

Kriptografi Visual untuk Multiple Secrets tanpa Perluasan Piksel

Raden Zaki Yamani Sinatrya Redha Soetanto
Jurusan Teknik Elektro Universitas Kristen Maranatha
email: here.iamzaki@yahoo.com

ABSTRAK

Konsep utama dari *visual secret sharing* adalah untuk mendekripsi *secret image* menjadi gambar yang tidak berarti. Tidak ada informasi yang bocor dari gambar yang dienkripsi dengan berbagai kombinasi dari semua *share image*. Visual kriptografi, sebuah pengembangan teknik kriptografi, untuk mendeskripsikan citra yang terenkripsi dapat menggunakan penglihatan manusia. Seperti pada teknik kriptografi yang lain, visual kriptografi memiliki persyaratan kerahasiaan, integritas data, otentikasi dan nir-penyangkalan. Sebagai pertimbangan keamanan, hal itu memastikan agar peretas tidak dapat melihat petunjuk apapun dari citra rahasia. Kriptografi visual adalah teknik kriptografi data berupa citra dengan cara membagi citra menjadi beberapa bagian. Setiap bagian citra tersebut adalah subset dari citra rahasia. Jika dihasilkan n bagian dalam proses enkripsi, maka jika hanya terdapat $n-1$ bagian, gambar tidak dapat didekripsi.

Pada tugas akhir ini menggunakan skema (2,2), sebuah citra rahasia berwarna akan dilakukan pengkodean menjadi dua buah citra bayang dan pendekodeannya diproses dengan menumpukkan dua buah citra bayang dengan menggunakan operasi logika “OR” untuk mendapatkan informasi berupa citra rahasia. Pada metoda ini skema VSSM (*Visual Secret Sharing Scheme for Multiple*) dapat menghasilkan dua buah citra rahasia dalam dua citra dengan bentuk persegi tanpa perluasan piksel. Hasil eksperimen menunjukkan bahwa metoda berhasil dilakukan dengan hasil yang bagus, tersamarkan dan tidak ada informasi yang bocor.

Kata kunci : Perluasan Piksel, Kriptografi visual, Kamuflase, *Multiple Secrets Images*, *Visual Secret Sharing*.

Cryptography Visual for Multiple Secrets Without Pixel Expansion

Raden Zaki Yamani Sinatrya Redha Soetanto
Department of Electrical Engineering Maranatha Christian University
Email : here.iamzaki@yahoo.com

ABSTRACT

The main concept of the original visual secret sharing (VSS) scheme is to encrypt a secret image into n meaningless share images. It cannot leak any information of the shared secret by any combination of the n share images except for all of images. Visual cryptography, an emerging cryptography technology, uses the human vision to decrypt encrypted images. Like the other cryptographic techniques, visual cryptography has confidentiality requirements, data integrity, authentication and non-repudiation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image. Visual cryptography is a cryptographic technique data such as pictures or images by dividing the image into several parts. Each section image is a subset of the first image. If the resulting N part in the encryption process, so if there are only $N-1$ parts, images cannot be decryption.

This essay used (2.2), a secret color image will be encoding into two share images and the decoding are processed by stacking two share images to get the information of the secret image. In this method a novel VSSM (Visual Secret Sharing Scheme for Multiple) scheme that can share two binary secret images on two rectangular share images with no pixel expansion. The experimental results show that this method successfully done with the good results, became meaningless image did not leak any information.

Keywords : Visual secret sharing, Pixel expansion, Camouflage, Multiple Secrets Images.

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS LAPORAN PENELITIAN	iii
PERNYATAAN PUBLIKASI LAPORAN PENELITIAN	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN	xiv
 BAB I PENDAHULUAN	 1
I.1 Latar Belakang	1
I.2 Perumusan Masalah	2
I.3 Tujuan	2
I.4 Pembatasan Masalah	2
I.5 Sistematika Penulisan	3
 BAB II LANDASAN TEORI	 4
II.1 Definisi Kriptografi	4

II.2 Tujuan Kriptografi	5
II.3 Pengenalan Kriptografi Visual.....	6
II.4 Metode Kriptografi Visual tanpa Perluasan Piksel	9
BAB III PERANCANGAN DAN REALISASI	20
III.1 Perancangan Perangkat Lunak	20
III.2 Prosedur Proses Enkripsi	21
III.3 Prosedur Proses Dekripsi	23
III.4 Perancangan Antarmuka Pemakai (<i>User Interface</i>)	24
BAB IV DATA PENGAMATAN DAN ANALISA DATA	26
IV.1 Data Pengamatan	26
IV.2 Analisa Data	46
BAB V KESIMPULAN DAN SARAN	54
V.1 Kesimpulan	54
V.2 Saran	55
DAFTAR PUSTAKA	54

DAFTAR TABEL

	Halaman
Tabel III.1 Penjelasan Rancangan Tampilan Perangkat Lunak	26
Tabel IV.1 Percobaan 1	27
Tabel IV.2 Percobaan 2	28
Tabel IV.3 Percobaan 3	28
Tabel IV.4 Percobaan 4	29
Tabel IV.5 Percobaan 5	29
Tabel IV.6 Percobaan 6	30
Tabel IV.7 Percobaan 7	30
Tabel IV.8 Percobaan 8	31
Tabel IV.9 Percobaan 9	31
Tabel IV.10 Percobaan 10	32
Tabel IV.11 Percobaan 11	32
Tabel IV.1 2 Percobaan 12	33
Tabel IV.1 3 Percobaan 13	33
Tabel IV.1 4 Percobaan 14	34
Tabel IV.1 5 Percobaan 15	34
Tabel IV.1 6 Percobaan 16	35
Tabel IV.1 7 Percobaan 17	35
Tabel IV.1 8 Percobaan 18	36
Tabel IV.1 9 Percobaan 19	36
Tabel IV.20 Percobaan 20	37
Tabel IV.21 Percobaan 21	38

Tabel IV.22 Percobaan 22	38
Tabel IV.23 Percobaan 23	39
Tabel IV.24 Percobaan 24	39
Tabel IV.25 Percobaan 25	40
Tabel IV.26 Percobaan 26	40
Tabel IV.27 Percobaan 27	41
Tabel IV.28 Percobaan 28	41
Tabel IV.29 Percobaan 29	42
Tabel IV.30 Percobaan 30	42
Tabel IV.31 Percobaan 31	43
Tabel IV.32 Percobaan 32	43
Tabel IV.33 Percobaan 33	44
Tabel IV.34 Percobaan 34	44
Tabel IV.35 Percobaan 35	45
Tabel IV.36 Percobaan 36	45
Tabel IV.37 Percobaan 37	46
Tabel IV.38 Percobaan 38	46
Tabel IV.39 Percobaan 39	47
Tabel IV.40 Percobaan 40	47
Tabel IV.41 Parameter Penilaian MOS	49
Tabel IV.42 Hasil Pengujian MOS 64x64 Piksel	50
Tabel IV.43 Hasil Pengujian MOS 128x128 Piksel	51
Tabel IV.44 Hasil Pengujian MOS 256x256 Piksel	52
Tabel IV.45 Hasil Pengujian MOS 200x360 Piksel	53

DAFTAR GAMBAR

	Halaman
Gambar II.1 Cara Kerja Kriptografi Visual	7
Gambar II.2 Contoh Penggunaan Skema k dari n ($k = 2, n = 3$)	9
Gambar II.3 Proses Dasar Enkripsi Kriptografi Visual Tanpa Perluasan Piksel	10
Gambar II.4 Proses Dasar Dekripsi	11
Gambar II.5 Tabel Kebenaran OR	11
Gambar II.6 Proses DSP (<i>Dividing and Separating Process</i>)	13
Gambar II.7 Proses DSP (<i>Dividing and Separating Process</i>)	14
Gambar II.8 Proses SP (<i>Sticking Process</i>)	15
Gambar II.9 Proses SP (<i>Sticking Process</i>)	16
Gambar II.10 Proses CMP (<i>Camouflaging with maximum density process</i>) ..	19
Gambar III.1 Diagram Blok Kriptografi Visual tanpa Perluasan Piksel	20
Gambar III.2 Diagram Alir Proses DSP dan SP	21
Gambar III.3 Diagram Alir Proses CMP	22
Gambar III.4 Diagram Alir Proses Dekripsi	23
Gambar III.5 Rancangan Tampilan Perangkat Lunak	24
Gambar III.6 Tampilan Perangkat Lunak saat Program dijalankan	25
Gambar III.7 Tampilan perangkat lunak setelah proses dijalankan	25

DAFTAR LAMPIRAN

Lampiran LIST PROGRAM MATLAB	A – 1
------------------------------------	-------