

**KRIPTOGRAFI PENGAMANAN DATA FILE BERUPA
GAMBAR MENGGUNAKAN METODE RSA DAN *DIGITAL*
*SIGNATURE***

SKRIPSI



Disusun oleh:

Surya Agung Pratama

15 621 016

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH GRESIK

2020

**KRIPTOGRAFI PENGAMANAN DATA FILE BERUPA
GAMBAR MENGGUNAKAN METODE RSA DAN *DIGITAL*
*SIGNATURE***

Diajukan sebagai syarat memperoleh gelar Sarjana Komputer
Program Studi Informatika Jenjang S-1 Fakultas Teknik
Universitas Muhammadiyah Gresik



Oleh:

Surya Agung Pratama

15 621 016

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH GRESIK**

2020

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat serta karunia-Nya kepada kita semua sehingga penulis dapat menyelesaikan Skripsi dengan judul **“KRIPTOGRAFI PENGAMANAN DATA FILE BERUPA GAMBAR MENGGUNAKAN METODE RSA DAN *DIGITAL SIGNATURE* ”**. Shalawat serta salam tak lupa kita ucapkan kepada junjungan kita Nabi Besar Muhammad SAW. Dalam menyelesaikan skripsi ini, penulis mengucapkan banyak terima kasih kepada semua pihak yang telah membantu dalam pembuatan Skripsi ini. Untuk itu tidak lupa penulis mengucapkan banyak terima kasih kepada :

1. Kedua orang tua, keluarga, dan kekasih, sahabat, teman kampus maupun kampung yang selalu memberikan semangat dan bantuan berupa moril dan materiil.
2. Bapak Harunur Rosyid, S.T., M.Kom., selaku dosen pembimbing.
3. Bapak Darmawan Aditama, S.Kom., M.T. selaku Ketua Program Studi Teknik Informatika Universitas Muhammadiyah Gresik.
4. Teman-teman angkatan 2015, 2016 dan 2017 Fakultas Teknik Program Studi Teknik Informatika Universitas Muhammadiyah Gresik yang selalu memberikan semangat.
5. Zain Kholisotul Ma'rufah selaku kekasihku yang selalu mensupport dan menyemangatiku tiada henti dan lelah.

Sebagai manusia biasa, penulis menyadari bahwa masih banyak kekurangan dalam penyusunan Skripsi ini. Oleh karena itu, penulis mohon saran dan kritik agar berguna dalam pembuatan skripsi selanjutnya.

Gresik, 16 Januari 2020

Surya Agung Pratama

KRIPTOGRAFI PENGAMANAN DATA FILE GAMBAR MENGGUNAKAN METODE RSA DAN *DIGITAL SIGNATURE*

Oleh

Surya Agung Pratama

15 621 016

Diajukan kepada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Gresik, pada tanggal *16 Januari 2020* untuk memenuhi sebagian persyaratan untuk memperoleh gelar derajat sarjana S-1 Program Studi Teknik Informatika

INTISARI

Pengamanan berupa data adalah hal yang sangat sensitif dalam menjaga sebuah kerahasiaan data ataupun informasi. Penggunaan informasi berupa gambar sudah sering dipergunakan dari jaman dahulu. Akan tetapi, penggunaan media informasi melalui gambar memiliki beberapa kelemahan, mudahnya file berupa gambar tersebut dirubah oleh pihak yang tidak memiliki kepentingan. Dengan cara menerapkan metode tanda tangan digital dan Algoritma RSA dalam hal pengamanan data file berupa gambar dapat mengetahui penerapan metode *Digital Signature* dengan Algoritma RSA dalam proses pengamanan file berupa gambar. Penelitian yang akan dilakukan adalah dengan mengkombinasikan metode RSA dengan metode DSA (*Digital Signature Algoritma*). Algoritma RSA merupakan salah satu algoritma enkripsi terkuat saat ini, dan lebih baik dibanding DSA ataupun SED *Digital signature* dapat diimplementasikan menggunakan algoritma RSA dan MD5 sehingga berfungsi menguji keutuhan dan otentifikasi suatu dokumen digital. Pengujian membuktikan bahwa dapat dideteksi perubahan dokumen dari hasil manipulasi rotasi, *mirror*, *crop*, *resize* dan manipulasi *pixel*. Penyisipan dilakukan dengan menggunakan algoritma *embedding* pada tiap warna. Pada file jenis PNG, Setelah penyisipan, maka dikembalikan ke format PNG, sehingga menyebabkan ukuran file citra digital penelitian dapat diarahkan untuk mendeteksi lokasi perubahan pada dokumen file berupa gambar. Jika deteksi dapat dilakukan, maka dapat dipisahkan antara piksel asli, dengan piksel termanipulasi. Sehingga pada bagian piksel yang asli masih dapat dimanfaatkan untuk informasi di dalamnya.

Kata kunci : Digital Signature, RSA, gambar, pengamanan data

Pembimbing : Harunur Rosyid, ST, M.KOM.

CRYPTOGRAPHY OF SECURING IMAGE FILE DATA USING RSA METHODS AND DIGITAL SIGNATURE

by

Surya Agung Pratama

15 621 016

Submitted to the Informatics Engineering Study Program, Faculty of Engineering, Muhammadiyah University Gresik, on January 16, 2020, to fulfill some of the requirements to obtain a Bachelor's degree in the Informatics Engineering Study Program.

Abstract

Security in the form of data is a very sensitive thing in maintaining the confidentiality of data or information. The use of information in the form of images has often been used from time immemorial. By applying the digital signature method and the RSA Algorithm in terms of securing data files in the form of images, you can find out the application of the Digital Signature method with the RSA Algorithm in the process of securing files in the form of images. The research that will be conducted is to combine the RSA method with the DSA (Digital Signature Algoritem) method. The RSA algorithm is one of the strongest encryption algorithms at this time, and better than DSA or SED Digital signature can be implemented using the RSA and MD5 algorithms so that it functions to test the integrity and authentication of a digital document. Testing proves that document changes can be detected from the results of rotational manipulation, mirrors , crop, resize and pixel manipulation. Insertion is done using the embedding algorithm for each color. In the PNG file type, after insertion, it is returned to PNG format, causing the research digital image file size to be directed to detect the location of changes in the document file in the form of an image. If detection is possible, it can be separated between the original pixels and the manipulated pixels. So that the original pixel can still be used for information in it.

Keywords : Digital Signature, RSA, pictures, data security

Supervisor : Harunur Rosyid, ST, M.KOM.



DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN JUDUL DALAM.....	ii
HALAMAN PERNYATAAN	iii
HALAMAN PERSETUJUAN	iv
HALAMAN PENGESAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR KODE PROGRAM.....	xiii
INTISARI	xiv
ABSTRACK	xv
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan Penelitian	3
1.4 Manfaat Masalah	3
1.5 Batasan Penelitian	3
1.6 Metodologi Penelitian	3
1.7 Sistematika Penelitian	4
BAB II LANDASAN TEORI	
2.1 Kriptografi	6
2.1.1 Pesan, Plaintext, dan Cipertext	7
2.1.2 Enkripsi dan Dekripsi.....	8
2.1.3 Macam-macam Algoritma Kriptografi	9
2.1.4 Tujuan Kriptografi	11
2.2 RSA (Rivest-Shamir-Adleman)	12

2.3 Tandatangan Digital	15
2.3.1 Sifat Umum dari Tanda Tangan Digital	15
2.3.2 Penandatanganan Pesan	16
2.4 Gambar	19
2.4.1 Jenis – Jenis Gambar	19
2.1.2 Format Gambar	19
2.5 Penelitian Sebelumnya	22
BAB III ANALISIS DAN PERANCANGAN SISTEM	
3.1 Analisis.....	24
3.2 Hasil Analisis	24
3.3 Dekripsi Sistem	25
3.3.1 Pembentukan Kunci	27
3.3.1.1 <i>Pre-Processing</i>	27
3.3.1.2 Pembangkitan Kunci <i>Public</i>	29
3.3.1.3 Pembangkitan Kunci <i>Private</i>	29
3.3.2 Pembentukan <i>Message Digest</i>	30
3.3.3 Pembentukan <i>Digital Signature</i>	32
3.3.4 Proses Verifikasi <i>Digital Signature</i>	36
3.4 Perancangan Sistem	37
3.4.1 <i>Use Case Diagram</i>	37
3.4.2 <i>Sequence Diagram</i>	41
3.4.3 <i>Activity Diagram</i>	43
3.5 Kebutuhan Pembuatan Sistem	45
3.5.1 Spesifikasi Perangkat Keras (<i>Hardware</i>).....	45
3.5.2 Spesifikasi Perangkat Lunak (<i>Software</i>)	46
3.6 Struktur Model Sistem	46
3.7 <i>Pre - Processing</i>	47
3.8 Perancangan Antarmuka Sistem	51
3.8.1 Antarmuka Form Pembentukan Kunci	51

3.8.2 Antarmuka Form Enkripsi	52
3.8.3 Antarmuka Form Dekripsi	52
3.8.4 Antarmuka Form <i>Tools</i>	53
3.8.5 Antarmuka Form <i>Help</i>	54
3.9 Skenario Pengujian.....	54
3.9.1 Pengujian RSA.....	54
3.9.2 Pengujian <i>Digital Signature</i>	55
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM	
4.1 Implementasi Sistem.....	56
4.1.1 Halaman Awal	56
4.1.2 Halaman Verifikasi	59
4.2 Pengujian Sistem.....	61
4.2.1 Halaman Awal.....	61
4.2.2 Halaman Verifikasi	62
4.3 Analisa Hasil Pengujian Sistem	62
4.3.1 Uji Otentikasi	63
4.3.2 Uji <i>Integrity</i>	64
BAB V PENUTUP	
5.1 Kesimpulan	67
5.2 Saran.....	67
DAFTAR PUSTAKA	57

DAFTAR TABEL

Tabel 2.1 Parameter RSA.....	13
Tabel 3.1 Contoh Susunan Nilai Warna Pada File Gambar	33
Tabel 3.2 Contoh Hasil Proses Tahap Pertama: Pembuatan Ringkasan/Hash	33
Tabel 3.3 Contoh Hasil Proses Tahap Pertama: Pembuatan Ringkasan/Hash	34
Tabel 3.4 Dokumentasi Naratif <i>Use - Case</i> Enkripsi File Gambar	38
Tabel 3.5 Dokumentasi Naratif <i>Use - Case</i> Enkripsi Kunci RSA.....	38
Tabel 3.6 Dokumentasi Naratif <i>Use - Case</i> Dekripsi Kunci RSA	39
Tabel 3.7 Dokumentasi Naratif <i>Use - Case</i> Dekripsi File Gambar.....	40
Tabel 3.8 Dokumentasi Naratif <i>Use - Case</i> Bangkitkan Kunci RSA.....	40
Tabel 3.9 Dokumentasi Naratif <i>Use - Case Digital Signature</i>	41

DAFTAR GAMBAR

Gambar 3.1 Gambaran Sistem Pengamanan File Berupa Gambar Menggunakan <i>Digital Signature</i> Dan Metode RSA	25
Gambar 3.2 Alur Pembentukan Kunci	27
Gambar 3.3 Alur Pembentukan <i>Message Digest</i>	31
Gambar 3.4 Alur Pemberian <i>Digital Signature</i>	32
Gambar 3.5 Alur Proses Verifikasi <i>Digital Signature</i>	36
Gambar 3.6 <i>Use Case Diagram</i>	37
Gambar 3.7 <i>Sequence Diagram</i> Proses Enkripsi	42
Gambar 3.8 <i>Sequence Diagram</i> Proses Dekripsi	43
Gambar 3.9 <i>Activity Diagram</i> Proses Enkripsi	44
Gambar 3.10 <i>Activity Diagram</i> Proses Dekripsi	45
Gambar 3.11 Struktur Model Sistem	47
Gambar 3.12 <i>Pre-Processing</i>	47
Gambar 3.13 Gambar <i>RGB</i> (304 x 304)	48
Gambar 3.14 Perbesar Gambar	49
Gambar 3.15 <i>Pixel</i> Pada Gambar	49
Gambar 3.16 Gambar <i>GreyScale</i>	51
Gambar 3.17 <i>Form</i> Pembentukan Kunci	51
Gambar 3.18 <i>Form</i> Enkripsi	52
Gambar 3.19 <i>Form</i> Dekripsi	53
Gambar 3.20 Menu <i>Tools</i>	53
Gambar 3.21 Menu <i>Help</i>	54

DAFTAR KODE PROGRAM

Kode Program 4.2 enkripsi.....	57
Kode Program 4.3 Browse file gambar.....	57
Kode Program 4.4 <i>signature</i> awal.....	58
Kode Program 4.5 <i>encrypt and embed</i>	59
Kode Program 4.7 Verifikasi.....	61

