PEMBANGUNAN PERANGKAT LUNAK STEGANOGRAFI MENGGUNAKAN TEKNIK *DYNAMIC CELL SPREADING* (DCS) DAN *DIGITAL SIGNATURE ALGORITHM* (DSA) UNTUK KEAMANAN DATA



Disusun oleh :

Rezki Nugraha

10107316


Apa itu steganografi?

While in Paris on business, Harvard symbologist Robert Langdon receives an urgent late-night phone call. The elderly curator of the Louvre has been murdered inside the museum, a baffling cipher found near the body. As Langdon and a gifted French cryptologist, Sophie Neveu, sort through the bizarre riddles, they are stunned to discover a trail of clues hidden in the works of Da Vinci—clues visible for all to see and yet ingeniously disguised by the painter.

The stakes are raised when Langdon uncovers a startling link: The late curator was involved in the Priory of Sion—an actual secret society whose members included Sir Isaac Newton, Botticelli, Victor Hugo, and Da Vinci, among others. Langdon suspects they are on the hunt for a breathtaking historical secret, one that has proven through the centuries to be as enlightening as it is dangerous. In a frantic race through Paris, and beyond,

(continued on back flap)

(continued from front flap)

Langdon and Neveu find themselves matching wits with a faceless powerbroker who appears to anticipate their every move. Unless they can decipher the labyrinthine puzzle, the Priory's secret—and an explosive ancient truth—will be lost forever.

Breaking the mold of traditional suspense novels, *The Da Vinci Code* is simultaneously lightning-paced, intelligent, and intricately layered with remarkable research and detail. From the opening pages to the unpredictable and stunning conclusion, bestselling author Dan Brown proves himself a master storyteller.

Contoh :

Is there no help for the widows son

Cukup amankah untuk menjaga keamanan isi datanya?

Kriteria apa yang dimiliki steganografi?



Impercepbility



Fidelity



Recovery

Apa yang kita butuhkan untuk menjaga keamanan isi datanya?


Digital
Signature

Kriteria apa yang dimiliki digital signature?



Confidentiality dan privacy



Authentication



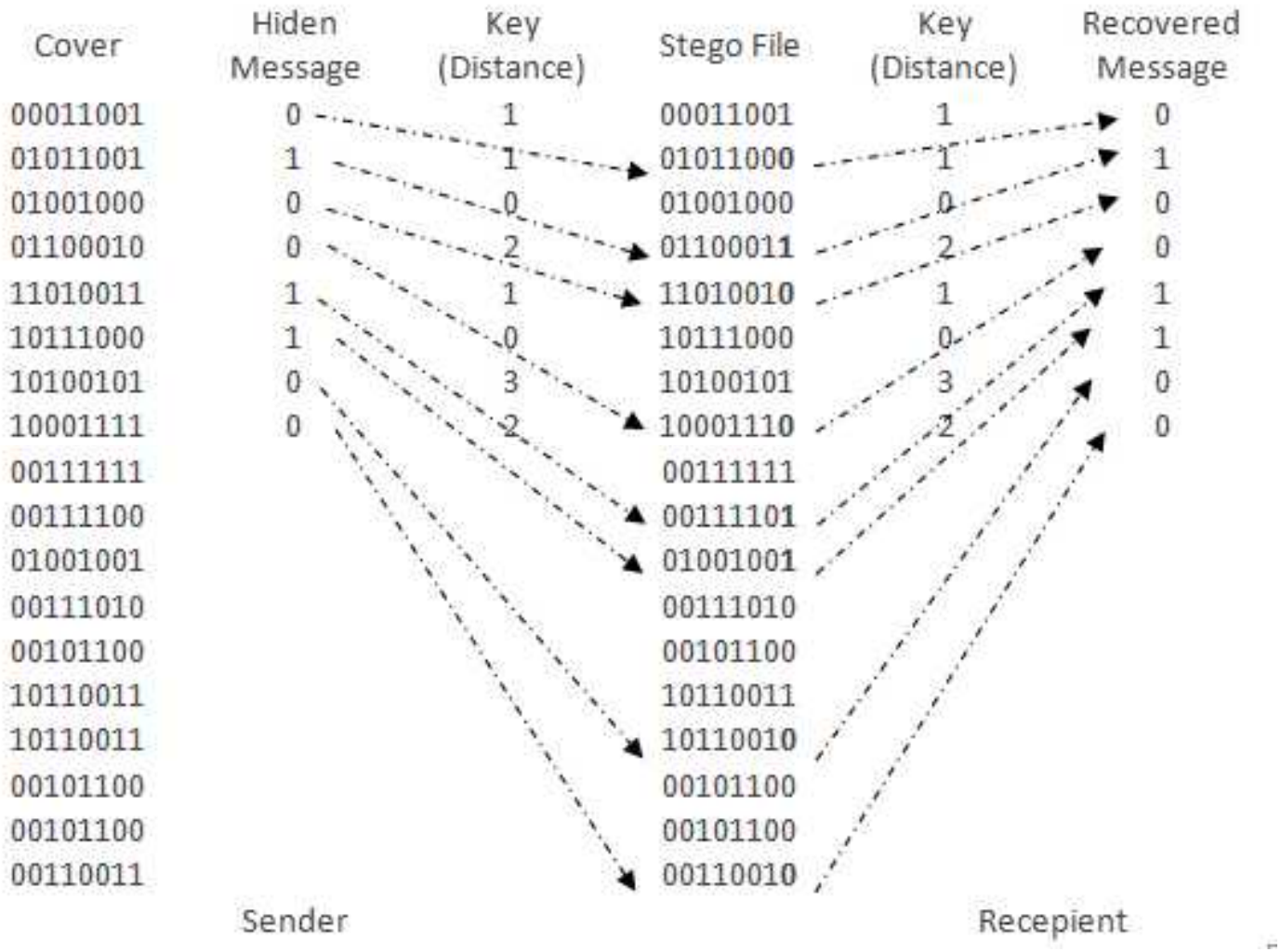
Integrity



Nonrepudation

Apa itu Dynamic Cell Spreading?

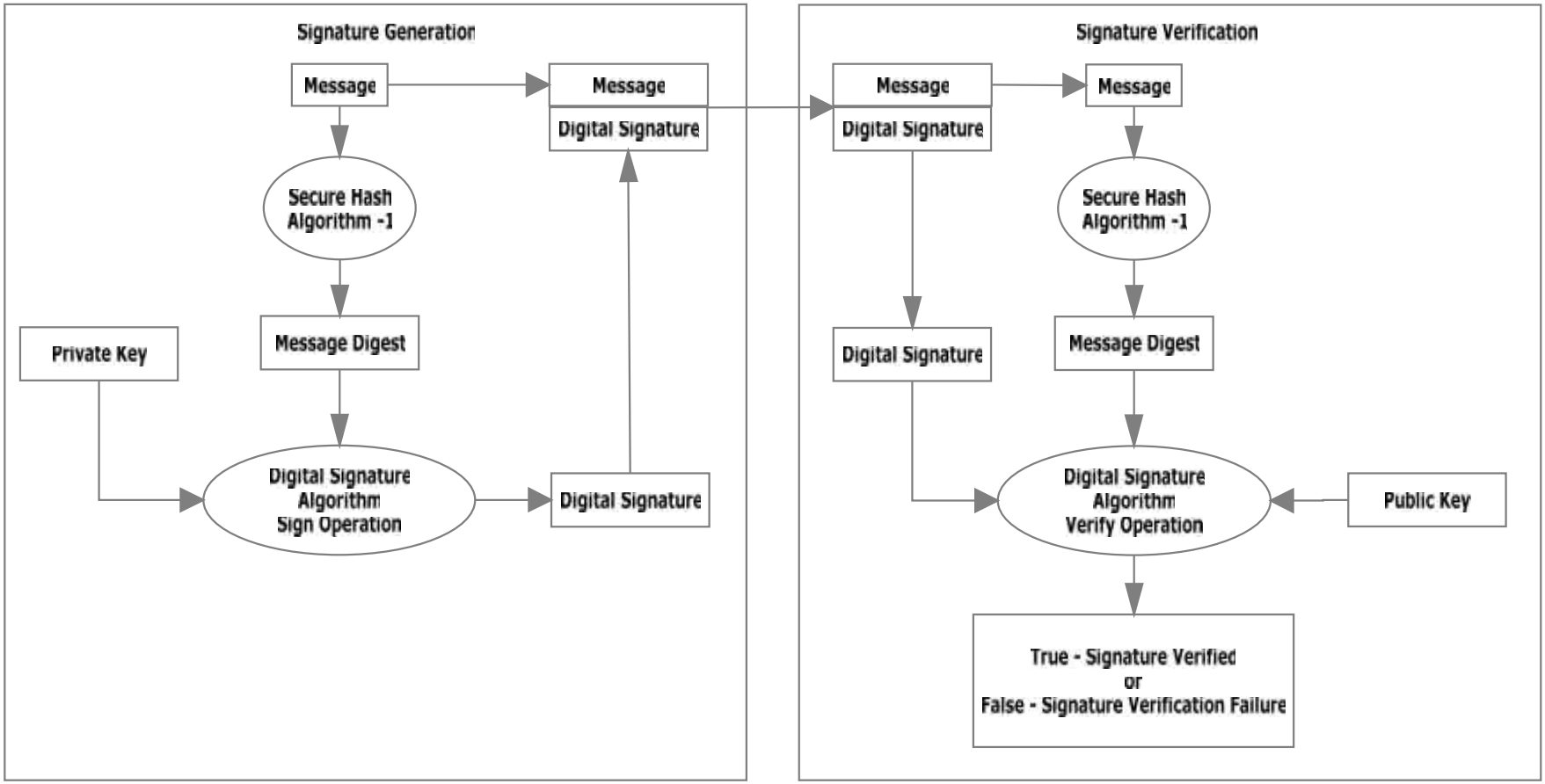
Skema Least Significant Bit (LSB)



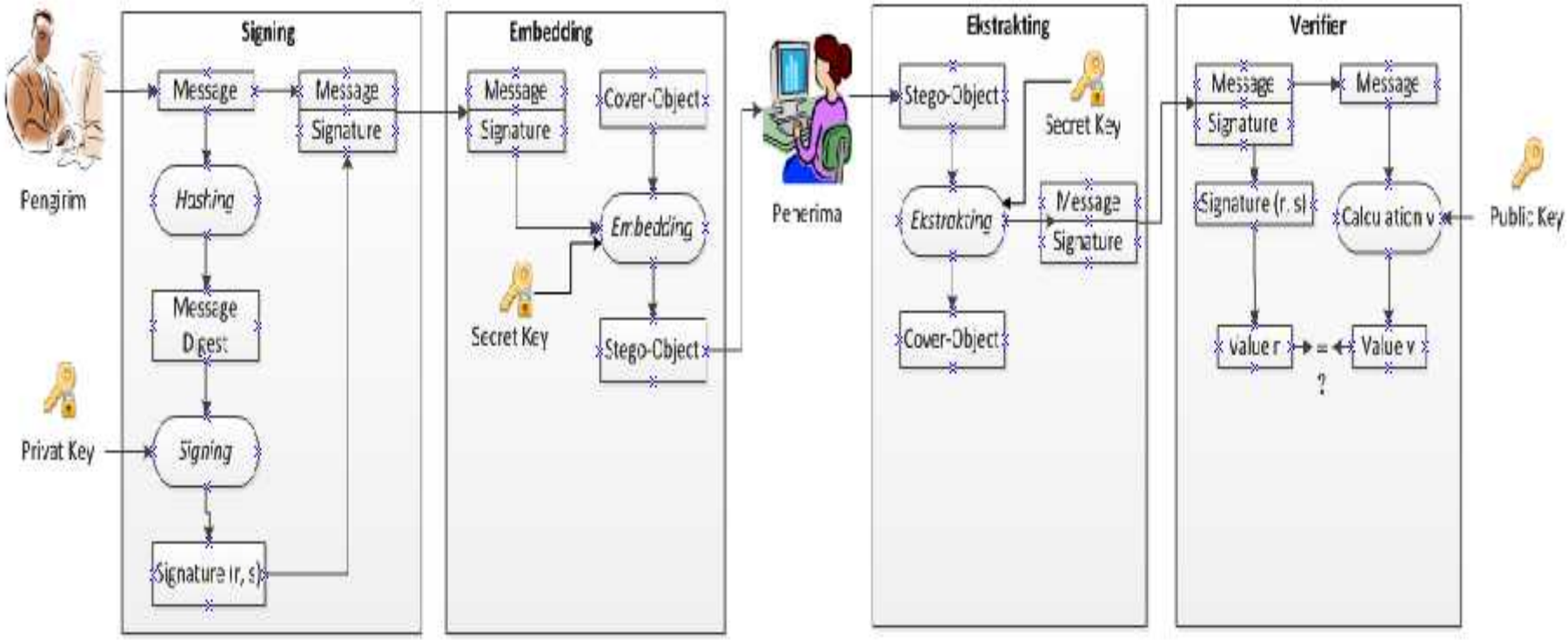
Digital Signature Algorithm

- **Pembentukan sepasang kunci**
- **Pembentukan tanda tangan**
- **Verifikasi tanda tangan**

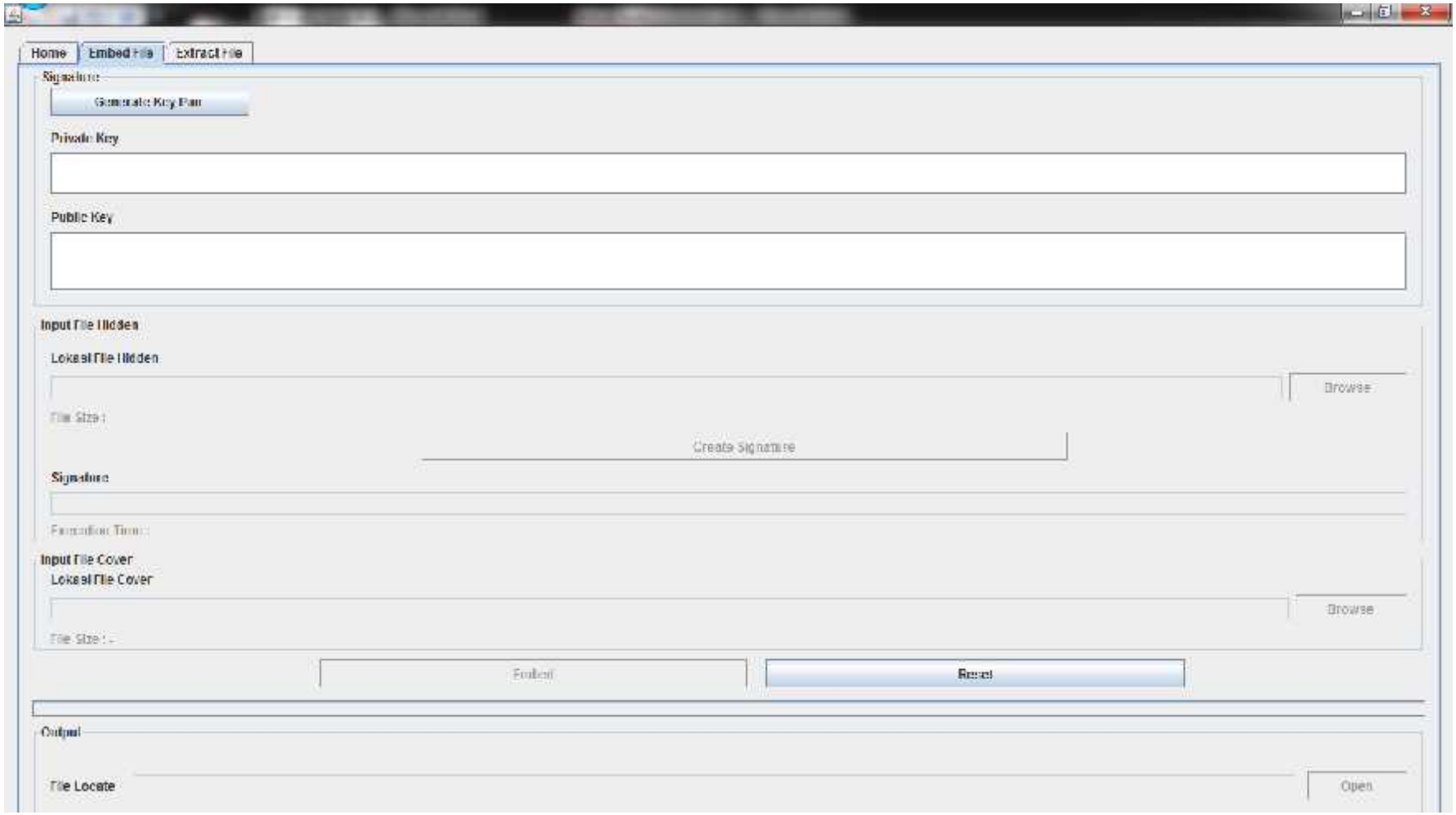
Skema Digital Signature Algorithm



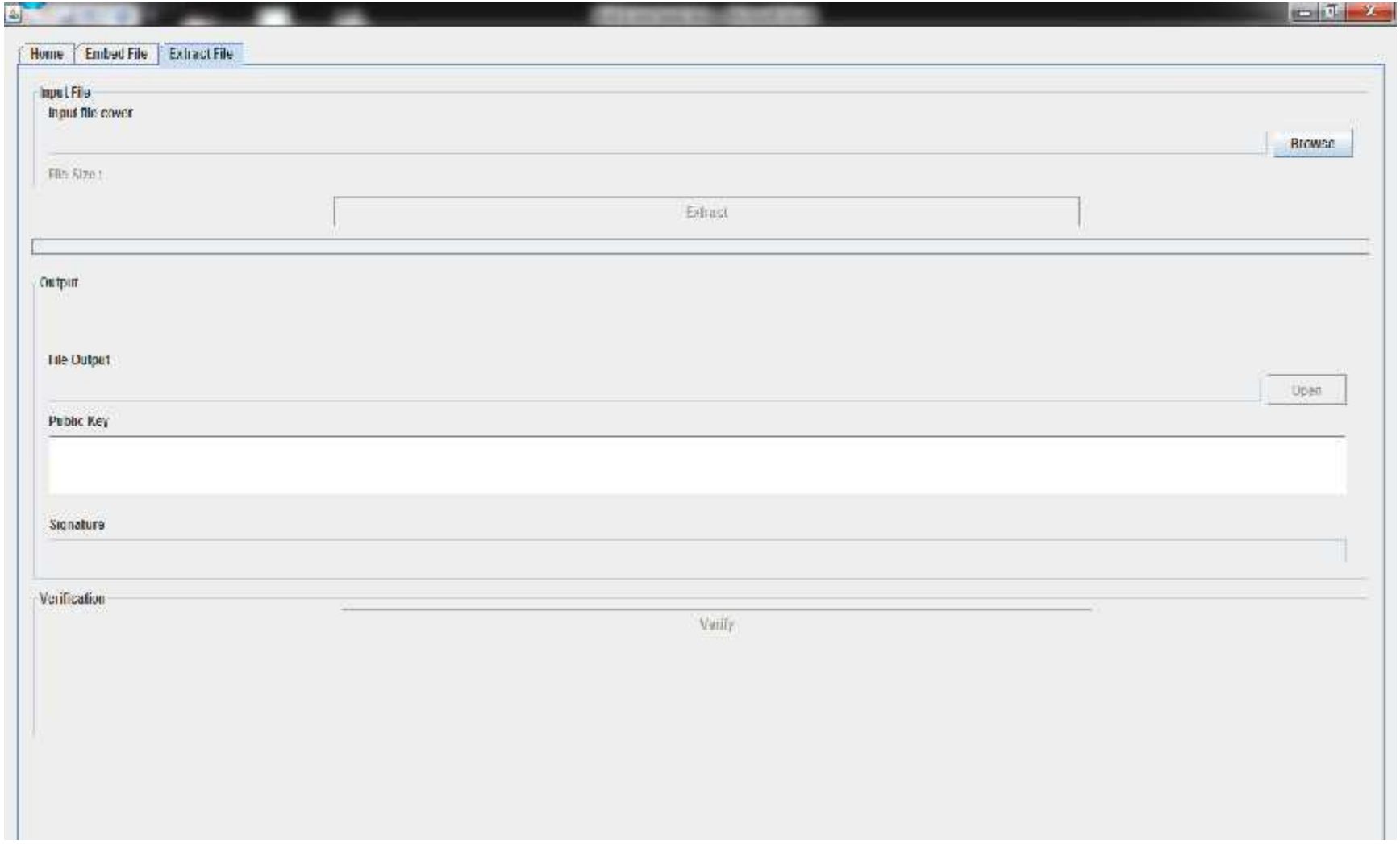
Gambaran Umum Sistem



Implementasi Sistem



Implementasi Sistem



Pengujian

No.	Proses	Jenis Pengujian
1	Generate Key Pair	White Box
2	Create Signature	White Box dan Black Box : Performance Testing
3	Verify	White Box dan Black Box : Performance Testing
4	Embed File	Black Box : Performance Testing
5	Extract File	Black Box : Robustness and Performance Testing

White Box

Cyclomatic Complexity

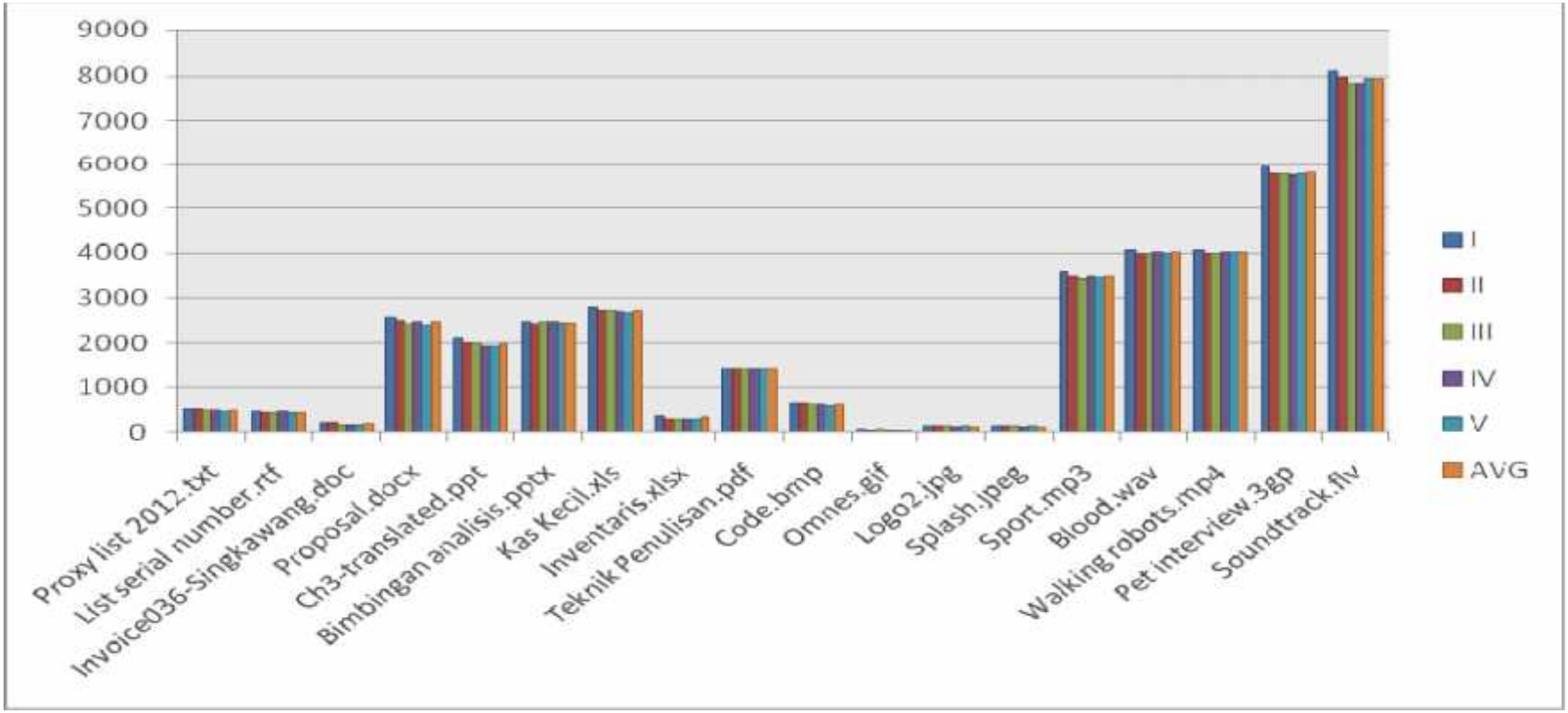
Proses Generate Key Pair = 5

Proses Create Signature = 2

Proses Verify Signature = 2

Black Box

Kecepatan Create Signature



Tabel 4.8, Hal 139

Black Box

Hasil Pengujian Penyisipan dan Ekstraksi

ID	Jenis File									
	BMP	GIF	JPG	WAV	MP3	3GP	MP4	FLV	MKV	AVI
H1										
H2										
H3										
H4										
H5										
H6										
H7										
H8										
H9										
H10										
H11										
H12										
H13										
H14										
H15										
H16										
H17										
H18										

	Valid
	Invalid
	Gagal *Extract*
	Gagal *Embedd*

Black Box

Pengujian Robustness Pada Citra

Jenis File	Rotate	Crop	Resize	Contrast	Exposure	Fill Light
BMP	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
GIF	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
JPG	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal

Black Box

Pengujian Robustness Pada Audio

Jenis File	Crop	Sample Rate
WAV	Gagal	Gagal
MP3	Gagal	Gagal

Black Box

Pengujian Robustness Pada Audio

Jenis File	Ekstraksi
3GP	Gagal
MP4	Gagal
FLV	Gagal
MKV	Gagal
AVI	Gagal

Black Box

Pengujian Pengunggahan File Stego

File Stego	Link Download	Ekstraksi	Verifikasi
stegobmp1.bmp	http://www.mediafire.com/?c061y7zu0dsvif0	Berhasil	Valid
stegojpg1.jpg	http://www.mediafire.com/?kd72kiai3h1gdg1	Berhasil	Valid
stegogif3.gif	http://www.mediafire.com/?j2pyewg3eokt7xr	Gagal	Gagal
stegowav1.wav	http://bzlink.us/hqghote2b8of/stegowav1.wav.html	Berhasil	Valid
stegomp31.mp3	http://www.indowebster.com/stegomp31.html	Berhasil	Valid
stego3gp1.3gp	http://bzlink.us/65441rcd7582/stego3gp1.3gp.html	Berhasil	Valid
stegomp42.mp4	http://bzlink.us/k620bzhwqusl/stegomp42.mp4.html	Berhasil	Valid
stegoflv1.flv	http://bzlink.us/7ny4u0kkmpol/stegoflv1.flv.html	Berhasil	Valid
stegomkv1.mkv	http://bzlink.us/1k5vh88mkxky/stegomkv1.mkv.html	Berhasil	Valid
stegoavi1.avi	http://www.indowebster.com/stegoavi1_1.html	Berhasil	Valid

Black Box

Pengujian Menggunakan Steganalisys

Tools	Deteksi
XStegSecret.Beta.v0.1	Tidak Terdeteksi
StegSpy v2.1	Terdeteksi Hiderman

Hasil Pengamatan Untuk Kategori Imperceptbility

File *Parent*	Hasil Pengamatan
BMP	Citra hasil penyisipan tidak mengalami perubahan sehingga kualitas gambar tidak dapat dibedakan dengan citra aslinya
GIF	Citra hasil penyisipan tidak mengalami perubahan, akan tetapi citra hasil penyisipan mengalami pengurangan jumlah frame sehingga tidak sama dengan yang aslinya.
JPG	Citra hasil penyisipan tidak mengalami perubahan sehingga kualitas gambar tidak dapat dibedakan dengan citra aslinya
WAV	Kualitas suara pada audio hasil penyisipan memiliki kualitas yang hampir sama, akan tetapi masih terdengar dengan jelas *noise* yang mengakibatkan kualitas suara kurang jernih..
MP3	Kualitas audio mengalami perubahan, dengan disisipinya file *child*, kualitas audio mengalami pemotongan dan perubahan *signal*, sehingga tidak sama dengan yang asli.
3GP	Kualitas video pada saat diputar mengalami kerusakan sehingga tidak dapat diputar dengan baik.
MP4	Kualitas video pada saat diputar mengalami kerusakan sehingga tidak dapat diputar dengan baik.
FLV	Kualitas video pada saat diputar mengalami kerusakan sehingga tidak dapat diputar dengan baik.
MKV	Kualitas video pada saat diputar mengalami kerusakan sehingga tidak dapat diputar dengan baik.
AVI	Kualitas gambar dan suara pada file video mengalami perubahan, bahkan apabila file yang disisipkan memiliki ukuran yang cukup besar, kualitas video akan berubah menjadi tidak dapat diputar dengan baik.

Hasil Pengamatan Untuk Kategori Fidelity

File *Parent*	Hasil Pengamatan
BMP	Ukuran media penampung tidak mengalami perubahan.
GIF	Ukuran media penampung mengalami perubahan dan jumlah frame pada media penampung tidak sama dengan yang asli.
JPG	Ukuran media penampung mengalami perubahan yang cukup besar sehingga tidak sama dengan yang asli.
WAV	Hasil ukuran media penampung memiliki ketergantungan terhadap besar ukuran file yang disisipkan dan file penampungnya.
MP3	Hasil ukuran media penampung memiliki ketergantungan terhadap besar ukuran file yang disisipkan dan file penampungnya.
3GP	Hasil ukuran media penampung memiliki ketergantungan terhadap besar ukuran file yang disisipkan dan file penampungnya.
MP4	Hasil ukuran media penampung memiliki ketergantungan terhadap besar ukuran file yang disisipkan dan file penampungnya.
FLV	Hasil ukuran media penampung memiliki ketergantungan terhadap besar ukuran file yang disisipkan dan file penampungnya.
MKV	Hasil ukuran media penampung memiliki ketergantungan terhadap besar ukuran file yang disisipkan dan file penampungnya.
AVI	Ukuran media penampung tidak mengalami perubahan. Hal itu disebabkan karena media penampung yang asli memiliki ukuran yang sangat besar.

Hasil Pengamatan Untuk Kategori Recovery

File *Parent*	Hasil Pengamatan
BMP	File yang disisipkan dapat diekstraksi dari media penampung.
GIF	File yang disisipkan tidak dapat diekstraksi dari media penampung.
JPG	File yang disisipkan dapat diekstraksi dari media penampung.
WAV	Media penampung yang tidak mengalami perubahan ukuran dapat mengekstraksi file yang disisipkan. Sedangkan media penampung yang mengalami perubahan ukuran tidak dapat mengekstraksi file yang disisipkan.
MP3	Media penampung yang tidak mengalami perubahan ukuran dapat mengekstraksi file yang disisipkan. Sedangkan media penampung yang mengalami perubahan ukuran tidak dapat mengekstraksi file yang disisipkan.
3GP	Media penampung yang tidak mengalami perubahan ukuran dapat mengekstraksi file yang disisipkan. Sedangkan media penampung yang mengalami perubahan ukuran tidak dapat mengekstraksi file yang disisipkan.
MP4	Media penampung yang tidak mengalami perubahan ukuran dapat mengekstraksi file yang disisipkan. Sedangkan media penampung yang mengalami perubahan ukuran tidak dapat mengekstraksi file yang disisipkan.
FLV	Media penampung yang tidak mengalami perubahan ukuran dapat mengekstraksi file yang disisipkan. Sedangkan media penampung yang mengalami perubahan ukuran tidak dapat mengekstraksi file yang disisipkan.
MKV	Media penampung yang tidak mengalami perubahan ukuran dapat mengekstraksi file yang disisipkan. Sedangkan media penampung yang mengalami perubahan ukuran tidak dapat mengekstraksi file yang disisipkan.
AVI	File yang disisipkan ke dalam media penampung dapat diekstraksi dengan baik.

Kesimpulan

Ukuran file *child* mempengaruhi dalam kecepatan pembentukan *signature*, semakin kecil ukuran file *child* semakin cepat algoritma DSA membuat *signature*. Sedangkan semakin besar ukuran file *child*, kecepatan algoritma DSA dalam membuat *signature* menjadi semakin menurun.

Kesimpulan

Kecepatan ekstraksi teknik DCS, lebih cepat dibandingkan pada saat penyisipan

Kesimpulan

Teknik DCS tidak cocok digunakan untuk media audio dan video. Karena setelah disisipi file, kualitas audio dan video tersebut menjadi rusak.

Kesimpulan

Penggabungan Steganografi dan Digital Signature terbukti dapat menjaga integritas dokumen setelah disisipkan ke dalam media penampung. Hal tersebut dapat dibuktikan dengan pengujian proses ekstraksi dan verifikasi dokumen.

Saran

Dilakukan analisa kembali terhadap teknik DCS agar media audio dan video dapat menampung file *child* tanpa merusak media penampung tersebut.

Saran

Diharapkan adanya pengembangan agar file steganografi dapat tahan terhadap berbagai macam serangan