BAB I

PENDAHULUAN

1.1 Pendahuluan

Bab 1 memberikan penjelasan umum mengenai keseluruhan penelitian. Antara lain membahas latar belakang masalah penelitian, perumusan masalah penelitian, tujuan penelitian dan manfaat penelitian. Pendahuluan dimulai dengan penjelasan mengenai teknik steganografi dan kriptografi serta metode-metode yang digunakan yang menjadi latar belakang dari penelitian ini.

1.2 Latar Belakang Masalah

Seiring dengan majunya perkembangan teknologi komputer, informasi dan komunikasi menjadikan kegiatan penyampaian informasi maupun data menjadi lebih mudah dan cepat, oleh karena itu sebagian besar masyarakat lebih memilih untuk menggunakan internet sebagai media utama untuk menyampaikan informasi maupun data.

Sayangnya dengan berkembangnya internet dan aplikasi menggunakan internet semakin berkembang pula kejahatan sistem informasi. Data atau pesan yang dikirim melalui internet dapat diretas (disadap) selama dalam proses pengiriman. Perkembangan internet juga dapat membuat aspek keamanan dan kerahasiaan data menjadi sangat penting.

Salah satu cara menghindari kejahatan terhadap suatu pesan adalah dengan memodifikasi pesan tersebut sehingga pihak yang tidak memiliki otoritas tidak

dapat membaca pesan tersebut. Salah satu cara penanganan masalah keamanan informasi dan data adalah dengan menggunakan teknik Steganografi dan Kriptografi.

Steganografi adalah teknik menyembunyikan keberadaan pesan kedalam bentuk media digital seperti teks, citra, audio, maupun video, dimana tujuannya untuk menghindari kecurigaan dari pihak ketiga (lawan). Sedangkan kriptografi adalah teknik menyembunyikan isi (content) pesan, dimana tujuannya agar pesan tidak dapat dibaca oleh pihak ketiga (lawan).

(Ahmad Aidil Fitri, Megah Mulya 2016) melakukan penelitian Steganografi Pada Citra Bewarna 32-bit Menggunakan Least Significant Bit (LSB). Hasil dari penelitian ini menjelaskan bahwa, Keuntungan dari penyisipan LSB pada citra bewarna 32-bit (RGBA) memiliki daya tampung yang besar dibandingkan dengan penyisipan LSB pada citra berwarna RGB dan menunjukkan kualitas citra hasil penyisipan terbilang baik dengan nilai *Mean Square Error (MSE)* kurang dari 2 dan *Peak Signal to Noise Ratio (PSNR)* diatas 45 dB (*decibel*) sehingga sulit untuk dibedakan oleh penglihatan manusia. Sedangkan kekurangnya adalah keamanan dan ketahanan (*robustness*) pada penelitian terbilang rendah, sehingga butuh teknik baru dalam penyaluran data tersembunyi dan teknik kriptografi untuk melakukan penyandian pesan.

Penelitian yang dilakukan oleh (Ali Mahmudi, Sandy Nataly Mantja dan Rozikin 2016) yang berjudul "Aplikasi Kriptografi dan Steganografi menggunakan Metode *Least Significant Bit (LSB)* dan *One Time Pad (OTP)*" dan penelitan yang dilakukan oleh (Najih 2017) yang berjudul "Kombinasi Teknik Steganografi dan

Kriptografi dengan *Discrete Cosine Transform (DCT), One Time Pad (OTP)* dan *PN-Sequence* pada Citra Digital" dengan menjawab kelemahan dari penelitian sebelumnya, diamana kurangnya keamanan dalam pesan.

Menurut (Kustov dan Protsko 2017) dalam penelitian "*Modeling Hidden Data by Combined LSB&DCT Algorithm*" yang menghasilkan Algoritma DCT & LSB lebih tahan terhadap berbagai stegoattacks dan distortion stegocontainer daripada LSB.

Terinspirasi dari penelitian yang dilakukan sebelumnya, penelitian kali ini akan menggunakan kombinasi metode *Discret Cosine Transform* (DCT) *& Least Signifcant Bit* (LSB) dalam penyisipan keberadaan pesan ke dalam citra digital dan metode *One Time Pad* (OTP) dalam penyandian pesan.

1.3 Rumusan Masalah

Rumusan masalah dari peneletian tugas akhir ini adalah bagaimana cara mengkombinasikan teknik steganografi DCT&LSB dan teknik kriptografi OTP.

Untuk menyelasaikan masalah di atas maka disusun menjadi pertanyaan penelitian (*Research Question)* :

1. Bagaimana cara kerja metode *Least Signifcant Bit* (LSB) di dalam teknik steganografi?
2. Bagaimana cara kerja metode *Discret Cosine Transform* (DCT) di dalam teknik steganografi?
3. Bagaimana cara kerja metode *One Time Pad* (OTP) di dalam teknik kriptografi?

4. Bagaimana cara mengkombinasikan teknik steganografi dengan metode LSB&DCT dan teknik kriptografi dengan metode OTP?
5. Apa keuntungan dan kekurangan dari kombinasi metode steganografi dengan metode LSB & DCT dan teknik kriptografi dengan metode OTP dibandingkan sebelum kombinasi?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah **:**

1. Mengetahui cara kerja metode LSB;
2. Mengetahui cara kerja metode DCT;
3. Mengetahui cara kerja metode OTP;
4. Mengembangkan teknik kombinasi steganografi dan kriptografi serta mengetahi cara mengkombinasikan DCT, LSB dan OTP.
5. Mengukur keuntungan dari kedua kombinasi dari segi keamanan dan ketahanan dalam proses *emmbed message* dan proses *encoder* atau *extraction.*

1.5 Manfaat Penelitian

Adapun manfaat peneltian :

1. Memahami dan mampu menerapkan metode *On Time Pad (OTP)*, *Discret Cosine Transform(DCT),* dan *Least Significant bit* dalam proses penyandian pesan dan penyisipan kedalam citra;
2. Mengembangkan metode kombinasi Stegano-Crypto System;

3. Hasil penelitian dapat dikembangkan atau menjadi perbandingan Stegano-Crypto System lainnya.
4. Mengetahui keuntungan dan kekurangan dari kombinasi metode *One Time Pad* (OTP), *Discret Cosine Transform* (DCT), dan *On Time Pad* (OTP).

1.6 Batasan Masalah

Ruang lingkup dalam penelitian ini adalah :

1. Citra berwarna 24 bit (*true color*);
2. Citra yang digunakan berekstensi (*.bmp);
3. Citra dan berkas teks digunakan secara offline;
4. Pengujian atau pembanding untuk mengukur kualitas citra stego dihitung menggunakan *Mean Square Error (MSE)* dan *Peak Signal to Noise Ratio (PSNR).*

1.7 Sistematika Penulisan

Sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Pada bab ini diuraikan mengenai latar belakang, perumusan masalah, tujuan dan manfaat penelitian, Batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti definisi-definisi kriptografi, steganografi, dan metode yang digunakan dalam steganografi dan kriptografi.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dibahas mengenai tahapan yang akan dilaksanakan pada penelitian ini. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja. Di akhir bab ini berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini akan dibahas mengenai perancangan perangkat lunak dan lingkungan implementasi Steganografi dan Kriptografi.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini, hasil pengujian berdasarkan langkah-langkah yang telah direncanakan disajikan. Analisis diberikan sebagai basis dari kesimpulan yang diambil dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga berisi saran-saran yang diharapkan berguna dalam penerapan teknik kombinasi Steganografi dan Kriptografi.

1.8 Kesimpulan

Penelitian ini akan berfokus pada kombinasi antara kedua teknik pengamanan pesan yaitu kriptografi dan steganografi. Metode yang digunakan dalam teknik kriptografi adalah *One Time Pad (OTP)*, sedangkan metode yang digunakan dalam steganografi adalah kombinasi dari algoritma *Discret Cosine Transform (DCT)* dan *Leas Significant Bit (LSB)*.

BAB II

KAJIAN LITERATUR

2.1 Pendahuluan

Pada bab I dijelaskan bahwa rumusan masalah penelitian ini adalah bagaimana cara mengkombinasikan teknik steganografi DCT&LSB dan teknik kriptografi OTP. Untuk memahami fundamental objek penelitian, penulis melakukan literature review terhadap jurnal, buku, dan artikel yang terkait dengan metode DCT,LSB,dan OTP.

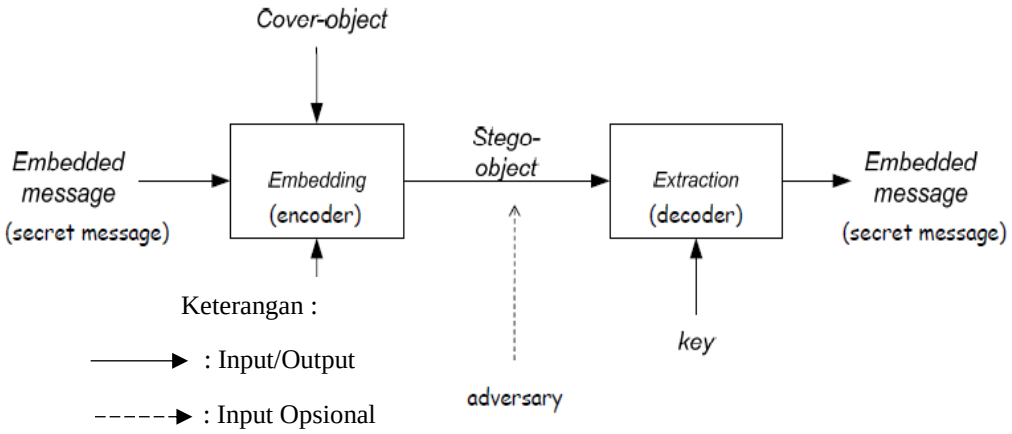
2.2 Steganografi

Steganografi berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan sehingga secara keseluruhan

artinya adalah tulisan yang disembunyikan. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

Steganografi digital dapat menyimpan pesan rahasia berupa teks, audio, gambar, maupun media lainnya dan disisipkan atau disembunyikan ke dalam media penampung (cover) berupa teks, audio, gambar, maupun media lainnya.

Ada dua buah proses dalam steganografi yakni proses penyisipan pesan *(embed)* dan proses ekstraksi pesan (*extract)*. Proses penyisipan pesan membutuhkan masukan media penyisipan, pesan yang akan disisipkan dan kunci. Keluaran dari proses penyisipan ini adalah media yang telah berisi pesan. Proses ekstraksi pesan membutuhkan masukan media yang telah berisi pesan. Keluaran dari proses ekstraksi pesan adalah pesan yang telah disisipkan. Adapun proses steganografi dapat dilihat pada gambar.



Gambar II-1. Proses Steganografi

Ada beberapa terminology dari steganografi yang memang harus dipahami antara lain, *embedded Message* atau *hiddentext* yaitu pesan atau informasi yang

disembunyikan, *cover-object* atau *covertext* yaitu pesan yang digunakan untuk menyembunyikan *embedded message*, *stego-object* atau s*tegotext* yaitu pesan yang sudah berisi *embedded message*.

Kriteria untuk menilai sebuah algoritma steganografi yaitu, *recovery* adalah algoritma steganografi harus dapat mengurai atau menampilkan kembali pesan yang tersembunyi pada *stego-object*, *imperceptibility* merupakan kemampuan untuk tidak dapat terasa atau terlihat oleh indera manusia, dan *fidelity* merupkan kualitas atau mutu pada media cover tidak mengalami perubahan berate karena dapat terlihat perbedaannya sehingga pihak ketiga (selain pengirim dan penerima) tidak curiga akan keberadaan pesan yang diselipkan pada media cover.

Penyisipan pesan (*Encoder*) pada algoritma-algoritma steganografi digital memiliki 2 teknik penyisipan secara sekuensial atau berurutan dan acak *(random)*. Teknik penyisipan secara sekuensial merupakan proses penyisipan pesan yang dilakukan secara berurutan pada bagian media penampung sedangkan teknik penyisipan pesan secara acak yaitu pesan disisipkan secara acak pada bagian-bagian tertentu pada media penampung. Misalkan media penampungnya adalah citra digital dengan dimensi 4x4 dengan menggunakan teknik sekuensial, penyisipan pesan dilakukan secara berurutan pada piksel dengan koordinat x,y mulai dari 0,0 hingga 3,3. Sedangkan teknik acak, penyisipan pesan dilakukan secara acak bisa disisipkan pada piksel dengan koordinat 1,3 terlebih dahulu kemudian kembali ke 0,2 lalu dapat lompat ke 3,3.

Perbedaan lainnya dari kedua teknik penyisipan tersebut yaitu teknik penyisipan sekuensial tidak memerlukan kunci keamanan, sedangkan acak sangat

bergantung pada kunci untuk dapat mengurai kembali pesan yang telah disisipkan pada objek *stego* sehingga penyisipan acak lebih unggul dari segi *level* atau tingkat pengamanan.

Banyak penelitian yang telah dilakukan telah membahas tentang metode-metode yang dapat diterapkan di dalam teknik steganografi terutama di dalam citra digital. Pada dasarnya teknik steganografi di dalam citra digital dibagi ke dalam 2 bagian yaitu *spatial domain* dan *transform domain*. *Spatial domain* mencakup metode bitwise yang mengaplikasikan metode penyisipan bit sedangkan untuk *transform domain* memanipulasi algoritma dan mentransformasi citra. Salah satu metode spatial domain adalah *Least Signicant Bit (LSB)* dan transform domain yang digunakan adalah *Discrete Cosine Transform (DCT)* di dalam teknik steganografi. Dari penelitian yang telah banyak dilakukan, peneliti ingin menggunakan kombinasi dari metode LSB dan DCT, serta teknik penyisipan sekuensial.

2.3 Citra Digital

Citra digital adalah kumpulan piksel-piksel yang disusun dalam larik dua dimensi. Indeks baris dan kolom (*x,y*) dari sebuah piksel yang dinyatakan dalam bilangan bulat dan nilai-nilai tersebut mendefinisikan suatu ukuran intensitas cahaya pada titik tersebut. Satuan atau bagian terkecil dari suatu citra disebut piksel (picture element).

Menurut (Kusumanto dan Tompunu 2011) Sebuah citra digital dapat diwakili oleh sebuah matriks dua dimensi f(x,y) yang terdiri dari M kolom dan N baris,

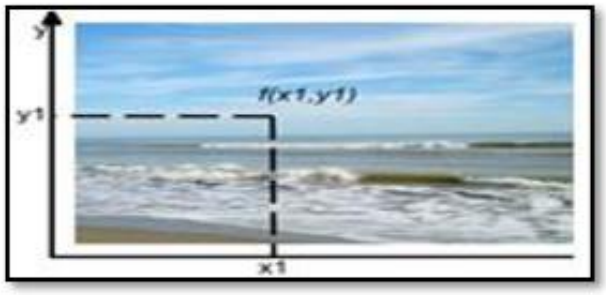
dimana perpotongan antara kolom dan baris disebut piksel (pixel = picture element) atau elemen terkecil dari sebuah citra.

$$f(x,y) \approx \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & f(1,M-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix}$$

Gambar II-2. Posisi Koordinat Citra Digital dalam Matrix (Kusumanto dan Tompunu 2011)

Format data citra digital berhubungan erat dengan warna, nilai data digital merepresentasikan warna dari citra, dalam penelitian ini menggunakan citra berwarna (*true color)*. Pada citra warna, setiap titik mempunyai warna spesifik yang merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru. Format citra ini sering disebut sebagai citra RGB (red, green dan blue).

Setiap warna dasar mempunyai intensitas sendiri dengan nilai maksimum 255 (8 bit). Misalnya warna kuning merupakan kombinasi warna merah dan hijau sehingga nilai RGB nya adalah [255,255,0], sedangkan warna ungu muda nilai RBG-nya adalah [150,0,150]. Dengan demikian, setiap titik pada citra berwarna membutuhkan data 3 byte atau sama dengan 24 bit. Jumlah kombinasi warna yang mungkin untuk format citra ini adalah 224 atau lebih dari 16 juta warna, dengan demikian bisa di anggap mencakup semua warna yang ada. Inilah sebabnya format ini dinamakan sebagai citra true color. Citra berwarna (true color) dapat diilustrasikan pada Gambar II-3.



Gambar II-3. Contoh citra berwarna (*true color)*

(Sumber : catatan penelitian.wordpress.com)

Format berkas citra digital standar yang digunakan dalam penelitian adalah Bitmap (.bmp). Format ini adalah format penyimpanan standar tanpa kompresi yang umum dapat digunakan untuk menyimpan citra biner hingga citra berwarna. Format ini terdiri dari beberapa jenis yang setiap jenisnya ditentukan dengan jumlah bit yang digunakan untuk menyimpan sebuah nilai piksel.

2.4 *American Standard Code for Information Interchange* (ASCII)

Tabel ASCII ini digunakan untuk proses pengubahan karakter teks ke dalam bentuk ASCII maupun proses mengubah deretan ASCII menjadi karakter kembali. Tabel ASCII yang digunakan dalam penelitian ini, berukuran 8 bit atau 127 karakter saja sesuai dengan yang ada pada keyboard.

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

Gambar II-4. Tabel ASCII

2.5 LSB

Metode LSB (*Least Significant Bit*) merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu. Untuk menjelaskan teknik penyembunyian LSB yang dipakai ini kita menggunakan citra digital sebagai covertext. Setiap pixel yang ada di dalam file citra berukuran 1 sampai 3 byte. Pada susunan bit dalam setiap byte (1 byte = 8 bit) , ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB)

Biner (Desimal : 151)	1	0	0	1	0	1	1	1
Berat bit (2^n)	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Posisi Bit	MSB	-	-	-	-	-	-	LSB

Bagian LSB atau paling kanan bernilai 2 pangkat 0 yaitu 1 merupakan nilai paling kecil sedangkan bagian MSB atau paling kiri bernilai 2 pangkat 7 yaitu 128 merupakan nilai paling besar.

Jumlah karakter pesan yang dapat ditampung oleh citra cover atau yang dapat disisipkan menggunakan LSB dapat dihitung dengan menggunakan rumus pada persamaan 2.2 dibawah ini :

$$\text{Daya Tampung} = \frac{((MN)i}{8}$$

Keterangan :

M : Tinggi Citra

N : Lebar Citra

i : Jumplah komponen warna

8 bit : 1 byte = 1 karakter

Sebagai contoh citra bewarna RGB dengan resolusi 620 x 500 akan mempunyai jumlah karakter pesan yang dapa ditampung sebanyak (persamaan 2.3) :

$$\text{Daya Tampung} = \frac{((620 \text{ x } 500) \text{ x } 3}{8} = 116250 \textit{ karakter}$$

2.6 DCT

Transformasi ini dikenal luas untuk pemrosesan citra digital. Pada dasarnya DCT merupakan suatu transformasi domain, yaitu proses perubahan pada citra digital dari satu domain ke domain lainnya. Dalam hal ini DCT melakukan

perubahan pada citra digital dari domain spasial ke domain frekuensi, *one-to-one mapping* dari suatu array yang terdiri dari nilai pixel menjadi komponen-komponen yang terbagi menjadi frekuensi. Rumus perhitungan *Discret Cosine Transform* :

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{M-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]cos\left[\frac{\pi(2y+1)v}{2M}\right]$$

Keterangan :

X = 0,1,2, …., N-1

Y = 0,1,2, M01

u = frekuensi spasial horisontal (baris)

v = frekuensi spasial vertikal (kolom)

C(u,v) = koefisien DCT pada koordinat (u,v) dan

$$u)dan\alpha(v) = \begin{cases} \sqrt{\frac{1}{8}} untukudanv = 0 \\ \sqrt{\frac{2}{8}} untukudanv \neq 0 \end{cases}$$

Untuk invers dari transformasi 2D DCT dapat dilihat pada persamaan di bawah ini:

$$C(u,v) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \propto (u) \propto (v) C(u,v) cos\frac{\pi(2x+1)u}{2N} cos\frac{\pi(2y+1)}{2N}$$

2.7 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknikteknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua aspek keamanan informasi ditangani oleh kriptografi. Enkripsi erat kaitannya dengan

dekripsi, untuk itulah muncul istilah kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan informasi yang telah dienkripsi tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut dengan kriptanalis.

2.8 OTP

One Time Pad (OTP) adalah salah satu algoritma kriptografi yang cukup populer dan sering digunakan dalam teknik enkripsi data. OTP juga terkenal sebagai algoritma enkripsi yang sempurna, karena pada algoritma ini kunci yang dipakai merupakan kunci acak dan hanya dapat digunakan sekali proses enkripsi.

OTP merupakan satu-satunya metode enkripsi yang tangguh yang tidak dapat dipecahkan secara sistematis karena proses enkripsi dan dekripsi hanya dapat dilakukan dalam satu waktu pemrosesan. Selain itu kunci yang digunakan dalam metode OTP merupakan kunci yang benar-benar acak dan sama sekali tidak mengandung informasi tentang plaintext dimana besar kunci adalah sama dengan besar palintext, selain itu kunci pada OTP ini juga hanya dapat digunakan satu kali pada proses enkripsi dan dekripsi pada satu waktu. Berikut adalah rumus enkripsi OTP :

$$c = (p + k) \bmod 2$$

Sedangkan rumus dekripsi OTP adalah :

$$p = (c - k) \bmod 2$$

Keterangan :

c = chipertext (pesan acak)

p = plaintext (pesan asli)

k = key / kunci rahasia yan digunakan

2.9 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 biasanya diukur dalam satuan desibel. Pada tugas akhir kali ini, PSNR digunakan untuk mengetahui perbandingan kualitas citra sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai rata-rata kuadrat dari error (MSE - Mean Square Error). Perhitungan MSE adalah sebagai berikut :

$$MSE = \frac{1}{mn} \sum_{i}^{m} \sum_{j}^{n} \; || \, I \, (i,j) - K \, (i,j) \, ||^{2}$$

Keterangan :

MSE = Nilai *Mean Square Error* dari citra tersebut

m = panjang citra tersebut (dalam piksel)

n = lebar citra tersebut (dalam piksel)

(i,j) = koordinat masing-masing piksel

I = nilai bit citra pada koordinat i,j

K = nilai derajat keabuan citra pada koordinat i, j

Dari persamaan diatas, dapat dihitung dari kuadrat nilai maksimum sinyal dibagi dengan MSE. Apabila diinginkan PSNR dalam decibel, maka nilai PSNR akan menjadi sebagai berikut :

$$PSNR = 20 \log_{10}\left(\frac{255}{\sqrt{MSE}}\right)$$

Keterangan :

PSNR = nilai PSNR citra (dalam dB)

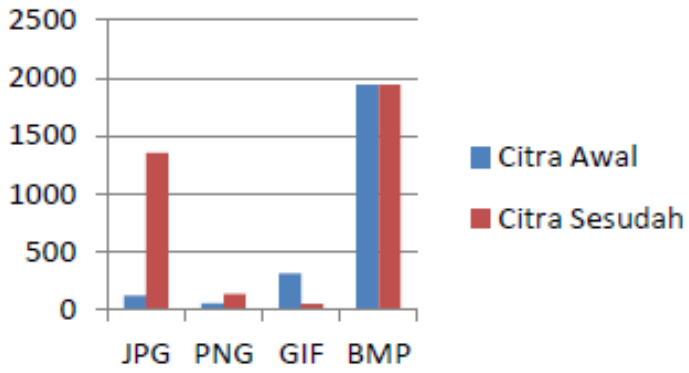
MSE = nilai MSE

Semakin besar ukuran berkas citra yang digunakan maka semakin baik nilai PSNR dalam decibel (dB) yang diperoleh dibandingkan dengan citra yang berukuran lebih kecil dengan jumlah sisipan karakter yang sama. Hal ini menunjukkan bahwa untuk memperoleh citra yang baik setelah proses penyisipan dan tidak mengalami perubahan yang cukup berarti dari citra sebelumnya maka besar ukuran file citra dalam piksel dan banyaknya karakter yang akan disisipkan perlu diperhatikan untuk memperoleh hasil yang baik.

2.10 Penelitian Lain yang Relevan

Penelitian mengenai penggabungan teknik steganografi dan kriptografi yang dilakukan oleh (Ali Mahmudi, Sandy Nataly Mantja dan Rozikin 2016) yang

berjudul aplikasi kriptografi dan steganografi menggunakan metode *least significant bit (LSB)* dan *One Time Pad* (OTP) dimana dari hasil pengujian yang dilakukan, dapat diketahui bahwa beberapa citra tidak dapat dibaca kembali pesan yang disisipkan, dikarenakan perbedaan format citra. Format citra yang masih dapat dibaca informasinya adalah JPG dan BMP sedangkan format citra PNG dan GIF tidak dapat lagi membaca informasi yang disisipkan.



Gambar II-5. Diagram pengujian berkas citra (Ali Mahmudi, Sandy Nataly Mantja dan Rozikin 2016)

Pengujian yang dilakukan membuktikan bahwa, kekuatan dari kriptografi dengan menggunakan metode OTP adalah pada keacakan kunci. Semakin acak kunci, maka semakin baik metode kriptografi ini untuk mengacak informasi. Panjang kunci pada kriptografi metode OTP dapat disesuaikan dengan jumlah informasi yang dimaksukkan sehingga probalitas terbentuknya huruf akan semakin banyak. Pesan yang akan disisipkan pada citra digital dengan metode LSB, terlebih dahulu akan di enkripsi dengan metode OTP, steganogarfi LSB pada citra digital dilakukan dengan mengganti tiap bit LSB intensitas RGB citra dengan bit-bit pesan yang telah dikonversi menjadi bilangan biner.

(Najih 2017) menggabungkan teknk steganografi dan kriptografi dengan *discret cosine transform (DCT), Onet Time Pad (OTP),* dan *pn-sequence* pada citra digital, dimana sistem yang dibuat harus mengenkripsi terlebih dahulu citra pesan sebelum disematkan pada citra digital lain (citra cover), dalam proses penyematannya, sistem ini memanfaatkan metode PN-Sequence yang digunakan sebagai penyebar embedding citra pesan pada citra cover. Berdasarkan hasil pengujian, penggabungan teknik yang diusulkan ini menghasilkan citra yang identik dengan citra cover. Selain perbedaannya tidak dapat dilihat secara kasat mata, pembuktian hal tersebut bisa dilihat dari nilai MSE dan PSNR yang tergolong sangat baik dan sekaligus menghasilkan ekstraksi yang sempurna. Selain itu dari sisi ketahanan, teknik yang diusulkan ini juga cukup kuat untuk diberikan serangan *JPEG Compression* dan *crop*, sedangkan pada pengujian serangan median filter menghasilkan nilai NCC yang tidak sebagus serangan yang lain, karena hasil recovery citra pesan terlihat rusak dan agak sulit dibaca atau dimengerti.

Penelitian yang dilakukan oleh (Kustov dan Protsko 2017) Menggunakan kombinasi metode LSB dan DCT (LSB & DCT) memungkinkan untuk menyembunyikan dan mengirim data yang ukurannya meskipun jauh lebih kecil dari stegocontainer, tapi memberikan resistensi terhadap kehadiran noise di saluran data. Kebisingan noise dari metode yang diusulkan berdasarkan LSB dan kombinasi metode DCT karena kemampuannya untuk menyembunyikan data daerah frekuensi (*spectral*) gambar, yang meningkatkan Kebisingan kekebalan data tersembunyi. Sebagai hasil pengujian model perangkat lunak yang dikembangkan. Algoritma

DCT & LSB lebih tahan terhadap berbagai stegoattacks dan distorsi stegocontainer adalah dari LSB.

2.11 Kesimpulan

Dalam bab kajian pustaka membahas tentang dasar-dasar atau penjelasan mengenai metode-metode yang digunakan dalam penelitian diantaranya untuk proses enkripsi pesan teks menggunakan teknik kriptografi dengan metode OTP *(One Time Pad),* pada proses selanjutnya yaitu penyisipan pesan teks kedalam media digital yaitu citra menggunakan teknik steganografi dengan gabungan metode DCT dan LSB.

BAB III

METODOLOGI PENELITIAN

3.1 Pendahuluan

Bab ini menjelaskan unit penelitian, tahapan penelitian yang diimplementasikan, metodologi penelitan, serta penjadwalan penelitian. Tahapan penelitian dijadikan sebagai acuan pada setiap fase pengembangan dan memberikan sebuah solusi untuk rumusan masalah dan mencapai tujuan penelitian.

3.2 Pengumpulan Data

Pengumplan data untuk penelitian digunakan untuk pengujian perangkat lunak dengan menggunakan system pemrosesan file. Sistem Pemroesesan file digunakan untuk data bersifat statis (seperti: citra cover (*.bmp) dan pesan teks (*.txt). Berikut data yang digunakan dalam penelitian, yaitu :

1. Data citra cover (*.bmp)

   Data citra cover berfungsi sebagai data masukkan yang digunakan untuk mendapatkan citra stego dengan menyisipkan isi pesan teks kedalam bit-bit kurang berarti dalam citra cover. Karakteristik data citra cover ditunjukkan pada table III-1.

Tabel III-1. Karakteristik Data Citra Cover

Jumlah	3 Citra Bewarna (24 bit)
Resolusi	512 x 512
Format	Bitmap

Keterangan	Citra ini merupakan citra standar dalam image processing yaitu citra lena, baboon dan peppers bewarna yang telah diubah menjadi 24 bit menggunakan aplikasi GIMP.

2. Data pesan teks (*.txt)

Data pesan teks berfungsi sebagai data pesan yang akan disematkan atau disembunyikan keberadaannya dan digunakan sebagai masukkan untuk proses penyisipan untuk menghasilkan citra stego (citra yang berisi pesan rahasia didalamnya). Karakteristik data pesan teks ditunjukkan pada table III-2.

Tabel III-2. Karakteristik Data Pesan Teks

Jumlah	3 berkas pesan teks
Ukuran	bervariasi
Format	TXT
Keterangan	Jumlah karakter pesan maksimal dilakukan dengan mengukur pesan maksimal yang diukur menggunakan kapasitas pesan yang dapat disimpan dalam citra. Dengan variasi pesan 10%, 50% dan 100%

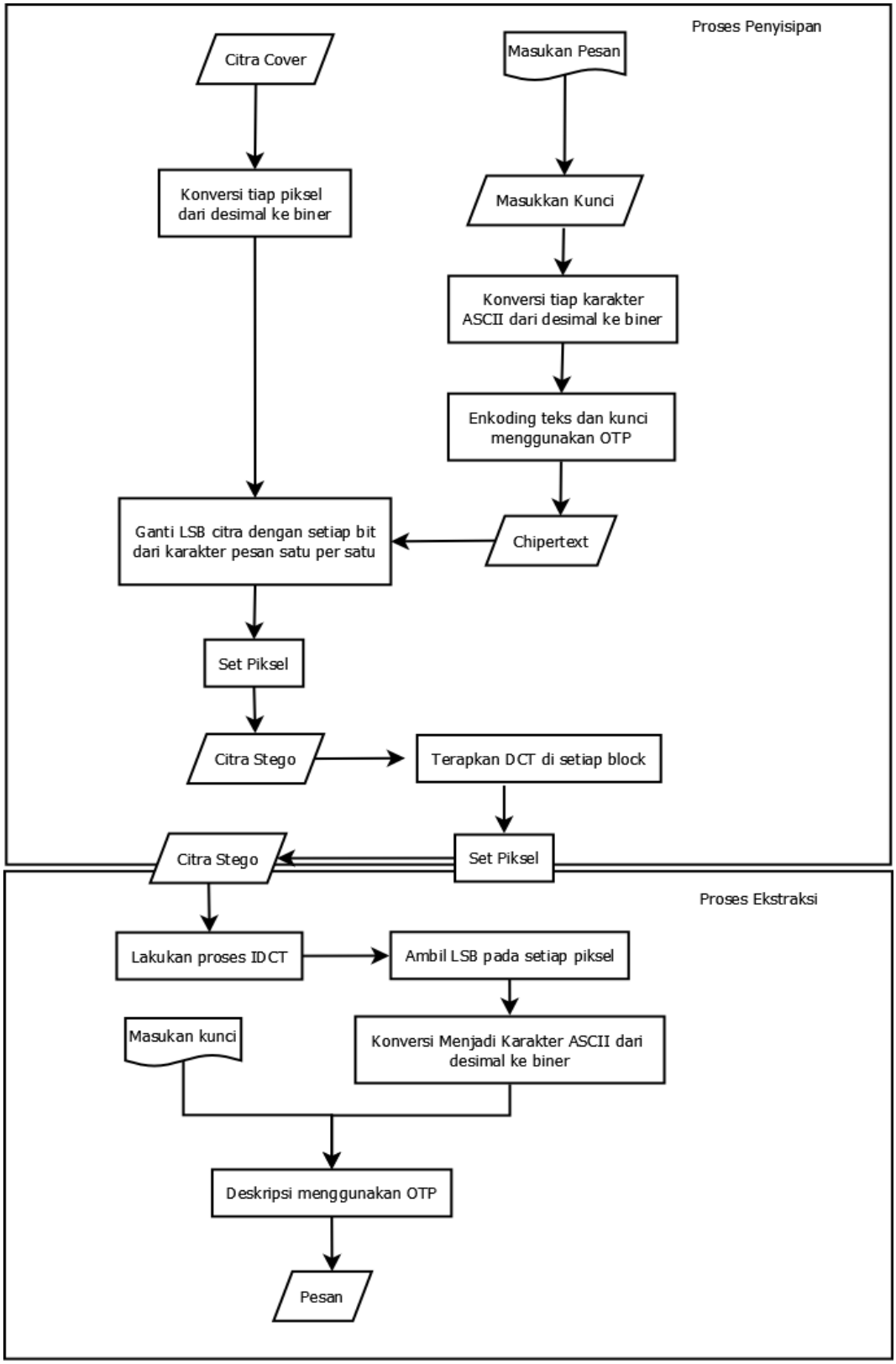
	yang dapat ditampung oleh citra cover.

3.3 Tahapan Penelitian

Untuk mengetahui tahapan-tahapan yang akan dilalui selama melaksanakan skripsi, meliputi :

3.3.1 Kerangka Kerja

Alur atau kerangka kerja penelitian digambarkan dengan flowchart dibawah ini:



Gambar III-1. Proses Penyisipan dan Ekstrasi.

3.3.2 Kriteria Pengujian

Kriteria dalam pengujian yaitu diukur dengan kapasitas dan ukuran dari 3 buah file teks dan 3 buah citra cover bewarna yang telah ditetukan pada subbab sebelumnya, pengujian kualitas dari citra *stego* dengan membandingkannya dengan citra asli menggunakan parameter MSE dan PSNR, dan pengujian perbandingan visual citra *cover* dan *stego.*

3.3.3 Alat yang Digunakan dalam Pelaksanaan Penelitian

Alat yang digunakan berupa perangkat keras (hardware), perangkat lunak (software) dan bahasa pemrograman. Perangkat keras yang digunakan adalah laptop dengan spesifikasi :

1. Processor intel ® Core™ i5-6198DU CPU @2.30GHz 2.40 GHz
2. Ram 4.00 GB DDR4.
3. Perangkat input berupa mouse atau touchpad dan keyboard.

Perangkat lunak yang digunakan pada adalah :

1. Sistem Operasi Windows 10 Professional 64-bit.
2. Compiler netbeans
3. Notepad.

Bahasa pemrograman yang digunakan pada penelitiann adalah Bahasa pemrograman Java.

3.3.4 Pengujian Penelitian

Pembahasan mengenai tahapan ini akan dijelaskan pada bab V. Pada tahapan pengujian penelitian, data hasil pengujian citra akan digambarkan dalam table III-3.

Tabel III-3. Hasil Pengujian Kapasitas dan Ukuran

No	Citra Cover	Dimensi Citra Cover	Ukuran Citra Cover	File Teks	Banyak Karater	Ukuran File Teks (KB)	Ukuran Citra Stego (KB)	Penyisipan	Ekstraksi
PS-1-1	Lena.bmp	512 x 512							
PS-1-2									
PS-1-3									
PS-1-4	Baboon.bmp	512 x 512							
PS-1-5									
PS-1-6									

PS-1-7	Peppers.bmp	512 x 512							
PS-1-8									
PS-1-9									

Tabel III-4. Hasil Pengujian Kualitas

No	Citra Cover	Citra Stego	Nilai MSE	Nilai PSNR (Db)
PS-1-1	Lena.bmp			
PS-1-2				
PS-1-3				
PS-1-4	Baboon.bmp			
PS-1-5				
PS-1-6				
PS-1-7				

PS-1-8	Peppers.bmp			
PS-1-9				

Tabel III-5. Perbandingan Visual Citra Cover dan Stego

Cita Cover	Citra Stego		
Lena.bmp	Lena 10%.bmp	Lena 50%.bmp	Lena 100%.bmp
Baboon.bmp	Baboon 10%.bmp	Baboon 50%.bmp	Baboon 100%.bmp
Peppers.bmp	Peppers 10%.bmp	Peppers 50%.bmp	Peppers 100%.bmp

3.3.5 Analisis Hasil Pengujian dan Membuat Kesimpulan

Sesuai dengan kriteria pengujian bahwa dapat diketahui bahwa Analisa dalam pengujian yaitu diukur dengan kapasitas dan ukuran dari 3 buah file teks dan 3 buah citra cover bewarna, dimana dengan mengukur size dari setiap citra *stego* dan dibandingkan dengan citra asli.

Pengujian kualitas dari citra *stego* dengan membandingkannya dengan citra asli menggunakan parameter MSE dan PSNR dimana rumus untuk mengukurnya telah dibahas pada bab tinjauan pustaka, dimana semakin tinggi nilai PSNR semakin bagus kualitas citra tersebut.

Pengujian perbandingan visual citra *cover* dan *stego,* dimana pada proses pengujian ini langsung melihat perbedaan visual dari gambar yang telah dilakukan proses penyisipan dengan citra asli, apakah perubahan citra *stego* berbeda atau berubah signifikan atau tidak.

3.4 Metode Pengembangan Perangkat Lunak

Metodologi yang diterapkan dalam pengembangan perangkat lunak sebagai alat penelitian tugas akhir ini berorientasi pada objek menggunakan metode Rational Unified Process (RUP). Secara umum, langkah-langkah yang akan dilakukan pada pengembangan perangkat lunak adalah fase insepsi, elaborasi, konstruksi, dan transisi (Pressman, 2005).

3.4.1 Fase Insepsi

Pada tahapan pemodelan bisnis, penulis menentukan *user requirements* dan fungsionalitas atau fitur-fitur yang dibutuhkan pada perangkat lunak. Pada

tahapan pengumpulan kebutuhan, penulis mengumpulkan data penelitian berupa jurnal berbahasa Indonesia dan inggris di (*ieeexplore.ieee.org/*) dan (*https://scholar.google.co.id/).* Pada tahap analisis dan desain, penulis membuat diagram *use case*. Pada tahap implementasi, penulis mendokumentasikan *user requirements*, fungsionalitas perangkat lunak dan diagram *use case*. Pada tahap pengujian, penulis memastikan apakah *user requirements* dan fungsionalitas perangkat lunak sudah valid.

3.4.2 **Fase Elaborasi**

Pada tahapan pemodelan bisnis, penulis menentukan arsitektur perangkat lunak, desain basis data, dan desain antar muka sesuai dengan *user requirements* dan fungsionalitas perangkat lunak yang telah didapatkan. Penulis dapat melengkapi *user requirement*, apabila dirasa belum lengkap, pada tahap pengumpulan kebutuhan. *Activity diagram* dan *sequence diagram* dibuat pada tahap analisis dan desain. Penulis menyusun dokumentasi yang memuat arsitektur perangkat lunak, desain basis data, desain antar muka, *activity diagram*, dan *sequence diagram* pada tahap implementasi lalu memastikan seluruhnya sudah valid pada tahap pengujian.

3.5.1 Fase Konstruksi

Pada tahapan pemodelan bisnis, penulis menentukan kelas-kelas yang dibutuhkan pada perangkat lunak. Pada tahap pengumpulan kebutuhan, ditentukan bahasa pemrograman yang digunakan untuk mengembangkan perangkat lunak,

yaitu Java. Kebutuhan lain dalam proses pengembangan perangkat lunak juga diidentifikasi, seperti perangkat keras dengan Processor intel ® Core™ i5-6198DU CPU @2.30GHz 2.40 GHz, Ram 4.00 GB DDR4, Perangkat input berupa mouse atau touchpad dan keyboard., dan Harddisk 1 TB, *dia.diagram*, dan Netbeans IDE 8.0.2. *Class diagram* dibuat pada tahap analisis dan desain. Pada tahapan implementasi, penulis mengembangkan perangkat lunak dengan mengimplementasi kelas-kelas yang telah ditentukan ke kode program dalam bahasa Java. Selanjutnya, penulis melakukan *unit testing* terhadap perangkat lunak yang telah dikembangkan.

3.5.2 Fase Transisi

Pada tahapan pemodelan bisnis, penulis membuat rencana atau skenario pengujian terhadap perangkat lunak. Penulis menentukan *tools* pengujian yang diperlukan di tahap pengumpulan kebutuhan. *Tools* pengujian merupakan perangkat keras yang sama saat digunakan untuk pengembangan perangkat lunak yaitu laptop dengan dengan Processor intel ® Core™ i5-6198DU CPU @2.30GHz 2.40 GHz, Ram 4.00 GB DDR4, Perangkat input berupa mouse atau touchpad dan keyboard., dan Harddisk 1 TB. Penulis lalu mendesain tabel skenario pada tahap analisis dan desain. Pada tahapan implementasi, penulis melakukan pengujian terhadap perangkat lunak berdasarkan skenario atau rencana pengujian. Skenario pengujian ditinjau ulang pada tahap pengujian.

3.5 Manajemen Proyek Penelitian

Penjadwalan merupakan perencanaan aktivitas penelitian dari tahap inisialisasi masalah sampai dengan pada tahap kesimpulan dari penelitian. Adapun kegiatan-kegiatan yang berlangsung selama penelitian dapat dilihat dalam *Work Breakdown Structure* (WBS) yang tertera pada Tabel III-5, dan *Gantt Chart* pada Gambar III-6, Gambar III-7, Gambar III-9, Gambar III-10, Gambar III-11, Gambar III-12, dan Gambar III-13.

DAFTAR PUSTAKA

Ahmad Aidil Fitri, Megah Mulya, Alfarissi. 2016. "Steganografi pada Citra Digital Berwarna 32-Bit Menggunakan Least Significant Bit." *Jurnal Informatika* 2 (1): 169–72.

Ali Mahmudi, Sandy Nataly Mantja, Dan, dan Achmad Rozikin. 2016. "Aplikasi Kriptografi dan Steganografi Menggunakan Metode Least Significant Bit (LSB) dan One Time Pad (OTP)." *Matics* 8 (1): 1. https://doi.org/10.18860/mat.v8i1.3473.

Kustov, Vladimir N, dan Dmitry K Protsko. 2017. "Modeling Hidden Data by Combined LSB & DCT Algoritnm," 155–58.

Kusumanto, R D, dan Alan Novi Tompunu. 2011. "Pengolahan Citra Digital Untuk Mendeteksi Obyek Menggunakan Pengolahan Warna Model Normalisasi RGB." *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011* 2011 (Semantik): 1–7.

Najih, Muhammad. 2017. "Kombinasi Teknik Steganografi dan Kriptografi dengan Discrete Cosine Transform (DCT), One Time Pad (OTP) dan PN-Sequence pada Citra Digital."