HASIL CEK_Imam Riadi , Sunardi, Dwi Aryanto

by Imam Riadi , Sunardi, Dwi Aryanto Eof, Pnsr, Steganografi.

Submission date: 15-Aug-2022 09:42AM (UTC+0700)
Submission ID: 1882571339
File name: Algoritma_End_of_File_dan_Rijndael_pada_Steganografi_Video.pdf (830.18K)
Word count: 2261
Character count: 13366

Jurnal Riset Sains dan Teknologi
Volume 5 No. 1 Maret 2021, 17 - 22
e-ISSN: 2549-9750
p-ISSN: 2579-9118

Algoritma *End of File* dan Rijndael pada Steganografi Video

End of File and Rijndael Algorithms on Video Steganography

Imam Riadi[1*], Sunardi[2], Dwi Aryanto[3]
[1]Program Studi Sistem Informasi, [2]Program Studi Teknik Elektro, [3]Program Studi Magister Teknik Informatika
Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[*1]imam.riadi@is.uad.ac.id, [2]sunardi@mti.uad.ac.id, [3]dwi1607048017@webmail.uad.ac.id

DOI; 10.30595/jrst.v5i1.9187

Histori Artikel:

Diajukan: 06/12/2020

Diterima: 13/03/2021

Diterbitkan: 25/03/2021

ABSTRAK

Teknik penyembunyian pesan dalam media digital dikenal dengan istilah steganografi. Penelitian dirancang untuk membuat sistem steganografi video, pesan yang disisipkan berupa teks terlebih dahulu dienkripsi dengan algoritma *Rijndael*. Metode untuk penyisipan pesan pada frame video adalah metode *End of File (EoF)*. Ekstraksi frame pada video menggunakan ffmpeg. Pengujian kualitatif dilakukan untuk melihat perubahan frame video dengan indera manusia. Pengujian kuantitatif dilakukan pada enam video dengan resolusi yang berbeda, disisipi pesan dengan ukuran Byte yang bervariasi. Frame yang telah disisipi pesan diukur noise-nya dengan *Peak Signal to Noise Rasio (PNSR).* Keunggulan dari metode EoF adalah frame video dapat menampung byte pesan yang tidak terbatas. Frame video setelah disisipi pesan dengan berbagai macam ukuran pesan tidak terjadi noise hal terlihat dari MSE bernilai 0 dan PNSR bernilai infinity.

Kata Kunci: *EoF, PNSR, Steganografi*.

ABSTRACT

The technique of hiding messages in digital media is known as steganography. This research is designed to create a video steganography system, the message that is inserted in the form of text is encrypted first with the Rijndael algorithm. The method for inserting messages in video frames is the End of File (EoF) method. Extraction of frames on video using ffmpeg. Qualitative testing is done to see changes in video frames with human senses. Quantitative testing was conducted on six videos with different resolutions, inserted messages with varying Byte sizes. The frame that has been inserted with a message is measured for noise with the Peak Signal to Noise Ratio (PNSR). The advantage of the EoF method is that the video frame can accommodate unlimited message bytes. After inserting a video frame with various message sizes, there is no noise. It can be seen that MSE is 0 and PNSR is infinity.

Keywords: EoF, PNSR, Steganography.

1. PENDAHULUAN

Informasi merupakan sesuatu yang sangat berharga yang perlu dijaga kerahasiaanya. Berbagai cara digunakan untuk merahasiakan informasi. Sebagai contoh Julius Caesar telah menggunakan metode pengacakan pesan

sebelum dikirim ke penerima, agar orang yang tidak berhak menerima pesan tidak dapat membacanya. Teknik penyandian ini dikenal dengan istilah kriptografi (Rafiudin, 2002).

Steganografi berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein artinya menulis. Steganografi adalah seni dan ilmu untuk berkomunikasi dengan cara menyembunyikan informasi sehingga informasi tidak dapat terdeteksi oleh pihak lain (Cachin C., 2005).

Penggabungan Steganografi dan kriptografi digunakan untuk meningkatkan keamanan dan kerahasian sebuah informasi. Perbedaan utama dari keduanya adalah pada steganografi pesan disembunyikan dalam media digital sedangkan pada kriptografi, pesan diacak agar orang lain tidak bisa membacanya. Steganografi dapat dibedakan berdasarkan tujuannya menjadi dua yaitu data hiding atau data embedding dan document marking. Data hiding adalah menyembunyikan informasi rahasia di dalam media digital, sedangkan document marking adalah pemberian tanda untuk media digital. Document marking terbagi menjadi dua, yaitu watermarking dan fingerprinting, keduanya berfungsi untuk menyembunyikan identifikasi yang unik sebagai suatu watermark pada data untuk mengidentikasi copy legal dari suatu dokumen(Cummins, et. al., 2004).

Algoritma Rijndael merupakan algoritma yang dibuat oleh Dr. Vincent Rijmen dan Dr. Joan Daemen pada tahun 2000 secara resmi dipilih oleh NIST (National institude of Standard and Technology) sebagai Advanced Encryption Standard (AES) mengalahkan beberapa algoritma lainnya. Hal ini karena Rijndael merupakan algoritma yang memiliki keseimbangan antara keamanan dan fleksebilitas dalam berbagai platform software dan hardware. (Wasino, at. al., 2012). Kombinasi steganografi metode Least Significant Bit (LSB) dan metode kriptografi Rijndael. Hasil pengujian menunjukkan bahwa metode LSB tidak bisa digunakan untuk penyisipan pesan yang ukuran Byte-nya lebih besar dari daya tampung frame video cover (Riadi et. al, 2020).

Penelitian tentang steganografi pada media digital dengan berbagai macam algoritma telah banyak dilakukan. Masing-masing Algoritma mempunyai kelebihan dan kekurangan masing-masing. Algoritma yang dipakai adalah End Of File(EoF), Least Significant Bit (LSB), Hashed Based LSB (HLSB), Discrete Cosine Transform (DCT), dan Modified Least Significant Bit (MLSB) (Hilal Almara'beh, 2016; Kurniawan dan Narupi, 2016; Irawan, 2013).

Penelitian steganografi pada video FLV dengan algoritma EoF untuk menyembunyikan pesan, file pesan yang disembunyikan dikompresi dengan kompresi Huffman. Tingkat keberhasilan metode kompresi Huffman mencapai 80%. Metode steganografi Injected at End of All Video Tag yang digunakan berhasil, sehingga tidak ada distorsi yang terlihat pada kualitas video dan audio dari pada video yang disisipi pesan (Arraziqi dan Ferdinandus, 2015).

Penelitian yang sama dengan algoritma EoF pada video berekstensi FLV. Hasil pada penelitian ini tidak terjadi distorsi pada video, akan tetapi terjadi peningkatan yang signifikan ukuran file video. Peningkatan ukuran file tergantung pada besarnya panjang pesan yang disisipkan (Cruz, at. al., 2012).

Steganografi menggunakan metode LSB berbasis Hash digunakan unuk penyisipan pesan. Pesan terlebih dahulu dienkripsi dengan RSA dan SHA-1 untuk menciptakan kunci hash yang aman. Metode Hash LSB berhasil menciptakan gambar hasil steganograi tidak mengalami distorsi(Meerunnisa et. al., 2015).

Penggabungan dua teknik motion detection dan LSB dirancang untuk mendeteksi gerak dan bit paling rendah. Motion detection digunakan untuk mengekstrak frame dari video. Bit yang paling rendah digunakan untuk menempatkan objek menggunakan algoritma LSB (Singh and Kaur 2015).

Stenanografi dengan metode End of File digunakan untuk penyisipan pesan ke dalam citra. Citra yang disisipi pesan disimpan dalam bentuk format BMP, JPEG, PNG dan TIFF. Hasil desteganografi menunjukkan bahwa ketika pengungkapan pesan dilakukan tanpa adanya manipulasi citra, tingkat keberhasilan mencapai 75% (Jannah et. al., 2018).

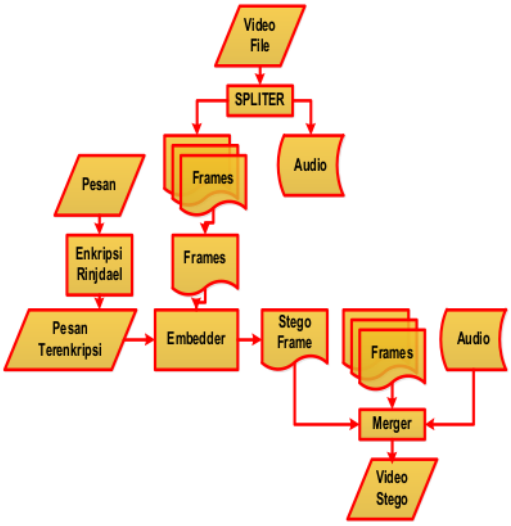
Penelitian ini bertujuan menerapkan Algoritma Rindjael untuk pengacakan pesan yang akan disisipkan pada salah satu frame video dengan format MP4 menggunakan algoritma End of File (EoF). Pengujian akan dilakukan secara kualitatif mengamati perubahan histogram frame video dan pengujian kuantitatif melihat nilai MSE dan PNSR .

2. METODE PENELITIAN

Perancangan sistem digunakan untuk membantu proses pengkodean. Perancangan sistem dalam penelitian ini terdiri dari perancangan proses penyisipan pesan pada video dan proses ekstraksi pesan dari video. Langkah–langkah yang dilakukan pada proses penyisipan pesan pada video adalah sebagai berikut:

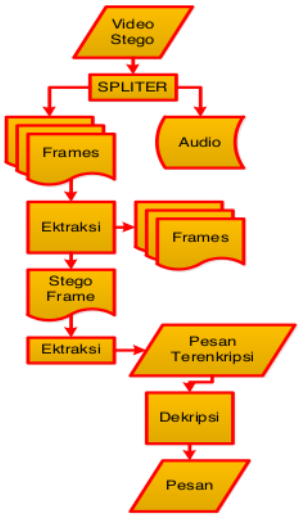
1. Menentukan *cover* video.
2. Memisahkan antara tag frame (video) dan tag audio.
3. Menentukan pesan yang akan diembedkan.
4. Menggabungkan kembali frame yang disisipi pesan, frames video, dan audio menjadi video yang tersisipi pesan.

Gambar 1 merupakan *flowchart* dan sistem yang dibuat pada proses penyisipan pesan.



Gambar 1. Rancangan proses penyisipan pesan pada video

Rancangan proses pengambilan pesan dari video stego dapat dilihat pada Gambar 2.



Gambar 2. Rancangan proses pengambilan pesan dari video stego

Penjelasan *flowchart* pada Gambar 2 adalah sebagai berikut:

1. Mengambil video stego.
2. Memisahkan antara tag frame (video) dan tag audio.
3. Ektrasi frame(s) video untuk memisahkan frame stego dan frame non stego
4. Frame stego di ekstraksi lagi untuk mendapatkan pesan ter-enkripsi.
5. Dekripsi dari pesan ter-enkripsi.

3. HASIL DAN PEMBAHASAN

Hasil dari rancangan sistem diimplementasikan menggunakan bahasa pemrograman *Microsoft Visual Basic 2010. Cover* dalam penelitian ini adalah video dengan format mp4, sedangkan pesan yang disisipkan berupa teks. Proses ekstraksi frame dan audio menggunakan ffmpeg.

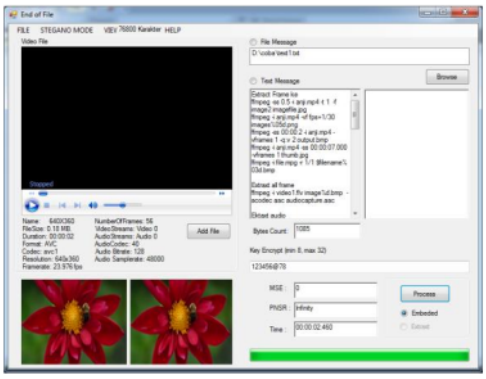
Proses ekstraksi frame dari video dilakukan dengan mengekstrak semua frame yang ada di video dalam format BMP. Informasi jumlah frame dalam video menghasilkan jumlah yang sama ketika video diekstrak menjadi frame. Frame dan audio hasil ekstraksi disimpan dalam

Setelah audio dan semua frame dalam video terekstrak, diambil salah satu frame yang akan disisipi pesan, frame yang disisipi adalah frame ke-10.

Pesan yang disisipkan adalah pesan teks dengan format txt atau pesan yang langsung ditulis, sekaligus memasukkan kunci enkripsi.

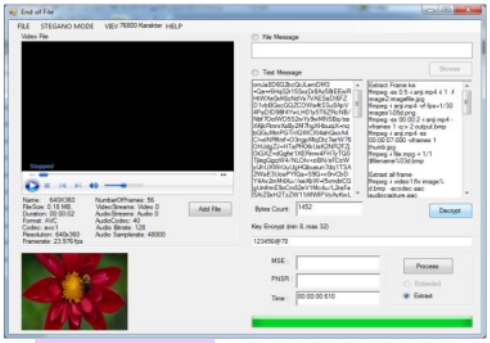
Proses selanjutnya adalah menyatukan kembali audio dan frame menjadi video.

Penyisipan pesan dengan Algoritma *EoF* dilakukan secara langsung pada *Byte* akhir file frame video. Pesan yang disisipkan pada akhir *file* akan memiliki tanda khusus sebagai pengenal awal dan akhir dari *Byte* pesan yang disisipkan pada frame video. Penanda awal pesan berupa karakter *ASCII* yang dialokasi berukuran maksimum 10 *Byte*. Selanjutnya ukuran pesan dialokasikan sebesar 4 *Byte*. Penanda pesan dan ukuran pesan disisipkan pada akhir pesan frame video, penanda pesan dan ukuran pesan disebut sebagai *header* pesan. Pada algoritma *EoF, header* pesan disisipkan di akhir *Byte* pesan. Proses penyisipan pesan dapat dilihat pada Gambar 3.



Gambar 3. Proses penyisipan pesan pada video

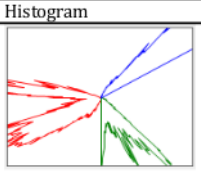
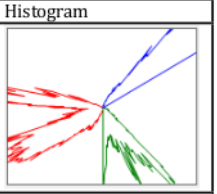
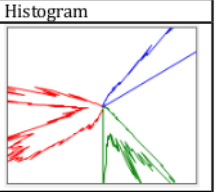
Ekstraksi pesan pada Algoritma EoF bertujuan untuk mengambil *Byte* pesan pada frame video *stego*. Proses ekstraksi pada Algoritma EoF dilakukan dengan tahapan mengekstraksi *header* pesan, karena *header* pesan sebagai penanda awal dan akhir dari pesan yang ada pada frame video *stego. Header* pesan terletak pada akhir frame video *stego,* dengan demikian proses ekstraksi dimulai dari *Byte* yang paling akhir. Proses pengambilan pesan dapat dilihat pada Gambar 4.

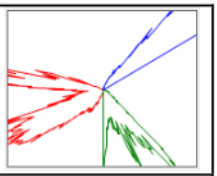
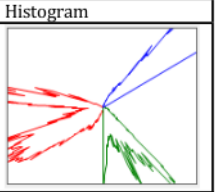


Gambar 4. Proses pengambilan pesan dari video.

Pengujian dilakukan untuk mengukur kinerja algoritma yang telah diimplementasikan. Pengujian dilakukan dengan dua cara, yaitu kualitatif dan kuantitatif. Pengujian kualitatif bertujuan untuk mengamati perubahan kualitas frame video *stego* dari bentuk citra asli berdasarkan pengamatan menggunakan visual manusia. Pengamatan bersifat subyektif untuk mendeteksi perubahan kualitas citra dan histogram citra yang terjadi pada frame video *stego*. Hasil dari Pengujian kualitatif dapat dilihat pada Tabel 1.

Tabel 1. Hasil pengujian kualitatif dengan berbagai macam panjang pesan pada video resolusi 640x360

No	Citra Asli	Histogram
1		
	Byte Pesan 1085	Histogram
2		
	Byte Pesan 4836	Histogram
3		
	Byte Pesan 8718	Histogram

4		
	Byte Pesan 34195	Histogram
5		

Pengujian kuantitatif dilakukan pada enam video dengan resolusi yang berbeda, disisipi lima buah pesan dengan panjang Byte yang bervariasi. Dari nilai MSE dan PNSR menunjukkan bahwa tidak terjadi perubahan pada kualitas citra pada frame yang disisipi pesan. Hasil pengujian kuantitatif ditunjukkan pada Tabel 2.

Tabel 2. Hasil pengujian penyisipan pesan pada video

No	Resolusi Video	Panjang Pesan(Byte)	MSE	PNSR
		1085	0	Infinity
		4836	0	Infinity
1	360 x 240	8718	0	Infinity
		34195	0	Infinity
		49879	0	Infinity
		1085	0	Infinity
		4836	0	Infinity
2	420 x 240	8718	0	Infinity
		34195	0	Infinity
		49879	0	Infinity
		1085	0	Infinity
		4836	0	Infinity
3	640 x 360	8718	0	Infinity
		34195	0	Infinity
		49879	0	Infinity
		1085	0	Infinity
		4836	0	Infinity
4	854 x 480	8718	0	Infinity
		34195	0	Infinity
		49879	0	Infinity
		1085	0	Infinity
		4836	0	Infinity
5	1280 x 720	8718	0	Infinity
		34195	0	Infinity
		49879	0	Infinity
		1085	0	Infinity
		4836	0	Infinity
6	1920 x 1080	8718	0	Infinity
		34195	0	Infinity
		49879	0	Infinity

4. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut: Frame video *cover* dapat menampung Byte pesan yang tidak terbatas. Frame video yang disisipi pesan tidak terjadi perubahan kualitas warna. Histogram frame video yang disisipi pesan tidak mengalami perubahan. Frame video setelah disisipi pesan dengan berbagai macam ukuran pesan tidak ada noise, hal ini dapat dilihat dari nilai MSE bernilai 0 dan PNSR yang bernilai infinity.

DAFTAR PUSTAKA

Cachin C., 2005. A Survey Prepared for the Encyclopedia of Cryptography and Security, *Digital Steganography,* IBM Research Zurich Research Laboratory, Switzerland.

Cruz, P., J., Libatique, J. dan N., Tangonan, G., 2012. Steganography and Data Hiding in Flash Video (FLV), Ateneo de Manila University, Quezon City, Philippines.

Cummins, J., Diskin, P., Lau, S., dan Parlett, R., 2004. *Steganography and Digital Watermakring*. Edgbaston: GNU Free Documentation.

D. E. Kurniawan and Narupi, 2016. "Teknik Penyembunyian Data Menggunakan Kombinasi Kriptografi Rijndael dan Steganografi Least Significant Bit (LSB)," J. Tek. Inform. dan Sist. Inf., vol. 2, no. 3, pp. 254–262.

Dwi Arraziqi dan F. X. Ferdinandus, 2015. Optimalisasi Steganografi pada File FLV Memanfaatkan Metode Injected at End of All Video Tag dengan Penambahan Kompresi, Seminar Nasional Inovasi dalam Desain dan Teknologi (IdeaTech).

Hilal Almara'beh, 2016. Steganographic Techniques Data Security Using Audio and Video, *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 6, Issue 2.

Imam Riadi, Sunardi dan Dwi Aryanto, 2020, Steganografi Video Digital dengan Algoritma LSB (*Least Significant Bit*) dan Rijndael, JINITA, Vol. 2, No. 2.

Lulu Maftukhatul Jannah, Imam Santoso, dan Yuli Cristyono, 2018. Kinerja Steganografi Metode End Of File Pada Data Citra Digital. TRANSIENT, VOL. 7, NO. 1.

Parwinder Singh and Navpreet Kaur, 2015. Hybridization of Motion Detection Technique in Video Steganography, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 5, Issue 7.

Rafiudin, 2002. *Security Unix.* PT Elex Media Komputindo, Jakarta.

Wasino, Rahayu, P. T. dan Setiawan, 2012. Implementasi Steganografi Teknik End of File dengan Enkripsi Rijndael, *Seminar Nasional Teknologi Informasi dan Komunikasi* (SENTIKA) Yogyakarta.

M. Irawan, 2013, Penggunaan Steganografi dengan Metode End of File (EOF) pada Digital Watermarking, vol. 2, no. 1, pp. 36–42

.

HASIL CEK_Imam Riadi , Sunardi, Dwi Aryanto

ORIGINALITY REPORT

6%	3%	3%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Tsani Elvia Nita, Lisna Zahrotun. "Penerapan Metode Single Linkage dengan Manhattan Distance Similarity dalam Mengelompokkan Trens Topik Kerja Praktik", JRST (Jurnal Riset Sains dan Teknologi), 2021 Publication	3%
2	id.123dok.com Internet Source	2%
3	doku.pub Internet Source	2%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		