STEGANOGRAFI VIDEO DIGITAL DENGAN ALGORITMA MODIFIKASI END OF FILE DAN RC4

Dwi Aryanto[1], Imam Riadi[2], Sunardi[3]

Magister Teknologi Informasi Universitas Ahmad Dahlan, Yogyakarta, Indonesia
dwi1607048017@webmail.uad.ac.id

ABSTRAK

Teknik penyembunyian pesan dalam media digital atau lebih sering dikenal dengan istilah steganografi sebagai pengembangan dari kriptografi. Steganografi merupakan ilmu dan seni untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui oleh orang lain, kecuali pengirim dan penerima. Steganografi lebih aman karena sifatnya yang tidak mengacak file yang disisipi, sehinga tidak mencurigakan. Banyak metode yang dapat digunakan untuk penyisipan pesan kedalam media digital. Penelitian ini membandingkan metode End of File (EoF), Modification End of File (MEoF) dan Modification Least Significant Bit (MLSB). Media digital yang digunakan dalam penelitian ini adalah video berekstensi FLV. Pesan yang disisipkan ke dalam video terlebih dahulu di enkripsi menggunakan metode RC4. Proses analisis hasil video stego terhadap video asli dilakukan dengan cara membandingkan hasil pengujian kualitatif dan kuantitatif. Pengujian kualitatif dilakukan dengan cara subyektif untuk melihat perubahan kualitas video stego, sedangkan kuantitatif secara obyektif untuk melihat perubahan kualitas video stego berdasarkan noise yang dihasilkan. Noise diperoleh dari kalkulasi nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Selain itu untuk pengujian kuantitatif juga dilakukan perbandingan untuk panjang pesan yang dapat disisipkan pada video dan perubahan ukuran file video stego dari video asli dari masing – masing algoritma. Hasil yang diharapkan dari penelitian ini adalah untuk membuktikan apakah algoritma MEof lebih baik dari metode EoF dan MLSB untuk steganografi video berekstensi FLV.

Kata Kunci: End of File (EoF), Modification End Of File (MEoF), Modification Least Significant Bit(MLSB), Steganografi.

I. PENDAHULUAN

Informasi merupakan sesuatu yang sangat berharga, pentingnya kerahasiaan suatu informasi telah menjadi suatu perhatian tersendiri. Berbagai cara digunakan untuk merahasiakan sebuah informasi, karena informasi yang jatuh ke orang yang tidak berhak akan menimbulkan kerugian. Zaman sekarang informasi tidak hanya dapat disandikan, tetapi dapat juga disisipkan kedalam media digital. Teknik menyisipkan pesan dikenal dengan nama steganografi. Rafiudin (2002) memaparkan kriptografi dapat diartikan sebagai ilmu dan seni penulisan rahasia terhadap informasi-informasi. Kriptografi disebut ilmu *(science)* karena menggunakan matematika aljabar dan disebut seni *(art)* karena dalam aplikasinya memiliki pola - pola tertentu dalam proses penyandian yang unik. Hingga era digital saat ini, kriptografi sangat dibutuhkan dan merupakan bagian penting dari sistem komunikasi modern.

Atoum dan Ibrahim (2012) memaparkan steganografi sebagai ilmu dan seni untuk menyembunyikan informasi sehingga informasi yang bersifat rahasia tidak dapat diketahui oleh orang lain, kecuali pengirim dan penerima. Proses steganografi biasanya melibatkan penyandian atau kriptografi. Proses yang dilakukan yaitu dengan enkripsi *plaintext* terlebih dahulu menjadi *Byte cipher* atau pesan rahasia. Kemudian *Byte cipher* disisipkan pada media digital berupa teks, audio, citra atau protokol.

Menurut Ariyus (2008). RC4 merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi. Algoritma kriptografi *Rivest Code* 4 (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh RSA Data Security Inc *(RSADSI)* yang berbentuk *stream chipper*. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu : Rivest, Shamir, dan Adleman).

RC4 digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman, karena RC4 termasuk dalam algoritma simetris maka kerahasiaan kunci harus dijaga dan dikirim di saluran komunikasi yang aman. Sampai saat ini diketahui tidak ada yang dapat memecahkan atau membongkarnya, hanya saja versi ekspor 40 *bit*nya dapat dibongkar dengn cara *brute force* (mencoba semua kunci yang mungkin). RC4 akan digunakan untuk enkripsi pesan yang akan disisipkan ke dalam file video.

Sebelumnya Wasino *et al.* (2012) dan Cruz *et. al.* (2012) juga melakukan penelitian tentang steganografi dengan algoritma *EoF,* tetapi memanfaatkan media digital video yang berekstensi *FLV* sebagai

penampung pesan. Hasil dari penelitian menunjukkan bahwa *file stego* dijalankan kembali akan tetap mempertahankan kualitas audio dan video seperti awal tanpa ada distorsi, tetapi secara signifikan akan meningkatkan ukuran *file stego,* peningkatan ukuran *file* tergantung pada besarnya panjang pesan yang disisipkan.

II. LANDASAN TEORI

Steganografi berasal dari bahasa Yunani yaitu *steganos,* yang artinya "tersembunyi atau terselubung" dan *graphein* artinya "menulis". Steganografi didefinisikan oleh (Cachin, 2005) adalah seni dan ilmu untuk berkomunikasi dengan cara menyembunyikan informasi sehingga informasi tidak dapat terdeteksi oleh pihak lain (indra manusia). Teknik steganografi telah digunakan selama ratusan tahun. Dengan meningkatnya penggunaan *file* dalam format elektronik, maka teknik baru untuk menyembunyikan informasi menjadi sesuatu yang mungkin untuk dilakukan.

Steganografi dan kriptografi keduanya digunakan untuk menjamin kerahasian data. Tetapi perbedaan utama dari keduanya adalah dengan kriptografi, komunikasi kedua belah pihak yang bersifat rahasia lebih rentan dapat diketahui oleh setiap orang, sedangkan dengan steganografi pesan disembunyikan keberadaannya dalam media digital sehingga pesan menjadi lebih terlindungi, dalam steganografi kasus yang terbaik adalah tidak ada yang bisa melihat bahwa telah terjadi komunikasi antara kedua pihak tanpa ada yang bisa melihat (Cummins *et al.* 2004).

RC4 adalah cipher aliran yang digunakan secara luas pada sistem keamanan seperti protokol SSL (secure Socket Layer). Algoritma kriptografi ini sederhana dan mudah diimplementasikan. RC4 dibuat oleh Ron Rivers dari Laboratorium RSA (RC adalah singkatan dari Ron's Code). RC4 membangkitkan aliran kunci (keystream) yang kemudian di-XOR-kan dengan plaintext pada waktu enkripsi (atau di-XOR-kan dengan bit -bit ciphertext pada waktu dekripsi). RC4 tidak seperti cipher aliran yang memproses data dalam bit, RC4 memproses data dalam ukuran byte (1 byte = 8 bit). RC4 menggunakan dua buah kotak substitusi (S-box) array 256 byte yang berisi permutasi dari bilangan 0 sampai 255 dan S-box kedua yang berisi permutasi fungsi dari kunci sepanjang variable (Emy Setyaningsih, 2013).

Format file FLV terdiri dari header pendek, diikuti oleh metadata, dan kemudian bergantian tag audio dan video atau packet. Header FLV terdiri dari nilai hex tiga yang pertama dari "46 4c 56" yang diterjemahkan menjadi "FLV" dalam nilai string heksadesimal, yang diikuti oleh version, flags, dan offset. Setelah nilai-nilai ini adalah urutan dari tag sampai akhir dari file (EOF). Jenis tag terdiri dari 0x08 untuk AUDIO, 0x09 untuk VIDEO, dan 0x12 untuk META. Setiap tag berisi type, body length, timestamp, timestamp extended, stream id, dan body (data aktual). Setelah setiap tag adalah previous tag size, yang harus selalu sama dengan size dari data aktual dalam byte ditambah 11 byte yang sesuai dengan type tag (1 byte), size body (3 byte), time stamp (3 byte), timestamp extended (1 byte), dan nilai stream id (3 byte) dari tag (Arraziqi dan Ferdinandus , 2015).

End of File adalah salah satu algoritma yang dapat digunakan dalam steganografi, algoritma ini melakukan penyisipan pesan dengan teknik pesan akan disisipkan pada akhir *file* media penampung. Dengan algoritma ini pesan dapat disisipkan sesuai dengan kebutuhan. Cruz *et al.* (2012) mengatakan algoritma *EoF* dikenal sebagai algoritma injeksi, teknik ini secara langsung menambahkan pesan pada akhir *file.* Keberhasilan algoritma injeksi menyisipkan pesan pada media penampung akan mempertahankan kualiatas media penampung. Tetapi algoritma ini secara signifikan akan mempengaruhi ukuran *file stego,* besarnya ukuran tergantung pada banyak pesan yang disisipkan pada media penampung.

Teknik penyisipan pesan dengan memanfaatkan *padding* selanjutnya disebut algoritma *MEoF* (Modifikasi *End of File).* Modifikasi yang dilakukan dari algoritma *EoF (End of File)* yaitu lokasi penyisipan pesan. *Padding* pada citra bitmap 24 bit adalah jika ukuran *width modulo* 4 ^ 0. Untuk citra bitmap dengan kondisi ukuran *width modulo* 4 = 0, penyisipan pesan dilakukan pada piksel terakhir citra, prosesnya dilakukan dengan cara nilai *Byte* citra piksel terakhir digantikan dengan *Byte* pesan. *Byte* yang mewakili piksel citra bitmap ditampilkan dalam bentuk baris, masing - masing baris merupakan kelipatan 4 *Byte* termasuk *padding (*Tarigan, 2015)

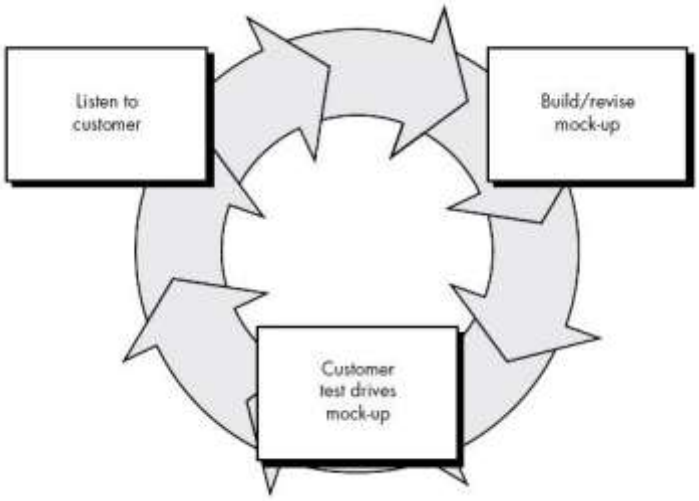
Johnson dan Jajodia (1998) dalam tulisan Cruz *et al.* (2012) mengatakan metode *Least Significant Bit (LSB)* adalah teknik penyembunyian pesan dengan cara menyisipkan pesan pada bit rendah atau bit paling kanan pada *file* media penampung sebagai media untuk menyembunyikan pesan. *Least Significant Bit* adalah barisan data biner yang ada pada media digital dan paling tidak terlalu berpengaruh terhadap perubahan jika nilai datanya dimodifikasi. Modifikasi yang dilakukan pada *Least Significant Bit (LSB)* yaitu, bit - bit pesan disisipkan pada *String* biner data citra yang memiliki nilai *Byte* 254 atau 255. Penyisipan bit - bit pesan pada citra menggunakan algoritma *MLSB* membutuhkan masukkan data antara lain *file* citra sebagai media untuk penyisipan pesan, *plaintext* karakter *ASCII* dan kunci sebagai kunci untuk enkripsi *plaintext* menjadi *Byte cipher.*

Menurut Moreno *et al.* (2013), *Peak Signal to Noise Ratio (PSNR)* adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. *PSNR*

biasanya diukur dalam satuan desibel (dB). *PSNR* digunakan untuk mengetahui perbandingan kualitas citra sebelum dan sesudah disisipkan pesan. *Mean Square Error (MSE)* merupakan parameter yang menunjukkan tingkat kesalahan piksel - piksel citra hasil pemrosesan sinyal *(stego image)* terhadap citra asli *(media cover).* Semakin kecil nilai *MSE* yang didapatkan maka kualitas citra keluaran akan semakin baik atau dapat dikatakan semakin mendekati citra aslinya.

III. METODE PENELITIAN

Metode yang dipakai dalam penelitian ini adalah *prototype* model. Bagan mengenai *prototype* model dapat dilihat pada Gambar 1.



Gambar 1. Prototype Model

Tahap-tahap dalam *prototype* model menurut Lukman (2016) adalah sebagai berikut :

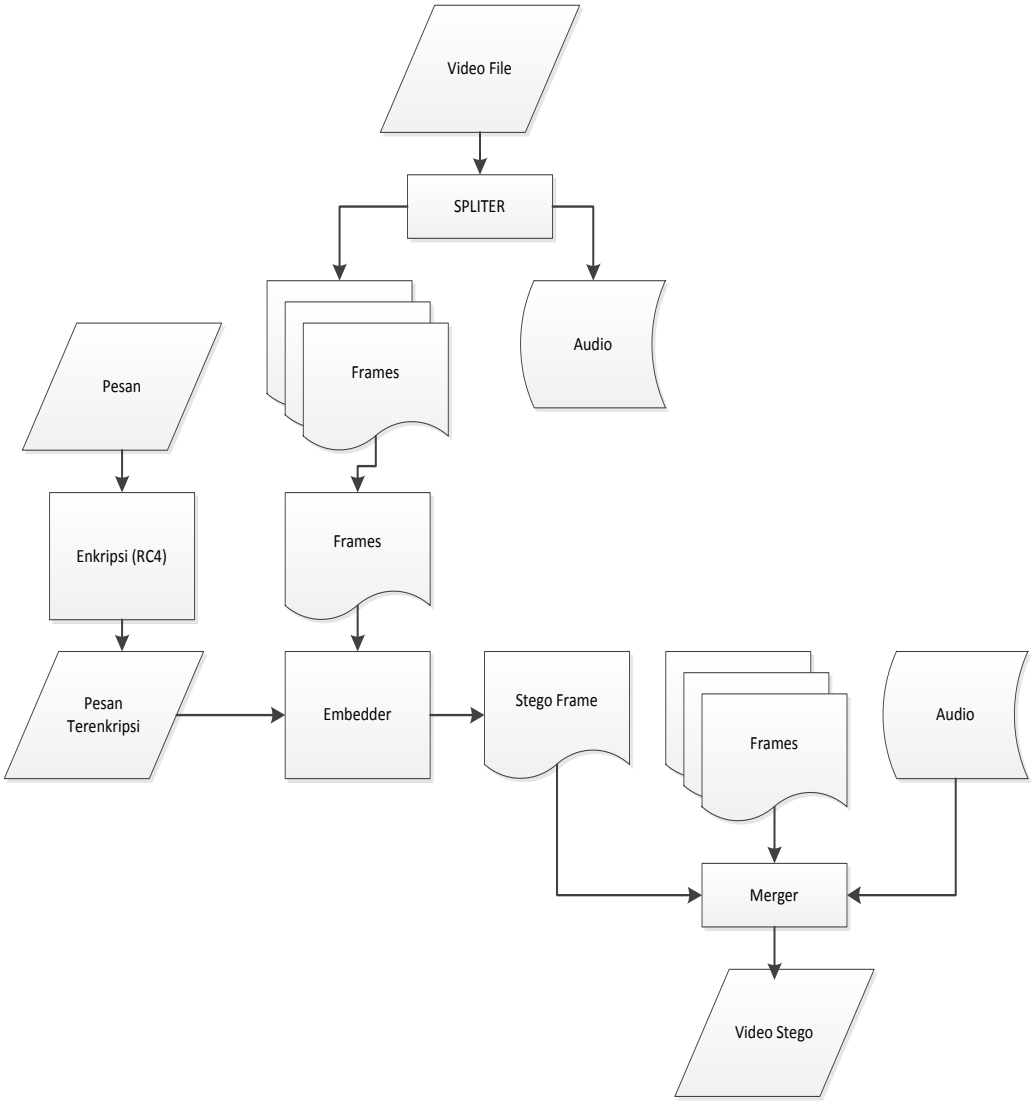
1) *Listen to Customer* : Pada tahap ini dilakukan analisis terhadap permasalahan yang ada, yaitu mendapatkan data dan literatur yang terkait dengan proses *embedding*, ekstraksi, enkripsi dan dekripsi data teks pada video.
2) *Buid/revise mock-up* : Membuat perancangan menggunakan *Unifield Modeling Language* (UML) mengenai system yang akan dibangun nantinya. Selain itu dilakukan pula perancangan *user interface* dan algoritma.
3) *Customer test drives mock-up* : Pada tahap ini dilakukan pengujian sistem yaitu menjalankan proses implementasi sistem dan melakukan analisa kualitatif dan kuantitatif terhadap video setego

A. Perancangan Sistem Proses Steganografi video

Langkah- langkah rancangan sistem steganografi 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 non stego frame, stego frame(s) dan audio menjadi stego video.

Rancangan proses steganografi video dapat dilihat pada Gambar 2.



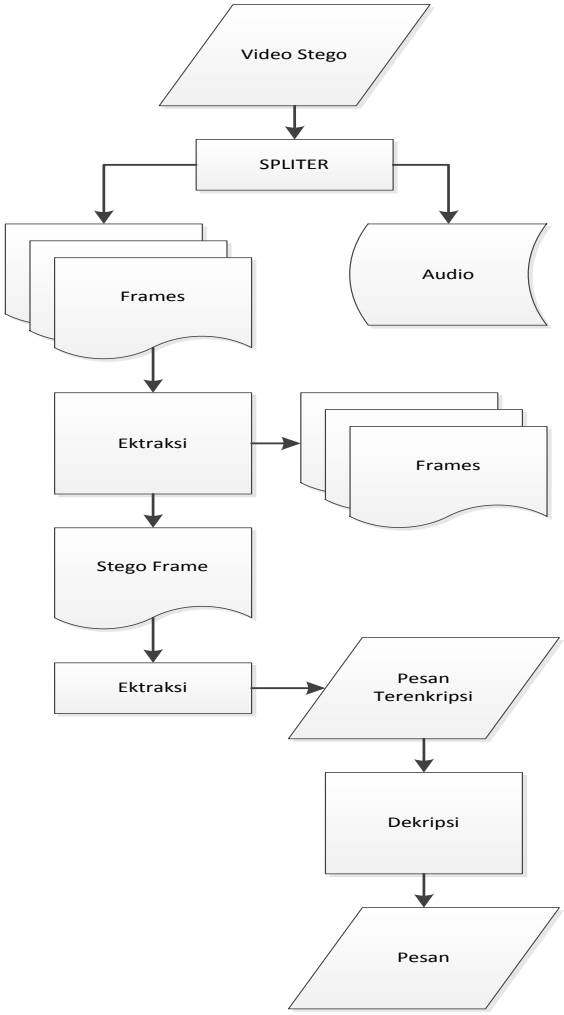
Gambar 2. Proses Steganografi Video

B. Perancangan Sistem Proses Pengambilan Pesan video stego

Langkah – langkah dalam pengambilan pesan dari video stego 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.

Rancangan Sistem Proses Pengambilan Pesan video stego dapat dilihat pada Gambar 3.



Gambar 3. Proses Pengambilan pesan dari video stego

IV. HASIL DAN PEMBAHASAN

Untuk memperoleh hasil yang diharapkan maka dalam penelitian ini akan dilakukan pengujian secara kualitatif dan kuantitatif. Teknik pengujian kualitatif (subyektif) dilakukan dengan pengamatan secara langsung terhadap video asli dan video *stego*, proses pengujian kualitatif dikerjakan sebagai berikut:

1) Melakukan pengolahan video memanfaatkan *tools freeware* untuk mendeteksi perubahan kualitas video *stego* berdasarkan pengamatan dengan visual manusia.
2) Melakukan pengamatan nilai *Byte* video *stego*, kemudian dibandingkan dengan nilai *Byte* video asli untuk mendeteksi perubahan kualitas video.

Pengujian kuantitatif untuk mengukur secara obyektif hasil video stego dari masing – masing algoritma, pengujian dilakukan dengan mengukur error pada video stego. Pada penelitian ini ada 3 pengukuran yang dilakukan secara obyektif, diantaranya :

1) Pengukuran kesalahan (error) dilakukan dengan cara mengkalkulasi nilai Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Pengukuran nilai error MSE berfungsi untuk mengukur kesamaan 2 buah video, yaitu video asli dengan video stego. PSNR untuk melakukan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut, semakin besar nilai PSNR maka video stego yang dihasilkan semakin baik.
2) Mengukur peningkatan ukuran file video stego dari jumlah pesan yang disisipkan.
3) Mengukur panjang pesan yang mampu disisipkan pada sebuah video.

Selanjutnya dari hasil pengukuran dilakukan analisis perbandingan antara algoritma *MEoF* dengan *EoF* dan *MLSB*. Hasil yang diharapkan dari penelitian ini adalah untuk membuktikan apakah algoritma MEof lebih baik dari metode EoF dan MLSB untuk steganografi video berekstensi FLV.

V. SIMPULAN DAN SARAN

Penelitian ini menguji Algoritma MEoF untuk steganografi video berekstensi FLV. Sebagai saran perlu dilakukan penelitian lebih lanjut Algoritma *MEoF* untuk format video yang lain.

DAFTAR PUSTAKA

Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi,* Penerbit Andi, Yogyakarta.

Atoum, M. S., Ibrahim, S., Sulong, G. dan M-Ahmad, A., (2012). *MP3 Steganography*: Review, International Journal of Computer Science Issues, *Vol. 9, Issue 6, No 3.*

Cachin C. (2005). *A survey prepared for the Encyclopedia of Cryptography and Security,* Digital Steganography, IBM Research Zurich Research Laboratory, Switzerland.

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

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.

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 2015).

Emy Setyaningsih. (2013). *Implementasi System Sandi Stream Cipher Untuk Pengamanan Data Image,* Seminar Nasional Teknologi Informasi dan Komputasi (SENASTIK).

Moreno, J., Jaime, B. dan Saucedo, S. (2013). *Towards No-Reference of Peak Signal to Noise Ratio Estimation Based on Chromatic Induction Model*, International Journal of Advanced Computer Science and Applications (IJACSA), *Vol. 4, No.1, Mexico.*

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

Tarigan, T.E. (2015) *Algoritma Meof (Modifikasi End Of File) Untuk Steganografi Pada Citra Bitmap 24 Bit,*Yogyakarta.

Wahyu Lukman (2016). *Prototyping Model*, diambil dari https://www.scribd.com/doc/58298607/Pengertian-Prototype.

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