PERBANDINGAN METODE *DATA ENCRYPTION STANDARD (DES)* DAN *ADVANCED ENCRYPTION STANDARD (AES)* PADA STEGANOGRAFI FILE CITRA

Apri Siswanto[1], Abdul Syukur[2], Ismatul Husna[3]

Teknik Informatika, Fakultas Teknik
Universitas Islam Riau[1,2,3]
email :
aprisiswanto@eng.uir.ac.id*[1]
abdulsyukur@eng.uir.ac.id[2]
Una03031994@gmail.com[3]
Jl. Kaharuddin Nasution 113 Pekanbaru Riau, 28284, Indonesia

Abstrak

Keamanan dan kerahasian pesan atau data merupakan hal yang sangat penting, apalagi pesan atau data yang akan dikirim bersifat rahasia. Karena banyaknya gangguan terhadap file atau data rahasia yang diganggu oleh orang yang tidak bertanggung jawab dapat merugikan pihak tersebut. Tujuan aplikasi ini adalah untuk membantu mengamankan pesan dengan menggunakan metode *DES(Data Encryption Standard)* dan *AES(Advanced Encryption Standard)* untuk proses enkripsi dan dekripsi pesan, sedangkan Steganografi nya untuk menyisipkan pesan yang akan dikirim. Sehingga dengan menggunakan metode tersebut dapat membandingkan kualitas gambar dan waktu proses enkripsi pesan. Sistem ini diimplementasikan dengan bahasa pemograman PHP *(Hypertext Preprocessor)*.

Kata kunci: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Kriptografi, steganografi, dan Least Significant Bit (LSB)

1 PENDAHULUAN

Keamanan dan kerahasaian pesan atau data merupakan hal yang sangat penting, apalagi pesan atau data yang akan dikirim bersifat rahasia atau penting. Karena banyaknya gangguan terhadap file atau data rahasia yang diganggu oleh orang yang tidak bertanggung jawab, penyadapan terhadap pesan atau informasi merupakan hal yang sangat merugikan bagi pengguna jaringan komunikasi saat ini (Siswanto, Yulianti, & Costaner, 2017).

Berdasarkan permasalahan ini lahirlah metode untuk menjaga kerahasiaan pesan yang disebut kriptografi. Kriptografi merupakan salah satu metode dalam menuliskan pesan dimana tidak ada seorang pun yang dapat membaca isi pesan tersebut selain dari pihak yang dituju, oleh karena itu untuk menjaga keamanan file tersebut maka dapat diterapkan teknik kriptografi, diantaranya algoritma DES *(Data Encryption Standard)* dan AES *(Advanced Encryption Standard)* (Dony, 2008). Algoritma DES *(Data Encryption Standard)* termasuk sistem kriptografi simetri dan tergolong jenis blok dan kode. Dan sering disebut juga sebagai algorima konvensional, yaitu algoritma yang menggunakan enkripsi dan dekripsi yang sama. Sedangkan AES *(Advanced Encryption Standard)* merupakan algoritma simetris yaitu menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES memiliki tiga pilihan kunci yaitu tipe: AES-128, AES-192, AES-256. Masing-masing tipe

menggunakan kunci internal yang berbeda yaitu round key untuk setiap proses putaran.

Steganografi adalah seni dan ilmu untuk menyembunyikan pesan yang bersifat rahasia didalam pesan lain, sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi memiliki dua proses, yaitu encoding dan decoding. Encoding merupakan proses penyisipan pesan kedalam media penampung (covertext) dalam hal ini adalah gambar/citra digital, sedangkan decoding, adalah proses ekstraksi pesan dari gambar stego (stegotext). Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan (Munir, 2004).

Citra digital merupakan suatu gambar yang tersusun dari pixel, dimana tiap pixel merepresentasikan warna (tingkat keabuan untuk gambar hitam putih) pada suatu titik digambar. Gambar digital merupakan dokumen berbentuk file yang dihasilkan melalui perangkat elektronik atau media digital. Berdasarkan permasalahan tersebut maka akan dibangun sebuah aplikasi perbandingan antara algoritma AES dan DES untuk mengamankan sebuah pesan yang disisipkan pada gambar.

2 TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, yairu crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan) (Rohmanu, 2017). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

Berikut ini adalah beberapa sistem kriptografi yaitu (Dony, 2008),

- Plaintext
- Secret Key
- Ciphertext
- Algoritma Enkripsi
- Algoritma Deksripsi

A. *Advanced Encryption Standard* (AES)

Advanced Encryption Standard (AES) merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES dapat memiliki panjang kunci bit 128, 192, 256 bit. Penyandian AES menggunakan proses yang berulang yang disebut dengan ronde. Jumlah ronde yang digunakan oleh AES tergantung dengan panjang kunci yang digunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya. Kunci ronde dibangkitkan berdasarkan kunci yang diberikan. Relasi antara jumlah ronde dan panjang diberikan oleh Sadikin (2012).

B. *Data Encryption Standard* (DES)

Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolah informasi Federal AS. DES dirancang oleh tim IBM yang dipimpin Horst Feistel dengan bantuan dari NSA (National Security Agency).

DES menggunakan kunci sebesar 64 bit untuk mengenkripsi blok juga sebesar 64 bit. Akan tetapi karena 8 bit dari kunci digunakan sebagai parity, kunci efektif hanya 65 bit. Dalam DES, penomoran bit adalah dari kiri kekanan dengan bit 1 menjadi most significant bit, untuk

64 bit, bit 1 mempunyai 263. Permutasi menggunakan inintial permutation dilakukan terhadap input sebesar 64 bit. Hasil permutasi dibagi menjadi dua blok L0 dan R0, masing-masing sebesar 32 bit, dimana L0 merupakan 32 bit pertama dari hasil permutasi dan R0 merupakan 32 bit sisanya (bit 33 bit hasil permutasi menjadi bit 1 R0). Sebanyak 16 putaran enkripsi dilakukan menggunakan fungsi cipher f dan setiap putaran menggunakan kunci 48 bit yang berbeda dan dibuat berdasarkan kunci DES. Efeknya adalah setiap blok secara bergantian dienkripsi, masing-masing sebanyak 8 kali. Pada setiap putaran, blok sebesar 32 bit dienkripsi menggunakan rumus (Kromodimoeljo, 2009) .

2.2 Metode Steganografi

Steganografi adalah ilmu menyembunyikan teks pada media lain yang telah ada sedemikian sehingga teks yang tersembunyi menyatu dengan media itu. Media tempat penyembunyian pesan tersebut dapat berupa media teks, gambar, audio atau video. Steganografi yang kuat memiliki sifat media yang telah tertanam teks tersembunyi sulit dibedakan dengan media asli namun teks tersembunyi tetap dapat diekstraksi (Amalia, Styoriny, & Rahayani, 2017).

Untuk mengetahui kualitas gambar, ada beberapa parameter pengukuran kesalahan atau error dalam pemrosesan citra. Dua parameter yang umum digunakan adalah:

2.2.1 Mean Square Error (MSE)

MSE merupakan ukuran yang baik untuk mengukur kesamaan 2 buah citra. Misalkan memiliki 2 buah citra f dan g dengan dimensi yang sama dengan M x N, MSE antara keduanya didefenisikan persamaan sebagai berikut:

$$MSE = \frac{1}{M\ x\ N} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f\ (i,j) - g(i,j)]2 \quad (1)$$

$$RMSE = \sqrt{\frac{1}{M\ x\ N}} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f\ (i,j) - g(i,j)]2 \quad (2)$$

MSE = nilai Mean Square Error dari citra
M = panjang citra
N = lebar citra
(i,j) = koordinat masing-masing piksel
I = citra asli
K = citra rekontruksi

2.2.2 Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besaran derau yang berpengaruh pada sinyal tersebut. Rentang nilai PSNR yang baik antara 20dB – 40dB. Nilai PSNR yang lebih tinggi artinya kemiripan lebih erat antara hasil stego dengan gambar asli. Rumus yang dapat digunakan:

MAX = nilai maksimum piksel input
MSE = nilai MSE

3 METODOLOGI PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah eksperimental dengan tahapan pengumpulan data seperti studi pustaka dan studi lapangan, penyiapan alat dan bahan, perancangan system, implementasi system dan evaluasi aplikasi dalam perbandingan DES dan AES pada file steganografi citra. Tahapan penelitiannya adalah sebagi berikut :

3.1 Studi Pustaka

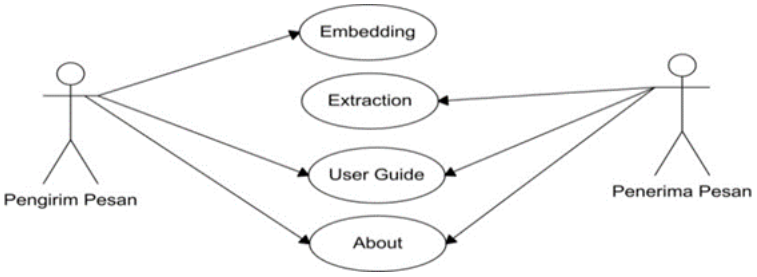
Mengumpulkan data dengan cara mencari dan mempelajari dari berbagai sumber yang berkaitan dengan masalah yang diteliti, baik dari internet, buku, jurnal ilmiah dan dari bacaan lain yang dapat dipertanggung jawabkan.

3.2 Penyiapan alat dan bahan

Pada tahap ini adalah persiapan penggunaan alat-alat yang digunakan dalam penelitian ini, yaitu penentuan spesifikasi perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini.

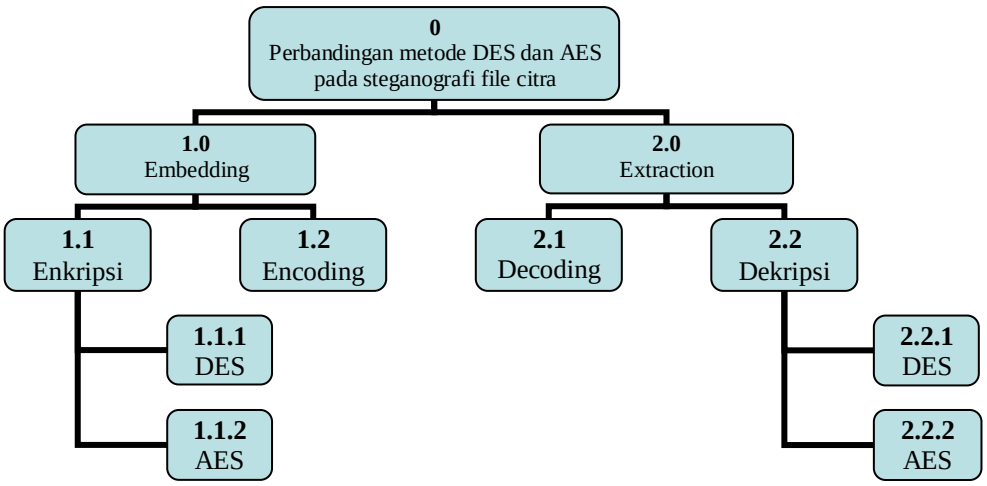
3.3 Perancangan Sistem

Perancangan system yang dilakukan seperti gambar 1.



Gambar 1 : use case diagram

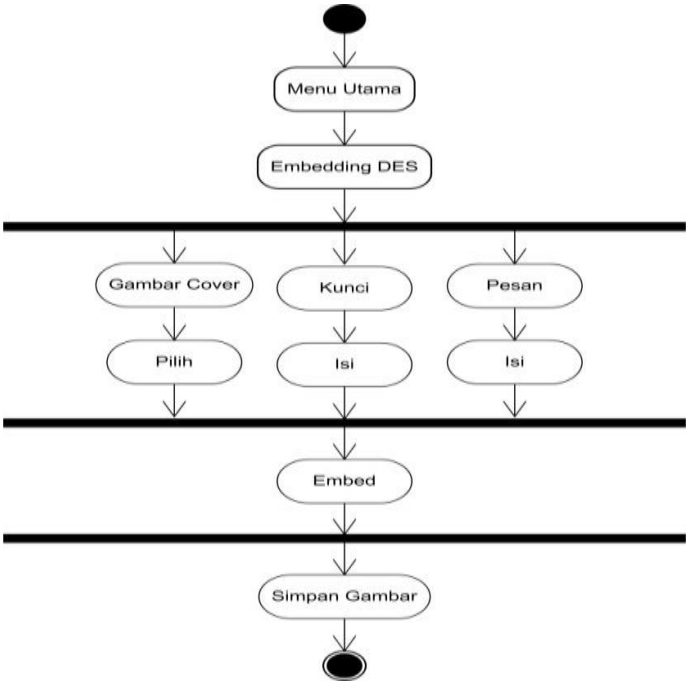
Pada gambar 1 diatas dapat dilihat pada aplikasi yang akan dibangun terdiri dari 2 aktor, pertama pengirim pesan dan kedua penerima pesan. Pada aplikasi ini terdiri dari 4 *case*, embedding, extraction, user guide, dan about. Selanjutnya hierarchy chart di buat berdasarkan use case diagram seperti pada gambar 2.



Gambar 2 : *Hierarchy chart*

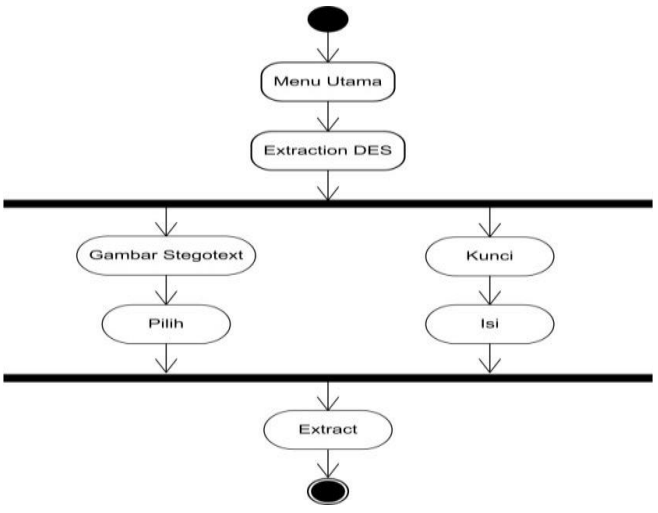
Berdasarkan Hierarchy Chart pada gambar 2, terdapat 2 proses utama yang akan dilakukan dalam system yang akan dibangun ini. Pertama adalah embedding, pada proses ini dilakukan enkripsi algoritma DES dan AES dan encoding yaitu proses penyandian dan penyembunyian

pesan pada gambar. Proses kedua adalah extraction, pada proses ini dilakukan proses decoding dan dekripsi algoritma DES dan AES. Setelah hierarchy chart digambarkan dengan detail maka selanjutnya adalah mengembangkan Activity Diagram seperti gambar 3.



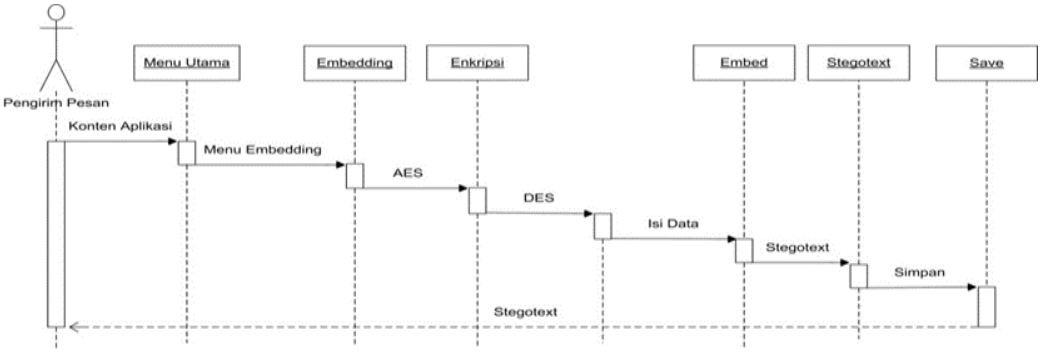
Gambar 3 : Activity Diagram Embedding DES

Berdasarkan gambar 3 diatas dapat dilihat setelah aplikasi dijalankan akan muncul menu utama dan pilih menu embedding dan kemudian pilih embedding DES , pada menu ini terdapat 3 field yang harus diisi. Pertama pilih gambar cover untuk menampung pesan. Yang kedua inputkan pesan yang akan disandikan, disisipkan dan mengenkripsi pesan dan mengubahnya kedalam chiperteks dan yang ketiga masukkan kunci, prosesnya seperti gambar 4.

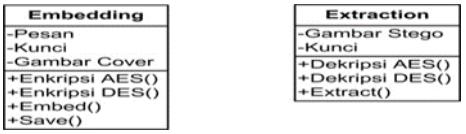


Gambar 4 : Activity Diagram Extraction DES

Pada gambar.4 diatas dapat dilihat, yang menjadi input pada proses ini yaitu gambar gambar stegotext, dan kunci yang sama pada saat embed. Dan dekripsi chiperteks ke plainteks membutuhkan kunci yang sama pada saat mengenkripsi pesan pada saat embedding. Proses rancangan dan pengembangan system selanjutnya adalah menggambarkan sequence diagram dan class diagram seperti pada gambar 5 dan gambar 6.



Gambar 5 : Sequence Diagram



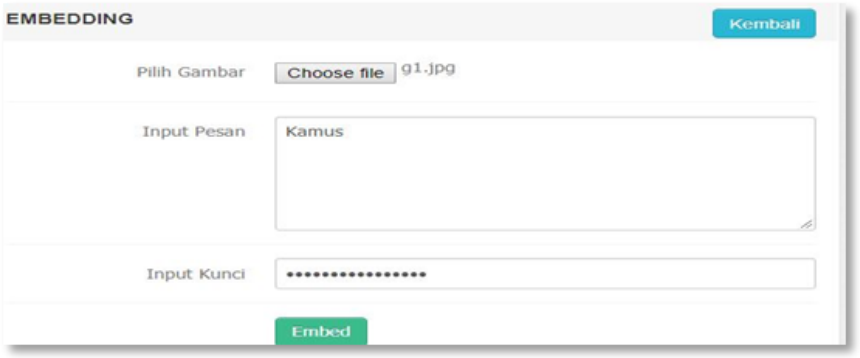
Gambar 6: Class Diagram

4 HASIL DAN PEMBAHASAN

4.1 Pengujian Perhitungan Pada Sistem

Pengujian Enkripsi

Dengan menggunakan metode DES dan AES Berikut contoh inputan pesan dan proses penyisipan pesan pada gambar yang akan di enkripsi. Dapat dilihat pada Gambar 7 dan pada Gambar 8 dan Gambar 9 dibawah ini.

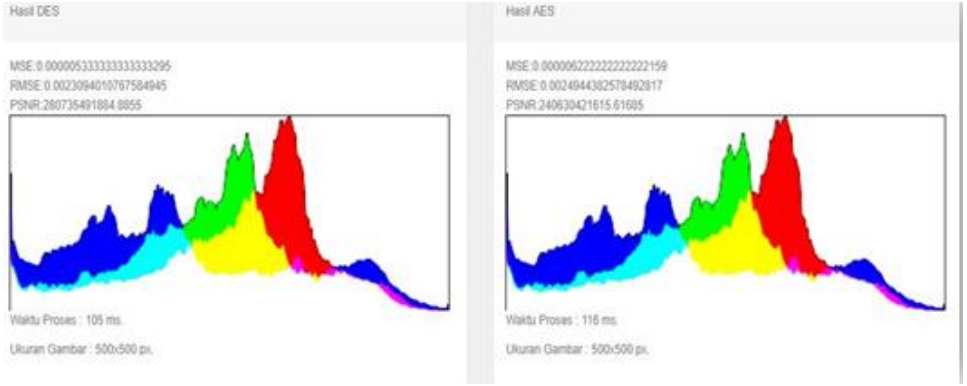


Gambar 7: Contoh Inputan Enkripsi Dan Penyisipan Pesan

Pada Gambar 7 diatas adalah contoh inputan pesan dan proses penyisipan pesan pada gambar yang akan di enkripsi. Untuk melihat hasil dari enkripsi diatas perhatikan pada Gambar 8 dan Gambar 9.

Gambar 8: Hasil Stego Image

Pada Gambar 8 dan Gambar 9 diatas dapat dilihat hasil dari proses enkripsi dan proses penyisipan pesan pada gambar yang telah dilakukan. Kemudian hasil enkripi tersebut dapat disimpan dan akan terbentuk ke dalam sebuah file dengan ekstensi .png .



Gambar 9: Hasil Waktu Enkripsi, MSE, RMSE,PNSR Pada DES dan AES

5 KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan penulis mengenai aplikasi Perbandingan Metode DES dan AES Pada Steganografi File Citra ini, maka dapat diambil kesimpulan sebagai berikut :

1. Penelitian ini telah berhasil membuat aplikasi Perbandingan Metode DES dan AES Pada Steganografi File Citra yang dapat digunakan untuk mengamankan Pesan.
2. Aplikasi ini telah berhasil melakukan enkripsi Pesan dengan benar sesuai dengan perhitungan manual.
3. Aplikasi ini telah berhasil melakukan dekripsi atau pengembalian pesan dengan benar sesuai perhitungan manual.
4. Hasil dari perbandingan waktu lebih cepat enkripsi menggunakan metode DES yaitu rata-rata = 133.6 ms (49.5%) , hal tesebut dikarenakan pada proses (*step-step*) algoritma DES lebih sedikit dibandingkan dengan AES yang memiliki step-step perhitungan manual yang lebih panjang dan ukuran pada gambar juga mempengaruhi pada waktu proses enkripsi.
5. Hasil dari perbandingan kualitas gambar untuk MSE lebih baik pada AES dengan rata-rata = 9.54333E-05 (40.63 %), hal tersebut dikarenakan pada MSE AES kesalalahan nilai kuadrat rata-rata lebih kecil.
6. Sedangkan hasil perbandingan kualitas gambar untuk RMSE pada AES yang lebih baik dengan rata-rata = 0.009168157 (45.34 %), karena nilai kuadrat rata-rata yang dihasilakan oleh suatu model prakiraan mendekati variasi nilai observasinya
7. Hasil perbandingan kualitas gambar untuk PSNR pada AES yang lebih baik dengan rata-rata = 62482146755 (57.96%), karena nilai terbaik PSNR adalah diatas 40 decibel (db).

Penelitian yang penulis lakukan ini tidak lepas dari kelemahan dan kekurangan. Maka untuk pengembangan aplikasi ini lebih lanjut diperlukan perhatian terhadap aplikasi ini, yaitu bisa dengan mengubah pesan yang akan disisipkan menjadi video.

Referensi

Amalia, A., Styoriny, W., & Rahayani, R. D. (2017). Steganografi dan Kriptografi pada Audio. *Jurnal Aksara Elementer, 3*(1).

Dony, A. (2008). Pengantar Ilmu Kriptografi. *Edisi Dua. Yogyakarta: CV Andi Offset*.

Kromodimoeljo, S. (2009). Teori dan aplikasi kriptografi. *SPK IT Consulting*.

Munir, R. (2004). Steganografi dan Watermarking. *Departemen Teknik Informatika, Institut Teknologi Bandung. Diakses dari http://informatika. stei. itb. ac. id/~ rinaldi. munir/Kriptografi/Steganografi% 20dan% 20Watermark ing. pdf*.

Rohmanu, A. (2017). Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File. *Jurnal Informatika SIMANTIK, 2*(1), 1-11.

Sadikin, R. (2012). Kriptografi untuk keamanan jaringan. *Yogyakarta: Andi*.

Siswanto, A., Yulianti, A., & Costaner, L. (2017). *Arsitektur Sistem Keamanan Rumah Dengan Menggunakan Teknologi Biometrik Sidik Jari Berbasis Arduino*. Paper presented at the Seminar Nasional Aptikom 2017.