Implementasi Secret Sharing Berbasis Kriptografi Visual Skema (k,n) Pada Citra Biner Menggunakan GUI Matlab

Puteri Bunga, Stephanie Pella, Molina Odja
Teknik Elektro Universitas Nusa Cendana

Correspondence Author: s.i.pella@gmail.com

Abstract

Kriptografi visual membagi sebuah citra rahasia menjadi beberapa share yang terlihat acak oleh mata pada proses enkripsi. Share-share tersebut ditumpukan pada proses dekripsi untuk menampilkan informasi dari citra asli. Penelitian ini bertujuan melakukan implementasi kriptografi visual pada citra black and white dengan skema (k,n) dimana n adalah jumlah share yang dihasilkan dan k adalah jumlah share yang dibutuhkan untuk mendapatkan informasi citra asli. Implementasi dilakukan untuk skema (2,4), (2,3) dan (3,3). Pengujian dilakukan dengan cara kualitatif (visual) dan kuantitatif menggunakan parameterMSE dan PSNR. Hasil pengujian menunjukan share yang dihasilkan setiap skema terlihat acak oleh mata dan tidak menunjukan informasi pada citra asli. Hasil dekripsi dari setiap skema berhasil menampilkan informasi pada citra asli dengan ketajaman yang berbeda-beda. Hasil uji kuantitatif menunjukan nilai MSE untuk skema (2,4), (2,3) dan (3,3) secara berurutan adalah 0.087, 0.058 dan 0. Sedangkan nilai PSNR untuk masing-masing skema adalah 10,6 dB, 12.4 dB dan infinity

Keyword: Kriptografi Visual, Skema (k,n), Keamanan Citra

1. PENDAHULUAN

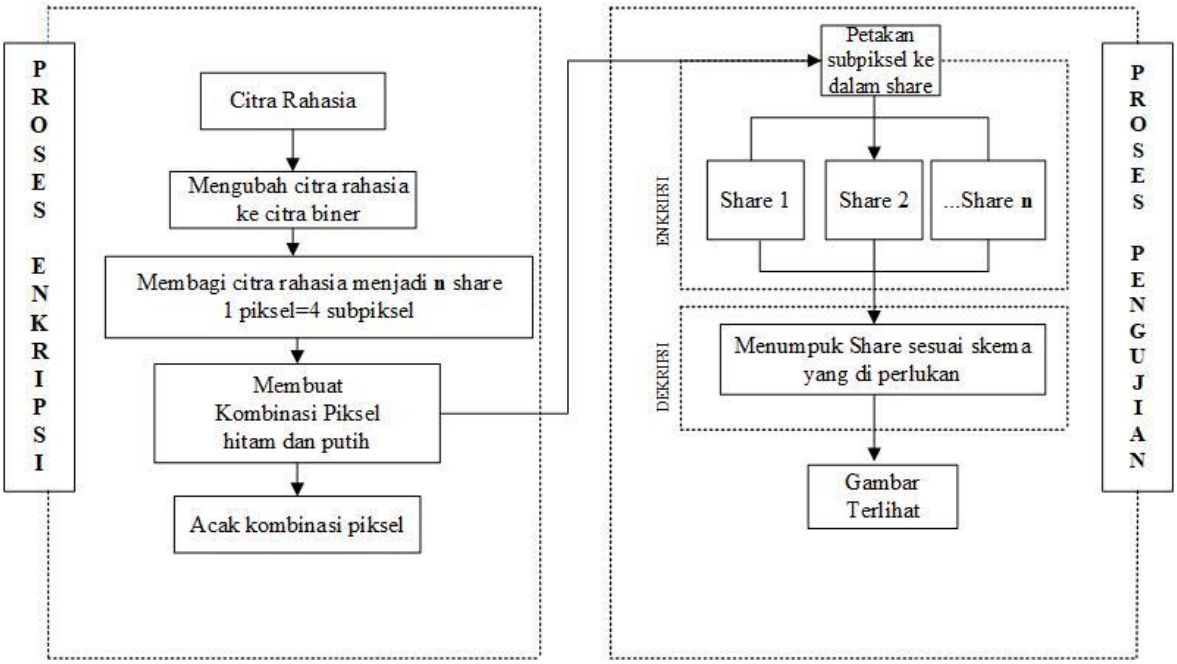
Kriptografi visual yaitu teknik kriptografi untuk gambar atau citra dengan membagi citra tersebut menjadi beberapa bagian yang disebut share.. Kriptografi visual diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam paper mereka yang berjudul Visual Cryptography, dimuat dalam jurnal Eurocrypt'94, pada tahun 1995 [1]. Moni Naor dan Adi Shamir melakukan Teknik visual kriptografi ini dengan mencetak bagian-bagian gambar pada kertas transparan untuk melihat gambar aslinya dengan cara menumpuk bagian-bagian gambar yang telah dicetak, sehingga algoritma Visual Kriptografi ini tidak membutuhkan perhitungan rumit untuk mendekripsi pesan, tetapi hanya menggunakan sistem penglihatan manusia atau operasi komputasi sederhana. Skema visual kriptografi bisanya dinyatakan dengan (k,n) dimana n adalah jumlah share yang dihasilkan pada proses enkripsa dan k merujuk pada jumlah share yang dibutuhkan pada proses dekripsi untuk mendapatkan informasi pada cira asli.

Terdapat beberapa penelitian tentang teknik Visual Kriptografi . Penelitian pada [2] mengimplementasikan kriptografi visual pada citra biner atau hitam putih . Penelitian lainnya [3] menggunakan kriptografi visual berrwarna untuk sistem digital safe deposit box. Citra yang dihasilkan cenderung lebih gelap dari citra awal dan ketajamannya berkurang. Penelitian pada [4] dan [5] menerapkan kriptografi visual untuk autentikasi pengguna pada transaksi online menggunakan skema Visual Cryptography 2,2

Penelitian-penelitian yang sudah dilakukan pada umumnya mewajibkan semua share digunakan pada proses dekripsi (nilai n sama dengan nilai k). Pada penelitian ini dilakukan implementasi visual kriptografi dengan nilai n dan k yang berbeda-beda. Pada beberapa skema di penelitian ini tidak semua share diperlukan untuk menampilkan informasi citra asli pada proses dekripsi. Implementasi visual kriptografi pada penelitian ini menggunakan skema(2,4), (2,3) dan (3,3).

2. METODE PENELITIAN

Perancangan sistem dikerjakan dengan beberapa tahap meliputi proses memasukkan citra biner, proses enkripsi citra dan dekripsi. Perancangan diawali dengan penggambaran blok diagram kerja sistem yang dapat dilihat pada Gambar 1



Gambar 1. Diagram Sistem

Gambar 1 menunjukan gambaran sistem secara keseluruhan untuk proses enkripsi dan dekripsi. Pada proses awal dilakukan dengan memasukan citra hitam putih atau citra greyscale yang nantinya akan diubah menjadi citra biner yang hanya memiliki kedalaman warna 1 bit. setelah itu citra akan dilakukan metode secret sharing dengan membagi citra tersebut dengan proses enkripsi menjadi beberapa bagian share yang dibutuhkan sesuai nilai n pada skema dengan cara setiap piksel akan di ekspansi menjadi 4 sub-piksel. Setelah itu dilakukan kombinasi piksel warna putih dan warna hitam dan acak kombinasi piksel, kombinasi piksel dilakukan untuk memetakan subpiksel pada masing-masing citra share. Setelah citra share telah di dapatkan maka di lakukan proses dekripsi atau proses penumpukan citra share menjadi 1 bagian, proses dekripsi dilakukan sesuai nilai k yang di perlukan pada setiap skema. setelah ditumpuk citra akan terlihat, apabila menghasilkan informasi sesuai citra awal maka proses enkripsi dan dekripsi berhasil di lakukan.

2.1 Proses Enkripsi

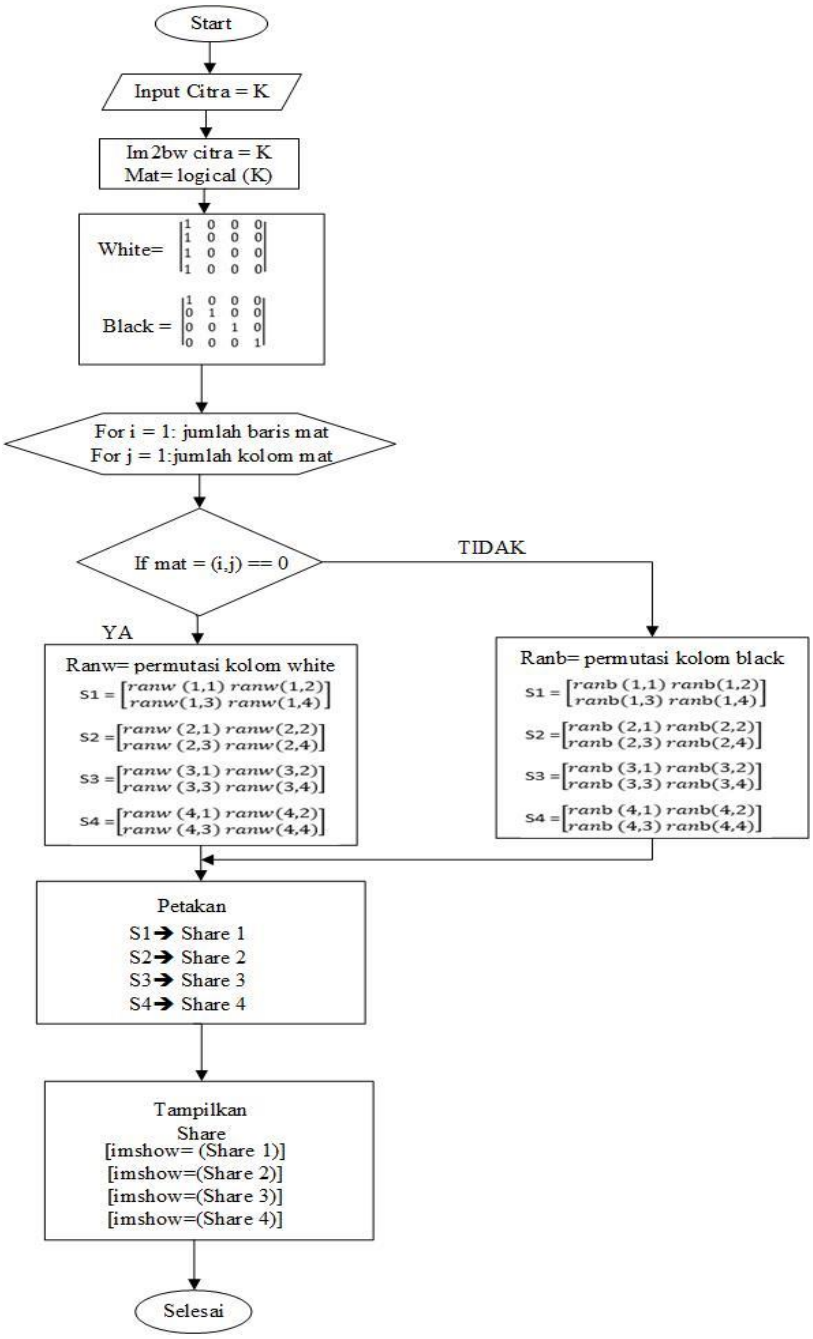
Diagram alir proses enkripsi untuk skema (2,4) dapat dilihat pada Gambar 2. Pada tahap pertama dilakukan pembacaan citra yang hendak dienkripsi kemudian citra tersebut dikonversi ke format biner (disimpan dalam matriks mat), setelah itu masukkan algoritma kriptografi visual skema (2,4) untuk membangkitkan *share* sebagai berikut:

$$\text{matriks putih}=\begin{vmatrix}1&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0\end{vmatrix}\begin{matrix}\rightarrow \text{Share 1}\\\rightarrow \text{Share 2}\\\rightarrow \text{Share 3}\\\rightarrow \text{Share 4}\end{matrix}$$

$$\text{dan matriks hitam}=\begin{vmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{vmatrix}\begin{matrix}\rightarrow \text{Share 1}\\\rightarrow \text{Share 2}\\\rightarrow \text{Share 3}\\\rightarrow \text{Share 4}\end{matrix}$$

untuk setiap baris pada matriks putih dan matriks hitam melambangan share.

Dalam matriks i merepresentasikan baris dan matriks j merepresentasikan kolom, jika matriks mat (i,j) bernilai 1 maka pixel adalah pixel hitam, dan jika matriks mat (i,j) bernilai 0 maka pixel adalah pixel putih. Jika mat (i,j) bernilai 0, maka dilakukan proses permutasi kolom matriks putih secara acak dengan fungsi matlab randperm, jika mat (i,j) bernilai 1, maka dilakukan proses permutasi kolom matriks hitam secara acak, kemudian dipetakan kedalam *share* 1, *share* 2, *share* 3 dan *share* 4. Lakukan secara berulang untuk setiap nilai baris dan kolom pada matriks



Gambar 2 Diagram Alir Skema (4,2)

2.2 Proses Dekripsi

Pada tahap dekripsi ini dilakukan penumpukan citra hasil enkripsi atau citra share, proses penumpukan share berdasarakan nilai dari n atau skema yang diperlukan. Pada proses penumpukan ini di lakukan dengan operasi X-OR terhadap kolom dan baris matriks pada citra share yang hendak di tumpukan.

2.3 Pengujian Sistem

Pengujian sistem dilakukan secara kualitatif dan kuantitatif. Pengujian kualitatif dilakukan secara visual terhadap hasil enkripsi dan dekripsi. Hasil Enkripsi diharapkan terlihat acak dan tidak mengandung informasi pada citra asli. Hasil dekripsi diharapkan dapat menampilkan informasi citra asli.

Pengujian kuantitatif dilakukan dengan menggunakan parameter MSE (*Mean Squared* Error) dan PSNR(*Peak Signal to Noise Ratio*) sesuai rumus dibawah ini.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(B_1(i,j) - (B_2(i,j))^2$$

$$PSNR = 10log_{10}\frac{MAXi^2}{MSE}$$

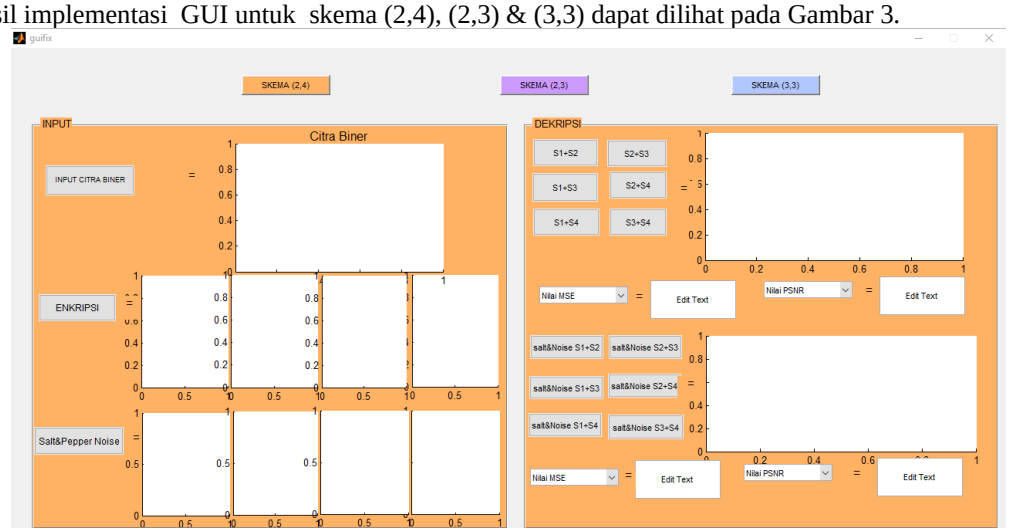
Dimana:
m : baris matriks citra hasil pemrosesan
n : kolom matriks citra hasil pemrosesan
B2 : pixel citra hasil pemrosesan
B1 : pixel citra asli

Selain itu dilakukan pengujian hasil dekripsi apabila share dikirimkan melalui kanal dengan menambahkan noise salt and paper.

3. HASIL DAN ANALISA (10 PT)

3.1 Hasil Implementasi GUI Matlab

Hasil implementasi GUI untuk skema (2,4), (2,3) & (3,3) dapat dilihat pada Gambar 3.

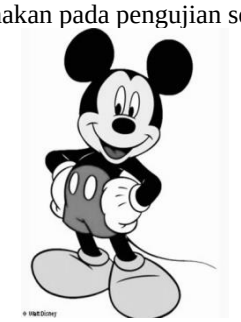


Gambar 3 GUI Matlab

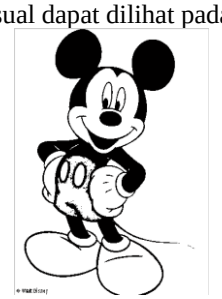
Pada bagian atar GUI terdapat menu skema enkripsi (2,4) , (2,3) dan (3,3). Bagian kiri GUI terdapat menu input citra, enkripsi dan hasil enkripsi serta penambahan noise salt and paper pada hasil enkripsi. Bagian kanan GUI terdapat display menu share yang dipilih untuk ditumpukan, hasil dekripsi tanpa dan dengan noise salt and paper serta perhitungan nilai MSE dan PSNR.

3.2 Hasil Proses Enkripsi dan Dekripsi

Citra yang digunakan pada pengujian setiap skema kriptografi visual dapat dilihat pada Gambar 4.



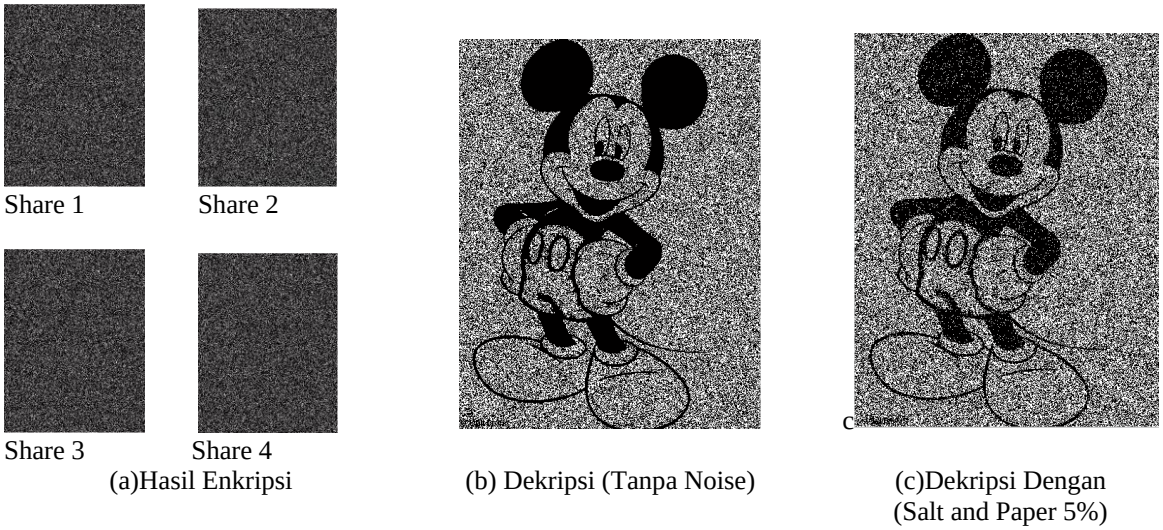
(a)



(b)

Gambar ***Error! No text of specified style in document.***. Citra Uji (a) Grayscale (b) Black and White

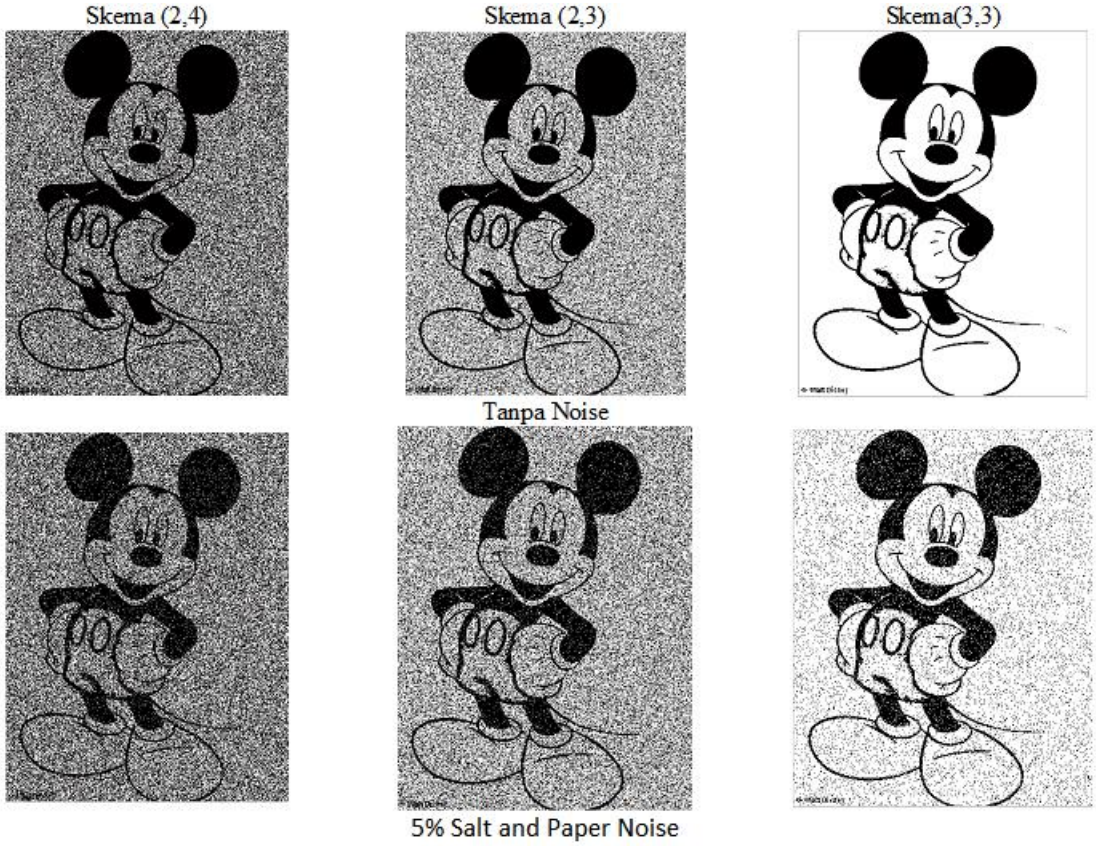
Hasil Proses Enkripsi dan dekripsi skema (2,4) dapat dilihat pada Gambar 5. Tampilan enkripsi dan dekripsi menggunakan skala yang berbeda untuk kemudahan pengaturan tata letak dan kejelasan perbedaan hasil dekripsi. Hasi enkripsi menghasilkan empat share pada Gambar 5 (a). Setiap share terlihat acak oleh mata dan tidak menunjukan informasi pada citra uji. Proses dekripsi dilakukan dengan "menumpukan" dua dari 4 share hasil enkripsi. Pada implementasi ini "penumpukan" dilakukan dengan melakukan operasi logika XOR pada setiap pixel share yang bersesuaian. Hasil dekripsi pada Gambar 5(b) menampilkan informasi cari citra asli. Bagian pixel putih citra asli tampak keabuan pada hasil dekripsi,tetapi cukup contrast dengan bagian citra hitam sehingga informasi pada citra asli dapat ditangkap oleh mata. Hasil dekripsi pada Gambar 5(b) juga cukup jelas oleh mata walaupun ketajaman gambar berkurang.



(a)Hasil Enkripsi (b) Dekripsi (Tanpa Noise) (c)Dekripsi Dengan (Salt and Paper 5%)

Gambar 5 Hasil Enkripsi dan Dekripsi Skema (2,4)

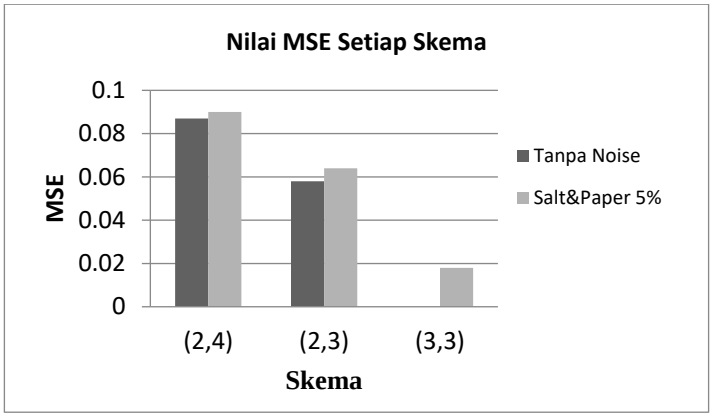
Enkripsi setiap skrema yang diimplementasikan menghasilkan share yang terlihat acak oleh mata. Bagian dekripsi menunjukan kualitas gambar yang berbeda-beda. Perbandingan hasil dekripsi setiap skema dapat dilihat pada Gambar 6.



Gambar 6 Perbandingan Hasil Dekripsi Setiap Skema

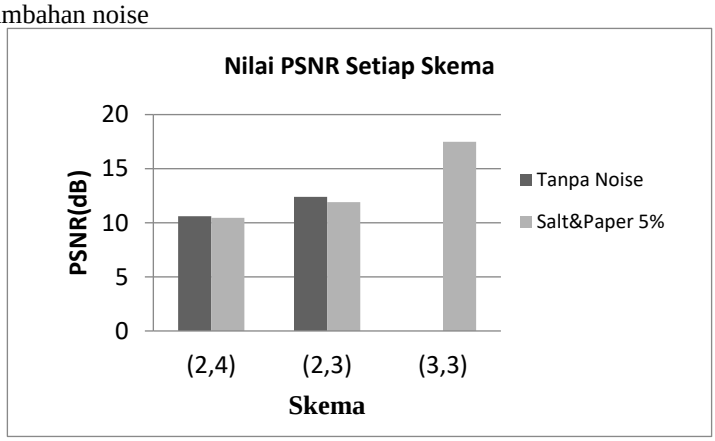
3.3 Hasil Pengujian Kuantitatif

Pengujian kuantitatif dilakukan dengan menghitung nilai *mean square error* (MSE) dan *peak signal to noise ratio* (PSNR) setiap skema. Karena proses enkripsi mengakibatkan perubahan ukuran citra gambar maka gambar asli diskalakan ke ukuran citra dekripsi sebelum dihitung nilai MSE dan PSNRnya. Hasil MSE untuk ketiga skema dapat dilihat pada Gambar 7.



Gambar 7 Perbandingan Nilai MSE setiap Skema

Hasil MSE untuk setiap skema sesuai dengan uji kualitatif (visual) pada bagian 3.2. Skema (2,4) menghasilkan MSE terbesar sedangkan skema (3,3) menghasilkan MSE 0 karena hasil dekripsi sama dengan citra asli. Nilai MSE hasil dekripsi dengan penambahan noise lebih besar daripada nilai MSE citra dekripsi tanpa penambahan noise



Gambar 8 Perbandingan Nilai PSNR Setiap Skema

Nilai PSNR setiap skema terlihat pada Gambar 8. PSNR untuk skema (3,3) tanpa noise bernilai *infinity* sehingg tidak tergambar pada grafik (citra dekripsi sama dengan citra asli).

4. KESIMPULAN

Berdasarkan pembahasan diatas dapat ditarik kesimpulan penerapan secret sharing pada citra biner dalam metode visual kriptografi dengan skema (2,4), (2,3) dan (3,3) menggunakan matlab bebasis GUI berhasil dilakukan. Hasil dekripsi skema (3,3) tanpa salt and pepper noise memperoleh nilai MSE 0 dan PSNR infinity, yang artinya citra hasil dekripsi sama dengan citra asli, dan dengan salt and pepper noise memperoleh nilai MSE 0.017827 dan nilai PSNR 17.891 dB artinya citra hasil dekripsi terlihat tidak jernih. Dibanding dengan skema (2,3) tanpa salt and pepper noise memperoleh nilai rata-rata MSE sebesar 0.057 dan nilai PSNR 12.37 dB, dan dengan salt and peppr noise nilai rata-rata MSE sebesar 0.064 dan nilai PSNR 11.91 dB. Dan untuk skema (2,4) tanpa salt and pepper noise memperoleh nilai rata-rata MSE sebesar 0.086 dan nilai PSNR 10.61 dB, dan dengan salt and peppr noise nilai rata-rata MSE sebesar 0.090 dan nilai PSNR 10.43. artinya citra hasil dekripsi dari skema (2,3) dan (2,4) kemiripannya dengan citra asli masih terlihat tidak terlalu mirip atau tidak jernih.

DAFTAR PUSTAKA

[1] N. and A. Shamir, “Visual cryptography,” 2008. doi: 10.1109/ICACTE.2008.184.
[2] L. HAKIM, “APLIKASI DAN IMPLEMENTASI SECRET SHARING MENGGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER,” 2014.
[3] W. S. Raharjo and D. Aguswahyudi, “Implementasi Skema Meaningful Sharing pada Kriptografi Visual Berwarna untuk Digital Safe Deposit Box,” J. Ultim., vol. 8, no. 1, pp. 16–22, 2017, doi: 10.31937/ti.v8i1.498.

[4] S. I. Pella, H. F. J. Lami, and I. Artikel, "IMPLEMENTASI TEKNIK KRIPTOGRAFI VISUAL PADA CITRA PENGGUNA PADA TRANSAKSI ONLINE," vol. X, no. 2, pp. 65–72, 2021.

[5] T. Yuniati and I. K. A, "Metode Pembayaran Elektronik yang Aman pada Online Shopping Berbasis Kriptografi Visual," Rekayasa Sist. dan Teknol. …, vol. 1, no. 10, pp. 319–328, 2020, [Online]. Available: http://repository.ittelkom-pwt.ac.id/id/eprint/5803.

[6] M. Kumar and R. Singh, "*A (2, n) and (3, n) Visual Cryptography Scheme for Black and White Images*," vol. 3, no. 3, pp. 574–577, 2014.