 59, no. 10, p. 43, 2016, Available: https://www.researchgate.net/profile/Qahtan-Shallal/publication/333118027_A_Review_on_Symmetric_Key_Encryption_Techniques_in_Cryptography/links/5d21134a299bf1547c9ef4d0/A-Review-on-Symmetric-Key-Encryption-Techniques-in-Cryptography.pdf

[3] D. R. Setiadi, C. Jatmoko, E. Rachmawanto, and C. Sari, "Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital", *Proceeding SENDI_U*, Aug. 2018.

[4] M. Diana and T. Zebua, "Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS," *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, vol. 2, no. 1, p. 12, Mar. 2018, doi: https://doi.org/10.30645/j-sakti.v2i1.52.

[5] Siswanto, A. S., & M. Anif, Aplikasi Kriptografi Video Menggunakan Algoritma Rivest-Shamir Adleman (RSA), *Prosiding SENTIA, 7*, 53-58, 2015.

[6] M. Minarni, A. Ikram, I. Warman, and G. Yoga Swara, "Implementasi Algoritma Vigenere Cipher Dan End Of File Pada Steganografi Video ", *jmp*, vol. 12, no. 1, pp. 432-441, May 2023.

[7] J. Utama, Deden R., "View of Implementasi Sistem Pendeteksi Target Berdasarkan Pengenalan Warna dan Pola untuk Robot Pengikut Bola," *Unikom.ac.id*, 2024. https://ojs.unikom.ac.id/index.php/telekontran/article/view/1013/767 (accessed Oct. 15, 2024).

[8] J. Hoffstein, J. Pipher, and J. H. Silverman, "An Introduction to Cryptography," *Undergraduate texts in mathematics*, pp. 1–59, Jan. 2014, doi: https://doi.org/10.1007/978-1-4939-1711-2_1.

[9] R. Álvarez and A. Zamora, "An Intermediate Approach to Spritz and RC4," *Advances in Intelligent Systems and Computing*, pp. 297–307, 2015, doi: https://doi.org/10.1007/978-3-319-19713-5_26.

[10] A. Y. Mulyadi, "Implementasi Algoritma Aes 128 Dan Sha-256 Dalam Pengkodean Pada Sebagian Frame Video CCTV MPEG-2 - UPI Repository," *Upi.edu*, Jan. 2018, doi: http://repository.upi.edu/34541/1/S_KOM_1301015_Title.pdf.