KRIPTOGRAFI VISUAL (4,4) UNTUK BERBAGI 3 CITRA RAHASIA LEWAT 4 CITRA TERSANDI

Jevri Eka Susilo
Email: jevriesusilo@gmail.com

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 (4,4), yaitu 3 citra rahasia akan diubah menjadi 4 citra terenkripsi. 3 citra yang digunakan adalah citra biner. Prosesnya adalah dengan mengubah 3 citra menjadi 2 citra terenkripsi, kemudian dari 2 citra tersebut akan dibuat masing 2 citra terenkripsi lagi, jadi akan ada 4 citra terenkripsi. Untuk proses dekripsinya menggunakan keseluruhan dari 4 citra terenkripsi tersebut.

Pengujian dilakukan dengan 15 citra berbeda yang memiliki tingkat detail yang berbeda. Dilakukan penilaian dengan PSNR (*Peak to Signal Noise Ratio*) dan MOS (*Mean Opinion Score*) pada citra hasil dekripsi, diperoleh nilai diatas 50 dB untuk PSNR dan diatas 3.5 untuk MOS.

Kata Kunci : Kriptografi, Kriptografi Visual

VISUAL CRYPTOGRAPHY (4,4) FOR SHARING 3 SECRET IMAGE WITH 4 ENCRYPTED IMAGE

Jevri Eka Susilo
Email: jevriesusilo@gmail.com

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 (4.4), which is 3 secret image will be converted into 4 encrypted image. 3 images used are binary image. The process is to convert the 3 secret image into 2 encrypted image, then from the 2 encrypted images will be made each two encrypted image again, so there will be 4 encrypted image. In order to decrypt, use the whole of the 4 encrypted image.

Tests carried out with 15 different images that have different levels of detail. Assessment conducted by PSNR (Peak Signal to Noise Ratio) and MOS (Mean Opinion Score) on the image decryption results, obtained for a value above 50 dB PSNR and above 3.5 for MOS.

keywords : cryptography, visual cryptography

DAFTAR ISI

LEMBAR PENGESAHAN
PERNYATAAN ORISINALITAS LAPORAN
PERNYATAAN PUBLIKASI LAPORAN TUGAS AKHIR
KATA PENGANTAR
ABSTRAK i
ABSTRACT ii
DAFTAR ISI iii
DAFTAR GAMBAR v
DAFTAR TABEL vi
BAB I PENDAHULUAN 1
I.1 Latar Belakang 1
I.2 Identifikasi Masalah 1
I.3 Rumusan Masalah 1
I.4 Tujuan Penelitian 2
I.5 Pembatasan Masalah 2
I.6 Sistematika Pembahasan 2
BAB II LANDASAN TEORI 4
II.1 Operator Boolean OR[6] 4
II.2 Operator Boolean XOR 5
II.3 Citra[3] 5
II.3.1 Format citra bitmap (BMP)[3] 6
II.3.2 Citra Biner[3] 7
II.3.3 Piksel[6] 8
II.3.4 Ekspansi Piksel[6] 8
II.3 Kriptografi Visual[6] 10

II.3 PSNR[4] 15
BAB III PERANCANGAN DAN REALISASI 17
III.1 Perancangan Perangkat Lunak 17
III.2 Prosedur Enkripsi 18
III.3 Prosedur Dekripsi 23
III.3.1 Prosedur Perbesaran citra Asli 25
BAB IV DATA PENGAMATAN DAN ANALISA DATA 29
IV.1 Data Pengamatan 29
IV.2 Analisa Data 43
BAB V KESIMPULAN DAN SARAN 46
V.1 Kesimpulan 46
V.2 Saran 46
Daftar Pustaka 47
Lampiran A ..... A
Lampiran B ..... B

DAFTAR GAMBAR

Gambar II.1 Hasil logika OR piksel hitam (bit 1) dan piksel putih (bit 0) 5
Gambar II.2 Hasil logika XOR piksel hitam (bit 1) dan piksel putih (bit 0) 5
Gambar II.3 Contoh citra biner 7
Gambar II.4 Huruf "B" dan representasi biner dari derajat keabuannya 7
Gambar II.5 Representasi piksel 8
Gambar II.6 Ekspansi piksel 9
Gambar II.7 Contoh perbesaran citra dengan ekspansi piksel 9
Gambar II.8 Ekspansi piksel untuk piksel awal putih dan hitam 10
Gambar II.9 Contoh model sederhana kriptografi visual 11
Gambar III.1 Diagram blok kriptografi visual (4,4) 17
Gambar III.2 Diagram alir proses enkripsi 19
Gambar III.3 Diagram alir proses dekripsi 24

DAFTAR TABEL

Tabel II.1 Hasil Operasi *Boolean* OR 4
Tabel II.2 Hasil Operasi *Boolean* XOR 5
Tabel II.3 Aturan pola share temporary 13
Tabel IV.1 Citra hasil percobaan 29
Tabel IV.2 Hasil dekripsi citra dengan 4 pola random share A 34
Tabel IV.3 Parameter penilaian MOS 42
Tabel IV.4 Hasil penilaian MOS 42
Tabel IV.5 Hasil penilaian PSNR dari masing-masing pola random 41