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, r*elative 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

DAFTAR GAMBAR

DAFTAR TABEL