SISTEM PENGAMANAN DATA MENGUNAKAN ALGORITMA AES DAN BLOWFISH DENGAN METODE LSB PADA CITRA PNG

TESIS

Oleh:
SITI MURYANAH
1611600980

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2018

SISTEM PENGAMANAN DATA MENGUNAKAN ALGORITMA AES DAN BLOWFISH DENGAN METODE LSB PADA CITRA PNG

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)

Oleh:
SITI MURYANAH
1611600980

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2018

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini

Nama Mahasiswa : Siti Muryanah

NIM : 1611600980

Konsentrasi : Teknologi Sistem Informasi

Menyatakan bahwa Tesis yang berjudul :

Sistem Pengamanan Data Menggunakan Algoritma AES dan Blowfish dengan Metode LSB Pada Citra PNG

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik pihak lain.
2. Saya izinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggungjawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila dikemudian hari pernyataaan ini tidak benar.

Jakarta, 08 Agustus 2018

Siti Muryanah

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN TESIS

Nama Mahasiswa	:	Siti Muryanah
NIM	:	1611600980
Konsentrasi	:	Teknologi Sistem Informasi
Judul Tesis	:	Sistem Pengamanan Data Mengunakan Algoritma AES dan Blowfish Dengan Metode LSB Pada Citra PNG

Jakarta, 08 Agustus 2018

Tim Penguji — Tanda Tangan

Ketua,

Ir. Wendi Usino, MM., M.Sc., Ph.D .....

Anggota,

Dr. Goenawan Brotosaputro, S.Kom., M.Sc .....

Pembimbing,

Dr. Ir. Nazori Az, M.T .....

Ketua Program Studi

Dr. M. Syafrullah, M.Kom., M.Sc

ABSTRAK

Di era internet sekarang ini transaksi online hampir setiap detik terjadi dan keamanan informasi menjadi suatu tantangan yang harus diselesaikan. Pada tahun 2014-2016 terdapat 36.6 juta insiden serangan *cyber* di Indonesia termasuk pencuriaan data). Kriptografi menjadi salah satu solusi dalam keamanan tersebut yaitu dengan membuat informasi menjadi tidak dimengerti oleh orang lain. Namun dengan kriptografi dinilai kurang cukup, sehingga diperlukan keamanan berlapis dengan metode lainnya seperti steganografi agar pesan tidak dicurigai oleh pihak yang tidak bertanggung jawab, karena hasil kriptografi disisipkan kedalam media digital sehingga informasi tersebut tidak akan menimbulkan kecurigaan oleh orang lain. Algoritma kriptografi yang digunakan adalah AES dan Blowfish dan metode steganografi dengan LSB (*least significant bit*). Pengujian citra dengan *mean square error* dan *peak signal to noise ratio,* yaitu dengan nilai hasil MSE masing-masing 1.814 dan 1.817 serta nilai PSNR 42.29. Untuk pengujian keamanan mengunakan *tools StegSpy 2.1* dengan mendeteksi keberadaan pesan dalam *stegoimage* yang hasilnya tidak terdeteksi di citra PNG.

Kata kunci: kriptografi, steganografi, AES, Blowfish, *least significant bit, mean square error, peak signal to noise ratio, stegoimage.*

ABSTRACT

In today's internet world, online transactions almost every second occur and information security is a challenge that must be resolved. In 2014-2016 there were 36.6 million incidents of cyber attacks in Indonesia including data theft. Cryptography is one of the solutions in security that is by making information not understood by others. However, with cryptography is considered insufficient, so there is a need for layered security with other methods such as steganography so that messages are not suspected by irresponsible parties, because cryptographic results are inserted into digital media so that information will not cause suspicion by others. Cryptgraphic algorithms used are AES and Blowfish and the steganography method with LSB (least significant bit). Image testing with mean square error and peak signal to noise ratio, namely with the MSE results of 1,814 and 1,817 and PSNR 42.29. For security testing use StegSpy 2.1 tools by detecting the presence of messages in stegoimage whose results are not detected in PNG images.

Keywords: cryptography, steganography, AES, Blowfish, least significant bit, mean square error, peak signal to noise ratio, stegoimage.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Segala puji dan syukur senantiasa terpanjatkan ke hadirat Allah SWT yang telah memberikan rahmat dan ridho-Nya sehingga penulis dapat menyelesaikan MENGUNAKAN ALGORITMA AES DAN BLOWFISH DENGAN METODE LSB PADA CITRA PNG".

Sholawat serta salam senantiasa tercurahkan kepada Rasulullah yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu.

Dalam penyusunan proposal tesis ini, penulis menyampaikan terima kasih yang setulusnya kepada:

1. Bapak dan Ibu yang senantiasa memberikan kasih sayang, nasihat, dukungan, semangat, pengorbanan yang tiada tara serta doa yang tak pernah berhenti mengalir.
2. Suamiku tercinta Muhammad Amin S.Sos dan anak-anakku Muhammad Luthfi Abdullah dan Muhammad Yusuf Abdullah yang menjadi penyemangat dalam menyelesaikan tesis ini
3. Bapak Prof. Dr. sc. agr. Ir. Didik Sulistyanto selaku Rektor Universitas Budi Luhur.
4. Bapak Dr.Suhartono, MBA, M.A selaku Direktur Program Pascasarjana Universitas Budi Luhur.
5. Bapak Dr. M. Syafrullah, M.Kom, M.Sc selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
6. Bapak Dr. Ir. Nazori Az, M.T, selaku dosen pembimbing yang telah membimbing dan memotivasi penulis dalam mengerjakan tesis ini.
7. Seluruh Bapak dan Ibu Dosen pengampu mata kuliah di Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang telah sabar memberikan ilmu pengetahuan, pencerahan, dan bimbingan dalam belajar.
8. Sahabat dan teman terbaikku Ismatul Maula S.Kom, yang selalu ada dan membantu dalam penyusunan proposal tesis ini.
9. Intan dan kawan-kawan MKOM UBL Kelas XC, XM di semester 1, 2 dan Kelas SI di semester 3.

"Tiada gading yang tak retak". Penulis menyadari penulisan tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun demi tercapainya penulisan yang lebih baik.

Saran dan kritik dapat dikirimkan ke alamat e-mail st.muryanah@gmail.com.

Wassalamu'alaikum. Wr. Wb.

Jakarta, Agustus 2018

Siti Muryanah

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

Anon, 2016. A Comparative Study and Performance Evaluation of Cryptographic Algorithms : AES and A Comparative Study and Performance Evaluation of Cryptographic Algorithms : AES and Blowfish. , (December).

Anon, SpyHunter. Available at: http://www.spy-hunter.com/stegspydownload.htm [Accessed September 1, 2018].

Baby, D. et al., 2015. A Novel DWT based Image Securing Method using Steganography. *Procedia - Procedia Computer Science*, 46(Icict 2014), pp.612–618. Available at: http://dx.doi.org/10.1016/j.procs.2015.02.105.

Bhardwaj, R. & Sharma, V., 2016. Image Steganography Based on Complemented Message and Inverted bit LSB. *Procedia - Procedia Computer Science*, 93(September), pp.832–838. Available at: http://dx.doi.org/10.1016/j.procs.2016.07.245.

CnnIndonesia, 2018. Mark Zuckerberg Angkat Bicara Soal Skandal Pencurian Data. *cnnindonesia.com*, p.1. Available at: https://www.cnnindonesia.com/teknologi/20180322114136-185-284972/mark-zuckerberg-angkat-bicara-soal-skandal-pencurian-data [Accessed June 10, 2018].

CnnIndonesia, 2016. No Title. *CnnIndonesia*. Available at: https://www.cnnindonesia.com/teknologi/20160111102243-185-103377/jawaban-lengkap-nadiem-soal-bug-aplikasi-gojek?

Gupta, A. & Walia, N.K., 2014. Cryptography Algorithms : A Review. , 2(2), pp.1667–1672.

Gyamfi, E., 2017. Using LSB Steganography Technique and 256 bits Key Length AES Algorithm for High Secured Information Hiding International Journal of Advanced Research in Using LSB Steganography Technique and 256 bits Key Length AES Algorithm for High Secured Information . , (June).