ARTIKEL

PERANCANGAN APLIKASI PENGAMANAN DATA MENGGUNAKAN KOMBINASI TEKNIK STEGANOGRAFI METODE *LEAST SIGNIFICANT BIT* DAN TEKNIK KRIPTOGRAFI KLASIK METODE *BIFID CIPHER* PADA MEDIA CITRA DIGITAL

Oleh:

ERIKODIONY ARIESSA WAHYUDI

13.1.03.02.0233

Dibimbing oleh :

1. Intan Nur Farida, M.Kom

2. Patmi Kasih, M.Kom

PROGRAM STUDI

FAKULTAS TEKNIK

UNIVERSITAS NUSANTARA PGRI KEDIRI

2018

SURAT PERNYATAAN
ARTIKEL SKRIPSI TAHUN 2018

Yang bertanda tangan di bawah ini:

Nama Lengkap	: Erikodiony Ariessa Wahyudi
NPM	: 13.1.03.02.0233
Telepon/HP	: +6285234005787
Alamat Surel (Email)	: erikodiony@live.com
Judul Artikel	: Perancangan Aplikasi Pengamanan Data Menggunakan Kombinasi Teknik Steganografi Metode *Least Significant Bit* dan Teknik Kriptografi Klasik Metode *Bifid Cipher* pada Media Citra Digital
Fakultas – Program Studi	: Teknik – Teknik Informatika
Nama Perguruan Tinggi	: Universitas Nusantara PGRI Kediri
Alamat Perguruan Tinggi	: Jalan K.H Ahmad Dahlan 76 Mojoroto - Kota Kediri

Dengan ini menyatakan bahwa :

a. artikel yang saya tulis merupakan karya saya pribadi (bersama tim penulis) dan bebas plagiarisme;

b. artikel telah diteliti dan disetujui untuk diterbitkan oleh Dosen Pembimbing I dan II.

Demikian surat pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari ditemukan ketidaksesuaian data dengan pernyataan ini dan atau ada tuntutan dari pihak lain, saya bersedia bertanggungjawab dan diproses sesuai dengan ketentuan yang berlaku.

Mengetahui		Kediri, 25 Januari 2018
Pembimbing I	Pembimbing II	Penulis,
Intan Nur Farida, M.Kom NIDN. 0704108701	**Patmi Kasih, M.Kom** NIDN. 0701107802	**Erikodiony Ariessa Wahyudi** NPM. 13.1.03.02.0233

PERANCANGAN APLIKASI PENGAMANAN DATA MENGGUNAKAN KOMBINASI TEKNIK STEGANOGRAFI METODE *LEAST SIGNIFICANT BIT* DAN TEKNIK KRIPTOGRAFI KLASIK METODE *BIFID CIPHER* PADA MEDIA CITRA DIGITAL

Erikodiony Ariessa Wahyudi
13.1.03.02.0233
Teknik – Teknik Informatika
erikodiony@live.com
Intan Nur Farida, M.Kom dan Patmi Kasih, M.Kom
UNIVERSITAS NUSANTARA PGRI KEDIRI

ABSTRAK

Penelitian ini mencoba menggabungkan teknik steganografi dan teknik kriptografi klasik untuk mengamankan data, yaitu dengan mengambil keuntungan pada tiap-tiap metode yang didasarkan oleh pengamatan dan pengalaman peneliti. Steganografi berguna untuk menyamarkan data rahasia agar tidak dapat dipersepsi oleh indera manusia. Kriptografi berguna untuk menyamarkan data rahasia agar sulit di pahami. Metode yang digunakan dalam teknik steganografi yaitu menggunakan metode *Least Significant Bit* sedangkan metode yang digunakan dalam teknik kriptografi klasik menggunakan metode *Bifid Cipher*.

Permasalahan yang dihadapi *user* adalah (1) Bagaimana mengimplementasikan dan mengkombinasikan steganografi metode *Least Significant Bit* dan kriptografi metode *Bifid Cipher* pada media citra digital. (2) Apakah aplikasi yang dibangun mampu menjaga keamanan dan kerahasiaan data. (3) Apakah aplikasi yang dibangun mampu memenuhi aspek *robustness*, *flexibility*, *recovery*, dan *consistency*.

Sistem dibangun berbasiskan *Universal Windows Platform* (UWP) dengan menggunakan bahasa pemrograman C# dan berhasil diimplementasikan pada perangkat Windows 10 versi *desktop* dan *mobile*. Hasil evaluasi *output image stego* menggunakan perhitungan MSE dan PSNR didapatkan nilai MSE terkecil yakni 0.0691 dan terbesar yakni 0.02387. Serta nilai PSNR terkecil yakni 64.351 dan terbesar yakni 69.711. Berdasarkan hasil nilai tersebut kualitas citra hasil steganografi dan kriptografi yang dihasilkan dapat dinyatakan cukup baik. Sedangkan hasil evaluasi menggunakan aspek *Human Computer Interaction* (HCI) antara lain mencakup aspek *robustness*, *flexibility*, *recovery* dan *consistency* didapatkan hasil bahwa aplikasi tidak mampu memenuhi aspek *robustness* sedangkan aspek *flexibility*, *recovery* dan *consistency* telah berhasil dipenuhi.

Berdasarkan hasil yang didapatkan disimpulkan bahwa (1) Sistem ini telah berhasil dibangun dan berfungsi sesuai dengan yang diharapkan. (2) Aplikasi mampu untuk menjaga keamanan dan kerahasiaan data. (3) Aplikasi telah memenuhi beberapa aspek *Human Computer Interaction*.

KATA KUNCI : *Bifid Cipher*, Citra, Keamanan Data, Kriptografi, *Least Significant Bit*, Steganografi

I. LATAR BELAKANG

Komunikasi merupakan salah satu bentuk aktivitas dasar manusia yang membuat manusia dapat saling berinteraksi satu sama lain dalam kehidupan sehari-hari. Ditinjau dari segi bagaimana pengirim pesan melakukan proses komunikasi, bentuk komunikasi dapat dilakukan secara langsung maupun tidak langsung. Komunikasi secara langsung dapat dilakukan apabila pihak pengirim dan penerima saling bertemu dan bertatap muka secara langsung tanpa melalui perantara. Sedangkan komunikasi secara tidak langsung merupakan bentuk komunikasi yang menggunakan media tertentu sebagai perantara proses terjadinya komunikasi. Dalam hal ini teknologi informasi berperan sebagai media perantara.

Namun seiring dengan perkembangan teknologi informasi yang semakin pesat dan maju, kebutuhan akan tingkat keamanan terhadap suatu informasi maupun data yang bersifat rahasia pun semakin meningkat. Hal ini diakibatkan semakin maraknya tindak kejahatan pencurian ataupun penyadapan informasi maupun data oleh pihak-pihak yang tidak bertanggung jawab atau yang tidak berhak. Selain dampak privasi yang telah dilanggar, orisinalitas informasi maupun data juga menjadi salah satu aspek yang patut diperhatikan. Hal ini disebabkan pihak-pihak tersebut selain berkemampuan untuk menyadap informasi atau data didalamnya, juga memungkinkan untuk memanipulasinya.

Menyadari betapa pentingnya aspek privasi dan keaslian informasi maupun data serta untuk mencegah dampak-dampak buruk tersebut, maka salah satu cara yang dapat digunakan untuk mengatasi permasalahan ini adalah dengan menggunakan teknik steganografi. Steganografi menyamarkan keberadaan data yang telah disisipkan ke media penampungnya. Media penampung tersebut dapat berupa audio, citra, video atau media lainnya. Adapun metode steganografi yang digunakan adalah *Least Significant Bit* (LSB). Dengan menggunakan metode ini memungkinkan media penampung yang telah disisipi oleh data rahasia (*stego image*) masih terlihat seperti layaknya *file* normal tanpa mengalami perubahan secara kasat mata. Sehingga tidak akan menimbulkan kecurigaan oleh orang lain.

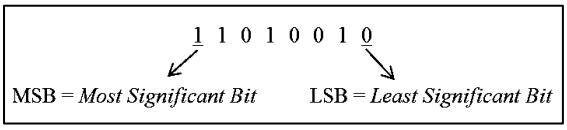
Untuk memperkuat segi keamanan dalam proses pembacaan atau pengeluaran (*extraction*) data rahasia, penulis mencoba untuk mengkombinasikan teknik steganografi tersebut dengan teknik kriptografi. Kriptografi merupakan teknik yang berusaha untuk mengubah data menjadi data yang sulit dimengerti agar

penyadap tidak dapat mengetahui isi informasi tersebut secara jelas dan gamblang. Adapun metode kriptografi yang digunakan adalah *Bifid Cipher*. Metode ini nantinya akan digunakan pada proses pengamanan data teks serta data *password* atau kode pengaman yang digunakan untuk proses *extraction* data rahasia dari citra *stego image*. Sehingga hanya pihak-pihak tertentu yang mengetahui *password* atau kode pengaman yang dapat mengekstraksi maupun membaca data rahasia dari citra *stego image* tersebut.

II. METODE

A. Steganografi *Least Significant Bit*

Kata "Steganografi" diartikan sebagai "ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian rupa sehingga keberadaannya pesan tidak terdeteksi oleh indra manusia" (Munir, 2004). Pada dasarnya metode *Least Significant Bit* (LSB) adalah suatu metode steganografi menggunakan teknik subsitusi yakni dengan cara menyimpan data ke dalam bit *cover image*. Bit dengan bobot terkecil dari setiap *pixel* suatu gambar diubah menjadi *bit* dari pesan yang akan disembunyikan. Seperti yang ditunjukkan pada gambar 1.1.



Gambar 2.1 Contoh MSB dan LSB

Untuk pemahaman lebih lanjut, dapat diilustrasikan sebagai berikut. Misalkan barisan bit dari data yang akan dimasukkan adalah "111111000000" dan akan dimasukkan pada beberapa pixel citra seperti pada Tabel 2.1. Selanjutnya barisan bit "111111000000" dimasukkan pada bit terakhir dari setiap nilai pada pixel citra seperti yang ditunjukan pada Tabel 2.2.

Tabel 2.1 Nilai - Nilai *Pixel* Sebelum Disisipi Data

Desimal		Biner	
252	252	11111100	11111100
223	224	11011111	11100000
175	176	10101111	10110000
253	253	11111101	11111101
221	221	11011101	11011101
172	172	10101100	10101100

Tabel 2.2 Nilai - Nilai *Pixel* Setelah Disisipi Data

Desimal		Biner	
253	253	1111110<u>1</u>	1111110<u>1</u>
223	225	1101111<u>1</u>	1110000<u>1</u>
175	177	1010111<u>1</u>	1011000<u>1</u>
252	252	1111110<u>0</u>	1111110<u>0</u>
220	220	1101110<u>0</u>	1101110<u>0</u>
172	172	1010110<u>0</u>	1010110<u>0</u>

Pada Tabel 2.1 dan Tabel 2.2, dapat dilihat bahwa perubahan yang terjadi sangat kecil dan hal ini akan mengakibatkan data yang disisipkan sulit terdeteksi dan tidak mengalami perbedaan bila diamati secara kasat mata.

B. Kriptografi *Bifid Cipher*

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti writing (tulisan).

Bifid cipher merupakan salah satu metode dari kriptografi klasik, dimana menggunakan karakter huruf angka beserta simbol untuk menyandikan pesan menjadi karakter yang sulit dipahami. *Bifid cipher* pertama kali ditemukan oleh Felix Delastelle pada tahun 1901 dan merupakan salah satu metode yang menggunakan prinsip dasar *subtitution cipher*, dimana pesan akan dienkripsikan dengan merubah huruf menjadi angka tertentu sesuai dengan posisi baris dan kolom huruf pada karakter yang sesuai dengan papan kunci yang berbentuk bujur sangkar 5 X 5 atau lebih yang biasa disebut *polybius square*. Dan dalam *bifid cipher* ini huruf "I" dan "J" disatukan dalam satu blok seperti pada Tabel 2.3 berikut.

Tabel 2.3 *Polybius Square*

	1	***2***	***3***	***4***	***5***
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Sebagai ilustrasi untuk contoh kasus dengan plainteks "UNPKEDIRI" akan diperoleh hasil identifikasi sebagai berikut.

Text :	**U**	**N**	**P**	**K**	**E**	**D**	**I**	**R**	**I**
Baris :	**4**	**3**	**3**	**2**	**1**	**1**	**2**	**4**	**2**
Kolom :	**5**	**3**	**5**	**5**	**5**	**4**	**4**	**2**	**4**

Kemudian aturan yang digunakan adalah dengan menjadikan koordinat baris dan kolom menjadi satu baris karakter angka dan kemudian membuatnya menjadi bigram (dipisahkan dua-dua) untuk dijadikan kordinat baru yang isi sel nya merupakan hasil enkripsi yang dilakukan. Seperti pada proses berikut.

4 3 3 2 1 1 2 4 2 5 3 5 5 5 4 4 2 4

Kordinat baris dan kolom dijadikan satu baris karakter angka. Lalu pisahkan menjadi bigram yang akan membentuk kordinat baris dan kolom.

43 32 11 24 25 35 55 44 24

Maka cipherteks adalah isi dari sel dengan kordinat baru yang terbentuk.

Baris :	**4**	**3**	**1**	**2**	**2**	**3**	**5**	**4**	**2**
Kolom :	**3**	**2**	**1**	**4**	**5**	**5**	**5**	**4**	**4**

Maka hasil enkripsi dengan menggunakan metode bifid cipher adalah sebagai berikut.

Text:	**U**	**N**	**P**	**K**	**E**	**D**	**I**	**R**	**I**
Cipher :	**S**	**M**	**A**	**I**	**K**	**P**	**Z**	**T**	**I**

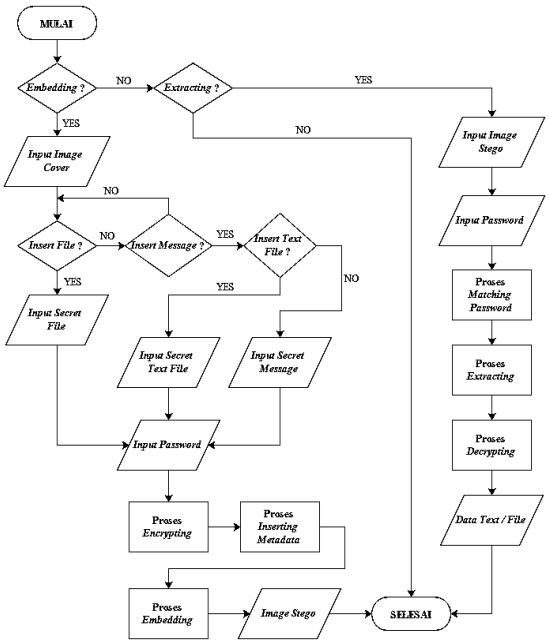
Adapun dalam proses dekripsi yang dilakukan merupakan kebalikan dari proses enkripsi dan dilakukan secara sekuensial dari urutan terbelakang proses enkripsi.

C. Pemodelan Sistem

Pada bagian ini akan dibahas mengenai pemodelan sistem yang akan dibangun menggunakan *Unified Modeling Language* (UML) yang antara lain diagram *flowchart*, diagram *use case*, diagram *activity* dan diagram *deployment*. Dimana akan digunakan sebagai acuan dalam proses perancangan dan membangun sistem aplikasi.

1. *Flowchart Diagram*

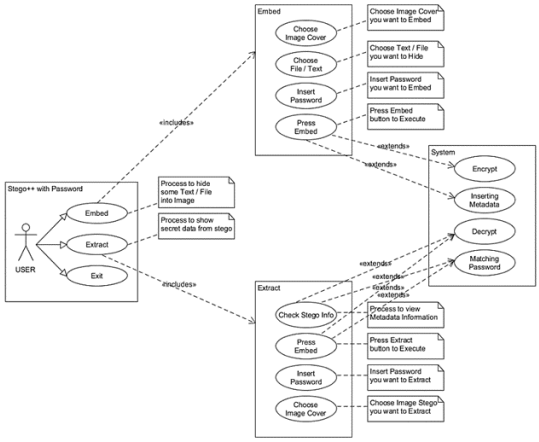
Pada *flowchart diagram* dijelaskan mengenai alur proses yang terjadi di dalam sistem secara keseluruhan pada bagian-bagian sistem. Terdapat dua proses utama dalam *flowchart* ini, yakni *embedding* sebuah obyek ke dalam *image cover* dan melakukan *extracting* dari sebuah *image stego*. Seperti yang ditunjukkan Gambar 2.2



Gambar 2.2 *Flowchart Diagram*

2. *Use Case Diagram*

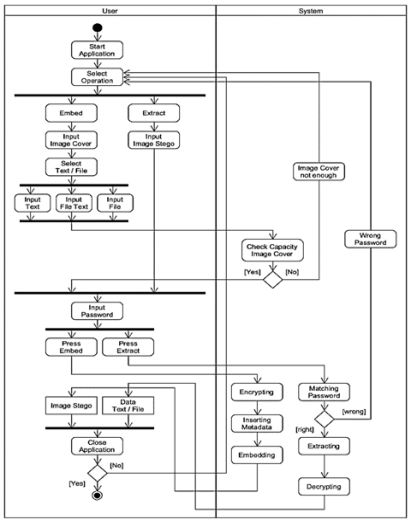
Diagram *use case* merupakan salah satu diagram untuk mendeskripsikan apa yang seharusnya dilakukan oleh sistem dari perspektif *user*. Seperti yang ditunjukkan Gambar 2.3



Gambar 2.3 *Use Case Diagram*

3. *Activity Diagram*

Activity Diagram merupakan salah satu pemodelan yang digunakan untuk mengambarkan aktivitas dari sistem yang dibangun. Seperti yang dijelaskan pada Gambar 2.4

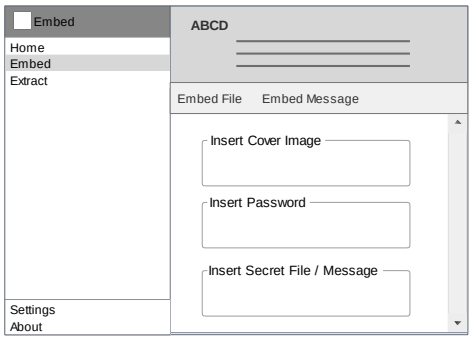


Gambar 2.4 *Use Case Diagram*

D. Rancangan *Interface*

1. *Interface Menu Embed*

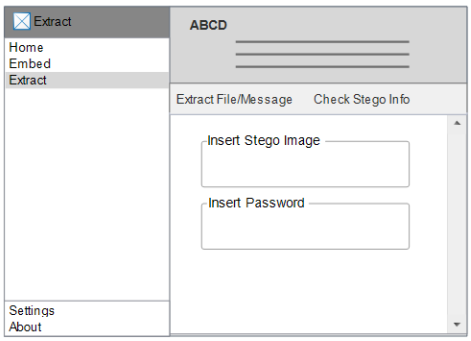
Pada *Menu Embed* berisi tentang *form-form* yang digunakan untuk menjalankan proses *embedding*. Terdapat dua *submenu* pada menu ini yakni *Embed File* dan *Embed Message*. *Embed File* untuk proses penyisipan dengan jenis penyisipan *file*. Adapun *Embed Message* untuk proses penyisipan dengan jenis penyisipan *text message*. Seperti yang ditunjukkan pada Gambar 2.5



Gambar 2.5 *Interface Menu Embed*

2. *Interface Menu Extract*

Pada *Menu Extract* berisi *form* yang digunakan untuk menjalankan proses *extracting*. Seperti yang ditunjukkan Gambar 8.



Gambar 2.6 *Interface Menu Extract*

E. Logika Sistem

1. *Embed*

Pada proses ini nantinya *password* beserta informasi pendukung lainnya akan dilakukan proses enkripsi terlebih dahulu menggunakan tabel *polybius* 10x10 yang sudah dimodifikasi dengan penambahan karakter-karakter baru, selanjutnya hasil enkripsi tersebut akan dilakukan proses penyisipan pada metadata citra yang terletak pada "tEXt/description". Sementara untuk data *file*/*text* yang akan diamankan, terlebih dahulu dikonversi menjadi nilai-nilai *bit*. Kemudian hasil konversi nilai *bit* dilakukan proses penyisipan ke dalam nilai-nilai citra. Yakni dengan cara membandingkan nilai antara nilai-nilai *pixel image cover* dengan nilai-nilai hasil gabungan data rahasia (*hidden object*) dengan ketentuan seperti berikut.

a. Apabila nilai *pixel* bernilai ganjil dan *hidden object* bernilai 1, maka nilai *pixel* adalah tetap.
b. Apabila nilai *pixel* bernilai genap dan *hidden object* bernilai 0, maka nilai *pixel* adalah tetap.
c. Apabila nilai *pixel* bernilai genap dan *hidden object* bernilai 1, maka nilai *pixel* adalah (nilai *pixel* + 1).
d. Apabila nilai *pixel* bernilai ganjil dan *hidden object* bernilai 0, maka nilai *pixel* adalah (nilai *pixel* - 1).

Sehingga *output* sistem yang dihasilkan yakni citra *image stego* yang telah terisi data rahasia (*hidden object*) didalamnya.

2. *Extract*

Sebelum melakukan proses *extract*, proses yang dilakukan adalah proses pencocokan *password*. Apabila *input password* oleh *user* telah sesuai dengan *password* pada *image stego*, maka sistem akan melanjutkan proses *extract*, yakni dengan ketentuan seperti berikut :

a. Konversi nilai citra menjadi nilai *bit* dengan cara melakukan perbandingan menggunakan rumus berikut
   - Apabila nilai *pixel* ganjil maka bernilai 1.
   - Apabila nilai *pixel* genap maka bernilai 0.
b. Simpan semua nilai *bit* citra ke dalam *array* dua dimensi di dalam sistem.
c. Kelompokkan nilai *array* yang masih dalam satu kesatuan tersebut sesuai dengan informasi data pada metadata
d. Konversikan hasil pengelompokan *array* tersebut menjadi nilai *byte*.
e. Lakukan proses deskripsi nilai *byte* tersebut menjadi ASCII untuk penyisipan jenis *message*. Atau konversikan menjadi sebuah *file* untuk penyisipan jenis *file*.

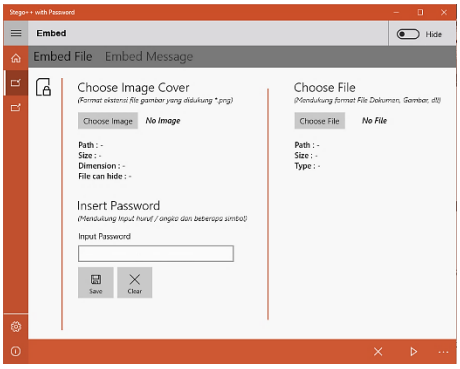
III. HASIL DAN KESIMPULAN

A. Tampilan Aplikasi

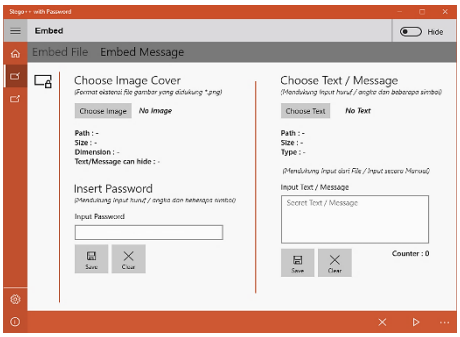
Pada tahap implementasi, sistem dibangun menggunakan *Integrated Development Environment* (IDE) Visual Studio 2017 *Community*.

1. *Interface Menu Embed*

Berikut ini merupakan tampilan *menu embed* yang ditunjukkan pada Gambar 3.1 dan Gambar 3.2



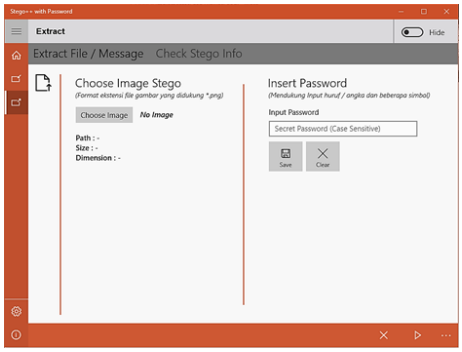
Gambar 3.1 *Interface Menu Embed File*



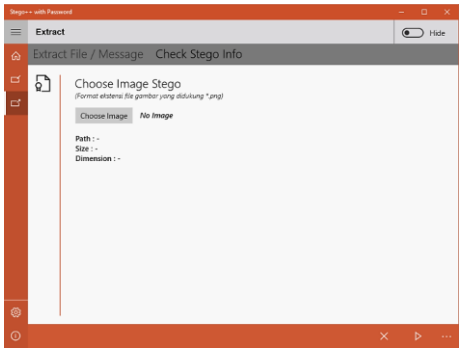
Gambar 3.2 *Interface Menu Embed Message*

2. *Interface Menu Extract*

Berikut ini merupakan tampilan *menu extract* yang ditunjukkan pada Gambar 3.3 dan Gambar 3.4



Gambar 3.3 *Interface Menu Extract*



Gambar 3.4 *Interface Menu Check Stego Info*

B. Pengujian Aplikasi

Aplikasi dibuat berdasarkan konsep *Universal Windows Platform* (UWP) berbasis C# dan pengujian dilakukan pada OS Windows 10 versi *desktop* dan *mobile*.

1. Data Uji

Tabel 3.1 Data Uji *Image Cover*

No	Nama File	Ukuran File
1	Banner.png	4.08 MB (8271x2365)
2	IMG_2403.png	16.2 MB (4272x2848)
3	Logo.png	1.20 MB (1946x2350)
4	Logo_Mesin.png	21.2 KB (100x100)

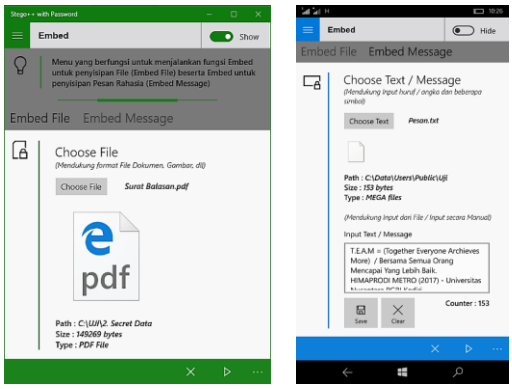
Sedangkan data *hidden object* (*file* yang akan diamankan dan disembunyikan) seperti yang ditunjukkan pada Tabel 3.2

Tabel 3.2 Data Uji *Hidden Object*

No	Nama File	Ukuran File
1	STRUKTURAL KEPENGURUSAN PERIODE 2017.doc	126 KB
2	Surat Balasan.pdf	145 KB
3	Surat Peminjaman Fasilitas.zip	108 KB
4	Teks “T.E.A.M = (Together Everyone Archieves More) / Bersama Semua Orang Mencapai Yang Lebih Baik. HIMAPRODI METRO (2017) - Universitas Nusantara PGRI Kediri” tersimpan dalam Pesan.txt	153 B

2. *Embed*

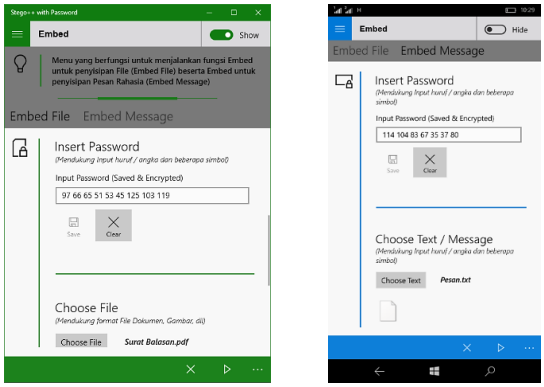
Proses *embed* akan dilakukan untuk semua *file* pada data uji, berikut ini merupakan tampilan dari proses yang terjadi pada masing-masing perangkat pada Gambar 3.5 dan Gambar 3.6.



(a) (b)

Gambar 3.5 Hasil *Input Hidden Object* Pada Aplikasi

(a) *Desktop* ; (b) *Mobile*



(a) (b)

Gambar 3.6 Hasil *Input Password* Pada Aplikasi

(a) *Desktop* ; (b) *Mobile*

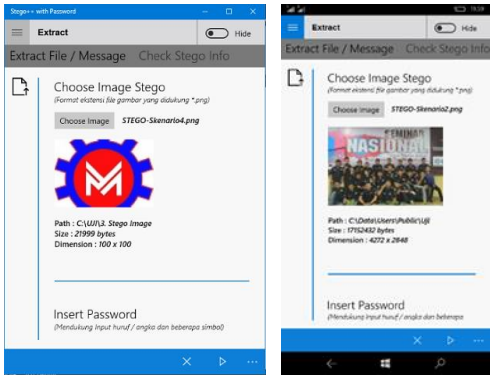
Setelah semua data telah di lakukan proses *embed* pada masing-masing perangkat, maka akan menghasilkan *output image stego* seperti yang ditunjukkan pada tabel 3.3

Tabel 3.3 Data *Output Image Stego*

Stego File	***Size***
STEGO-Skenario1.png	4.30 MB
STEGO-Skenario2.png	16.3 MB
STEGO-Skenario3.png	1.42MB
STEGO-Skenario4.png	21.4 KB

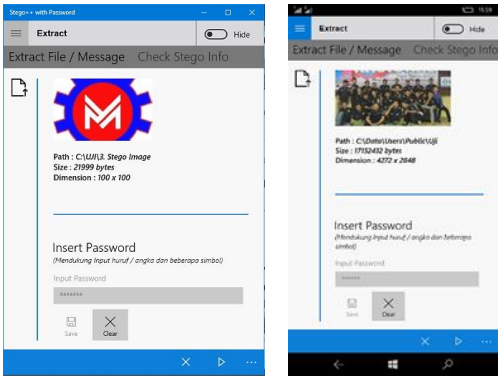
3. *Extract*

Sedangkan proses *extract* dilakukan menggunakan data *image stego* yang dihasilkan pada proses *embed*, berikut ini merupakan tampilan dari proses yang terjadi pada masing-masing perangkat yang ditunjukkan pada Gambar 3.7 – 3.9.



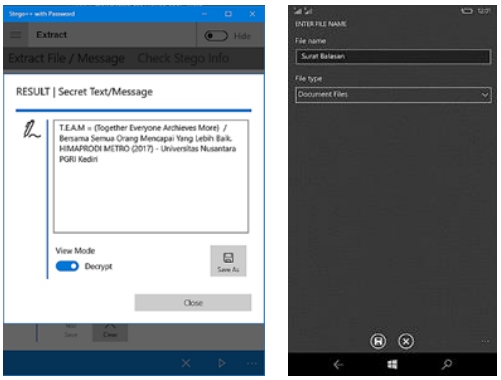
(a) (b)

Gambar 3.7 Hasil *Input Image Stego* Pada Aplikasi
(a) *Desktop* ; (b) *Mobile*



(a) (b)

Gambar 3.8 Hasil *Input Password Stego* Pada Aplikasi
(a) *Desktop* ; (b) *Mobile*



(a) (b)

Gambar 3.9 Hasil *Extract Image Stego* Pada Aplikasi
(a) *Desktop* ; (b) *Mobile*

C. Evaluasi Hasil *Output*

Hasil *output image stego* dari aplikasi akan diuji untuk mengetahui sejauh mana kualitas yang dihasilkan yakni evaluasi menggunakan perhitungan rumus MSE dan PSNR.

1. MSE dan PSNR

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR diukur dalam satuan *desibel*. Sebelum menentukan nilai PSNR, terlebih dahulu harus ditentukan *Mean Square Error* (MSE). MSE adalah nilai *error* kuadrat rata-rata antara *image cover* dengan *image stego*. "Sehingga semakin rendah nilai MSE maka akan semakin baik, dan semakin besar nilai PSNR maka semakin baik kualitas citra steganografi" (Cheddad, 2010). Secara matematis MSE dirumuskan seperti pada persamaan 1 berikut :

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[l(x,y) - l'(x,y)]^2 \quad \ldots. (1)$$

Dimana :

M = Panjang *image stego* (dalam *pixel*)

N = Panjang *image cover* (dalam *pixel*)

$l(x,y)$ = Nilai *pixel* dari *image stego*

$l'(x,y)$ = Nilai *pixel* dari *image cover*

Setelah mendapatkan hasil perhitungan MSE, maka proses perhitungan PSNR dapat dilakukan, yakni menggunakan persamaan 2 berikut :

$$PSNR = 10.\log\left(\frac{MAXi^2}{MSE}\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Dimana:

MSE = nilai MSE

MAXi = nilai maksimum dari *pixel* citra yang digunakan

Berikut ini merupakan Tabel 3.4 dan Tabel 3.5 yang menjelaskan tentang hasil dari analisis pengamatan menggunakan perhitungan MSE dan PSNR.

Tabel 3.4 Hasil Perhitungan MSE

Data	MSE				
	B	G	R	A	$\frac{B+G+R+A}{4}$
Hasil 1	0.0065	0.0071	0.0065	0.0073	0.00691
Hasil 2	0.0122	0.0122	0.0122	0.0120	0.01221
Hasil 3	0.0239	0.0238	0.0237	0.0238	0.02387
Hasil 4	0.0232	0.0174	0.0154	0.0193	0.01882

Tabel 3.5 Hasil Perhitungan PSNR

Data	PSNR				
	B	G	R	A	$\frac{B+G+R+A}{4}$
Hasil 1	69.927	69.531	69.931	69.455	69.711
Hasil 2	67.249	67.172	67.241	67.311	67.243
Hasil 3	64.332	64.352	64.367	64.352	64.351
Hasil 4	64.475	65.725	66.255	65.275	65.433

Berdasarkan data hasil perhitungan tersebut dapat disimpulkan bahwa hasil akhir PSNR untuk keseluruhan data memiliki nilai diatas 60 dB, sehingga merujuk kesimpulan yang dipaparkan oleh Cheddad (2010) bahwasanya "Apabila nilai PSNR jatuh dibawah 30 dB, mengindikasikan kualitas citra relatif rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas. Akan tetapi kualitas *image stego* yang tinggi berada pada nilai 40 dB dan diatasnya". Maka dapat disimpulkan bahwa kualitas citra *image stego* dalam keadaan cukup baik.

2. Evaluasi berdasarkan HCI

Terdapat berbagai macam aspek dalam *Human Computer Interaction* (HCI), namun penulis mencoba untuk mengambil beberapa aspek yang menjadi dasar dalam analisis ini yakni *Robustness*, *Flexibility*, *Recovery*, dan *Consistency*.

a. *Robustness*

Pengujian ini dilakukan untuk menguji ketahanan *image stego* dengan teknik *rotate* dan *flip* pada semua *image stego*. Hasilnya bahwa ketika *image stego* dilakukan perubahan, ternyata data *hidden object* yang sebelumnya disisipkan di dalam *image stego* tidak dapat di ekstraksi, hal ini kemungkinan besar terjadi akibat perubahan dari struktur koordinat nilai *x* dan *y* pada *pixel image stego* sehingga apabila keadaan koordinat telah berubah, maka sistem tidak dapat membaca dan mengekstraksi data tersebut. Berdasarkan hasil tersebut dapat diperoleh kesimpulan bahwa sistem tidak dapat memenuhi aspek *robutsness*.

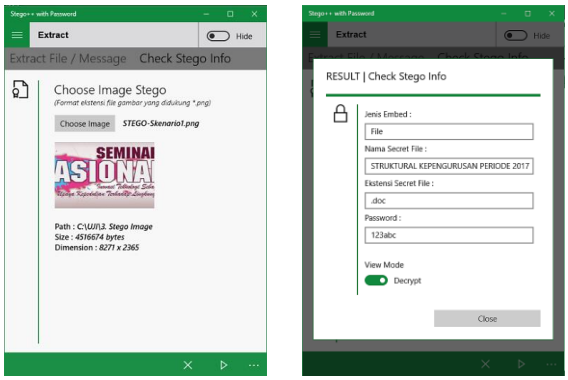
b. *Flexibility*

Dijelaskan pada tahap pengujian sistem yakni aplikasi mampu dijalankan pada aplikasi *dekstop* dan *mobile*. Karena sistem dibangun berbasiskan *Universal Windows Platform* (UWP) dimana dengan sistem ini aplikasi dapat dijalankan pada semua platform Windows 10 baik pada perangkat *desktop* dan *mobile* dengan sedikit

penyesuaian kode. Sehingga mengacu simpulan tersebut, maka aplikasi telah memenuhi aspek *flexibility*.

c. *Recovery*

Untuk memenuhi aspek *recovery*, pada menu aplikasi telah ditambahkan fitur *recovery password*, seperti yang ditunjukkan Gambar 3.10



Gambar 3.10 Proses Pemulihan *Password Image Stego*
(a) Tampilan *Form* ; (b) Hasil *Output* Program

Sehingga berdasarkan hasil tersebut, maka aplikasi telah memenuhi aspek *recovery*.

d. *Consistency*

Aplikasi ini telah di uji bahwa hasil *image stego* telah berhasil melakukan proses *embed* maupun *extract* pada perangkat *desktop* dan *mobile* yang berbeda, dengan hasil yang masih konsisten.

Berdasarkan hasil dari berbagai simpulan hasil pada masing-masing proses disimpulkan bahwa :

1) Sistem ini telah berhasil dibangun berbasiskan UWP dan berjalan pada perangkat OS Windows 10 versi *desktop* dan *mobile* serta telah berfungsi sesuai dengan yang diharapkan oleh *user*.
2) Pada hasil perhitungan PSNR untuk tiap-tiap data uji menghasilkan nilai diatas 60 dB. Sehingga dalam kondisi ini kualitas citra *image stego* yang dihasilkan dapat dinyatakan cukup baik.
3) Berdasarkan hasil evaluasi mengunakan aspek HCI (*Human Computer Interaction*). Diperoleh hasil berikut :
   a. Aplikasi telah mampu memenuhi aspek *flexibility*, *recovery* dan *consistency*.
   b. Aplikasi tidak mampu memenuhi aspek *robustness*, disebabkan karena ketika dilakukan perubahan pada susunan *pixel* maka struktur nilai-nilai dan koordinat *pixel* juga akan berubah mengakibatkan data rahasia yang terdapat di dalam *image stego* tidak dapat di ekstraksi.

IV. DAFTAR PUSTAKA

Munir, Rinaldi. 2004. *Steganografi dan Watermarking*. Bandung: Informatika Bandung.

Cheddad, A. 2010. *Digital Image Steganography : Survey and Analysis of Current Methods. Signal Processing*. Northern Ireland, UK: Elsevier.