JURNAL FASILKOM
(FAKULTAS ILMU KOMPUTER)
Vol. 7 Nomor 2 (2018) 255–259 ISSN : 2089-3353

IMPLEMENTASI STEGANOGRAFI PADA TEKS TERENKRIPSI DENGAN ALGORITMA RSA MENGGUNAKAN METODE BPCS

Yulia Fatma[1)], Harun Mukhtar[2)], Muhammad Taufik[3)]
[123]Ilmu Komputer, Universitas Muhammadiyah Riau
[1]email: yuliafatma@umri.ac.id
[2]email: harunmukhtar@umri.ac.id
[3]email: muhammadtaufik29@gmail.com

Abstract

The internet network is growing rapidly and has a great impact on human life. The development of the internet network has enabled many people to exchange information or messages,one of tham by using email media. Apparently the internet is a path that in ni not too safe because it is a common communication media that can be used by everyone so prone to tapping information or messages. Therefore, security and confidentiality are needed in data communications. One may to keep messages safe is to use steganography technique. The steganography method used is the method of message insertion using BPCS (Bit Plane Complexity Segmentation). Before the message is inserted, the message is first encrypted using cryptography techniques. The cryptographic algorithm used is RSA algorithm. RSA algorithm consists of encryption algorithm and decryption algorithm. The confidential message is encrypted using RSA encryption algorithm and inserted using the insertion method of BPCS. With the technique of steganography on the image media then the delivery of a secret message will have a good level of security because it can not be detected directly by the senses of human vision.

Keywords: *cryptography, steganography, RSA, method BPCS*

Abstrak

Jaringan internet berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Perkembangan jaringan Internet telah memungkinkan banyak orang untuk saling bertukar informasi atau pesan salah satunya dengan media email. Ternyata, internet merupakan jalur yang tidak terlalu aman karna merupakan media komunikasi umum yang dapat digunakan semua orang sehingga rawan penyadapan informasi atau pesan. Oleh karena itu, keamanan dan kerahasiaan sangat dibutuhkan dalam komunikasi data. Salah satu cara untuk menjaga keamanan pesan adalah menggunakan teknik steganografi. Metode steganografi yang digunakan adalah metode penyisipan pesan, dengan menggunakan metode BPCS (Bit Plane Complexity Segmentation). Sebelum pesan disisipkan terlebih dahulu pesan tersebut dienkripsi dengan menggunakan teknik kriptografi. Algoritma kriptografi yang digunakan adalah algoritma RSA. Algoritma RSA terdiri dari algoritma enkripsi dan algoritma dekripsi. Pesan rahasia disandikan menggunakan algoritma enkripsi RSA dan disisipkan menggunakan metode penyisipan BPCS. Dengan adanya teknik steganografi pada media citra maka pengiriman suatu pesan yang bersifat rahasia akan memiliki tingkat keamanan yang baik karena tidak dapat dideteksi langsung oleh indera penglihatan manusia.

Keywords: *Kriptografi, Steganogari, RSA, Metode BPCS*

PENDAHULUAN

Masalah privasi dan keamanan pesan, data, informasi menjadi hal yang penting di era kemajuan teknologi komputer. Pertukaran informasi banyak dilakukan menggunakan media internet, salah satunya adalah menggunakan *e-mail* (*electronic mail*). Dengan menggunakan *email*, pesan menjadi lebih cepat tersampaikan bahkan hanya dalam hitungan detik serta tidak memakan banyak biaya.

Namun di sisi lain, ternyata internet merupakan jalur yang tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan secara bebas oleh siapapun sehingga sangat rawan penyadapan informasi baik pasif maupun aktif oleh pihak-pihak yang tidak bertanggung jawab. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada [1]. Permasalahan tersebut dapat dihadapi demgan membuat aplikasi untuk mencegah pihak yang tidak bertanggung jawab dapat membaca data, . menjamin keaslian, agar hanya dapat diterima dan dibaca oleh orang-orang yang berhak mendapatkan akses terhadap data [2].

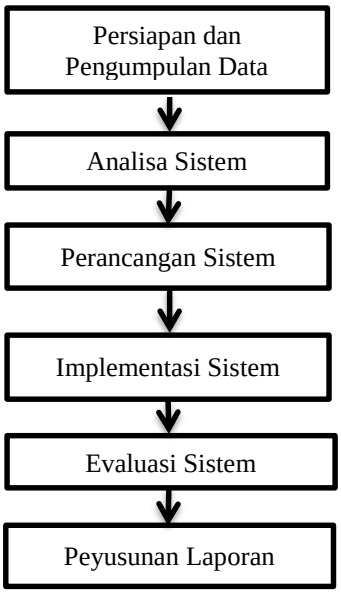
Adapun pada penelitian ini informasi bersifat rahasia yang akan diamankan adalah DPO (Daftar Pencarian Orang) yang terdapat di kapolri. Jika diperlukan untuk melakukan penangkapan terhadap tersangka, maka daftar DPO tersebut di kirim ke satuan polri lainnya dan meneruskan informasi tersebut kejajaran ketika proses penangkapan tersangka tersebut. Informasi mengenai DPO sendiri harus dijaga kerahasiaanya, karena jika tersebar luas maka orang yang ada didalam DPO tersebut dapat berpindah ke tempat lainya, sehingga menyulitkan bagi pihak kepolisian dalam menemukan dan mengungkap kasusnya. Kasus pencurian data atau informasi digital masih menjadi salah satu ancaman dengan total persentase yang paling tinggi [3].

Cara untuk mengamankan data atau pesan adalah menggunakan kriptografi untuk melakukan penyandian terhadap data atau pesan yang akan dikirim. Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan [4]. Berdasarkan kunci yang digunakan, kriptografi dibedakan menjadi kriptografi kunci-simetri (*symetric-key cryptography*) yang biasa disebut kriptografi kunci-privat dan kriptografi kunci nirsimetri (*asymetric key cryptography*) yang biasa disebut kriptografi kunci-publik [5]. Salah satu algoritma kriptografi kunci-publik yang populer adalah algoritma RSA. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Algoritma RSA termasuk algoritma yang baik (aman secara komputasi). Dengan jumlah cipherteks yang lebih banyak dari plainteks mengakibatkan faktor kerja untuk pemecahan chiperteks membutuhkan waktu yang lebih lama [6]. Keutamaan dari kriptografi RSA adalah tantangan pada ukuran modulus *n* yang dimliki RSA [7], algoritma ini dikatakan aman jika penyerang sulit dalam memfaktorkan modulus *n* menjadi *p* dan *q* [8].

Untuk lebih meningkatkan kerahasiaan pada data maka hasil penyandian berupa cipherteks dapat dikombinasikan dengan teknik steganografi. Steganografi berfungsi untuk menyembunyikan pesan rahasia dalam pesan lain, sehingga keberadaan pesan rahasia menjadi tidak terlihat [4]. *Bit-Plane Complexity Segmentation* (BPCS) adalah salah satu teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan R. O. Eason pada tahun 1997 untuk mengatasi kekurangan yang muncul pada beberapa teknik steganografi konvensional seperti *Least Significant Bit* (LSB), teknik *transform embedding*, dan teknik *masking perceptual* [9]. Steganografi menggunakan BPCS memiliki kemampuan kapasitas *embedding* data yang tinggi [10].

METODE PENELITIAN

Pada penelitian ini, metode yang digunakan adalah SDLC (*System Development Life Cycle*) yang diterapkan dalam suatu basis sistem informasi komputerisasi, yaitu seperti terlihat pada Gambar 1:

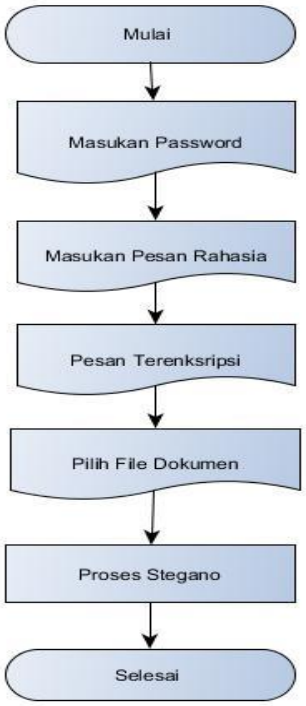


Gambar 1. Metode Penelitian SDLC

HASIL DAN PEMBAHASAN

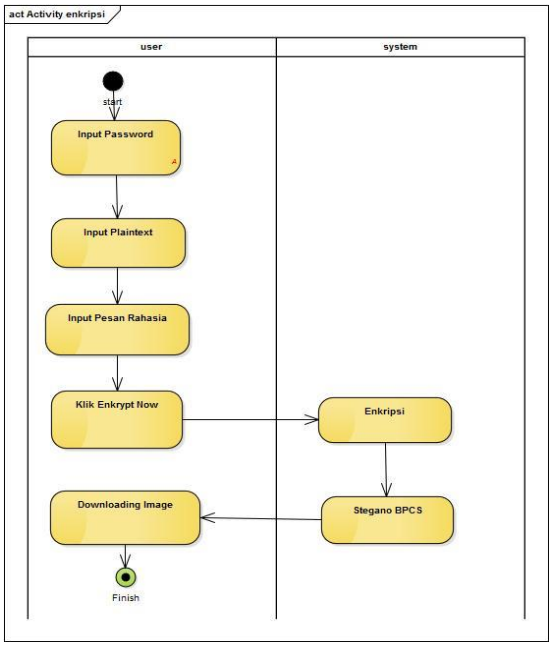
1. Proses Enkripsi (*Encryption*)

Proses enkripsi diawali dengan memasukan password kemudian berlanjut dengan memasukan pesan text asli, selanjutnya memasukan pesan terenksripsi dan proses terakhir memilih gambar untuk dikirim (*Choose file*). Hasil dari proses enkripsi berupa *ciphertext*, *simetric key* dan *file signature*. Gambar proses Enkripsi dapat dilihat pada Gambar 2:



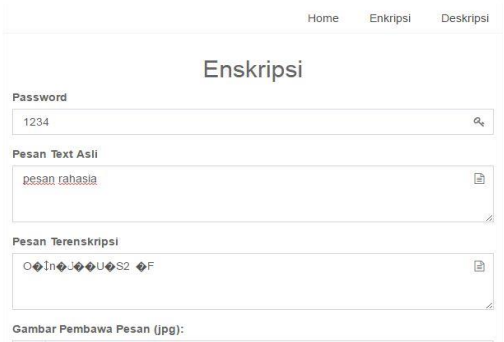
Gambar 2. Proses Enkripsi

Proses enkripsi dimulai dengan memasukkan kunci rahasia pada form yang sudah ada. Kemudian memasukkan pesan rahasia lalu memilih gambar. Lalu mengklik tombol *encrypt now* sehingga sistem dapat melakukan enkripsi steganografi. Sistem akan mendownload gambar hasil enkripsi. Activity Diagram Proses Enkripsi dapat dilihat pada Gambar 3:



Gambar 3. Activity Diagram Proses Enkripsi

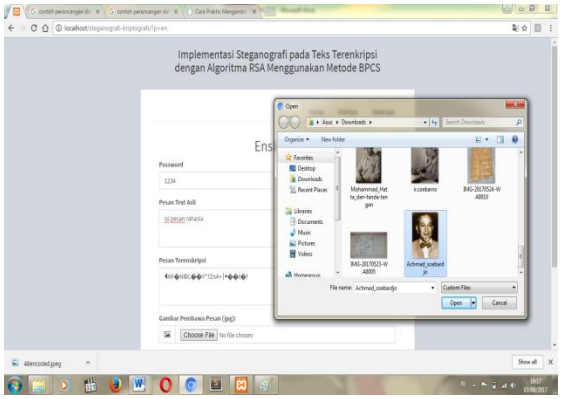
Berikut adalah hasil implementasi rancangan antarmuka dari proses enkripsi hingga proses menyisipkan pesan ke gambar. Tahap pertama yang dilakukan pada proses enkripsi adalah pengguna memasukkan kata kunci dan pesan yang akan dienkrip seperti terlihat pada Gambar 4.



Gambar 4. Antarmuka Form Enkripsi

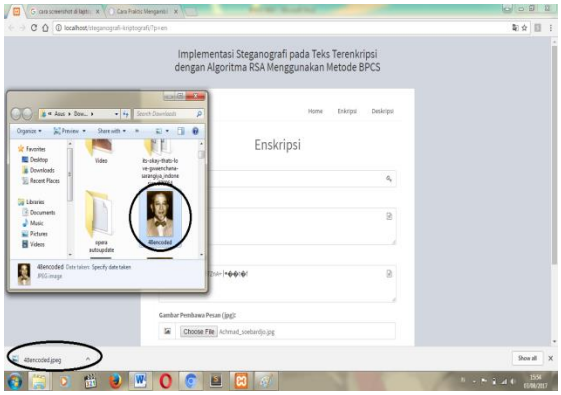
Proses selanjutnya pengguna harus *choose file* untuk memilih gambar yang akan digunakan

sebagai media menyembunyian pesan yang diinginkan dapat dilihat pada Gambar 5.



Gambar 5. Proses Pemilihan gambar

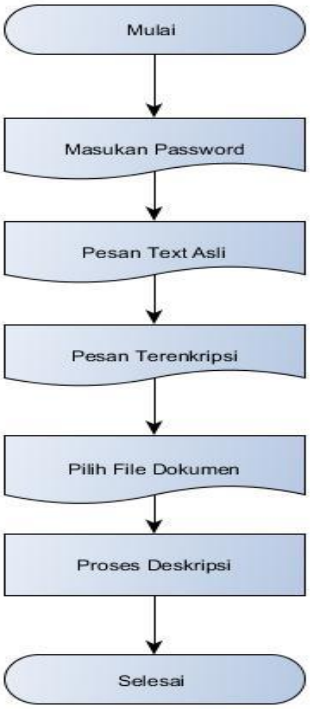
Setelah pemilihan gambar yang diinginkan pengirim dapat melakukan enkripsi. Kemudian gambar akan secara otomatis terdonwload sesuai kode yang sudah ditentukan. Hasil gambar dapat dilihat pada Gambar 6.



Gambar 6. Proses donwload gambar

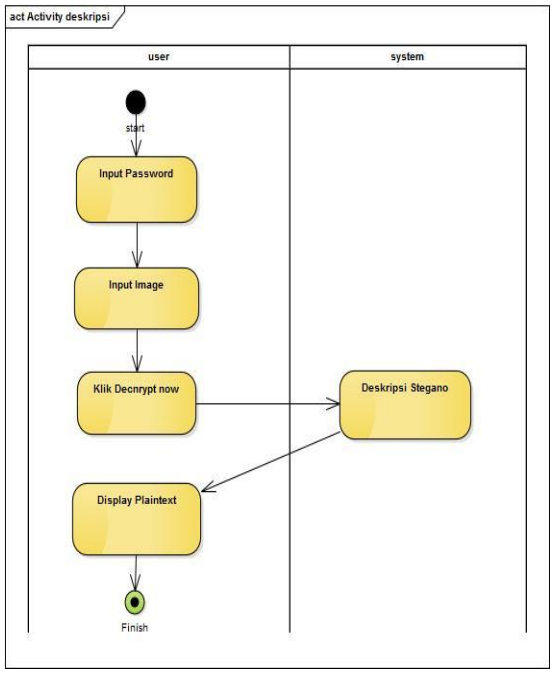
2. Proses Dekripsi (*Decryption*)

Proses dekripsi diawali dengan *document* (data yang sudah dienkripsi/ stegano) beserta *simetric key* dan *file signature*. Proses berlanjut pada memasukan *password.* Selanjutnya memilih gambar yang dikirim oleh pengirim. Proses berikutnya dilakukan validasi. Jika kata kunci rahasia yang didapatkan cocok/sesuai dengan yang dimasukan pada proses enkripsi/stegano, proses dilanjutkan ke proses dekripsi untuk mengembalikan *Ciphertext document* ke bentuk *Plaintext document*. Jika yang didapatkan pada proses validasi tidak cocok maka proses dihentikan atau gagal. proses Dekripsi dapat dilihat pada Gambar 7.



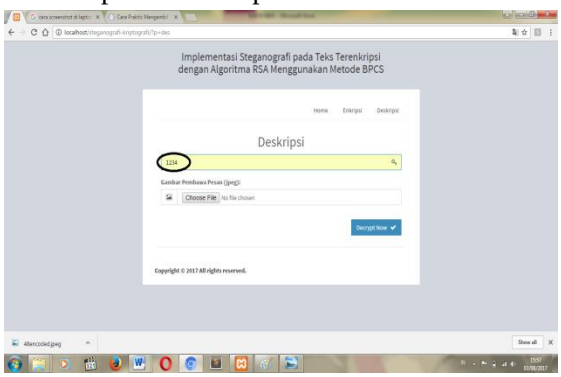
Gambar 7. Proses Dekripsi

Dalam proses dekripsi, user juga harus melakukan input kunci rahasia terlebih dahulu. Kemudian memilih gambar yang ingin diekstrak pesannya. Klik tombol *decrypt now* maka sistem akan melakukan ekstraksi gambar sehingga menampilkan *output* yang isinya merupakan *ciphertext*. *Ciphertext* kemudian didekripsi sehingga menghasilkan *plaintext*.



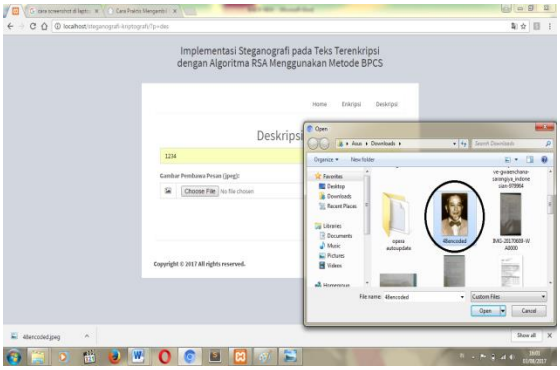
Gambar 8. Activity Diagram Proses Dekripsi

Berikut adalah hasil implementasi rancangan antarmuka dari proses dekripsi. Tahap pertama yang dilakukan pada proses dekripsi adalah pengguna memasukkan kata kunci seperti terlihat pada Gambar 9.



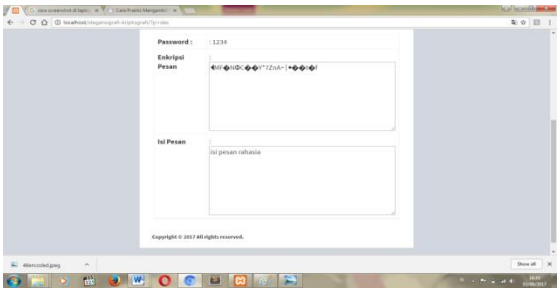
Gambar 9. Antarmuka Form Dekripsi

Selanjutnya penerima memilih gambar yang akan diekstrak *ciphertext*nya seperti tampak pada Gambar 10.



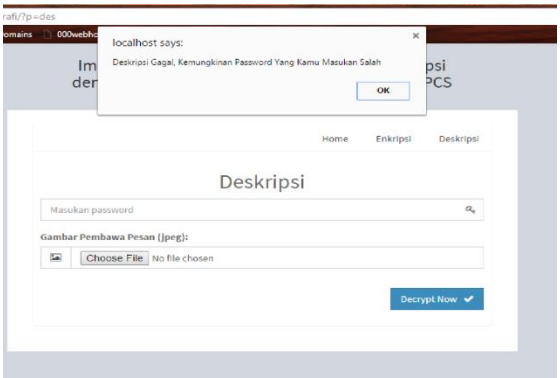
Gambar 10. Pemilihan Gambar Dekripsi

Kemudian tekan tombol *decrypt now* sehingga didapat *ciphertext* dan *plaintext* seperti tampak pada Gambar 11.



Gambar 11. Hasil Dekripsi

Proses dekripsi yang dilakukan terhadap kata kunci rahasia yang tidak sesuai dengan yang diberi oleh pengirim maka akan gagal dijalankan. Hal ini disebabkan karena adanya ketidak cocokan password antara nilai hash asli dengan nilai hash dekripsi atau dengan kata lain dokumen yang akan didekripsi tidak sesuai dengan *message digest* yang ditambahkan ke dalam *file* tersebut seperti tampak pada Gambar 12.



Gambar 12. Proses Dekripsi Gagal

SIMPULAN DAN SARAN

Dengan adanya sistem keamanan data dengan menggunakan kriptografi dan

steganografi untuk menjaga keamanan data dengan menggunakan metode RSA (*Rivert Shamir Adelman)* dan BPCS (Bit-Plane Complextiy Sigmentation) maka didapatkan kesimpulan sebagai berikut:

1. Sistem dapat melakukan proses penyandian (enkripsi) dan dekripsi dengan algoritma RSA.
2. Sistem dapat melakukan peroses menyisipan pesan yang sudah dienkripsi, kedalam media gambar dengan menggunakan metode BPCS.
3. Gambar hasil dari steganografi terlihat sama seperti gambar aslinya, tidak terlihat perbedaannya secara visual.

Dalam perancangan aplikasi ini masih banyak terdapat kekurangan. Saran yang diberikan untuk pengembangan selanjutnya antara lain :

1. Dapat menambahkan metode enkripsi yang baru atau menambahkan enkripsi yang lebih handal dari RSA.
2. Menambah media penampung steganografi berupa gambar berformat GIF dan PNG.

TERIMA KASIH

Puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan rahmat dan karunianya, sehingga penulis dapat menyelesaikan penelitian dengan judul "Implementasi Steganografi pada Teks Terenkripsi dengan Algoritma RSA menggunakan Metode BPCS".

Terima kasih kepada keluarga dan teman-teman penulis yang selalu memberikan dukungan dan bantuan selama mengerjakan penelitian ini. Serta kepada semua pihak yang tidak dapat disebutkan satu per satu, terima kasih atas kerjasamanya.

DAFTAR PUSTAKA

[1] Kominfo, "KEAMANAN JARINGAN INTERNET DAN FIREWALL," 2017. [Online]. Available: https://aptika.kominfo.go.id/index.php/artikel/190-keamanan-jaringan-internet-dan-firewall.

[2] Siswanto, M. Anif, and W. Gata, "Penerapan algoritma kriptografi tea dan base64 untuk mengamankan email," *ELTIKOM*, vol. 2, no. 1, pp. 34–41, 2018.

[3] Symantec, "Internet Security Threat Report 2014: Volume 19," vol. 19, no. April, 2014.

[4] B. Schneier, *Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (cloth)*, Second Edi. John Wiley & Sons, Inc, 1996.

[5] R. Munir, *Kriptografi*. 2006.

[6] A. P. Wahyadyatmika, R. R. Isnanto, and M. Somantri, "Implementasi Algoritma Kriptografi RSA pada Surat Elektronik (E-Mail)," *Transient*, vol. 3, no. 4, pp. 1–9, 2014.

[7] W. Stallings, *Cryptography and Network Security*, Sixth Edit., vol. 139, no. 3. Pearson, 2014.

[8] S. Verma and D. Garg, "An Improved RSA Variant," *Int. J. Adv. Technol.*, vol. 5, no. 2, pp. 161–169, 2014.

[9] P. L. T. Irawan, D. J. D. H. Santjojo, and M. Sarosa, "Implementasi Kripto-Steganografi Salsa20 dan BPCS untuk Pengamanan Data Citra Digital," *J. EECCIS*, vol. 8, no. 2, pp. 175–180, 2014.

[10] G. R. Manjula and A. Danti, "Embedding Multiple Images in an Image Using Bit Plane Slicing," *AJOMCOR*, vol. 2, no. 3, pp. 136–142, 2015.