

**IMPLEMENTASI KEAMANAN HASIL SUARA PEMILU DALAM
STEGANOGRAFI CITRA LSB MODIFIKASI MENGGUNAKAN
METODE ECB DAN ELGAMAL**

SKRIPSI

diajukan untuk memenuhi sebagian dari

Syarat Memperoleh Gelar Sarjana Komputer

Program Studi Ilmu Komputer



Oleh :

Muhamad Yogi

1501810

**PROGRAM STUDI ILMU KOMPUTER
DEPARTEMEN PENDIDIKAN ILMU KOMPUTER
FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS PENDIDIKAN INDONESIA**

2019

**IMPLEMENTASI KEAMANAN HASIL SUARA PEMILU DALAM
STEGANOGRAFI CITRA LSB MODIFIKASI MENGGUNAKAN
METODE ECB DAN ELGAMAL**

Oleh

Muhamad Yogi

NIM 1501810

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh
Gelar Sarjana Komputer di Fakultas Pendidikan Matematika dan Ilmu
Pengetahuan Alam

© Muhamad Yogi 2019

Universitas Pendidikan Indonesia

Agustus 2019

Hak Cita Dilindungi Undang-Undang

Skripsi ini tidak boleh diperbanyak seluruhnya atau sebagian, dengan dicetak
ulang, difoto kopi, atau cara lainnya tanpa izin dari penulis

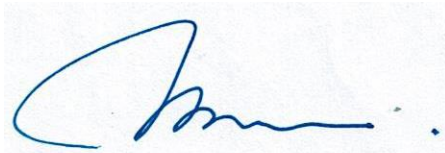
Muhamad Yogi

1501810

**IMPLEMENTASI KEAMANAN HASIL SUARA PEMILU DALAM
STEGANOGRAFI CITRA LSB MODIFIKASI MENGGUNAKAN
METODE ECB DAN ELGAMAL**

DISETUJUI DAN DISAHKAN OLEH PEMBIMBING:

Pembimbing I,



Dr. Muhamad Nursalman, M.T.

NIP. 197909292006041002

Pembimbing II,



Eddy Prasetyo Nugroho, M.T.

NIP. 197505152008011014

Mengetahui,

Ketua Departemen Pendidikan Ilmu Komputer



Lala Septem Riza, MT.Ph.D

NIP. 197809262008121001

PERNYATAAN

Dengan ini penulis menyatakan bahwa skripsi dengan judul “Implementasi Keamanan Pesan Rahasia dalam steganografi Citra LSB Modifikasi Untuk Mengatasi Bentuk Kecurangan Pada Pemilu” ini beserta seluruh isinya adalah benar-benar karya penulis sendiri. Penulis tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, penulis siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya penulis ini.

Bandung, Agustus 2019
Yang Membuat Pernyataan,

Muhamad Yogi
NIM 1501810

IMPLEMENTASI KEAMANAN HASIL SUARA PEMILU DALAM STEGANOGRAFI CITRA LSB MODIFIKASI MENGGUNAKAN METODE ECB DAN ELGAMAL

Oleh

Muhamad Yogi – muhamad_yogi@student.upi.edu
1501810

ABSTRAK

Dalam hasil suara pemilihan umum Presiden dan Wakil Presiden pada tahun 2019 telah terjadinya tudingan-tudingan bentuk kecurangan dalam perubahan hasil suara maupun berbagai bentuk lainnya. Setelah menganalisa bentuk kecurangan perubahan hasil suara tersebut maka penulis mengatasi dengan steganografi untuk mengamankan pesan hasil suara. Setelah penulis melakukan studi literatur penulis menggunakan steganografi dengan teknik *Least Significant Bit* (LSB) dikarenakan teknik tersebut mempunyai pengacakan penempatan pada bit-bit pixel citra secara teratur dan tidak terlalu mengacak. Agar pesan hasil suara tersebut keamanannya lebih terjadi penulis menggunakan dua metode simetris dan asimetris untuk enkripsi dan dekripsi pesan tersebut, metode pertama untuk enkripsi rahasia yaitu mode *Electronic Code Book* (ECB) sedangkan enkripsi dan dekripsi metode asimetris yaitu menggunakan algoritma elgamal. Algoritma elgamal memproses *generate* kunci dengan bilangan cukup besar hingga dapat dikatakan hasil karakter *ciphertext* lebih banyak dari karakter sebelumnya. Agar penelitian ini berhasil maka penulis menguji steganografi citra dengan aplikasi retas, salah satunya adalah *stegSpy* setelah melakukan uji coba keamanan pesan di dalam citra LSB modifikasi, aplikasi *stegSpy* tidak dapat mendeteksi adanya pesan dalam citra tersebut.

Kata kunci: pemilu 2019, kriptografi simetris, kriptografi asimetris, steganografi LSB modifikasi

SECURITY IMPLEMENTATION OF ELECTION SOUND RESULT IN MODIFICATION OF LSB IMAGE STEGANOGRAPHY USING ECB AND ELGAMAL METHODS

Arranged by

*Muhamad Yogi --- muhamad_yogi@student.upi.edu
1501810*

ABSTRACT

In the results of 2019 presidential and vice presidential election there have been allegations of fraud in forms of changing voting results or various other fraudulent form. After analyzing the forms of fraudulent in changing voting result, the author comes up with steganograph to secure voting result message. After conducting literature study, the author chooses to use steganograph with Least Significant Bit (LSB) method due to its placement randomization on image pixel bits that is quite regular and not too random. To ensure the security of voting result message, the author uses two methods of symmetrical and asymmetrical both for message encryption and decryption. The first method of encryption used is Electronic Code Book (ECB) mode, as for asymmetrical encryption and decryption Elgamal algorithm is used. Elgamal algorithm processes key generate with numbers large enough to be able to say that chipertext character result is more in amount than previous character. In order for this study to succeed, the author tests image steganography using hacking application, one of which is stegSpy. After testing the message security in modified LSB image, stegSpy can not detect the message contained in the image.

Keywords: 2019 election, symmetrical cryptography, assymetrical cryptography, modified LSB steganograph

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah swt. Karena haya dengan kehendak, berkat, serta karunia-Nya lah penulis dapat menyelesaikan skripsi yang berjudul “Implementasi Keamanan Hasil Suara Pemilu Dalam Steganografi Citra LSB Modifikasi Menggunakan Metode ECB Dan Elgamal” ini dapat terselesaikan.

Penyusunan skripsi ini ditunjukan untuk memenuhi dan melengkapi salah satu syarat untuk penyusunan skripsi yang merupakan syarat untuk mendapatkan gelar sarjana komputer atas jenjang studi S1 pada Program Studi Ilmu Komputer Fakultas Pendidikan Matematika dan Ilmu Pengetahuan Alam Universitas Pendidikan Indonesia.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat banyak kekurangan dan keterbatasan yang perlu disempurnakan. Oleh karena itu, penulis sangat mengharapkan saran maupun kritik yang membangun agar tidak terjadi kesalahan yang sama dikemudian hari dan dapat meningkatkan kualitas tahap lebih baik.

Bandung, Agustus 2019

Penyusun

UCAPAN TERIMAKASIH

Alhamdulillahirabilalamin, puji dan syukur kehadiran Allah SWT Yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis diberikan kelancaran dalam menyelesaikan penulisan skripsi ini. Dalam proses menyelesaikan penelitian dan penyusunan skripsi ini, peneliti banyak mendapat bimbingan, dorongan, serta bantuan dari berbagai pihak. Oleh karena itu, pada kesempatan ini peneliti mengucapkan terimakasih serta penghargaan yang setinggi-tingginya, kepada:

1. Kedua orang tua yaitu Drs. Atong Effendi dan Ety Kurniasih yang selalu memberikan doa dan dukungan moral dan materil, serta selalu menjadi penyemangat utama dalam menempuh pendidikan tinggi sehingga penulis dapat menyelesaikan skripsi ini.
2. Kakak saya Erna Karnia, S.E yang selalu memberikan doa dan dukungan moral dan materil, serta selalu menjadi penyemangat dalam menempuh pendidikan tinggi sehingga penulis dapat menyelesaikan skripsi ini.
3. Seluruh bagian keluarga yang selalu memberikan doa dan dukungan moral, serta selalu menjadi penyemangat dalam menempuh skripsi ini.
4. Bapak Yaya Wihardi, M.kom. selaku Pembimbing Akademik yang telah membimbing secara akademik pada awal perkuliahan hingga akhir perkuliahan demi terselesaikannya perkuliahan ini.
5. Bapak Dr. Muhammad Nursalman, M.T. selaku Pembimbing I atas segala waktu yang dicurahkan untuk membimbing penulis demi terselesaikannya penelitian skripsi ini.
6. Bapak Eddy Prasetyo Nugroho, M.T. selaku Pembimbing II yang telah memberikan saran kepada penulis selama proses penyelesaian penulisan skripsi.
7. Bapak Lala Septem Riza, MT.Ph.D selaku Kepala Departemen Pendidikan Ilmu Komputer FPMIPA Universitas Pendidikan Indonesia sekaligus penguji II yang telah menguji penelitian ini agar isi penulisan penelitian lebih baik.
8. Bapak Dr. Yudi Wibisono, M.T. selaku penguji III yang telah menguji penelitian ini agar isi penulisan penelitian lebih baik.
9. Ibu Dr. Rani Megasari, M.T. selaku Ketua Program Studi Ilmu Komputer yang telah memberikan kesempatan kepada penulis untuk melakukan sidang.
10. Bapak dan Ibu Dosen Prodi Pendidikan Ilmu Komputer dan Ilmu Komputer yang telah berbagi ilmu yang sangat bermanfaat kepada penulis.

11. Sahabat Itok Meti, Farhan, Dimas, Rahman, Arga, Adie, Hapidz, Fiko, Trisna, Ammar, Fakhri yang senantiasa memberikan dukungan, semangat, canda dan tawa kepada penulis baik selama proses perkuliahan maupun selama proses pengerjaan skripsi.
12. Endah Permatasari selaku orang terdekat penulis yang selalu memberikan segala dukungan untuk penulis dalam menjalani hidup.
13. Kelas C 2015, yang sama-sama berjuang dari awal perkuliahan dari awal hingga ke titik akhir perkuliahan
14. Semua pihak yang telah membantu penulis dalam menyelesaikan skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Semoga semua amal baik yang telah diberikan kepada penulis mendapatkan balasan yang berlipat dari Allah SWT. Aamiin.

Bandung, Agustus 2019

Muhamad Yogi

DAFTAR ISI

ABSTRAK.....	ii
<i>ABSTRACT</i>	iii
KATA PENGANTAR.....	iv
UCAPAN TERIMAKASIH	v
DAFTAR ISI	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR	xi
DAFTAR PUSTAKA	xiii
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	5
1.3 Tujuan Penelitian	6
1.4 Manfaat Penelitian	6
1.5 Batasan Masalah	6
1.6 Sistematika Penulisan.....	6
BAB 2 KAJIAN PUSTAKA	8
2.1 Jaringan Komputer.....	8
2.2 Keamanan Komputer	8
2.3 Kriptografi	10
2.3.1 Tujuan Kriptografi	11
2.3.2 Metode Kriptografi	12
2.3.3 Metode Simetris.....	14
2.3.4 Metode Asimetris.....	15
2.3.5 Metode Algoritma Elgamal	15

2.4	Metode Blok <i>Chiper</i>	17
2.4.1	Mode Operasi Cipher Blok.....	18
2.4.2	Electronic Code Book (ECB)	18
2.4.3	Cipher Block Chaining (CBC)	20
2.4.4	Cipher Feedback (CFB)	23
2.4.5	Output Feedback (OFB).....	24
2.5	Steganografi.....	25
2.5.1	Metode <i>Least Significant Bit</i> (LSB).....	28
2.5.2	Ukuran data Yang disembunyikan.....	29
2.6	Header citra/gambar format JPG	29
2.7	Modifikasi Metode <i>Least Significant Bit</i> (LSB).....	31
BAB 3	METODOLOGI PENELITIAN.....	33
3.1	Desain Penelitian	33
3.2	Metode penelitian.....	35
3.3	Alat dan Bahan Penelitian	40
3.3.1	Alat Penelitian	40
3.3.2	Bahan Penelitian	40
3.4	Teknik Analisis	40
BAB 4	HASIL DAN PEMBAHASAN.....	41
4.1	Pengumpulan Data.....	41
4.1	Perancangan Model.....	44
4.2	Pengembangan Sistem	45
4.2.1	Analisis.....	46
4.2.2	Desain.....	47
4.2.3	Coding	47
4.2.4	Pengujian.....	70
4.2.5	Analisa Hasil Uji.....	76

BAB 5 KESIMPULAN DAN SARAN..... 80

5.1 Kesimpulan..... 80

5.2 Saran..... 80

DAFTAR TABEL

Tabel 2.1 Data layout dari file JPG (jpg-signature-format @ www.file-recovery.com, n.d.)	29
Tabel 2.2 Data header dan footer file.....	30
Tabel 4.1 Pseudocode enkripsi metode simetris mode ECB.....	48
Tabel 4.2 <i>Pseudocode</i> dari enkripsi metode asimetris algoritma elgamal	52
Tabel 4.3 <i>Pseudocode</i> penyisipan pesan dengan steganografi LSB modifikasi ...	56
Tabel 4.4 <i>Pseudocode</i> ekstraksi steganografi citra LSB modifikasi	61
Tabel 4.5 <i>Pseudocode</i> dekripsi metode asimetris algoritma elgamal	66
Tabel 4.6 <i>Pseudocode</i> dekripsi metode simetris mode ECB	69
Tabel 4.7 Analisa Hasil Pengujian Enkripsi.....	76
Tabel 4.8 Analisa Hasil pengujian Dekripsi.....	77
Tabel 4.9 Empat bentuk keamanan kriptografi	78

DAFTAR GAMBAR

Gambar 2.1 Skema enkripsi dan dekripsi (Liwandouw et al., 2017).....	13
Gambar 2.2 Enkripsi dan Dekripsi algoritma simetris (Dafid, 2006).....	14
Gambar 2.3 Skema Algoritma Asimetris (Sanyal, 2014)	15
Gambar 2.4 Skema enkripsi dan dekripsi dengan mode ECB (Munir, 2004).....	19
Gambar 2.5 Skema enkripsi dan dekripsi dengan mode CBC (Munir, 2004)	21
Gambar 2.6 Mode CFB (Bruce, 1996).....	23
Gambar 2.7 Mode OFB (Bruce, 1996)	24
Gambar 2.8 Skema penempatan bit (Munir, 2004)	28
Gambar 2.9 Bit-bit penempatan LSB pada citra (Munir, 2004).....	28
Gambar 3.1 Desain Penelitian	33
Gambar 3.2 Metode enkripsi dan penyisipan teks pada citra di aplikasi	36
Gambar 3.3 Metode dekripsi dan unsteغانografi LSB pada citra di aplikasi	38
Gambar 4.1 Model Proses data hasil suara disisipkan ke dalam citra formulir C1	44
Gambar 4.2 Model proses bisnis	45
Gambar 4.3 Flowchat enkripsi metode simetris mode ECB	48
Gambar 4.4 <i>Coding</i> Enkripsi Simetris Mode ECB.....	49
Gambar 4.5 <i>Ouput</i> Metode Enkripsi Simetris Mode ECB.....	50
Gambar 4.6 <i>Flowchart</i> enkripsi metode asimetris algoritma elgamal.....	51
Gambar 4.7 <i>Flowchart</i> penyisipan pesan dengan steganografi LSB modifikasi ..	55
Gambar 4.8 Implementasi <i>Coding</i> Steganografi Citra LSB Modifikasi.....	59
Gambar 4.9 Hasil <i>Output</i> citra Steganografi LSB modifikasi.....	60
Gambar 4.10 <i>Flowchart</i> ekstraksi steganografi citra LSB modifikasi	61
Gambar 4.11 Implentasi <i>Coding</i> Ekstraksi citra.....	63
Gambar 4.12 Hasil <i>Output</i> Ekstraksi Citra	64
Gambar 4.13 <i>Flowchart</i> dekripsi metode asimetris algoritma elgamal	65
Gambar 4.15 Hasil <i>Output</i> Dekripsi Algoritma Elgamal.....	67
Gambar 4.14 Implemtasi <i>Coding</i> Dekripsi Algoritma Elgamal	67
Gambar 4.16 <i>Flowchart</i> dekripsi metode simetris mode ECB	68
Gambar 4.17 Implementasi <i>Coding</i> Dekripsi Mode ECB	69

Gambar 4.18 Hasil <i>Output</i> Metode simetris Mode ECB	70
Gambar 4.19 Pengujian Citra yang Berisikan Pesan Rahasia	71
Gambar 4.20 Pengujian Tanpa Algoritma Elgamal.....	72
Gambar 4.21 Hasil Pengujian Tanpa Algoritma Elgamal.....	72
Gambar 4.22 Pengujian citra dengan kualitas buram	73
Gambar 4.24 Pengujian <i>StegSpy</i> dengan kualitas citra buram	74
Gambar 4.23 Pengujian dekripsi dan ekstraksi citra formulir C1 kualitas Buram	74
Gambar 4.25 Hasil Pengujian Aplikasi Dengan Angka dan Simbol	75
Gambar 4.26 Pengujian Aplikasi Dengan Angka dan Simbol	76

DAFTAR PUSTAKA

- Aditya, Y., Pratama, A., & Nurlifa, A. (2010). *Studi pustaka untuk steganografi dengan beberapa metode*. 2010(Snati), 32–35.
- Andrian, Y. (2013). Modifikasi Metode Least Significant Bit (LSB). 23–24.
- Cahyadi, T. (2012). Implementasi steganografi lsb dengan enkripsi vigenere cipher pada citra jpeg. *Transient*, 1(4), 281–288. Retrieved from <http://ejournal-s1.undip.ac.id/index.php/transient/article/viewFile/1284/1306>
- Bruce, Schneier. (1996). *Applied Cryptography, Second Edition Protocol, Algorithms and Source Code in C*. John Wiley and Sons, Inc.
- Dafid, D. (2006). Kriptografi Kunci Simetris Dengan Menggunakan Algoritma Crypton. *Jurnal Ilmiah STMIK*, 2, 20–27.
- Diffie, W., Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. <https://doi.org/10.1109/TIT.1976.1055638>
- Hasugian, A. H. (2017). Implementasi Algoritma Hill Cipher. (August 2013). *jpg-signature-format @ www.file-recovery.com*. (n.d.).
- Keraf A. Sonny. (2001). Books @ Books.Google.Co.Id. *Kanisius*, p. 160.
- Liwandouw, V., dan, A. W.-S. T. I. (2017). Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris. *Researchgate.Net*, (March).
- Maradilla, T. (2012). *Aplikasi Steganografi Untuk Penyisipan Data Teks Ke dalam Citra Digital*.
- Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography*, 1–48.
- Munir, R. (2004). *Steganografi dan Watermarking Departemen Teknik Informatika Institut Teknologi Bandung*. *Bahan Kuli*, 1–7.
- Munir, R. (2004). Tipe dan Mode Algoritma Simetri Departemen Teknik Informatika Institut Teknologi Bandung. (Bagian 2), 1–18.

- Nani, P. A. (2011). Penerapan Enkripsi Algoritma Blowfish Pada Proses Steganografi Metode Eof. *Snatika*, (Vol 1, No 1 (2011): SNATIKA 2011). Retrieved from <http://ejournal.aptikomid.org/index.php/snatika/article/view/53/55>
- Sasongko, J. (2005). Pengamanan Data Informasi menggunakan Kriptografi Klasik. *Jurnal Teknologi Informasi DINAMIK*, X(3), 160–167.
- Munir, R. (2008). *Pengantar Ilmu Kriptografi Departemen Teknik Informatika Institut Teknologi Bandung*, 1-16.
- Indonesia, C. (2019, Mei 27). *BPN Adukan 5 Bentuk Kecurangan Pemilu, Buktinya Berita Online*. Retrieved from CNN Indonesia: <https://www.cnnindonesia.com/nasional/20190527015637-32-398584/bpn-adukan-5-bentuk-kecurangan-pemilu-buktinya-berita-online>
- Indonesia, C. (2019, April 09). *Jokowi Tetapkan 17 April 2019 Hari Libur Nasional*. Retrieved from CNN Indonesia: <https://www.cnnindonesia.com/nasional/20190409143509-32-384590/jokowi-tetapkan-17-april-2019-hari-libur-nasional>
- Massandy, D. T. (2016). ALGORITMA ELGAMAL DALAM PENGAMANAN PESAN RAHASIA. 1 - 5.
- Munir, R. (2006). KRIPTOGRAFI. *Penerbit Informatika*, 304.
- News, D. (2019, Mei 29). *Menakar Kecurangan Pemilu*. Retrieved from Detik News: https://news.detik.com/kolom/d-4569912/menakar-kecurangan-pemilu?_ga=2.41625570.1787817198.1565884231-976932813.1560071021
- News, T. (2019, Mei 7). *Ini Cara Mudah Ketahui Form C1 Asli atau Palsu*. Retrieved from Tribun News: <https://www.tribunnews.com/pilpres-2019/2019/05/07/ini-cara-mudah-ketahui-form-c1-asli-atau-palsu>
- News, T. (2019, April 21). *Temuan Kesalahan Input Data Penghitungan Suara, Ketua KPU: Tidak Ada Niat Curang*. Retrieved from Tribun News: <https://www.tribunnews.com/pilpres-2019/2019/04/21/temuan-kesalahan-input-data-penghitungan-suara-ketua-kpu-tidak-ada-niat-curang?page=2>
- Rochmat, dkk, N. (2012). IMPLEMENTASI ALGORITMA KRIPTOGRAFI ELGAMAL UNTUK KEAMANAN PESAN (MESSAGE SECURITY). *TRANSIENT, VOL. 1, NO. 3, SEPTEMBER 2012, ISSN: 2302-9927, 83, 1 - 7.*

Sanyal, D. (. (2014). A comparative survey of symmetric and asymmetric key. *International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, 1 - 11.

Tamam, M. T. (2010). Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra. *Jurnal EECCIS Vol. IV*, 1 - 4.