Bigint Computing Journal
Open Access
Publisher Ali Institute of Research and Publication

Implementasi Security System Menggunakan Kriptografi Algoritma Simetris Untuk Pengamanan Video

Afifah Balqis Pasaribu [1], Fiqri Fakhrizal [2,], Sahnas Wulandari [3], Raissa Amanda Putri[4]*

[1,2,3,4] Fakultas Sains Dan Teknologi, Universitas Islam Negeri Sumatera Utara, Medan, Indonesia

A B S T R A K

Untuk menjaga keaslian informasi pada sebuah video diperlukan pengamanan yang baik. Dengan menggunakan aplikasi kriptografi dapat menjaga dan melindungi keamanan. Aplikasi kriptografi mampu membuat tampilan video menjadi tidak jelas. Deskripsi dan enkripsi menggunakan kunci simetris. Untuk menjaga keaslian video kunci simetris, harus dirahasiakan agar keamanan tidak dilanggar oleh pihak yang tidak bertanggung jawab. Sebuah video memiliki tingkat keamanan yang telah disesuaikan dengan enkripsi, semakin banyak kombinasi tombol yang digunakan maka akan semakin rumit untuk memecahkan passwordnya. Metode hill cipher merupakan metode yang menggunakan model matematis yang dapat membuat video menjadi acak sehingga informasi yang didapat tidak jelas. Menggunakan model matriks untuk menghitung piksel bingkai modulo 256. Aplikasi kriptografi video ini dapat digunakan untuk mencegah penyalahgunaan informasi.

Kata Kunci:
Keamanan, Kriptografi, Enkripsi, Dekripsi, Kunci Simetris

A B S T R A C T

To maintain the authenticity of information in a video, good security is needed. By using cryptographic applications can maintain and protect security. Cryptographic applications are capable of making video displays unclear. Description and encryption using a symmetric key. To maintain the authenticity of the symmetric key video, it must be kept secret so that security is not breached by irresponsible parties. A video has a level of security that has been adjusted to encryption, the more key combinations used, the more complicated it will be to crack the password. The hill cipher method is a method that uses a mathematical model that can make the video random so that the information obtained is not clear. Uses the matrix model to calculate frame modulo 256 pixels. This application of video cryptography can be used to prevent misuse of information

Keywords:
Security, Cryptography, Encryption, Decryption, Symmetric Key

Info Artikel

* Penulis Korespondensi: Fiqri Fakhrizal, Fakultas Sains Dan Teknologi, Universitas Islam Negeri Sumatera , Indonesia
E-mail:fiqri.fakhrizal@gmail.com

(Naskah masuk: 05 Januari 2023; diterima untuk diterbitkan: 20 Maret 2023)

PENDAHULUAN

Keamanan yang diterapkan pada sesuatu data selaku wujud penjagaan dari mungkin terjalin serbuan dari pihak luar sehingga bisa menjamin integritas sesuatu data. Pemakaian data oleh pihak tidak bertanggung jawab hendak menyebabkan kesalahpahaman dalam menerima data yang di informasikan. Kerahasiaan sesuatu data yang tersimpan pada pc wajib diberikan pengamanan serta ialah persyaratan absolut yang sangat dibutuhkan buat melindungi data terhadap bermacam ancaman semacam bisa dengan gampang memandang, mengganggu, mencuri serta maupun menyalahgunakan informasi ataupun data berarti dari sesuatu lembaga

ataupun perusahaan[1]. Menjamin kerahasian data senantiasa terpelihara diperlukan sesuatu sistem yang diketahui dengan kriptografi. Kriptografi ialah metode buat mengenkripsi data yang disusun secara acak memakai kunci enkripsi sehingga susah buat dibaca untuk yang tidak memiliki kunci dekripsi[2]. Riset terpaut yang sudah dicoba Afif Malvani serta Painem(2020) bertujuan buat membuat aplikasi pengamanan file foto memakai algoritma kriptografi RSA dengan memadukan metode steganografi algoritma End to File(EoF). Proses pengamanan file pada riset ini memakai 2 sesi, ialah dengan proses enkripsi memakai tata cara RSA yang menciptakan file terenkripsi serta diiringi dengan sesi penyisipan file terenkripsi kedalam media penampung memakai tata cara EoF. Hasil pengujian proses pengamanan file dihasilkan tingkatan keberhasilan aplikasi menggapai 100% dengan rata- rata waktu proses pengamanan file(embedding) sebesar 5, 561 detek serta waktu proses ekstraksi file sebesar 17, 533 detek.

Proses komputasi enkripsi yang dicoba memakai kunci yang berbeda- beda pada masing-masing mata kuliah sehingga membuat chipertext buat kata yang sama jadi berbeda. Bila terjalin manipulasi pesan, hingga hendak ada pemberitahuan kalau pesan tersebut sudah dimanipulasi keasliannya. Proses enkripsi memerlukan waktu yang lumayan lama bila dibanding dengan proses dekripsi. pengukuran efektifitas kriptografi dicoba memakai tata cara Avalanche Effect[5]. Enkripsi serta dekripsi yang digunakan pada aplikasi kriptografi yang diimplementasikan memakai tata cara hill cipher.

Hill cipher ialah satu algoritma kriptografi yang menggunakan matriks selaku kunci buat melaksanakan enkripsi serta dekripsi dari aritmatika modulo[6]. Pada proses enkripsi informasi asli dipecah jadi blok- blok berentetan yang cocok dengan dimensi matriks pada kunci yang digunakan[7]. Kunci yang digunakan pada proses enkripsi serta dekripsi memakai kunci simetris. Kunci simetris merupakan kunci yang digunakan buat enkripsi sama dengan kunci yang digunakan buat dekripsi ataupun diucap dengan kunci privat[2].

Kunci simetris dapat dilakukan oleh siapapun termasuk pihak yang tidak diinginkan maka perlu untuk menjaga kerahasian kunci privat ini agar tidak disalah gunakan. Kriptografi simetris banyak digunakan karena dapat bekerja secara cepat, sehingga membutuhkan daya komputasi lebih kecil[8]. Pengunaan kunci simetris biasanya digunakan dalam bentuk text, namun kunci simetris pada kriptografi ini menggunakan data dalam bentuk video. Video yang akan dienkripsi terlebih dahulu akan diekstrak menjadi beberapa buah frame. Jumlah frame yang dihasilkan berdasarkan lama durasi video yang diputar. Hasil frame video yang didapatkan diproses dengan kunci menggunakan metode hill cipher sehingga merubah bentuk informasi menjadi sulit untuk dipahami. Kembalinya informasi video menjadi utuh seperti asli menggunakan kunci yang sama pada saat melakukan enkripsi. Proses dekripsi hampir sama dengan proses enkripsi dimana video yang enkripsi akan diekstrak terlebih dahulu menjadi beberapa buah frame terenkripsi. Hasil frame didekripsi akan render kembali sehingga menjadi sebuah video asli. Penerapan keamanan video dengan menggunakan kriptografi dapat menjaga informasi yang disampaikan secara rahasia. Terbukti bahwa video tidak bisa dimengerti tanpa harus didekripsi terlebih dahulu. Tingkat keamanan suatu informasi didasarkan pada jumlah kombinasi kunci yang digunakan pada saat melakukan sebuah enkripsi. Semakin banyak kombinasi kunci yang digunakan dalam proses pengaman informasi, maka tingkat kerumitan pemecahan sandi semakin kuat. Proses keamanan informasi yang diterapkan dengan menggunakan sistem kriptografi dapat mengurangi kejahatan yang terjadi terhadap penyalahgunaan suatu informasi. Penerapan metode Kriptografi ini sudah banyak digunakan terutama dalam transaksi online baik e-commerce, e-tiket maupun internet banking[8].

METODOLOGI

Tata cara riset yang digunakan buat melaksanakan proses pada aplikasi kriptografi memakai tata cara hill cipher. Bersumber pada tipe kunci yang dipakai, tata cara hill cipher tercantum kedalam algoritma simetris sebab tata cara ini memakai sesuatu kunci yang sama buat proses enkripsi serta dekripsi. Melaksanakan proses enkripsi serta dekripsi tata cara ini memakai suatu matriks serta mempraktikkan aritmatika modulo[9]. Matriks merupakan sekumpulan bilangan yang disusun bersumber pada baris serta kolom, dan ditempatkan didalam ciri kurung, baik itu kurung biasa() ataupun kurung siku[]. Matriks memiliki suatu dimensi yang diucap dengan ordo. Ordo matriks ini bersumber pada dari banyak baris serta banyak kolom pada matriks. Matriks dalam konsep pemrograman dituangkan dalam struktur informasi Array ialah penyimpanan informasi dalam ruang memori dimana tiap ruang tersebut mempunyai indeks pengenal tiap- tiap. Citra digital umumnya berupa persegi panjang, secara visualisasi ukuran ukurannya besar kali lebar dan dinyatakan dalam titik ataupun piksel[10]. Tata cara hill cipher ini dipergunakan pada citra bertipe JPG, BMP, Gif sebab tiap komponen Red Green Blue(RGB) piksel mempunyai panjang 8 bit yang bernilai 0- 255, hingga Sistem modulo yang dipakai dalam penyandian merupakan 256[11]. Warna bawah ialah merah, hijau serta biru ataupun yang diketahui dengan citra RGB dikombinasikan sehingga mewakili tiap titik ataupun piksel pada citra warna. Terus menjadi besar resolusi yang dihasilkan diakibatkan banyaknya titik yang tercantum dalam citra, sehingga visualisasi yang dihasilkan lebih halus[10]. Proses enkripsi serta dekripsi dicoba dengan mengambil nilai RGB dari tiap piksel pada frame yang dihasilkan setelah itu dioperasikan dengan matriks. Piksel yang didapatkan pada frame video nampak pada Tabel 1 di dasar ini.

Tabel 1. Nilai piksel frame asli

Piksel	Nilai 1	Nilai 2	Nilai 3
R	255	34	72
G	252	141	146
B	87	146	233

$$P = \begin{bmatrix} 255 & 252 & 87 \\ 34 & 141 & 196 \\ 72 & 146 & 233 \end{bmatrix}$$

Setelah didapatkan nilai matrik maka metode *hill cipher* bisa dijalankan dengan cara mengalikan nilai RGB pada piksel kunci yang akan dipakai.

$$C = \begin{bmatrix} 255 & 102 & 102 \\ 255 & 102 & 102 \\ 255 & 102 & 102 \end{bmatrix} * \begin{bmatrix} 255 & 252 & 87 \\ 34 & 141 & 196 \\ 72 & 146 & 233 \end{bmatrix}$$

Hasil yang diperoleh dari perkalian dua matrik di atas setelah diproses modulo 256 adalah:

$$C = \begin{bmatrix} 254 & 100 & 34 \\ 33 & 56 & 78 \\ 71 & 58 & 92 \end{bmatrix}$$

Selanjutnya hasil yang telah didapatkan disusun kembali sehingga akan terbentuk *frame* yang terenkripsi. Piksel *frame* video yang terenkripsi seperti pada Tabel 2 di bawah ini.

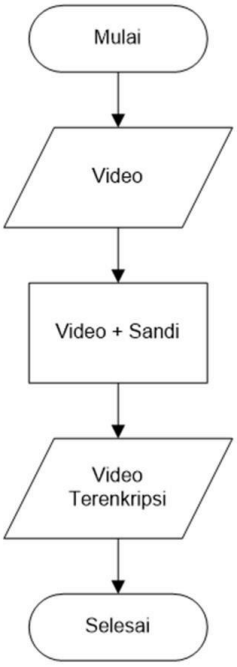
Tabel 2. Nilai Piksel Frame Terenkripsi

Piksel	Nilai 1	Nilai 2	Nilai 3
R	254	100	34
G	33	56	78
B	71	58	92

Sedangkan untuk mendapatkan hasil dekripsi dari video yang dienkripsi dengan melakukan proses yang sama pada saat mengenkripsinya. Perbedaannya adalah matriks kunci harus dibalik terlebih dahulu.

1. Enkripsi

Enkripsi yaitu suatu proses pengacakan sebuah data pada suatu aplikasi dengan menggunakan sandi sehingga informasi tidak bisa dipahami dengan baik[1]. Pada saat melakukan proses enkripsi video akan tetap terlihat namun *frame* yang dihasilkan pada video menjadi terlihat samar atau kurang jelas. Proses enkripsi yang dilakukan pada video menggunakan kunci simetris seperti pada Gambar 1 di berikut ini.

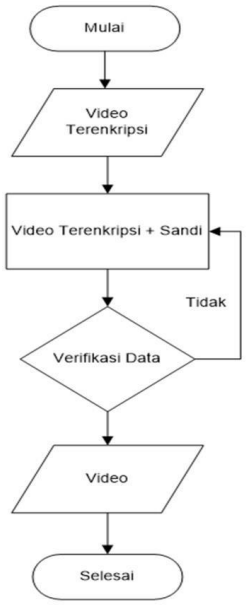


Gambar 1. Flowchart Enkripsi Video

Pada flowchart enkripsi seperti Gambar 1 di atas langkah yang dilakukan pertama menentukan video yang akan dienkripsi, selanjutnya menginputkan sandi atau kunci yang digunakan untuk enkripsi video. Hasil dari proses pengolahan video dengan sandi akan memberikan video terenkripsi.

2. Dekripsi

Dekripsi ialah proses pengembalian ataupun pemulihan suatu data yang sudah dienkripsi pada sesuatu aplikasi[1]. Proses dekripsi video yang dilakukan seperti pada Gambar 2 di bawah ini.

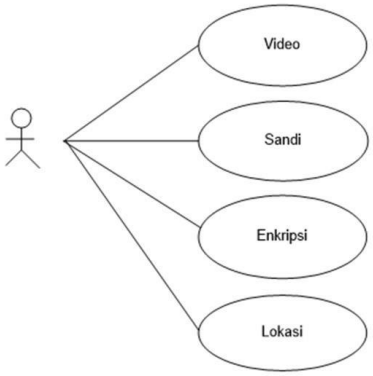


Gambar 2. Flowchart Dekripsi Video

Pada Gambar 2 di atas video yang sudah dienkripsi dimasukkan kembali untuk diproses dengan sandi yang digunakan pada saat melakukan proses enkripsi, jika salah menggunakan sandi atau kunci pada video yang terenkripsi maka informasi belum bisa untuk dimengerti, namun jika kunci yang dimasukkan adalah benar pada saat melakukan proses dekripsi maka informasi pada video terenkripsi kembali untuk dapat dibaca dan dipahami.

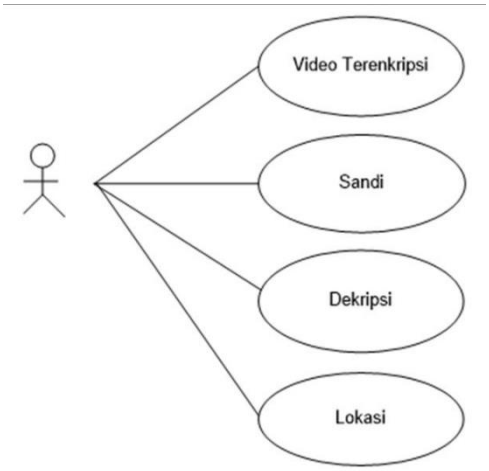
3. Use Case Diagram

Use case diagram mendekripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibangun. *Use case* digunakan untuk mengetahui fungsi yang ada didalam sistem[12]. Berikut adalah *use case* diagram dari sistem yang dirancang seperti yang terlihat pada Gambar 3 berikut ini.



Gambar 3. Use Case Diagram Enkripsi

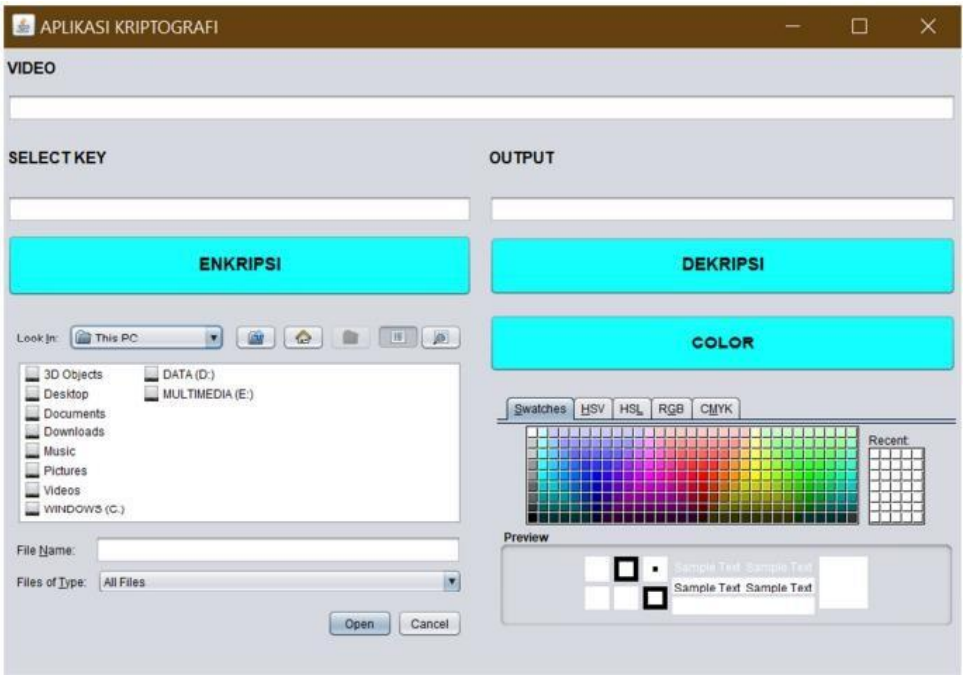
Proses enkripsi pada Gambar 3 di atas pengguna menentukan video yang dienkripsi dan memilih jenis sandi yang akan digunakan, selanjutnya proses enkripsi bisa dijalankan, untuk melihat hasil video terenkripsi dapat dilihat dilokasi penyimpanan. Sedangkan untuk proses dekripsi dapat dilihat pada Gambar 4 berikut ini



Gambar 4. Use Case Diagram Dekripsi

HASIL DAN PEMBAHASAN

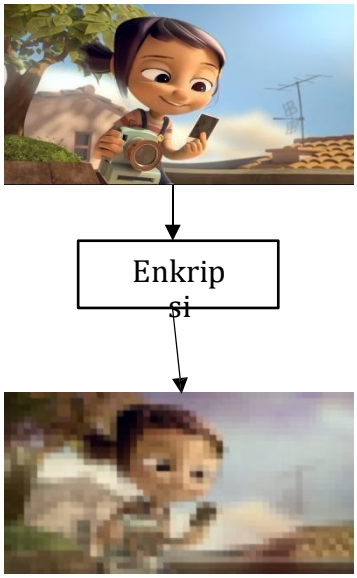
Aplikasi kriptografi dibangun menggunakan bahasa pemrograman java, dan aplikasi ini dapat berjalan disistem operasi windows 10. Hasil dari implementasi yang dilakukan oleh peneliti adalah aplikasi ini dapat membantu menjaga dan mengamankan informasi yang ada didalam video sehingga pihak yang tidak bertanggung jawab tidak bisa memanipulasi data yang ada divideo tersebut. Untuk pertama menjalankan aplikasi ini, pengguna akan memilih jenis video akan diamankan atau dienksripsi. kemudian pengguna akan memilih jenis penguncian dalam bentuk warna, lalu memilih lokasi video setelah dienkripsi. maka, video yang telah selesai dienkripsi akan berada dilokasi yang sudah dipilih sebelumnya. untuk proses dekripsi video, pertama pilih dahulu video yang akan didekripsi, lalu gunakan kunci yang simetris atau yang sama untuk mengembalikan informasi yang ada didalam video yang asli.



Gambar 5. Aplikasi Kriptografi

1. Hasil Enkripsi

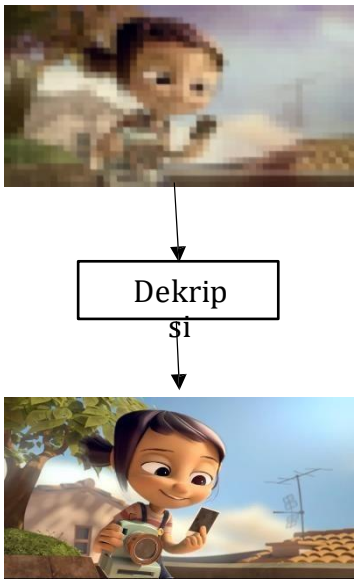
Metode hil chiper digunakan dalam pengimplementasian proses enkripsi, hasilnya adalah video terenkripsi dengan hasil frame yang diacak. Hasil video yang dienkripsi masih dapat dibaca tapi hasil framnya sedikit kabur atau kurang jelas. ini disebabkan karena metode hill chiper hanya merubah nilai RGB pada tiap piksel gambar dan metode ini tidak merubah piksel makanya pola gambar masih terlihat.



Gambar 6. Hasil Enkripsi

2. Hasil Dekripsi

Hasil dari proses dekripsi menjadikan video yang terkunci atau diamankan menjadi dapat dibaca informasinya.



Gambar 7. Dekripsi

3. Waktu proses enkripsi

Pada proses enkripsi, proses untuk menjalankan algoritma ini membutuhkan waktu. untuk melihat perbandingan waktu tersebut, peneliti melakukan percobaan terhadapt 3 video yang berbeda dengan durasi panjang video yang berbeda. hasi; dari percobaan tersebut dapat dilihat dari tabel dibawah ini.

Tabel 3. Waktu proses enkripsi

Nama Video	Durasi panjang video	Waktu enkripsi
Last Shoot.Mp4	00:00:06	01:55:60
Haikyuu.Mp4	00:00:12	05:35:45
Onepiece.Mp4	00:00:15	07:06:05

Melihat pada tabel 3 diatas, dapat kita ambil kesimpulan bahwa waktu proses enkripsi akan semakin lama jika durasi video yang dienkripsi panjang.

4. Waktu proses dekripsi

Pada proses dekripsi sebenarnya memakan waktu yang sama dengan proses enkripsi. untuk melihat waktu yang didapatkan pada proses dekripsibisa dilihat pada tabel berikut ini.

Tabel 4. Waktu proses dekripsi

Nama Video	Durasi panjang video	Waktu enkripsi
Cocomelon.Mp4	00:00:14	02:41:65
Haikyuu.Mp4	00:00:19	08:31:75
Onepiece.Mp4	00:00:24	11:01:69

Berdasarkan tabel diatas, dapat dilihat waktu proses mendekripsikan atau mengembalikan video yang asli jumlah durasi nya berbeda, karena perbedaan panjang durasi.

5. Hasil uji coba blackbox

Pengujian ini dilakukan dengan tujuan agar peneliti mengetahui apakah aplikasi kriptografi yang dirancang dapat berjaland dengan baik sehingga menghasilkan video enkripsi dan dekripsi dengan baik. hasil ujicoba ini dapat dilihat dari tabel dibawah ini.

Tabel 5. Hasil ujicoba blackbox

No	Nama aplikasi kriptografi	Hasil ujicoba	Validasi
1	Memilih jenis video yang akan dienkripsi	Aplikasi menampilkan jenis video untuk yang akan dienkripsi	Sesuai
2	Menentukan jenis kunci yang akan digunakan atau kunci simetris	Aplikasi berhasil membuat video terenkripsi dengan kunci yang digunakan	Sesuai
3		Aplikasi berhasil Menampilkan video	Sesuai

	Mencari video yang terenkripsi untuk didekripsikan.	terenkripsi untuk dikembalikan	
4	Melakukan proses dekripsi menggunakan kunci simetris.	Aplikasi berhasil membuat video terenkripsi menjadi dapat dibaca seperti asli.	Sesuai

Berdasarkan hasil ujicoba diatas bahwasanya aplikasi kriptografi ini dapat beralan dengan baik sehingga dapat memberikan manfaat terhadap video yang mengandung informasi penting didalamnya.

KESIMPULAN

Keamanan data yang dihasilkan dengan memakai aplikasi kriptografi sukses membuat video jadi terenkripsi. Enkripsi video dengan kunci simetris yang dihasilkan membuat frame video jadi kurang jelas ataupun berbeda dengan frame aslinya. Enkripsi yang dihasilkan buat menghalangi hak akses dalam menerima sesuatu data sehingga keamanan bisa terpelihara dengan baik. Mengambalikan data buat bisa dibaca oleh pihak yang mempunyai wewenang dengan mengunakan dekripsi. Proses dekripsi yang dihasilkan oleh aplikasi kriptografi ini membuat pihak yang diijinkan bisa membaca data di informasikan. Enkripsi serta dekripsi yang dicoba pada sistem kriptografi ini memakai tata cara hill cipher, tata cara ini memakai perhitungan matrik. Tata cara hill cipher sukses membuat video terenkripsi serta pula bisa melaksanakan proses dekripsi dengan baik. Waktu yang diperlukan dalam proses enkripsi serta dekripsi didasarkan pada panjang durasi video yang diputar, terus menjadi panjang durasi video yang seleksi hingga proses enkripsi serta pula dekripsi memerlukan waktu yang lebih lama. Kunci simetris yang digunakan pada dikala melaksanakan proses enkripsi serta dekripsi buat wajib senantiasa disembunyikan diakibatkan sebab bila kunci simetris ini bisa dibaca oleh pihak lain hingga kerahasian sesuatu data bisa dibaca dengan gampang. Pengaman video yang diterapkan dengan aplikasi kriptografi ini membuat sesuatu data senantiasa terpelihara kerahasiaannya sehingga pihak yang tidak ijinkan tidak dapat mengakses.

DAFTAR PUSTAKA

[1] Y. Wiharto and A. Irawan, “Enkripsi Data Menggunakan Advanced Encryption Standart 256,” Kilat, Vol. 7, No. 2, pp. 91–99, 2018, doi: 10.33322/kilat.v7i2.352.

[2] D. I. Mulyana, A. P. Heryani, and V. Khoirunnisa, “Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text,” Vol. 03, No. 01, pp. 32–39, 2022.

[3] A. Malvi, “Pengamanan File Gambar pada Media Video dengan Kriptografi Algoritma RSA dan Steganografi Algoritma End of File (EOF),” Vol. 4221, pp. 67–74, 2020.

[4] A. Des, “Implementasi Kriptografi untuk Keamanan Data dan Jaringan Menggunakan Algoritma DES,” Vol. 5, No. 1, pp. 31–38, 2021.

[5] F. Rizky, “Implementasi Kriptografi Dengan Metode Advanced Encryption Standard (AES) Untuk Realtime Chat Berbasis Mobile pada E-Learning Politeknik Negeri Lhokseumawe,” pp. 1–8, 2019.

[6] R. T. Tarigan, “Pengamanan Pesan Rahasia Menggunakan Metode Algoritma Hill Cipehr,” Publ. Ilm. Teknol. …, Vol. 3, No. November, pp. 161–165, 2018, [Online]. Available: http://jurnalnya.stmikneumann.ac.id/index.php/pitin/article/download/61/62.

[7] E. R. Febrianto and E. A. Sarwoko, "Kriptografi Citra Digital Menggunakan Algoritma Hill Cipher dan Affine Cipher Berbasis Android," J. Masy. Inform., Vol. 10, No. 2, pp. 11–21, 2018, [Online]. Available: http://eprints.undip.ac.id/80038/.
[8] K. A. Seputra, G. Arna, and J. Saskara, "Kriptografi Simetris Rc4 pada Transaksi," Kriptografi Simetris Rc4 pada Transaksi Online Book. Engine Syst., Vol. 17, No. 2, pp. 286–295, 2020.
[9] Y. W. Hasibuan, R. B. Veronica, J. Matematika, U. N. Semarang, K. S. Gunungpati, and I. Artikel, "Perancangan dan Implementasi Aplikasi Kriptografi Algoritma Hill Cipher Dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode ASCII," Vol. 11, No. 1, pp. 54–68, 2022.
[10] A. Sujjada and E. Juniar, "Implementasi Algoritma Hill Cipher Untuk Proses Enkripsi Data Menggunakan Media," Vol. 3, No. 1, pp. 1–17, 2021.
[11] "Penggunaan Metode Hill Cipher Untuk Kriptografi pada Citra Digital. Muhammad Rizal 1), Afdal 2) - PDF Free Download.pdf.".
[12] M. A. Nasuton et al., "Penerapan Metode Hill Cipher dan Stream Cipher Dalam Mengamankan Database MySQL," pp. 532–544, 2020.