Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202296769
Vol. 9, No. 7, Desember 2022, hlm.1663-1670 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 36/E/KPT/2019 e-ISSN: 2528-6579

PENGAMANAN CITRA BERWARNA MENGGUNAKAN KRIPTOGRAFI VISUAL SKEMA *MEANINGFUL SHARES* DAN STEGANOGRAFI LSB

Fariz Abid Darmawan[1], Ari Kusyanti*[2], Rakhmadhanny Primananda[3]

[1,2,3]Universitas Brawijaya, Malang
Email: [1]Arizad@student.ub.ac.id, [2]Ari.kusyanti@ub.ac.id , [3]Rakhmadhany@ub.ac.id
*Penulis Korespondensi

(Naskah masuk: 09 Desember 2022, diterima untuk diterbitkan: 26 Desember 2022)

Abstrak

Keamanan informasi merupakan hal penting agar *file* yang bersifat rahasia, dapat terjaga dari orang yang tidak berhak, untuk itulah ada Kriptografi dan Steganograf. Kriptografi digunakan untuk mengenkiripsi *file* dengan mengubahnya, sementara Steganografi menyisipkan tanpa mengubah *file* tersebut. Untuk *file* gambar, cabang kriptografi yang dapat digunakan untuk mengamankannya yaitu Kriptografi Visual menggunakan *secret sharing.* Metode ini memungkin informasi rahasianya dipegang oleh beberapa partisipan dengan membagi *secret* menjadi potongan *shares,* sehingga kerahasiannya lebih terjaga. Salah satu skema dari *secret sharing* adalah *Meaningful Share,* yang berarti outputnya bukanlah gambar abstrak. Namun karena lebih buram dan terdapat *noise,* output terlihat berbeda dengan gambar aslinya,. Ini dapat menimbulkan kecurigaan yang dapat mengancam keamanan informasi didalamnya. Untuk menambah keamanan, dibutuhkan Steganografi LSB untuk menyisipkan lagi citra *shares* kedalam cover baru sehingga kualitas dan keamanan akan meningkat. Ini dibuktikan dari pengujian dengan menghitung nilai PSNR citra stego, dimana didapat hasil PSNR antara 32-33 dB. Dari segi keamanan, pengujian berpusat pada aspek kerahasiaan. Dengan melakukan serangan menggunakan Autopsy dan Stegspy hanya 3 dari 30 stego image yang dapat dideteksi citra *shares*nya, ini baru sebatas citra *shares,* dan untuk merekonstruksi ulang citra *secret*nya dibutuhkan sepasang shares, jadi diambil kesimpulan bahwa penggabungan metode ini berhasil mengamankan informasi didalamnya.

Kata kunci: *kriptografi visual, steganografi LSB, secret sharing, meaningful shares.*

COLOR IMAGE SECURITY USING VISUAL CRYPTOGRAPHY MEANINGFUL SHARES AND STEGANOGRAPHY LSB

Abstract

Information security is important so that files that are confidential can be protected from unauthorized persons, therefor there is Cryptography and Steganograph. Cryptography is used to encrypt files by changing it, while Steganography inserts the file without changing it.for image, there is the branch that can be used to secure it, namely Visual Cryptography secret sharing scheme. This method allows the confidential information to be held by several participants by dividing the secret into pieces of shares, so it makes the secret more secure. One of the schemes is Meaningful Shares, it make the output is not an abstract image, but it still looks different from the original image because the shares image is blurry and contains noise. So that it raises the suspicion of an attacker who threatens the security of the information in it. To add security, we need Steganography LSB, we can insert the image shares again into the new cover so that the quality and security will increase. This is proven from the test by calculating the PSNR values of the stego image, where the PSNR results are between 32-33 dB. for security by using Autopsy and Stegspy only 3 stego images can detect the share image, this is only a share image, and to reconstruct the secret image it takes a pair of shares, so it can be concluded that this combining method successfully secures the secret image in it.

Keywords: *visual cryptography,steganography LSB, secret sharing, meaningful shares.*

1. PENDAHULUAN

Sebagai dampak dari kemajuan teknologi informasi yang berkembang dengan sangat cepat, keamanan informasi menjadi isu yang hangat diperbincangkan akhir-akhir ini. Hal ini berkaitan dengan kemudahan akses informasi yang mengakibatkan ancaman-ancaman tentang kerahasian dan keamanan nya juga semakin meningkat. Kebocoran informasi rahasia dalam

kegiatan penting seperti penyimpanan barang berharga, transaksi bisnis, dan juga informasi pribadi dapat menimbulkan kerugian dari pihak yang memiliki informasi rahasia tersebut. Misalnya kejadian bocornya data pribadi seperti kartu pengenal dari pengguna yang merupakan petinggi negara yang dibobol lalu dibagikan oleh orang yang tidak bertanggung jawab dari salah satu situs resmi pemerintah (Alfons, 2021), atau informasi data penting dari organisasi perusahaan ataupun militer yang dapat diketahui oleh orang tidak berhak. Informasi rahasia juga dapat berbentuk sebuah gambar yang banyak digunakan dalam berbagai bidang seperti keamanan, medis, seni dan lain sebagainya (Bangdes & Muhathir, 2018). Misalnya informasi tentang *blueprint* produk dari suatu perusahaan, informasi lokasi *camp* kemiliteran dan juga informasi pribadi seperti kartu tanda pengenal. Maka dari itu diperlukan ilmu pengamanan atau penyembunyian informasi yang dapat menjaga kerahasian data dari orang yang tidak berhak mengetahuinya, salah satunya kita dapat menggunakan metode *Secret Sharing* dari Kriptografi visual.

Kriptografi merupakan ilmu yang mempelajari tentang penyandian informasi rahasia. Kata kriptografi sendiri berasal dari Yunani yang artinya penulisan rahasia (Goots et al, 2003). Sedangkan *Secret sharing* merupakan metode yang dapat digunakan untuk membagi sebuah informasi rahasia menjadi potongan-potongan informasi yang disebut dengan *shares* (Shamir, 1979). Artinya dengan menggunakan metode ini keamanan pesan rahasia dapat ditingkatkan karena pesan rahasia nantinya dapat diubah menjadi potongan *shares* yang dapat dibagikan kepada beberapa orang yang berhak memiliki informasi rahasia ini. Untuk informasi gambar, *secret sharing* diterapkan pada kriptografi visual. Diusulkan pada tahun 1994 oleh Naor dan Shamir dengan nama "*(k, n)-treshold visual secret sharing scheme*" yang akhirnya berubah menjadi visual cryptography atau kriptografi visual (Naor & Shamir, 1995). Penelitian mereka berhasil mengamankan informasi gambar dengan memecahnya menjadi beberapa *shares,* yang dapat direkonstruksi ulang dengan menumpuk *shares* tanpa harus menggunakan komputasi yang kompleks sehingga *secret* akan kembali terlihat. Dengan metode ini masalah tentang keamanan informasi gambar dapat diatasi. Namun kelemahan dari metode ini ialah hasil *shares* nya berupa gambar abstrak dan terbatas pada citra biner saja sehingga bisa menarik perhatian dan menimbulkan kecurigaan dari *hacker*. Kemudian pada tahun 2008 Hsien-Chu Wu, Hao-Cheng Wang dan Rui-Wen Yu mengemukakan pengembangan algoritma kriptografi visual yang dinamai *Meaningful Shares* (Wu et al, 2008). Skema *meaningful shares* ini dapat disebut sebagai penyempurnaan dari penelitian sebelumnya. Dengan menggunakan skema *meaningful shares* ini maka citra yang dihasilkan dari skema ini sama sekali tidak menunjukan informasi dari citra yang disembunyikan dan yang paling penting skema ini *meaningful* yang artinya citra yang dihasilkan tidak berupa abstrak walaupun mungkin agak lebih gelap dan ketajaman berkurang. Maka dengan penelitian ini kelemahan dari penelitian sebelumnya telah teratasi.

Dengan skema *meaningful shares* informasi citra rahasia memang dapat dikatakan telah aman, namun dengan hasil citra yang kurang tajam dan lebih gelap itu dapat memberi petunjuk tentang keberadaan informasi rahasianya, untuk itu digunakanlah steganografi. Pertama informasi gambar akan di enkripsi menggunakan kriptografi visual sebagai tingkat keamanan pertama lalu disisipkan kedalam citra lain menggunakan steganografi sebagai tingkat keamanan kedua (K & Kumar, 2010). Steganografi sendiri digolongkan menjadi ilmu komunikasi, yang memilki arti teknik dan seni dalam menyembunyikan informasi dan data digital dibalik informasi digital lainnya sehingga informasi yang sesungguhnya tidak terlihat lagi (Fuad et al, 2011). Ada banyak metode yang dipakai dalam steganografi diantaranya *Least Significant Bit* (LSB). *Least Significant Bit* ialah penerapan dari metode substitusi dimana data normal pada sebuah *file* diganti dengan data rahasia. Sistem ini akan dibuat dalam bentuk program desktop berbasis java, dimana sistem akan menyatukan 2 algoritma diatas. Steganografi LSB akan menjadi pengamanan pertama dan kriptografi visual *meaningful shares* menjadi pengamanan lapis kedua, jadi seperti menympan sebuah box didalam box. Output program yang sebelumnya adalah gambar shares yang buram, gelap, dan menimbulkan kecurigaan akan disisipkan lagi kedalam citra cover baru menggunakan *Least Significant Bit* (LSB).

Tujuan dari penelitian ini ialah merancang dan membangun suatu aplikasi yang dapat mengenkripsi sebuah citra berwarna menggunakan skema *meaningful shares* lalu menyisipkan hasil citranya kedalam citra lain menggunakan steganografi metode *Least Significant Bit* (LSB). Lalu setelahnya akan diukur kualitas dan keamanan nya. Sementara permasalahan yang dapat kita identifikasi ialah isu keamanan informasi yang marak terjadi, pengamanan informasi gambar yang jarang dilakukan dan pembuktian penerapan dari kedua metode yang dipakai.

Strategi atau metode pada penelitian ini ialah Diawali dengan identifikasi masalah lalu studi literature, analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian, analisis hasil pengujian dan terakhir kesimpulan. Tipe penelitian implementatif pengembangan, dengan harapan output nya perangkat lunak yang dapat mengamankan gambar dengan menggabungkan metode visual kriptografi skema *meaningful shares* dan steganografi *least significant bit.* Hardware yang digunakan: laptop dengan Processor Intel(R) Core(TM) i5-7200U CPU @ 2.50Ghz, *Harddisk* 500

GB, Memory (RAM) 8 GB. Software yang digunakan ialah sistem Operasi Windows 10 64bit, Netbeans IDE, Autopsy, Stegspy.

2. METODE PENELITIAN

Penelitian ini dilakukan dengan mengidentifikasi masalah lalu mencari referensi pada studi literatur, kemudian menganalisis kebutuhan dalam perancangan sistem, lalu merancang sistem, setelah itu sistem akan diimplementasikan baru kemudian dilakukan pengujian berdasarkan parameter uji yang sudah dibahas sebelumnya, lalu menganalisa hasil dari pengujian sistem, dan yang terakhir melakukan penarikan kesimpulan tentang penelitian yang telah dilakukan.

Tipe penelitian ini adalah pengembangan implementatif dengan harapan output dari penelitian ini ialah perangkat lunak yang dapat mengamankan gambar dengan menggabungkan metode visual kriptografi skema *meaningful shares* dan steganografi *least significant bit.* Penelitian berlokasi pada rumah penulis. Untuk pengumpulan data hasil penelitian dilakukan dengan metode observasi terhadap hasil pengujian output program. untuk data ujinya menggunakan 30 gambar berwarna dengan 3 resolusi yang berbeda bersumber dari http://chaladze.com/l5/ dan http://www.cs.tut.fi/sgn/imaging/tampere17/.

3. PEMBAHASAN

3.1. Kajian pustaka

Penelitian terkait visual kriptografi salah satunya dilakukan oleh (Hou, 2003) dengan judul "*Visual Cryptografi for Color Images".* Hou melakukan kriptografi visual dengan 3 skema yang dikemukakannya yang kemudian dikenal dengan skema Hou. Hou mengatakan kriptografi visual memiliki keuntungan dimana untuk mendekripsikan hasil nya cukup dengan menggunakan mata manusia tanpa menggunakan komputasi yang kompleks .

Penelitian selanjutya ialah terkait dengan skema *meaningful shares* yang dilakukan oleh (Wu, Wang, & Yu, 2008) yang berjudul "*Color Visual Cryptografi Using Meaningful Shares".* Pada penelitian ini Hsien-Chu Wu mengemukakan skema *meaningful shares* dimana citra shares hasil enkripsi nya itu berupa citra yang *meaningful* atau memiliki arti dalam kata lain tidak berupa citra abstrak.

Penelitian selanjutnya tentang penggabungan kriptografi visual dengan steganografi untuk pengamanan citra penelitian ini dilakukan oleh (K & Kumar, 2010) dengan judul *"Multi Layer Information Hiding – A blend of Steganography and Visual Cryptography".* Dalam penelitian ini K. Jitesh dan Shentil Kumar melakukan penggabungan kriptografi visual dan steganografi dengan algoritma *Discrete Wavelet Transform* (DWT). Hasil penelitian ini ialah kedua teknik pengamanan ini dapat membantu proses penyederhanaan perhitungan dibandingkan dengan metode sebelum digabungkan.

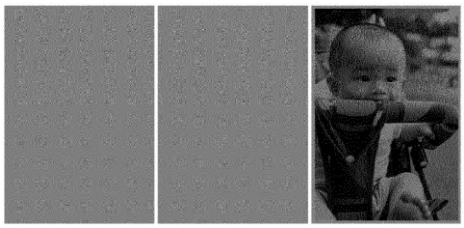
3.2. Error Diffusion

Error diffusion merupakan suatu teknik *halftone transformation* yang digunakan untuk mengubah gambar berwarna menjadi gambar *halftone* berwarna, teknik ini digunakan untuk mengurangi kesalahan pada proses *thresholding* (Raharjo & Aguswahyudi, 2016). Metode ini dikemukakan oleh Floyd dan Steinberg pada tahun 1976, metode ini membulatkan piksel ke nilai warna terdekat dan sisa pembulatannya akan ditambahkan ke piksel tetangga dengan ketentuan sebagai berikut:

$$\begin{pmatrix} \dots & x & \frac{7}{16} \\ \frac{3}{16} & \frac{5}{16} & \frac{1}{16} \end{pmatrix} \quad (1)$$

3.3. Kriptografi Visual

Kriptografi visual memanfaatkan kemampuan visual manusia untuk dapat melihat pesan rahasia yang disembunyikan tanpa perlu komputasi yang kompleks. Dikemukakan oleh Naor dan Shamir metode ini dapat menyembunyikan pesan rahasia dalam n share. Masing-masing share akan terlihat seperti kumpulan piksel yang acak namun setelah share ini ditumpuk bersamaan maka akan memperlihatkan gambar rahasia (Wu, Wang, & Yu, 2008). Untuk contohnya ialah seperti gambar 1.



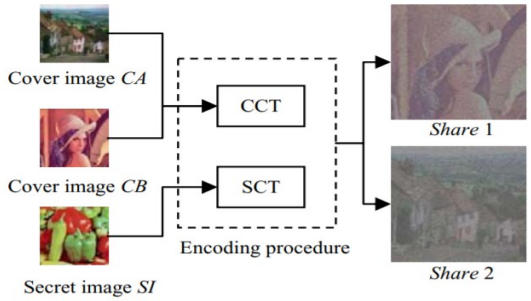
Gambar 1. Contoh kriptografi visual

Skema Meaningful Shares

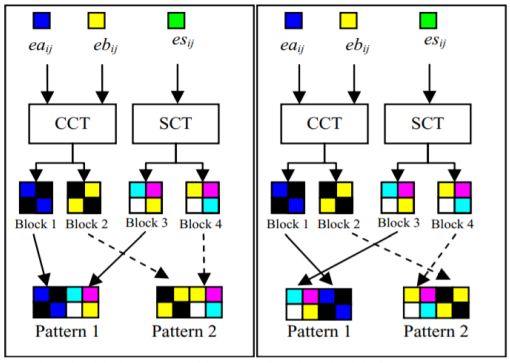
Pada tahun 2008 Hsien-Chu Wu, Hao-Cheng Wang dan Rui-Wen Yu menggagas pengembangan dari kriptografi visual yang bernama skema *meaningful shares.* Ide skema yang mereka gagas ialah menggunakan 2 citra sebagai sampul (cover) yang untuk menyembunyikan 1 citra rahasia (*secret*). Dimana shares yang dihasilkan dapat dikenali oleh karna itu dinamakan dengan *meaningful shares.* Terdapat dua proses yakni *Encoding* dan *Decoding.*

Encoding

Proses encoding membutuhkan 3 citra, 2 untuk sampul dan 1 untuk citra rahasia secara garis besar proses ini akan memasukan setengah citra rahasia kedalam 1 sampul dan setengahnya lagi kedalam sampul lainnya seperti pada gambar 2 dan proses lebih jelasnya dapat dilihat pada gambar 3.



Gambar 2. Prosedur encoding

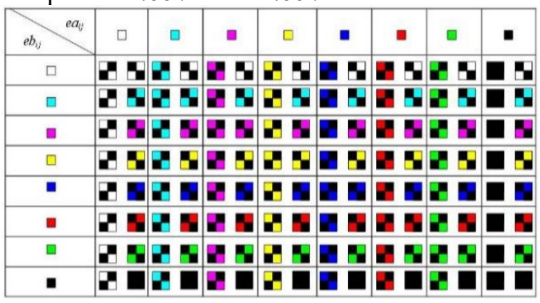


(a) The pixel belongs to odd row (b) The pixel belongs to even row

Gambar 3. Proses pembentukan shares

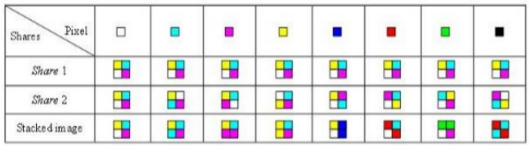
Langkah-langkahnya ialah sebagai berikut :

1. Menyediakan citra *cover* (CA dan CB) dan citra *secret* (CS) dimana keduanya berdimensi *N* x *N*
2. Melakukan preprocessing pada masing-masing citra dengan cara *Halftoning* citra lalu melakukan piksel extraction sehingga dihasilkan citra halftone berukuran ½ *N x N* (CA, CB, CS)
3. Mengubah piksel citra sampul CA(i,j) dan CB(i,j) menjadi *Block* dengan mengacu pada table *Code Coding Table* (CCT) gambar 4 sehingga didapatkan *Block* 1 dan *Block* 2.



Gambar 4. Cover coding table

4. Mengubah piksel citra rahasi CS(i,j) menjadi 2 *Block* dengan cara mengacu pada tabel *Secret* Coding Table (SCT) gambar 5 ES kemudian berubah menjadi *Block* 3 dan *Block* 4

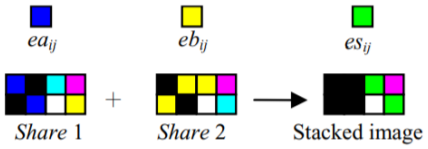


Gambar 5. *Secret* coding table

5. Membentuk citra *share1* dan *share2* dengan ketentuan :
   Jika citra CA(i,j) CB(i,j) dan CS(i,j)Pada baris ganjil maka *Share1* diambil dari *block* 1 dan 3. *Share2* dari *block* 2 dan 4. Jika pada baris ganjil maka *Share1* diambil dari *block* 1 dan 3. *Share2* dari *block* 2 dan 4.
6. Mengulang langkah 3 sampai 5 hingga semua piksel CA, CB, dan CS berubah menjadi *Block* semua.

Decoding

Untuk proses *decoding*nya dapat dilakukan dengan cara menumpuk citra shares yang dihasilkan seperti gambar 6.



Gambar 6. Proses decoding

3.4. Steganografi Least Significant Bit

Least Significant Bit (LSB) merupakan algoritma steganografi dengan melakukan penyisipan data pada bit-bit yang tidak significant sehingga tidak mengubah citra yang disisipkan. Selain LSB ada juga *Most Significant Bit* (MSB) yang mewakili data bit paling significant.

Embedding

Proses *Embedding LSB* pada penelitian ini dilakukan dengan semua piksel citra diambil nilai komponen warna RGB nya, setiap komponen warna akan diwakilkan menjadi 8 bit yang dinamakan *channel*, setelah itu bit yang paling tidak significant(LSB) dari setiap komponen warna pada piksel cover akan diganti dengan bit paling significant (MSB) dari data rahasia.

Extraction

untuk proses *extraction*nya mengambil *Least Significant bit* dari komponen warna pada masing-masing piksel stego image lalu menjadikannya *Most Significant Bit* sehingga menjadi citra *secret* kembali

3.5. Perancangan Sistem

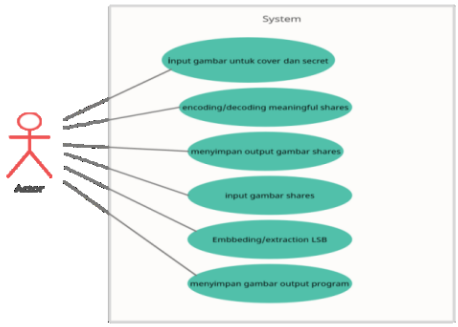
Pada perancangan sistem ini akan membahas tentang kerangka sistem yang ingin di buat sebagai gambaran umum dan petunjuk dalam pengimplementasian sistem terdapat 2 proses utama yang ada pada sistem yakni:

1. Proses enkripsi dan dekripsi citra berwarna menggunakan kriptografi visual skema *meaningful shares*
2. Proses embedding dan decoding atau penyisipan citra *shares* kedalam *cover image* baru dengan steagnografi LSB.

Untuk usecase diamgramnya dapat dilihat pada gambar 7.

Aktor pada sistem ini dapat melakukan beberapa hal seperti menginput gambar yang akan digunakan

untuk proses *meaningful shares*, melakukan proses encoding ataupun proses decoding meaningful shares, menyimpan gambar output meaningful shares, melakukan input gambar shares hasil proses sebelumnya, melakukan proses embbeding atau extraction LSB, menyimpan hasil keluaran program kelokasi yang diinginkan. Sistem ini akan dibuat menggunakan bahasa pemograman java.



Gambar 7. usecase diagram

3.6. Pengujian Sistem

Terdapat dua macam pengujian yang akan dilakukan yaitu:

Pengujian Kinerja

Pengujian ini bertujuan untuk mengukur keberhasilan kinerja metode yang digunakan. Pengujian dilakukan dengan menghitung nilai *Mean Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio.*

MSE digunakan untuk mengukur rata-rata kuadrat kesalahan, kesalahan yang dimaksud merupakan jumlah dari berapa piksel dari *stego image* yang berbeda dari *cover image*nya. Sedangkan PNSR merupakan rasio antara kekuatan sinyal maksimum dan kekuatan kebisingan yang mempengaruhi *stego image*. Semakin tinggi nilai PNSR semakin baik pula stego image tersebut (Rawat & Bhandari, 2013). Perhitungannya ialah sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{X=1} M \sum_{Y=1} N \,(S_{xy} - C_{xy})^2 \qquad (2)$$

$$PSNR = 10\log_{10}(\frac{C^2 max}{MSE}) \qquad (3)$$

Keterangan :

S : nilai bit citra pada koordinat x,y

C : nilai derajat keabuan pada koordinat x,y

C^2_{max} : nilai maksimal piksel

Pengujian Keamanan

Dalam mekanisme pengamanan menggunakan kriptografi terdapat 3 unsur yang harus diperhatikan yaitu *Confidentiality* (Kerahasiaan), *Integrity* (Integritas) dan *Availability* (Ketersediaan) yang disebut dengan CIA. Dalam penelitian ini akan terfokus kepada unsur kerahasiaan atau Confidentiality dari gambar yang dihasilkan dari penggabungan kriptografi visual skema *meaningful shares* dengan Steganografi LSB. Pengujian dilakukan dengan cara menganalisa metadata gambar rahasia hasil program yang telah dibuat menggunakan *tool* Autopsy dan selanjutnya mencari keberadaan gambar rahasianya menggunakan *tool* Stegspy.

3.1 Implementasi Sistem

Secara umum terdapat 3 algoritma yang akan diimplementasikan untuk membangun keseluruhan sistem, algoritma tersebut ialah:

Algoritma dithering Floyd-Steinberg

Merupakan proses preprosesing yang digunakan untuk mempermudah kita dalam memproses warna dalam gambar yang akan dipakai. Untuk output dari algoritme ini merupakan citra halftone dengan ukuran ½ NxN. Beberapa fungsi algoritma ini yakni:

1. Fungsi findClosestPaletteColor

Fungsi yang akan digunakan untuk menemukan warna dasar terdekat dari warna piksel yang sedang diambil dengan cara mencari nilai selisih warna piksel yang diambil dengan warna pada palette.

2. Fungsi Piksel Extraction

M erupakan fungsi yang akan digunakan untuk mengubah citra NxN menjadi citra dengan ukuran ½ NxN dengan cara menghilangkan piksel yang berada pada baris ganjil atau genap pada gambar tersebut.

3. Fungsi floydSteinbergDithering

Merupakan fungsi utama pada algoritme ini pertama-tama dalam fungsi ini akan diinisiasikan palette yang telah digunakan pada fungsi sebelumnya, lalu selanjutnya mengambil nilai rgb dari piksel dimana nilai RGB dari piksel tersebut akan dicari nilai terdekatnya dengan fungsi findClosestPalette, kemudian hasil selisih tersebut akan dimasukan kedalam variable error yang akan dikalikan kedalam matrik filter yang telah dikemukakan Floyd-steinberg.

Algoritma Meaningful shares

Selanjutnya akan membahas tentang tahapan pengimplementasian program visual crypthography skema meaningful shares. Secara umum tahapannya ialah sebagai berikut:

1. Fungsi pembentuk *block* CCT

terdapat dua buah *block* yang akan kita buat yang pertama *block* CCT (Cover Coding Table) dan *Block* SCT (*Secret* Coding Table). *Block* CCT dibuat berdasarkan piksel cover yang diambil lalu diubah menjadi 4 piksel yang disusun menyerupai *block* berdasarkan dengan data yang ada pada Cover Coding Table *block* ini dinamai dengan *block*1 dan *block*2.

2. Fungsi pembentuk *block* SCT

Sama halnya Seperti fungsi pembentuk *block* CCT sebelumnya *block* SCT juga terdiri dari 4 buah piksel yang disusun. Perbedaannya kalau CCT mengacu pada Cover Coding Table maka SCT mengacu pada *Secret* Coding Table sehingga mengahasilkan dua buah *block* berbeda yang dinamai *block*3 dan *block*4.

3. Fungsi generateShares

Dalam fungsi ini akan dilakukan penggabungan *block-block* menjadi sebuah citra-citra baru yang dinamai shares1 dan shares2, Untuk tahap awal dilakukan dithering untuk citra yang akan diproses lalu melakukan seleksi piksel satu persatu diubah menjadi *block* piksel dengan fungsi SCT dan CCT sebelumnya lalu *block-block* tersebut akan disusun untuk membentuk citra baru, dengan aturan apabila piksel yang diproses pada baris ganjil maka susunanya *block* CCT lalu diikuti *block* SCT, begitupula sebaliknya. terakhir lakukan perulangan sampai semua piksel berubah menjadi *block* piksel dan menciptakan citra baru yakni shares1 dan shares2.

4. Fungsi decrypt

Terkakhir ialah fungsi decrypt yang digunakan untuk merekonstruksi ulang shares-shares hasil enkripsi sebelumnya menjadi citra *secret*. Dalam kodingan dapat kita lakukan dengan cara mengambil nilai RGB dari masing-masing piksel per masing-masing shares lalu melakukan operasi dan (&) sehingga didapat kan nilai RGB baru hasil penggabungan shares yang kemudian disusun kembali menjadi sebuah citra *secret*

Algoritma Least Significant Bit

Algoritma ini secara umum dibagi menjadi dua macam fungsi yang pertama ialah fungsi *Embbedding* atau fungi penyisipan citra *secret* kedalam citra *cover* selanjutnya yang kedua ialah fungsi *Decoding* atau *Extract* yakni fungsi untuk merekonstruksi ulang citra *secret*. Untuk penjelasan lebih lanjut sepoerti di bawah ini:

1. Fungsi Embed

Pada fungsi ini kita akan melakukan penyisipan bit citra *secret* kedalam citra cover. Penyisipan dilakukan dengan cara mengganti nilai *least significant bit* (LSB) dari citra cover dengan nilai *most significant bit* (MSB) dari citra *secret*.

2. Fungsi Extract

Pada fungsi *extract* digunakan untuk merekonstruksi ulang gambar rahasia yang sebelumnya disisipkan kedalam gambar cover menggunakan fungsi *embedd*. Dilakukan dengan memecah kembali bit pada citra stego dan mengambil LSB nya lalu menjadikannya MSB untuk gambar baru.

3.2 Pengujian Dan Pembahasan

Pengujian Kinerja

Pada pengujian ini akan disediakan 30 gambar stego dengan resolusi yang berbeda, natara lain 256x256, 512x512 dan 1024x1024. Semua gambar tersebut akan dihitung nilai PSNR dan diperoleh hasil citra *shares* didalamnya didapatkan nilai PSNR pada rentang 32-33 dB.

Pengujian Keamanan

Pengujian keamanan akan berfokus pada salah satu aspek dari CIA Triad yakni aspek Confidentiality atau kerahasiaan. Pengujian bertujuan untuk memastikan pesan atau *file* rahasia sulit untuk dideteksi. pertama menggunakan *tool* autopsy, disini tidak didapatkan informasi terkait citra rahasia yang disisipkan didalam citra cover kita hanya dapat melihat informasi metadata dari citra cover tersebut seperti nama, resolusi, dan informasi kapan *file* dibuat, diubah, dan diakses.

Kedua dengan menggunakan stegspy dari 30 citra stego yang diuji hanya 3 citra yang didalamnya terdeteksi menggunakan steganografi. Namun sekalipun *attacker* tau dan dapat mengekstrak citra stego tersebut, attacker hanya akan mendapatkan 1 shares sementara dibutuhkan 2 shares untuk mendekripsikannya menjadi citra *secret* kembali.

4. KESIMPULAN DAN SARAN

4.1 KESIMPULAN

1. Program Kriptografi Visual skema *Meaningful Shares* dan Steganografi *Least Significant Bit*(LSB) berhasil dibuat menggunakan bahas pemograman java, melalui proses preprosesing dithering Floyd-Steinberg, lalu kemudian proses enkripsi menghasilkan 2 citra *shares,* dimana masing-masing *shares* ini selanjutnya akan disisipkan kedalam gambar cover baru dengan fungsi *embedding* steganografi LSB. Untuk proses rekonstruksi *secret* dilakukan dengan meng-*extract* gambar masing-masing shares dari citra stego hasil steganografi LSB lalu didekripsi kan dengan pasangannya maka munculah gambar *secret*.

2. Berdasarkan pengujian kinerja dengan menggunakan 30 gambar dengan 3 resolusi atau ukuran yang berbeda-beda dapat kita simpulkan bahwa kualitas gambar stego yang sudah disisipkan dengan citra *shares* didalamnya didapatkan nilai PSNR yang berada pada rentang 32-33 dB.

3. Penggabungan dua metode ini berhasil memberikan keamanan terhadap citra rahasia, dari metadata menggunakan *tool* Autopsy tidak ada data rahasia yang dapat digunakan oleh attacker. Steganografi didalamnya cukup terjaga kerahasiaannya dimana dari 30 sample stego image hanya 3 image yang terdeteksi menggunakan *tool* Stegspy.

4.2 SARAN

Saran yang dapat penulis berikan dari penelitian ini ialah penelitian terkait selanjutnya diharapkan dapat menggunakan image dengan ukuran dan resolusi yang lebih bervariasi untuk *secret* dan covernya sehingga nilai PSNR dapat lebih baik. Penelitian selanjutnya juga diharapkan dapat melakukan pengujian keamanan dari aspek lain seperti *availability* atau *integrity*.

DAFTAR PUSTAKA

ALFONS, M. 2021. *NIK Jokowi Tersebar, Kemendagri Minta Warga Tak Sembarang Unggah KTP*. Retrieved from Detik.com: https://news.detik.com/berita/d-5709343/nik-jokowi-tersebar-kemendagri-minta-warga-tak-sembarang-unggah-ktp

BANGDES, & MUHATHIR. 2018. Perbandingan Algoritma Blowfish dan Twofish untuk Kriptografi *File* Gambar. *Journal Of Informatics And Telecommunication Engineering*, 23-32.

FUAD, N. 2011. Teknik Steganografi dengan Menggunakan Metode Visual Attacks dan Statistical Attacks. *Jurnal JITIKA, Vol. 5, No. 2*, 28-36.

FUAD, N., SUYONO, & SETYATI, E. 2011. Teknik Steganografi dengan Menggunakan Metode Visual Attacks dan Statistical Attacks. *Jurnal JITIKA, Vol. 5, No. 2*, 28-36.

GOOTS, N., IZOTOV, B., MOLDOVYAN, A., & MOLDOVYAN, N. 2003. *Modern Cryptography: Protect Your Data With Fast Block Chipers.* A-list Publishing.

HOU, Y.-C. 2003. Visual Cryptografi for Color Images. *The Journal of The Pattern Recognition 36*, 1619-1629.

K, J., & KUMAR, D. A. 2010. Multi Layer Information Hiding -A Blend of Steganography and Visual Cryptography. *Journal of Theoretical and Applied Information Technology*, 109-116.

NAOR, M., & SHAMIR, A. 1995. Visual Cryptography. *Advances in Cryptology-EUROCRYPT'94*, 1-12.

NIK GOOTS, B. I. 2003. *Modern Cryptography: Protect Your Data With Fast Block Chipers.* A-list Publishing.

PIPER, F., & MURPHY, S. 2002. *Cryptografi: A Very Short Introduction.* Oxford University Press.

RAHARJO, W. S., & AGUSWAHYUDI, D. 2016. Implementasi Skema Meaningful Sharing pada Kriptografi Visual Berwarna untuk Digital Safe Deposit Box. *Ultimatics, Vol. VIII, No. 1*, 16-22.

RAWAT , D., & BHANDARI, V. 2013. A Steganography Technique For Hiding Image in an Image Using LSB Method for 24 Bit Color Image. *International Journal of Computer Application*, 15-19.

WU, H.-C., WANG, H.-C., & YU, R.-W. 2008. Color Visual Cryptography Scheme Using Meaningful Shares. *Eight International Conference on Intellegent System Design and Aplication*, 173-178.

Halaman ini sengaja dikosongkan