

PERANCANGAN PERANGKAT LUNAK KRIPTOGRAFI VISUAL TANPA EKSPANSI PIKSEL DAN ALGORITMA RLE

Dhina Bangkit Kumalasari

Email: dhina_kumalasari@hotmail.de

Jurusan Teknik Elektro, Fakultas Teknik

Universitas Kristen Maranatha

Jl. Prof. Drg. Suria Sumantri 65, Bandung 40164, Indonesia

ABSTRAK

Kriptografi visual diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1995. Kriptografi visual digunakan pada media yang dapat dicetak, misalkan citra. Pada skema (n,n) , sebuah citra rahasia akan diubah menjadi n buah citra enkripsi yang dicetak dalam bentuk transparansi. Untuk mendekripsinya tidak membutuhkan komputasi matematis, tetapi dilakukan dengan menumpuk n buah citra terenkripsi dengan tepat dan dilihat dengan pandangan mata. Pada tugas akhir ini penumpukan dilakukan menggunakan logika OR. Untuk jumlah citra kurang dari n , maka tidak ada informasi apapun yang dapat diperoleh mengenai citra rahasia.

Pada tugas akhir ini skema yang digunakan adalah kriptografi visual $(3,3)$, yaitu sebuah citra rahasia akan diubah menjadi 3 citra terenkripsi. Citra yang digunakan adalah citra biner. Prosesnya adalah dengan mengubah citra tersebut menjadi 3 citra terenkripsi, kemudian matriks dari 3 citra *share* tersebut akan diproses dengan algoritma metode RLE. Untuk proses dekripsinya matriks-matriks *share* yang telah diproses dengan algoritma RLE akan diproses kembali menjadi matriks semula kemudian didekripsi menggunakan logika OR sehingga didapatkan citra semula.

Pengujian dilakukan dengan 6 citra berbeda yang memiliki ukuran piksel yang berbeda. Hasil pengujian yang didapatkan yaitu program penyembunyian citra rahasia menggunakan Visual Kriptografi (3,3) tanpa ekspansi piksel menggunakan *software* MATLAB berhasil direalisasikan, citra hasil dekripsi pada citra rahasia yang bergaris tipis tidak dapat dikenali, *relative difference* (α) yang menunjukkan seberapa baik kontras citra hasil dekripsi dengan *additional basis* yaitu sekitar 0,375 lebih besar daripada kontras citra hasil dekripsi tanpa *additional basis* yaitu sekitar 0,25, nilai PSNR (*Peak Signal to Noise Ratio*) dan MOS (*Mean Opinion Score*) yang didapatkan kecil.

Kata Kunci : Kriptografi, Kriptografi Visual

VISUAL CRYPTOGRAPHY WITHOUT PIXEL EXPANSION SOFTWARE DESIGN AND RLE ALGORITHM

Dhina Bangkit Kumalasari

Email: dhina_kumalasari@hotmail.de

**Department of Electrical Engineering, Faculty of Engineering
Maranatha Christian University**

Jl. Prof. Drg. Suria Sumantri 65, Bandung 40164, Indonesia

ABSTRACT

Visual cryptography was introduced by Moni Naor and Adi Shamir in 1995. Visual Cryptography is used in the media that can be printed, eg image. In scheme (n, n) , a secret image will be converted into n pieces of encrypted image is printed in the form of transparency. To decrypt it does not require mathematical computation, but is done by stacking n encrypted image. With the right image, secret image will be seen or use logic OR. In this final project stacking performed using a logical OR. For the number of images is less than n , then there is no any information that can be obtained about the secret image.

In this final assignment used scheme of a visual cryptography (3.3), which is the secret image will be converted into 3 encrypted image. The image used are binary image. The process is to convert the image into 3 encrypted image, then the matrix of 3 share images will be processed with RLE algorithm. For decryption process share matrices that has been processed with RLE algorithm will be processed back into matrix before processed with RLE algorithm and decrypted using a logical OR to obtain the original image.

Tests carried out with 6 different images that have different levels of detail and different pixel size. The test result were obtained that the program of a secret image hiding using visual cryptography (3.3) without pixel expansion using MATLAB software successfully realized, the decrypted image of thin striped secret image can not be recognized, the relative difference (α) which indicates how well the contrast of the image of the decryption with additional basis about 0.375 more than contrast image of the decryption without additional basis about

0.25, the value of PSNR (Peak Signal to Noise Ratio) and MOS (Mean Opinion Score) are small.

keywords : cryptography, visual cryptography

DAFTAR ISI

LEMBAR PENGESAHAN

PERNYATAAN ORISINALITAS LAPORAN

PERNYATAAN PUBLIKASI LAPORAN TUGAS AKHIR

KATA PENGANTAR

ABSTRAK	i
ABSTRACT	iii
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	x
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Identifikasi Masalah	2
1.3 Rumusan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Batasan Masalah	3
1.6 Sistematika Pembahasan	3
BAB II LANDASAN TEORI	5
2.1 Citra Digital ^[11]	5
2.1.1 Format Citra Bitmap (BMP) ^[11]	6
2.1.2 Citra Biner ^[11]	7
2.1.3 Piksel ^[10]	7
2.2 Operator <i>Boolean</i> OR ^[9]	8
2.3 Ekspansi Piksel ^[9]	9
2.4 Kriptografi Visual ^{[5][9]}	10
2.4.1 Metode Kriptografi tanpa Ekspansi Piksel ^{[2][3]}	12

2.4.2	Gambaran Proses Enkripsi	16
2.4.3	Gambaran Proses Dekripsi.....	18
2.5	Algoritma RLE (<i>Run Length Encoding</i>)	19
2.6	PSNR.....	19
BAB III PERANCANGAN DAN REALISASI		21
3.1	Perancangan Perangkat Lunak	21
3.2	Prosedur Enkripsi	23
3.2.1	Prosedur Enkripsi tanpa <i>Additional Basis Matrix</i> AS^0 untuk Piksel Putih	23
3.2.2	Prosedur Enkripsi dengan <i>Additional Basis Matrix</i> AS^0 untuk Piksel Putih	28
3.3	Prosedur Dekripsi.....	33
BAB IV DATA PENGAMATAN DAN ANALISA DATA		37
4.1	Data Pengamatan.....	37
4.2	Analisa Data	72
BAB V SIMPULAN DAN SARAN		86
5.1	Simpulan	86
5.2	Saran.....	87
Daftar Pustaka		88
Lampiran A		A
Lampiran B.....		B

DAFTAR GAMBAR

Gambar 2.1 Bitmap dengan Nilai Matriksnya	6
Gambar 2.2 Representasi Piksel.....	7
Gambar 2.3 Hasil Logika OR Piksel Hitam (bit 1) dan Piksel Putih (bit 0)	8
Gambar 2.4 Ekspansi Piksel	9
Gambar 2.5 Ekspansi Piksel untuk Piksel Awal Putih dan Hitam	10
Gambar 2.6 Contoh Model Sederhana Kriptografi Visual.....	11
Gambar 3.1 Diagram Blok Kriptografi Visual.....	21
Gambar 3.2 Diagram Alir Proses Enkripsi tanpa <i>Additional Basis Matrix</i> AS^0	24
Gambar 3.3 Diagram Alir Proses Enkripsi dengan <i>Additional Basis Matrix</i> AS^0	29
Gambar 3.4 Diagram Alir Proses Dekripsi	34
Gambar 4.1 Percobaan 1	37
Gambar 4.2 Citra Rahasia 1	38
Gambar 4.3 <i>Share</i> 1.....	38
Gambar 4.4 <i>Share</i> 2.....	39
Gambar 4.5 <i>Share</i> 3.....	39
Gambar 4.6 <i>Share</i> 1 di-OR <i>Share</i> 2 di-OR <i>Share</i> 3.....	39
Gambar 4.7 Percobaan 2	40
Gambar 4.8 Citra Rahasia 2	40
Gambar 4.9 <i>Share</i> 1.....	41
Gambar 4.10 <i>Share</i> 2.....	41
Gambar 4.11 <i>Share</i> 3.....	41
Gambar 4.12 <i>Share</i> 1 di-OR <i>Share</i> 2 di-OR <i>Share</i> 3.....	42
Gambar 4.13 Percobaan 3	42
Gambar 4.14 Citra Rahasia 3	43
Gambar 4.15 <i>Share</i> 1.....	43
Gambar 4.16 <i>Share</i> 2.....	44

Gambar 4.17 <i>Share 3</i>	44
Gambar 4.18 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	45
Gambar 4.19 Percobaan 4	45
Gambar 4.20 Citra Rahasia 4	46
Gambar 4.21 <i>Share 1</i>	46
Gambar 4.22 <i>Share 2</i>	47
Gambar 4.23 <i>Share 3</i>	47
Gambar 4.24 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	48
Gambar 4.25 Percobaan 5	48
Gambar 4.26 Citra Rahasia 1	49
Gambar 4.27 <i>Share 1</i>	49
Gambar 4.28 <i>Share 2</i>	49
Gambar 4.29 <i>Share 3</i>	50
Gambar 4.30 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	50
Gambar 4.31 Percobaan 6	51
Gambar 4.32 Citra Rahasia 2	51
Gambar 4.33 <i>Share 1</i>	52
Gambar 4.34 <i>Share 2</i>	52
Gambar 4.35 <i>Share 3</i>	52
Gambar 4.36 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	53
Gambar 4.37 Percobaan 7	53
Gambar 4.38 Citra Rahasia 3	54
Gambar 4.39 <i>Share 1</i>	54
Gambar 4.40 <i>Share 2</i>	55
Gambar 4.41 <i>Share 3</i>	55
Gambar 4.42 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	56
Gambar 4.43 Percobaan 8	56
Gambar 4.44 Citra Rahasia 4	57
Gambar 4.45 <i>Share 1</i>	57

Gambar 4.46 <i>Share 2</i>	58
Gambar 4.47 <i>Share 3</i>	58
Gambar 4.48 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	59
Gambar 4.49 Percobaan 9	59
Gambar 4.50 Citra Rahasia 5	60
Gambar 4.51 <i>Share 1</i>	60
Gambar 4.52 <i>Share 2</i>	61
Gambar 4.53 <i>Share 3</i>	61
Gambar 4.54 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	62
Gambar 4.55 Percobaan 10	62
Gambar 4.56 Citra Rahasia 6	63
Gambar 4.57 <i>Share 1</i>	63
Gambar 4.58 <i>Share 2</i>	64
Gambar 4.59 <i>Share 3</i>	64
Gambar 4.60 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	65
Gambar 4.61 Percobaan 11	65
Gambar 4.62 Citra Rahasia 5	66
Gambar 4.63 <i>Share 1</i>	66
Gambar 4.64 <i>Share 2</i>	67
Gambar 4.65 <i>Share 3</i>	67
Gambar 4.66 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	68
Gambar 4.67 Percobaan 12	68
Gambar 4.68 Citra Rahasia 6	69
Gambar 4.69 <i>Share 1</i>	69
Gambar 4.70 <i>Share 2</i>	70
Gambar 4.71 <i>Share 3</i>	70
Gambar 4.72 <i>Share 1 di-OR Share 2 di-OR Share 3</i>	71

DAFTAR TABEL

Tabel 2.1 Hasil Operasi <i>Boolean OR</i>	8
Tabel 4.1 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 1)	72
Tabel 4.2 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 2)	73
Tabel 4.3 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 1)	73
Tabel 4.4 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 2)	74
Tabel 4.5 Hasil Detail Jumlah Piksel Pada Citra Rahasia 3 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 1)	74
Tabel 4.6 Hasil Detail Jumlah Piksel Pada Citra Rahasia 3 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 2)	75
Tabel 4.7 Hasil Detail Jumlah Piksel Pada Citra Rahasia 4 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 1)	75
Tabel 4.8 Hasil Detail Jumlah Piksel Pada Citra Rahasia 4 tanpa <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 2)	76
Tabel 4.9 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 dengan <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 1)	76
Tabel 4.10 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 dengan <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 2)	77
Tabel 4.11 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 dengan <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 1)	77
Tabel 4.12 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 dengan <i>Additional Basis</i> <i>Matrix AS⁰</i> (Percobaan 2)	78

Tabel 4.13 Hasil Detail Jumlah Piksel Pada Citra Rahasia 3 dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 1)	78
Tabel 4.14 Hasil Detail Jumlah Piksel Pada Citra Rahasia 3 dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 2)	79
Tabel 4.15 Hasil Detail Jumlah Piksel Pada Citra Rahasia 4 dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 1)	79
Tabel 4.16 Hasil Detail Jumlah Piksel Pada Citra Rahasia 4 dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 2)	80
Tabel 4.17 Hasil Detail Jumlah Piksel Pada Citra Rahasia 5 yang merupakan citra bergaris tipis tanpa <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 1)	80
Tabel 4.18 Hasil Detail Jumlah Piksel Pada Citra Rahasia 5 yang merupakan citra bergaris tipis tanpa <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 2)	81
Tabel 4.19 Hasil Detail Jumlah Piksel Pada Citra Rahasia 6 yang merupakan citra bergaris tipis tanpa <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 1)	81
Tabel 4.20 Hasil Detail Jumlah Piksel Pada Citra Rahasia 6 yang merupakan citra bergaris tipis tanpa <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 2)	82
Tabel 4.21 Hasil Detail Jumlah Piksel Pada Citra Rahasia 5 yang merupakan citra bergaris tipis dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 1)	82
Tabel 4.22 Hasil Detail Jumlah Piksel Pada Citra Rahasia 5 yang merupakan citra bergaris tipis dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 2)	83
Tabel 4.23 Hasil Detail Jumlah Piksel Pada Citra Rahasia 6 yang merupakan citra bergaris tipis dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 1)	83
Tabel 4.24 Hasil Detail Jumlah Piksel Pada Citra Rahasia 6 yang merupakan citra bergaris tipis dengan <i>Additional Basis Matrix</i> AS ⁰ (Percobaan 2)	84
Tabel 4.25 Parameter penilaian MOS	85
Tabel 4.26 Hasil penilaian MOS Untuk Citra Rahasia tanpa <i>Additional Basis</i>	85
Tabel 4.27 Hasil penilaian MOS Untuk Citra Rahasia dengan <i>Additional Basis</i>	85