



STEGANOGRAPHI



Oleh : Rusito, M.Kom

Steganografi

- ◉ Steganografi berasal dari bahasa Yunani yaitu kata *Stegos*, yang artinya tertutup atau tersembunyi, dan *graphos*, yang artinya tulisan.
- ◉ steganografi merupakan bagian dari bidang ilmu yang membahas tentang metode-metode atau teknik-teknik tentang menyembunyian informasi (*information hiding*) di dalam informasi lainnya

Steganografi Vs Kriptografi

- Pada kriptografi pesan yang di sandikan masih dapat dilihat karena metode yang di gunakan adalah menghilangkan informasi dengan melakukan enkripsi data (data dikacaukan) sehingga tidak dimengerti orang lain. Sedangkan, pada steganografi pesan di sembunyikan pada pesan (informasi) lain sehingga menjadi suatu pesan yang tidak terlihat
- Kriptografi menarik perhatian karena pesan di ubah. Sedangkan, steganografi tidak menarik perhatian karena pesan disembunyikan

Penggunaan Steganografi

- metode steganografi menghilangkan keberadaan suatu pesan informasi sehingga pesan informasi tersebut menjadi suatu pesan yang tak terlihat (*invisible*) sehingga pesan rahasia tidak akan menarik perhatian, baik terhadap pesan itu sendiri, terhadap pembawa pesan, atau penerima pesan.
- Contoh penggunaan Steganografi adalah pemberian tanda-air digital (*digital watermark*) pada suatu berkas. biasanya digunakan untuk melindungi hak kepemilikan intelektual pada berkas tersebut dan digunakan dalam bidang komunikasi rahasia (*covert communications*).

Media Pembawa (Carrier)

- ◉ Dalam steganografi berbasis komputer, media pembawa (*carrier*) dapat berupa citra digital, audio, video, grafik, dan sebagainya.
- ◉ Pada steganografi berkas pembawa berupa teks kurang cocok untuk di terapkan karena Berukuran kecil sehingga dapat mengubah total pesan pembawa

Kriteria Berkas Pembawa

- Berkas-berkas tersebut telah dikompresi dengan algoritma tertentu, sehingga pesan yang disisipkan juga ikut terkompresi.
- Berkas-berkas tersebut biasanya berukuran besar, sehingga pesan informasi rahasia dapat disisipkan tanpa mempengaruhi atau mengubah berkas pembawa secara signifikan.
- Berkas-berkas tersebut merupakan pengalih perhatian yang baik bagi pesan rahasia yang akan disembunyikan.

Cara Kerja Steganografi

- ◉ Steganografi bekerja dengan mengganti bit-bit data yang tidak berguna atau tidak terpakai dalam berkas-berkas komputer umumnya (seperti grafik, suara, teks, HTML, atau bahkan disket) dengan bit-bit yang berbeda,
- ◉ yaitu informasi yang tak terlihat. Pesan rahasia yang disembunyikan terlebih dahulu dikonversi ke dalam suatu aliran bit informasi.
- ◉ Kemudian bit-bit informasi ini disisipkan ke dalam berkas yang berperan sebagai pembawa.
- ◉ Metode ini memanfaatkan bit-bit LSB berkas (*file*) pembawa dan menggantinya dengan bit-bit dari pesan informasi.
- ◉ Informasi yang tersembunyi ini dapat berupa teks biasa (*plain text*), teks tersandi (*chiper text*), atau suatu citra.

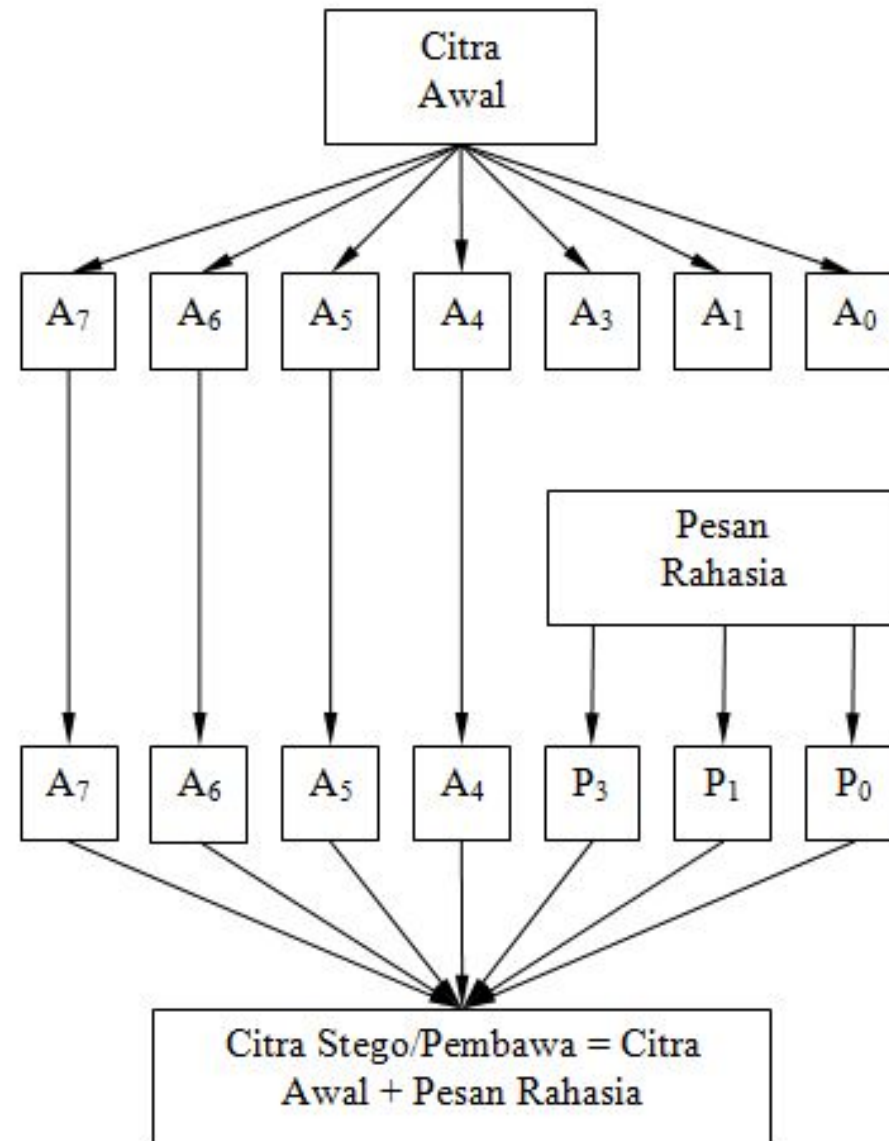
Steganografi Berbasis Citra

- Steganografi berbasis citra digital dapat dikategorikan dalam dua kategori, yaitu:
 - steganografi dalam kawasan citra dan
 - dalam kawasan alih ragam.
- Dalam kawasan citra, steganografi dilakukan dengan metode penggantian atau penyisipan bit pada LSB atau sering disebut manipulasi derau (*noise manipulation*).
- Disebut demikian karena pesan rahasia pada citra yang disisipkan, akan mengubah piksel tertentu pada citra.
- Jika perubahan tersebut terlihat, akan nampak seperti derau pada citra tersebut.
- Pendekatan ini melibatkan citra berformat tak berugi, dan pesan disisipkan dan diambil secara langsung, tanpa melibatkan proses alih ragam.
- Sedangkan dalam kawasan alih ragam, proses dilakukan dengan melibatkan manipulasi dari algoritma alih ragam citra.

Steganografi Berbasis Citra

- ◉ Dalam metode penyisipan LSB, steganografi dilakukan dengan cara mengganti satu atau beberapa bit-bit RGB piksel citra awal ($A_0 - A_3$) dengan bit-bit dari pesan rahasia ($P_0 - P_3$) yang akan disembunyikan.
- ◉ Berkas citra pembawa yang telah disisipi pesan rahasia, atau disebut juga berkas atau citra stego, dapat dikirimkan ke penerima.
- ◉ Penerima dapat mengekstraksi pesan tersebut atau melakukan aksi desteganografi dari citra pembawa sehingga mendapatkan bit-bit pesan tersembunyi dari citra pembawa.

Steganografi Berbasis Citra



Gambar 2.2 Steganografi berbasis citra digital dengan metode penggantian atau penyisipan LSB.

CONTOH SOAL :

Suatu citra pembawa memiliki 9 piksel (ukuran citra 3X3), resolusi 8 bit, dengan nilai-nilai intensitasnya ditunjukkan dengan gambar berikut :

215	103	72
79	44	7
33	10	59

Informasi yang akan disisipkan adalah teks “Aku”. Bagaimanakah pesan dalam desimal setelah dilakukan steganografi, jika diketahui 3-bit LSB pada citra pembawanya dapat disisipi oleh informasi teks tsb?

TABEL ASCII

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
	00 0000	01 0001	02 0010	03 0011	04 0100	05 0101	06 0110	07 0111	08 1000	09 1001	10 1010	11 1011	12 1100	13 1101	14 1110	15 1111	
	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI	
0	☐	┐	└	┌	↯	⊠	✓	␣	↵	➤	≡	∇	⇓	⇐	⊗	⊙	8
	16 0001	17 0010	18 0011	19 0100	20 0101	21 0110	22 0111	23 1000	24 1001	25 1010	26 1011	27 1100	28 1101	29 1110	30 1111	31 1111	
	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US	
1	☐	⊖	⊕	⊗	⊙	✓	␣	↵	⊠	†	‡	⊖	⊕	⊗	⊙	⊙	9
	32 0010	33 0011	34 0100	35 0101	36 0110	37 0111	38 1000	39 1001	40 1010	41 1011	42 1100	43 1101	44 1110	45 1111	46 1111	47 1111	
2	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/	A
	48 0011	49 0100	50 0101	51 0110	52 0111	53 1000	54 1001	55 1010	56 1011	57 1100	58 1101	59 1110	60 1111	61 1111	62 1111	63 1111	
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?	B
	64 0100	65 0101	66 0110	67 0111	68 1000	69 1001	70 1010	71 1011	72 1100	73 1101	74 1110	75 1111	76 1111	77 1111	78 1111	79 1111	
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	C
	80 0101	81 0110	82 0111	83 1000	84 1001	85 1010	86 1011	87 1100	88 1101	89 1110	90 1111	91 1111	92 1111	93 1111	94 1111	95 1111	
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_	D
	96 0110	97 0111	98 1000	99 1001	100 1010	101 1011	102 1100	103 1101	104 1110	105 1111	106 1111	107 1111	108 1111	109 1111	110 1111	111 1111	
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	E
	112 0111	113 0111	114 0111	115 0111	116 0111	117 0111	118 0111	119 0111	120 0111	121 0111	122 0111	123 0111	124 0111	125 0111	126 0111	127 0111	
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL	F

Konversi teks 'Aku':

ASCII ('A') = 01000001_b

ASCII ('k') = 01101011_b

ASCII ('u') = 01110101_b

Sedangkan konversi piksel-per piksel adalah sbb.

215 = 11010111 7 = 00000111

103 = 01100111 33 = 00100001

72 = 01001000 10 = 00001010

79 = 01001111 59 = 00111011

44 = 00101100

JAWAB:

215 = 11010111
103 = 01100111
72 = 01001000
79 = 01001111
44 = 00101100

7 = 00000111
33 = 00100001
10 = 00001010
59 = 00111011

Konversi teks 'Aku':

ASCII ('A') = 01000001_b

ASCII ('k') = 01101011_b

ASCII ('u') = 01110101_b

Penyisipan teks 'Aku'

215 □ 11010110 = 2147 □ 00000110 = 6

103 □ 01100111 = 10333 □ 00100010 = 34

72 □ 01001000 = 72 10 □ 00001001 = 9

79 □ 01001110 = 78 59 □ 00111010 = 58

44 □ 00101000 = 40

Sehingga Hasilnya setelah di
steganografi menjadi

214	103	72
78	40	6
34	9	58

TERIMA KASIH