Kriptografi Visual pada Citra Biner dan Citra Berwarna serta Pengembangannya dengan Steganografi dan Fungsi *XOR*

Muhammad Arif Romdhoni
13503108

Program Studi Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung

Email: arif.romdhoni@gmail.com

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 (k,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 minimal k buah citra dengan tepat dan dilihat dengan pandangan mata. Untuk jumlah citra kurang dari k, maka tidak ada informasi apapun yang dapat diperoleh mengenai citra rahasia.

Pada awalnya, kriptografi visual didefinisikan pada model citra biner. Kemudian pada akhir paper, Moni Naor dan Adi Shamir memberikan kemungkinan penggunaan untuk model citra abu-abu. Setelah itu, banyak paper yang membahas pengembangan algoritma kriptografi visual, di antaranya pada citra berwarna, kriptografi visual dengan steganografi dan kriptografi visual dengan fungsi XOR.

Sekilas Kriptografi

Kriptografi berasal dari bahasa Yunani, yang berarti ilmu tentang penulisan rahasia [NIK03]. Sesuai dengan namanya, kriptografi digunakan untuk mengaburkan informasi rahasia sehingga tidak bisa dimengerti oleh orang lain yang tidak berhak [FRE02]. Selain itu, kriptografi juga digunakan untuk otentikasi pesan [WIL96].

Kriptografi Visual

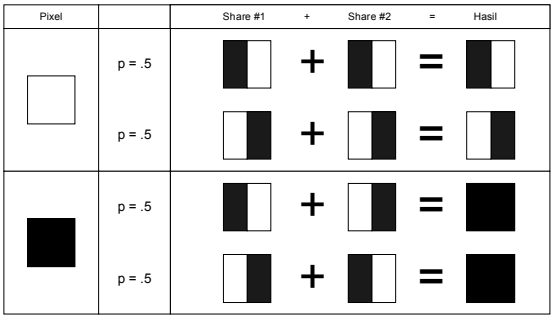
Kriptografi visual diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam *paper* mereka yang berjudul *Visual Cryptography*, dimuat dalam jurnal *Eurocrypt'94*, pada tahun 1995. Berbeda dengan kebanyakan algoritma kriptografi, algoritma ini tidak membutuhkan perhitungan rumit untuk mendekripsi pesan, tetapi hanya menggunakan sistem penglihatan manusia [MON95].

Model Sederhana

Model paling sederhana yang dikemukakan oleh Moni Naor dan Adi Shamir dalam kriptografi visual berupa citra biner, yakni hanya memiliki warna hitam dan warna putih. Setiap *pixel* pada citra rahasia akan diperlakukan secara terpisah. Masing-masing *pixel* tersebut akan muncul dalam *n* buah variasi, dinamakan *share*. Setiap *share* memiliki *m* buah *subpixel* berwarna hitam dan putih yang dicetak secara berdekatan sehingga sistem penglihatan manusia akan memandang rata distribusi warna hitam dan putih tersebut [MON95].

Hasilnya dapat dimodelkan dalam matriks *Boolean* *S* berukuran *nxm*, di mana *S[i,j] = 1*, jika dan hanya jika *subpixel* ke-*j*, pada *share* ke-*i* berwarna hitam. Jumlah baris pada matriks tersebut menyatakan banyaknya *share* dihasilkan dan jumlah kolom menyatakan jumlah *subpixel* pada masing-masing *share* [MON95].

Dari model tersebut, penumpukan *share* dapat dianggap sebagai hasil fungsi *OR* pada baris-baris terkait dari matriks *S* tersebut. Hal ini sesuai bahwa warna hitam pada satu *subpixel* tidak dapat dihilangkan oleh warna putih pada *subpixel* lain yang bertumpuk dengannya. Tingkat keabu-abuan yang dihasilkan dari penumpukan ini akan dianggap sebagai warna hitam jika memenuhi bobot $H(V) \geq d$ dan dianggap warna putih jika memenuhi bobot $H(V) < d-\alpha m$ [MON95]. Hal ini dapat digambarkan sebagaimana dalam Gambar 1.



Gambar 1 Model Kriptografi Visual [MON95]

Definisi Solusi

Untuk C_0 dan C_1 merupakan kumpulan matriks solusi untuk *pixel* putih dan *pixel* hitam, solusi pada kriptografi visual dapat didefinisikan sebagai berikut [MON95]:

1. Untuk sembarang matriks S pada C_0 pada sejumlah k baris manapun dari n, memiliki bobot $H(V) \geq d$.
2. Untuk sembarang matriks S pada C_1 pada sejumlah k baris manapun dari n, memiliki bobot $H(V) < d-\alpha m$.
3. Untuk sembarang *subset* dengan kardinalitas q, di mana $q<k$, maka sejumlah q baris manapun dari S_0 dan S_1 memiliki bobot yang sama.

Definisi ke-1 dan ke-2 di atas menyatakan kontras yang dihasilkan pada algoritma kriptografi visual. Sedangkan definisi ke-3 menyatakan keamanan.

Parameter Penting

Beberapa parameter yang penting dalam kriptografi visual, yakni [MON95]:

1. Parameter m, menyatakan jumlah *subpixel* pada masing-masing *share*. Parameter ini merepresentasikan besarnya resolusi yang hilang dari citra plain. Diusahakan parameter ini sekecil mungkin.
2. Parameter α, menyatakan perbedaan relatif nilai bobot Hamming hasil penumpukan *shares* antara *pixel* warna putih dan warna hitam dari citra plain. Parameter ini merepresentasikan besarnya kontras. Diusahakan parameter ini sebesar mungkin.
3. Parameter r, menyatakan besarnya kumpulan matriks C_0 dan C_1. Besar kumpulan matriks antara C_0 dan C_1 sebenarnya tidak harus sama, tetapi dalam konstruksi di sini dianggap sama, yakni jumlah permutasi kolom yang mungkin untuk setiap matriks dalam C_0 dan C_1, yakni $m!$.

Algoritma Enkripsi

Enkripsi pada algoritma kriptografi visual dilakukan per masing-masing *pixel*. Untuk masing-masing *pixel* dilakukan hal-hal sebagai berikut [DOU02]:

1. Membangkitkan permutasi acak p pada himpunan $\{1,...,m!\}$.
2. Jika *pixel* P berwarna hitam, maka ambil matriks boolean S dari C_0 pada indeks ke-p. Sedangkan jika berwarna putih, diambil dari C_1.
3. Untuk $1 \leq i \leq n$, baris ke-i pada S menyatakan seluruh *subpixel* dari P pada *share* ke-i.

Algoritma Dekripsi

Secara umum, algoritma dekripsi pada kriptografi visual dilakukan dengan cara menumpuk citra *share* sejumlah minimal tertentu secara tepat, bersesuaian antar *subpixel* terkait [MON95].

Solusi Beberapa Skema

Solusi beberapa skema yang diberikan oleh Moni Naor dan Adi Shamir sebagai berikut [MON95]:

Skema (2,2)

C_0 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

C_1 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

Skema (2,n)

C_0 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}$

C_1 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$

Skema (3,3)

C_0 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$

C_1 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$

Skema (3,n)

C_0 : Himpunan seluruh matriks hasil permutasi kolom dari $c(BI)$

C_1 : Himpunan seluruh matriks hasil permutasi kolom dari BI

di mana BI: $\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \\ 1 & \cdots & 1 \\ 1 & \cdots & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$

Skema (4,4)

C_0 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$

C_1 : Himpunan seluruh matriks hasil permutasi kolom dari $\begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$

Skema (k,n)

Salah satu skema (k,n) memenuhi persyaratan sebagai berikut [GIU96]:

1. $m \geq 2^{\binom{n}{n-k}-1}$
2. $\alpha \leq 2\text{-}\Omega(k)$

Skema (n,n)

Skema (n,n) memenuhi persyaratan sebagai berikut [MON95]:

1. $m \geq 2n\text{-}1$
2. $\alpha \leq 2\text{-}(k\text{-}1)$
3. $r \geq (2n\text{-}1)!$

Pengembangan

Dalam perjalanannya, kriptografi visual mengalami pengembangan dari model dasarnya, di antaranya: kriptografi visual pada citra berwarna, kriptografi visual dan steganografi (EVCS), steganografi teknik Chang dan Youmaran, dan kriptografi visual dengan fungsi *XOR*.

Kriptografi Visual pada Citra Berwarna

Citra berwarna sulit untuk dienkripsi karena dua hal, yakni:

1. Sepertinya tidak mungkin untuk mengenkripsi sebuah citra berwarna dengan pengembangan *pixel* yang kecil.
2. Faktor kecerahan citra hasil rekonstruksi dibandingkan dengan citra aslinya.

Definisi Solusi

Anggap kita dapat membangun seluruh warna pada citra rahasia (citra plain) dengan menggunakan himpunan warna $C = \{c_1, c_2, ..., c_J\}$. Sebuah koleksi dari J matriks G_i berukuran nxm dengan masukan berasal dari himpunan $\{0, 1, c_1, c_2, ..., c_J\}$ membangun sebuah skema visual kriptografi (k,n) jika memenuhi persyarat-persyaratan berikut in [AVI02]:

1. Untuk sembarang i, di mana $(1 \leq i \leq J)$, vektor sepanjang m yang merupakan hasil penumpukan sembarang k baris dari G_i minimal sejumlah L_i berwarna c_i; masing-masing warna c_j lainnya muncul maksimal U_{ij} dalam vektor ini.
2. Untuk sembarang subhimpunan $\{i_1, i_2, ..., i_j\}$ dari $\{1, .., n\}$, submatriks G_i' diperoleh dengan melakukan restriksi masing-masing G_i pada baris-baris $i_1, i_2, ..., i_j$ adalah identik sama dengan sebuah permutasi kolom

Kriptografi Visual dan Steganografi (EVCS)

Salah satu pengembangan algoritma kriptografi visual ialah ditambahkannya unsur steganografi. Kelebihan model ini ialah citra *share* yang dihasilkan memiliki makna, sehingga dapat mengurangi kecurigaan bagi yang melihatnya.

Definisi Solusi

Solusi untuk algoritma kriptografi visual dengan steganografi didefinisikan sebagai berikut: Sebuah kumpulan multiset matriks-matriks Boolean $\{(C_w^{c1,c2,..ct}, C_b^{c1,c2,..ct})\}_{c1,c2,...ct \in \{b,w\}}$ menghasilkan skema kriptografi jika terdapat $C_0 \in C_w^{(c1,c2,..ct)}$ dan $C_1 \in C_b^{(c1,c2,..ct)}$ yang memenuhi syarat-syarat berikut [GIU96]:

1. Untuk sembarang matriks S pada C_0, bobot Hamming untuk sejumlah k dari n baris memenuhi persamaan $H(V) \leq d - \alpha m$.
2. Untuk sembarang matriks S pada C_1, bobot Hamming untuk sejumlah k dari n baris memenuhi persamaan $H(V) \geq d$.
3. Untuk sembarang subset $\{i_1, i_2, ..., i_q\}$ dari $\{1, 2, ..., n\}$ di mana $q<k$, dua buah kumpulan matriks Boolean berukuran qxm, yakni D_0 dan D_1, yang diperoleh dari hasil restricting masing-masing matriks Boolean berukuran nxm dari C_0 dan C_1 pada baris-baris $i_1, i_2, ..., i_q$ tidak dapat dibedakan satu sama lainnya karena memiliki matriks yang sama dengan frekuensi yang sama.
4. Setelah citra plain dienkripsi, citra yang dihasilkan masih memiliki makna. Setiap partisipan akan memahami citra yang dimilikinya.

Contoh beberapa matriks dasar untuk membangun skema $(2,2)$ kriptografi visual dengan steganografi sebagai berikut:

$$S_w^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \text{ dan } S_b^{ww} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S_w^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \text{ dan } S_b^{wb} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

$$S_w^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \text{ dan } S_b^{bw} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

$$S_w^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \text{ dan } S_b^{bb} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Algoritma Chang Yu dan Youmaran

Pada tahun 2001, Chang dan Yu mengembangkan algoritma kriptografi visual dengan steganografi sehingga dapat menyimpan informasi citra dengan kedalaman warna 8-*bit* menggunakan citra penutup berupa dua buah citra berwarna. Algoritma ini menghasilkan citra rekonstruksi yang sempurna tetapi citra kamuflase yang dihasilkan memiliki gangguan (*noise*). Kekurangan ini kemudian ditutup oleh Youmaran [YOU01].

Algoritma Chang dan Yu

Algoritma untuk menyembunyikan citra pada dua citra penutup yang dikemukakan Chang dkk sebagai berikut [YOU01]:

1. Mengambil sebuah citra rahasia dengan kedalaman warna 256 (8-*bit*) I_{HL} dan dua buah citra penutup (*cover image*) O^1_{HL} dan O^2_{HL} yang memiliki dimensi lebar dan tinggi yang sama.
2. Untuk masing-masing *pixel* pada I_{HL}, diubah menjadi 8-*bit binary string*, $k = k_1k_2...k_8$.
3. Pilih sebuah bilangan bulat acak r_p. di mana $1 \leq r_p \leq 9$ untuk masing-masing *pixel* di atas.
4. Berdasarkan nilai r_p dan k, dibentuk sebuah matriks S yang memenuhi persamaan sebagai berikut:
   $k_i = S_{1\,j}$ *XOR* $S_{2\,j}$.
   $j = i$, jika $i < r$; dan $j = i+1$ jika $i \geq r$.
5. Mengambil *pixel* pada O^1 dan O^2 yang bersesuaian letak dengan *pixel* yang hendak disembunyikan tersebut. Berdasarkan S yang telah dihasilkan, dibentuk sebuah *block* berukuran 3x3 B^1_p dan B^2_p. Untuk masing-masing *subpixel* yang bernilai "1", diisi dengan warna *pixel* yang bersesuaian dari O. Sedangkan yang bernilai "0", dibiarkan tetap transparan.
6. Setelah seluruh *pixel* terproses, dua citra kamuflase telah terbentuk. Untuk menghindari kehilangan resolusi pada citra yang direkonstruksi, nilai bilangan acak r_p disimpan untuk digunakan pada waktu rekonstruksi.

Adapun algoritma untuk rekonstruksi dari dua buah citra kamuflase dijabarkan sebagai berikut:

1. Mengambil *block* berukuran 3x3 dari masing-masing citra O^1 dan O^2.
2. Bentuk kembali S dari *block-block* tersebut.
3. Dengan menggunakan r_p yang telah tersimpan sebelumnya, dibangun kembali variabel k.
4. Masukkan k ke dalam *pixel* bersesuaian dengan *block* yang telah diambil.
5. Jika seluruh *block* telah diproses, maka citra berhasil direkonstruksi.

Algoritma Youmaran

Perbaikan algoritma Chang dan Yu yang diusulkan oleh Youmaran ialah pada saat hendak melakukan proses penyembunyian informasi citra, seluruh *pixel* pada citra penutup dipastikan tidak memiliki nilai 0, yakni dengan jalan menambahkan 1 pada setiap *pixel* yang memiliki nilai kurang dari 255. Kemudian sewaktu proses penyembunyian informasi, nilai "0" pada langkah 5 algoritma Chang dan Yu di atas tidak dibiarkan transparan, tetapi diisi dengan nilai warna *pixel* bersesuaian dikurangi 1.

Pada proses rekonstruksi, nilai *pixel* pada blok yang diambil ditentukan oleh banyaknya *pixel* tersebut pada blok. Jika $count_k > count_{k-1}$, warna *k-1* dianggap transparan. Sedangkan jika sebaliknya, warna *k* yang dianggap transparan.

Kriptografi Visual dengan Fungsi *XOR*

Berbeda dengan algoritma kriptografi visual pada awalnya, model ini menggunakan fungsi *XOR* untuk algoritma enkripsi dan dekripsinya. Oleh karena itu, proses dekripsi tidak bisa dilakukan dengan hanya menumpuk transparansi.

Skema yang telah dikembangkan untuk kriptografi visual dengan fungsi *XOR* ialah (*2,n*) dan (*n,n*). Untuk skema (*n,n*), dapat diperoleh hasil rekonstruksi citra yang sempurna, sama dengan citra rahasia yang dienkripsi. Adapun untuk skema (*2,n*), terdapat *noise* pada citra yang dihasilkan [WAN05].

Skema (*n,n*)

Untuk mengenkripsi dalam skema ini, dilakukan dengan cara sebagai berikut:

1. Anggap citra plain yang dienkripsi ialah citra *P*, citra *share* yang dihasilkan berupa $A_1, ..., A_n$, dan matriks acak untuk membantu enkripsi, yakni $B_1, ..., B_{n-1}$. Seluruh variabel yang terlibat di sini memiliki lebar dan panjang yang sama.
2. Skema (*n,n*) dapat dihasilkan dengan persyaratan:

$A_1 = B_1$;
$A_2 = B_1$ *XOR* B_2;
...
$A_{n-1} = B_{n-2}$ *XOR* B_{n-1};
$A_n = B_{n-1}$ *XOR* P

3. Seluruh citra *share* untuk skema (n,n) telah dihasilkan.

Untuk merekonstruksi citra, dilakukan dengan jalan menggunakan fungsi *XOR* pada seluruh citra *share*, yang dijabarkan sebagai berikut:

A_1 *XOR* A_2 *XOR* A_3 *XOR* ... *XOR* A_{n-1} *XOR* A_n
$= B_1$ *XOR* $(B_1$ *XOR* $B_2)$ *XOR*$(B_2$ *XOR* $B_3)$ *XOR*..
XOR $(B_{n-2}$ *XOR* $B_{n-1})$ *XOR* B_{n-1} *XOR* A
$= (B_1$ *XOR* $B_1)$ *XOR* $(B_2$ *XOR* $B_2)$ *XOR* B_3
XOR.. *XOR* B_{n-2} *XOR* $(B_{n-1}$ *XOR* $B_{n-1})$ *XOR* A
$= A$

Skema (k,n)

Untuk skema $(2,n)$, citra plain tidak dapat direkonstruksi seperti semula. Namun pola citra plain masih dapat diperoleh. Untuk membangun skema $(2,n)$, dilakukan dengan langkah-langkah sebagai berikut:

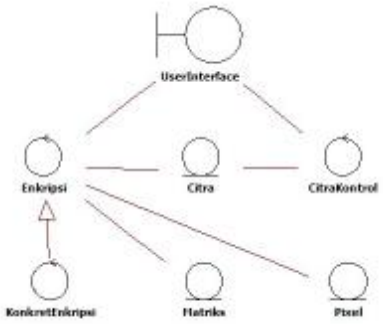
1. Anggap citra plain yang dienkripsi ialah citra P, citra *share* yang dihasilkan berupa A_1, ..., A_n, dan matriks acak untuk membantu enkripsi, yakni B_1, ..., B_{n+1} dan C_1, ..., C_n. Seluruh variabel yang terlibat di sini memiliki lebar dan panjang yang sama.
2. Skema $(2,n)$ dihasilkan dengan persyaratan:
   $C_i = B_i$ *AND* P;
   $A_i = B_{n+1}$ *XOR* C_i

Analisis dan Perancangan Perangkat Lunak

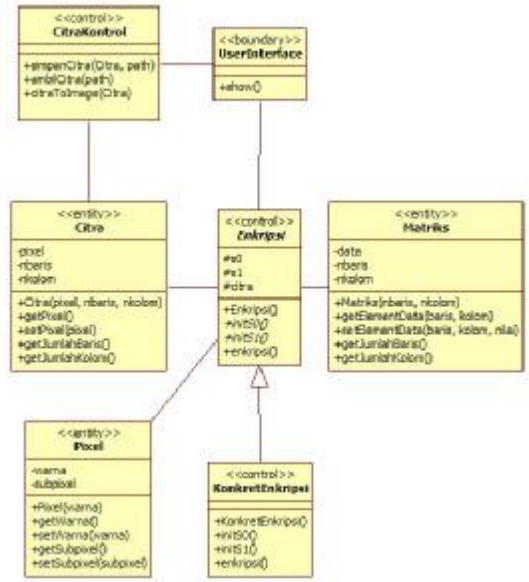
Diagram *use case* untuk perangkat lunak yang dibangun sebagai implementasi algoritma kriptografi visual dapat dilihat pada Gambar 2.

Gambar 2 Diagram *use case*.

Sedangkan diagram kelas analisis dan diagram kelas perancangan masing-masing dapat dilihat pada Gambar 3 dan Gambar 4.



Gambar 3 Diagram kelas analisis.



Gambar 4 Diagram kelas perancangan.

Pengujian

Pengujian dilakukan dengan tujuan mengetahui performansi citra yang dihasilkan pada algoritma kriptografi visual secara kualitatif. Pengujian dilaksanakan pada beberapa skema algoritma kriptografi visual.

Penutup

Kesimpulan

Dari hasil pengujian yang dilakukan penulis dengan mengimplementasikan algoritma-algoritma kriptografi visual tersebut di atas, diperoleh kesimpulan bahwa:

1. Kriptografi visual pada citra biner akan menghasilkan citra *share* dan citra rekonstruksi yang memiliki gangguan (*noise*) pada warna putih.
2. Untuk skema kriptografi visual (k,n) pada citra biner dan jumlah citra lebih dari atau sama dengan k, maka semakin banyak jumlah citra yang ditumpuk, kontras yang dihasilkan akan semakin besar.

3. Kriptografi visual dengan steganografi (EVCS) skema (2,2) diperoleh citra kamuflase yang dapat dikenali walaupun juga mempunyai gangguan (*noise*) pada citra tersebut. Dari proses rekonstruksi, dihasilkan citra yang mirip dengan citra rahasia terenkripsi.
4. Kriptografi visual pada citra berwarna skema (2,*n*) akan menghasilkan citra *share* dengan banyak *noise*. Semakin banyak citra yang ditumpuk, kontras akan semakin besar. Akan tetapi, hasil yang diperoleh tidak terlalu baik.
5. Kriptografi visual dan steganografi dengan menggunakan teknik Chang dan Yu menghasilkan citra kamuflase yang memiliki gangguan (*noise*) dan apabila citra penutup memiliki warna putih (atau transparan) maka citra hasil rekonstruksi bisa menjadi tidak sempurna. Hal ini dikarenakan pada *pixel* putih di citra penutup tersebut, seluruh blok *pixel* yang terbentuk akan berwarna putih.
6. Kriptografi visual dengan fungsi *XOR* pada skema (2,*n*) memiliki citra rekonstruksi yang tidak baik. Selain itu, apabila jumlah *share* yang dikenai fungsi *XOR* adalah ganjil, citra tidak terekonstruksi dengan baik.
7. Kriptografi visual dengan fungsi *XOR* pada skema (*n,n*) dapat menghasilkan citra rekonstruksi yang sempurna sesuai dengan citra rahasia yang dienkripsi.

Saran

Saran untuk penelitian dan pengembangan lebih lanjut mengenai kriptografi visual ini sebagai berikut:

1. Memperbaiki kontras yang dapat dihasilkan dari skema (*k,n*) algoritma kriptografi visual. Pada saat ini, terdapat beberapa *paper* yang telah membahas mengenai kontras optimal yang dapat diperoleh dalam suatu skema kriptografi visual tertentu.
2. Memperbaiki algoritma kriptografi visual dengan fungsi *XOR* pada skema (2,*n*).
3. Menyempurnakan skema-skema yang belum diimplementasikan, terutama dalam pada citra berwarna, kriptografi visual dengan steganografi.

Daftar Pustaka

[ATE96] Ateniese, Carlo Blundo, Alfredo De Santis, Douglas R. Stinson, *Extended Schemes for Visual Cryptography*, 14 Juni 1996.

[AVI02] Avishek Adhikari, Somnath Sikdar, *A new (2,n) – Visual Threshold Scheme for Color Images*, 2002.

[FRE02] Fred Piper, Sean Murphy, *Cryptography: A Very Short Introduction*, Oxford University Press, 2002.

[GIU96] Giuseppe Ateniese, Alfredo De Santis, dan Douglas R. Stinson, *On the Contrast in Visual Cryptography Schemes,* 27 September 1996.

[MON95] Moni Naor, Adi Shamir, *Visual Cryptography*, Springer-Verlag, Berlin, 1995.

[NIK03] Nik Goots, Boris Izotov, Alex Moldovyan, dan Nick Moldovyan, *Modern Cryptography: Protect Your Data with Fast Block Ciphers*, A-List Publishing, 2003.

[WAN05] Wang Dao Shun dkk. *Secret Color Images Sharing Schemes Based on XOR Operation*. 2005.