Implementasi Fungsi *Xor* pada Kriptografi Visual Skema (2,n) dengan Ekspansi Subpiksel

Muhammad Rafi Buldan Azizi[1], Asmunin[2]

[1,2]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
[1]muhammadazizi16051204034@mhs.unesa.ac.id
[2]asmunin@unesa.ac.id

***Abstrak*—Kriptografi visual sendiri adalah salah satu teknik kriptografi yang mengolah informasi berupa visual atau gambar atau citra digital. Informasi yang berupa gambar atau citra digital ini akan dibagi menjadi beberapa bagian sebelum dikirimkan, dan perlu disatukan kembali bila ingin mengetahui informasinya. Setiap bagian dari gambar yang telah dibagi adalah subset dari gambar awal. Kriptografi visual memiliki variasi dalam skema yang digunakan seperti skema (2,2), skema (3,3) atau (n,m). selain skema yang bervariasi kriptografi visual juga dapat dikembangkan dengan menambahkan fungsi *XOR* untuk meningkatkan kerahasiaannya atau dengan mengekspansi piksel / sub-piksel sehingga mampu menghasilkan lebih banyak variasi subset. Pada penelitian ini, kriptografi visual dengan skema (2,n) pada enkripsinya akan ditambahkan ekspansi sub-piksel dan dekripsinya akan menggunakan fungsi *XOR*. Dibandingkan dengan penelitian terdahulu yang tidak menggunakan ekspansi subpiksel, pada penelitian ini mencoba untuk mengembangkan hal tersebut dengan memanfaatkan ekspansi subpiksel serta mengubah skema yang digunakan,apabila pada penelitian terdahulu menggukan skema (2,2), pada penelitian ini skema yang digunakan (2,n). Hasil akhirnya pada proses enkripsi citra awal dapat menghasilkan *shares* yang diinginkan dan tiap *shares* sangat berbeda dengan citra awal. Kemudian ketika dekripsi apabila *shares* bersumber dari citra awal yang sama maka hasil dekripsi sama dengan citra awal, namun apabila *shares* bersumber dari citra yang berbeda hasil dekripsi berbeda dengan citra awal.**

Kata Kunci*—*Kriptografi Visual, Fungsi XOR, Subpiksel, Skema, Ekspansi.

I. PENDAHULUAN

Pada zaman modern ini, teknologi semakin berkembang dengan pesat terutama di bidang Komunikasi. Tingginya perkembangan teknologi komunikasi menyebabkan semakin banyak bermunculan metode baru dalam pengiriman informasi. Dengan semakin banyak metode pengiriman informasi muncul membuat tuntutan mengenai kehandalan sebuah metode dalam pengiriman informasi yang ada terutama dibidang kemanannya.

Dengan adanya tuntutan mengenai keamanan terhadap kerahasiaan sebuah informasi yang saling dipertukarkan teersebut, semakin meningkat. Di berbagai kegiatan seperti bisnis, kesehatan, keamanan negara dan data pribadi amat memerlukan jaminan keamanan dan kerahasiaan sehingga tidak merugikan pihak yang memiliki informasi tersebut. Walaupun informasi yang dikirimkan tersebut tidak ditujukan kepada pihak asing, tidak menutup kemungkinan informasi tersebut dapat tersebar tanpa sepengetahuan pemiliknya sehingga mengakibatkan kebocoran informasi yang merugikan pemilik informasi. Beberapa penyebabnya adalah lemahnya metode keamanan, sederhananya algoritma, virus, atau serangan dari pihak asing. Adapun dalam berkomunikasi dengan pihak tertentu tanpa diketahui pihak ketiga, kedua pihak memerlukan kesepakatan untuk berkomunikasi dengan menggunakan kode atau simbol yang hanya diketahui oleh kedua belah pihak. Dengan banyaknya tuntutan dari pengguna seperti perusahaan ataupun orang yang tidak ingin suatu informasi yang disampaikannya diketahui oleh pihak yang tidak perlu atau yang bukan haknya untuk mengetahui informasi tersebut. Oleh karena itu dikembangkanlah ilmu yang mempelajari tentang cara pengamanan data atau yang dikenal dengan kriptografi.

Pada algoritma kriptografi terdapat konsep utama yaitu enkripsi dan dekripsi. Enkripsi merupakan proses awal dimana informasi yang akan dikirimkan diacak dengan metode atau algoritma tertentu sehingga menjadi tidak dapat dimengerti oleh orang yang tidak berhak.[2] Sedangkan dekripsi merupakan proses mengembalikan informasi yang telah diacak untuk mengetahui isi dari informasi tersebut. Kriptografi memiliki bermacam macam teknik dalam melakukan enkripsi dan dekripsi, salah satunya adalah kriptografi visual.

Kriptografi visual sendiri adalah salah satu teknik kriptografi yang mengolah informasi berupa visual atau gambar atau citra digital.[4] kriptografi visual merupakan teknik berbagi rahasia dimana dekripsi dilakukan dengan

menumpuk bagian yang telah terbagi unutk mengungkapkan gambar asli yang ada.[8] Skema kriptografi visual Naor-Shamir standar, melayani juga sebagai protokol berbagi rahasia visual, diciptakan lebih dari dua dekade lalu. Sejak itu banyak kurang lebih sukses generalisasi telah diajukan, termasuk rahasia bertingkat pengaturan berbagi dan kriptografi visual berwarna.[9] Informasi yang berupa gambar atau citra digital ini akan dibagi menjadi beberapa bagian sebelum dikirimkan, dan perlu disatukan kembali bila ingin mengetahui informasinya. Setiap bagian dari gambar yang telah dibagi adalah subset dari gambar awal.[3] Kriptografi visual memiliki variasi dalam skema yang digunakan seperti skema (2,2), skema (3,3) atau (n,m). selain skema yang bervariasi kriptografi visual menerapkan fungsi gerbang logika dalam proses dekripsinya. Skema kriptografi visual memiliki kualitas visual yang buruk untuk citra rahasia yang direkonstruksi. Operasi dibangun di bawah hasil stacking adalah operasi Boolean OR. Banyak skema kriptografi visual konvensional didasarkan pada operasi OR, yang disebut sebagai skema kriptografi visual (OVC) berbasis OR.[10] Kriptografi visual juga dapat dikembangkan dengan menambahkan fungsi *XOR* untuk meningkatkan kerahasiaannya atau dengan mengekspansi piksel / sub-piksel sehingga mampu menghasilkan lebih banyak variasi subset.

Penelitian dengan menerapkan sebuah skema tertentu yang dikombinasikan dengan fungsi *XOR* telah dilakukan oleh Max E, dkk dengan judul " *A (2,n) XOR-based visual cryptography scheme without pixel expansion*"[6] dalam penelitian ini penggunaan fungsi *XOR* pada Skema (2,n) menghasilkan skema yang kuat dan mudah untuk digunakan dan memberikan hasil visual yang cukup baik.

Berdasarkan uraian diatas, maka penulis mengusulkan sebuah ide untuk untuk menerapkan ekspansi 4-subpiksel pada pembuatan subset dari gambar. Gambar yang digunakan adalah gambar hitam putih yang nantinya akan di enkripsi dengan kriptografi visual menggunakan skema (2,n) dan fungsi *XOR*. Alasan penulis menerapkan ekspansi 4-subpksel karena diharapkan hasil dari dekripsi akan semakin terlihat jelas dikarenakan banyaknya kombinasi yang dapat digunakan, sehingga nantinya kontras dari warna hitam putih semakin nampak dan membuat gambar semakin mudah untuk ditangkap oleh mata.

II. PENELITIAN TERKAIT

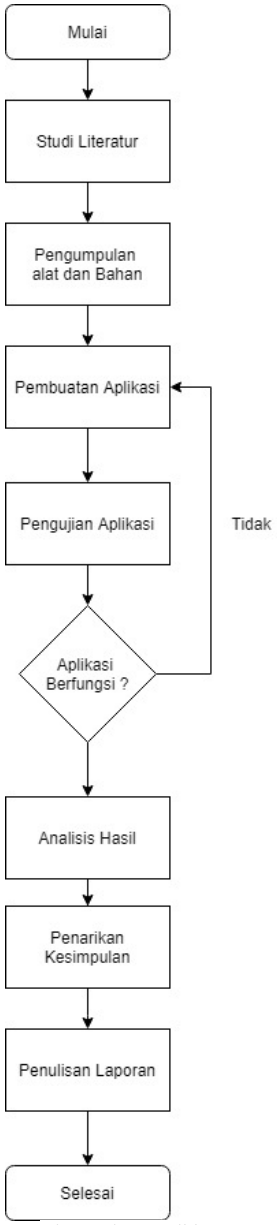
Topik mengenai penentuan kriptografi visual sudah banyak dilakukan akhir-akhir ini. Seperti yang dilakukan oleh Max E. Vizcarra Melgar dan Mylene C.Q. Farias tahun 2017 dengan judul " A (2,2) *XOR*-based visual cryptography scheme without pixel expansion".[6] Pada penelitian ini, peneliti mencoba menerapkan kombinasi metode yang digunakan untuk kriptografi visual dengan mengkombinasikan skema (2,2) dengan fungsi *XOR* tanpa adanya ekspansi piksel. Penelitian ini tidak mengekspansi piksel atau subpiksel namun memperbesar ukuran piksel dari gambar tersebut. Peneliti melakukan beberapa skema percobaan seperti resolusi spatial, intensitas cahaya dan sudut pengambilan. Jurnal tersebut menyatakan bahwa hasil yang didapat dari skema ini cukup bagus dengan ketahanan (robust) yang baik dan kemudahan dalam penggunaannya. Peneliti juga menyatakan bahya skema memiliki banyak potensi dalam pengaplikasian yang bertujuan untuk pengembangan dari kriptografi visual.

Balasubramaian R. dan Manoj M. tahun 2018 dengan judul " *A (n,n) Threshold Non-Expansible XOR Based Visual Cryptographywith unique meaningful Shares*".[7] Pada penelitian ini, peneliti mencoba untuk menerapkan sebuah kombinasi skema (n,n) dengan fungsi *XOR* pada kriptografi visual. Tanpa ada piksel ekspansi membuat *Shares* berukuran sama seperti pesan rahasianya. Peneliti menggunakan skema (n,n) bertujuan tidak membatasi *Shares* yang akan dibuat agar pengaplikasiannya mudah kedalam masalah yang nyata. Pada penelitian ini terdapat codebook dan meaningful unik pada *Shares*, dengan tujuan menghasilkan dekripsi yang sempurna dan kualitas visual yang baik pada setiap *Shares* dan hasil dekripsinya. Tujuan dari jurnal ini adalah mengetahui seberapa sempurna pengembalian dari sebuah pesan rahasia dengan peningkatan yang signifikan pada kontrasnya. Membagi menjadi 3 bagian algoritma yang pertama bertujuan membentuk matriks dasar, yang kedua membentuk subset acak dan yang ketiga subset acak yang memiliki makna untuk mencapai tujuan dekripsi. Berdasarkan hasilnya, gambar setelah di dekripsi tidak hilang. Sehingga skema ini sangat efisien untuk digunakan saat mentransmisikan informasi rahasia.

Penelitian terakhir yang menjadi landasan artikel ini ialah skripsi dari Luqman Hakim tahun 2014 dengan judul "APLIKASI DAN IMPLEMENTASI SECRET SHARING MENGGUNAKAN KRIPTOGRAFI VISUAL PADA CITRA BINER".[1] Pada penelitian ini, peneliti membuat sebuah aplikasi secret sharing menggunakan algoritma kriptografi visual. Tujuan dari aplikasi ini mengenkripsi sebuah crita dan menentukan presentase keberhasilan dalam penyembunyian informasi. berdasarkan jurnal ini metode secret sharing ini mampu mencapai presentase 100% dalam menyembunyikan informasi.

III. METODE

Alur penelitian dalam menerapkan fungsi *XOR* pada kriptografi visual dengan ekspansi subpiksel dijelaskan pada Gbr. 1



Gbr. 1 Alur penelitian

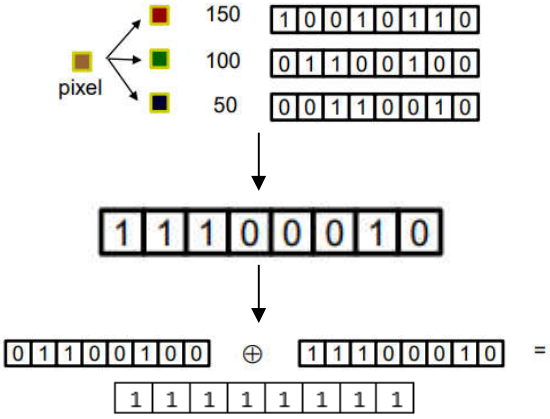
Penelitian ini dilakukan mengunakan *software* bernama *Matlab* yang dipasang pada PC

Parameter penilaian didasarkan pada hasil enkripsi apakah gambar yang di enkripsi tidak sama dengan gambar awal. parameter kedua adalah hasil dekripsi apakah hasil gambar dapat ditangkap oleh mata isinya atau gambarnya apakah menyerupai gambar awal.

A. *Perancangan Sistem*

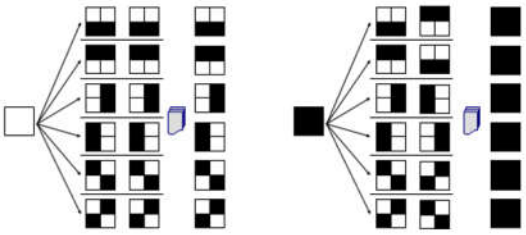
Berdasarkan alur diatas dapat dijabarkan proses kriptografi visual sebagai berikut :

1. Kriptografi visual diawal dengan memasukkan gambar asli (*Plain Image*) yang akan diproses dengan kriptografi visual skema (2,n) dengan fungsi *XOR* dan ekspansi subpiksel.
2. Kemudian gambar asli akan mengalami *preprocessing* dengan merubah tiap piksel menjadi biner kemudian dibagi ke masing masing warna *RGB,* setelahnya tiap warna dimampatkan kemudian di RGB yang telah termampatkan disambung. Kemudian array akan ditambahkan kunci untuk mengubah menjadi hitam putih.



Gbr. 2 Proses Preprocessing

3. Setelah menjadi sebuah array hitam putih, proses enkripsi selanjutnya akan membagi menjadi n buah *Shares*. Setelah penentuan jumlah *Share* yang akan dibuat dilanjutkan dengan proses enkripsi dengan mengambil sebuah piksel, misal piksel P. piksel P subpikselnya akan diekspansi yang awalnya 2 subpiksel menjadi 4 sub piksel, dengan kemungkinan sebagai berikut :



Gbr. 3 Kombinasi 4 subpiksel hitam putih

4. Kemudian jika piksel P berwarna putih, ambil secara acak sebuah matriks S pada C_0 Jika P berwarna hitam, ambil secara acak sebuah matriks S pada C1. Misalkan n = 2 kemudian piksel pertama adalah P

berwarna hitam dan matriks yang diambil dari C_1 adalah sebagai berikut:

$$S = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Maka *Share* 1 adalah baris 1 dari S dan *Share* 2 adalah baris 2 dari S. kemudian langkah tersebut diulangi kembali hingga seluruh piksel selesai di enkripsi. Berikut adalah contoh permutasi dari skema (2,n)

C_0 = { seluruh matriks hasil permutasi kolom $\begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & 0 \end{bmatrix}$ }

C_1 = { seluruh matriks hasil permutasi kolom $\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$ }

Gbr. 4 Permutasi untuk skema (2,n)

```
[m,n] = size(W);
bar = 1;
for i=1:m
    kol = 1;
    for j=1:n
        if W(i,j) == 0
            x = randi(6);
            S1(bar,kol:kol+1) = C0(1,1:2,x);
            S1(bar+1,kol:kol+1) = C0(1,3:4,x);
            S2(bar,kol:kol+1) = C0(2,1:2,x);
            S2(bar+1,kol:kol+1) = C0(2,3:4,x);
            kol = kol + 2;
        else
            x = randi(6);
            S1(bar,kol:kol+1) = C1(1,1:2,x);
            S1(bar+1,kol:kol+1) = C1(1,3:4,x);
            S2(bar,kol:kol+1) = C1(2,1:2,x);
            S2(bar+1,kol:kol+1) = C1(2,3:4,x);
            kol = kol + 2;
        end
    end
    bar = bar + 2;
end
```

Gbr. 5 Pseudocode proses enkripsi

5. Untuk proses dekripsi kedua *Share* akan ditumpuk dengan menggunakan fungsi operasi *XOR* pada seluruh piksel. Skema dari dekripsi menggunakan fungsi operasi *XOR* adalah berikut ini.

Piksel_kom [n] = piksel_s1[n] *XOR* piksel_s2[n]

```
[m,n]=size(handles.image);
[k,l]=size(handles.image2);
out = bitxor([m,n],[k,l]);
```

Gbr. 6 *Pseudocode* Proses *XOR*

6. Setelah seluruh piksel selesai ditumpuk menggunakan fungsi operasi *XOR*, dilanjutkan dengan menghilangkan kunci dari tiap piksel. Kemudian membagi array tersebut menjadi tiap RGB dan menggabungkan untuk menjadi warna aslinya.

B. *Skenario Uji Coba*

Dalam uji coba untuk penelitian ini terdapat beberapa langkah yang harus dilakukan sebagai berikut :

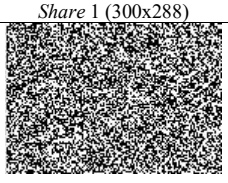
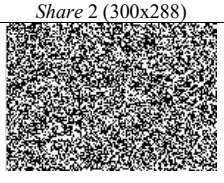
1. Uji coba enkripsi diawal dengan memilih citra yang akan digunakan untuk dienkripsi dan ditentukan akan dibagi menjadi berapa *shares*. Kemudian citra yang telah dipilih akan diubah menjadi citra biner (mengalami *image processing*). Setelah diubah menjadi citra biner, citra tersebut akan dienkripsi menajdi beberapa share sesuai dengan ketentuan diawal. Setelah selesai dibagi menjadi shares sesuai ketentuan, shares tersebut akan disimpan untuk digunakan ketika akan didekripsi. Hal ini dilakukan ke seluruh sampel citra yang ada.
2. Untuk uji coba dekripsi akan ada 2 metode uji coba, yang pertama akan diambil 2 dari share yang tersedia dari citra awal yang sama kemudian dilakukan proses dekripsi. Metode kedua akan diambil 2 dari share yang tersedia dari citra awal yang berbeda kemudian dilakukan proses dekripsi.

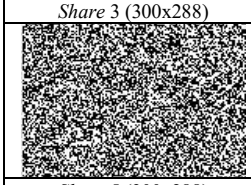
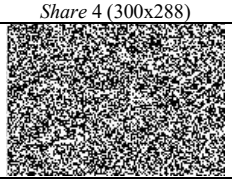
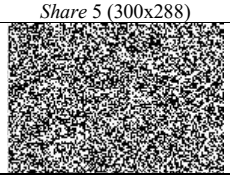
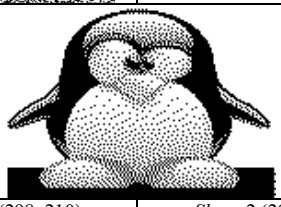
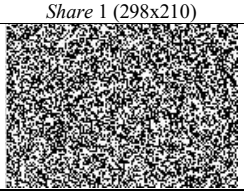
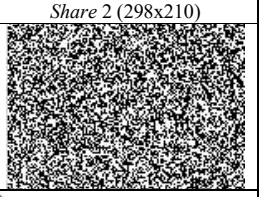
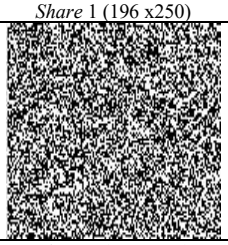
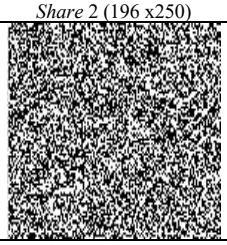
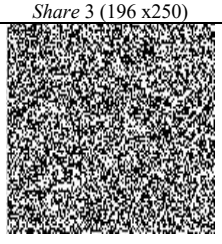
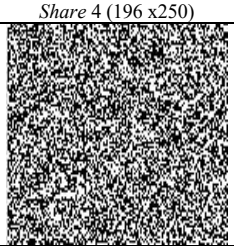
IV. HASIL DAN PEMBAHASAN

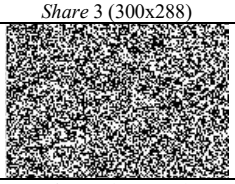
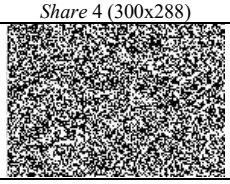
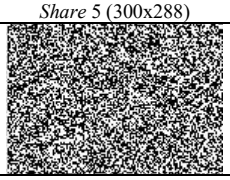
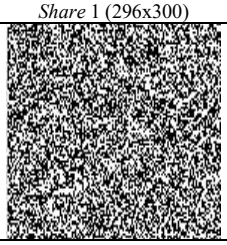
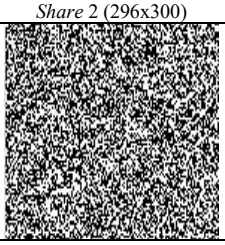
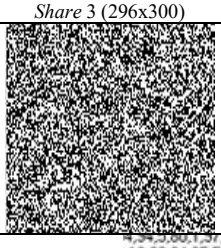
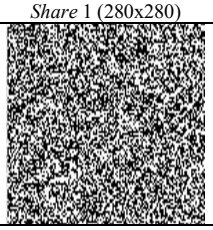
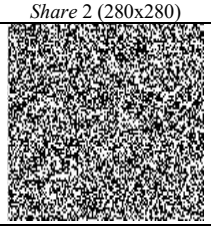
A. *Hasil Uji Enkripsi*

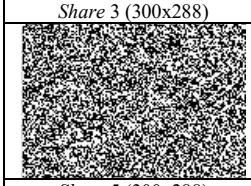
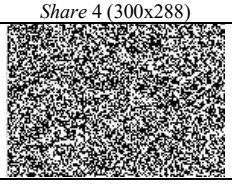
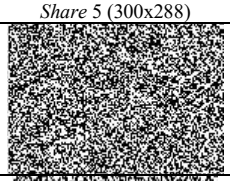
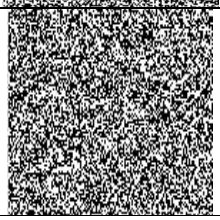
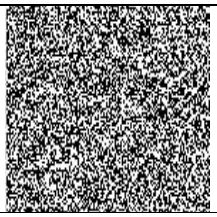
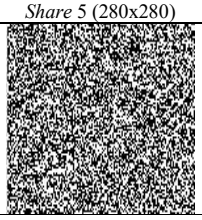
Pengujian untuk mengtahui kesesuaian hasil enkripsi dari gambar apakah mengalami perubahan piksel baik dari ukuran dan gambar. Dalam pengujian ini akan diperhatikan juga kesesuaian jumlah *Shares* yang dihasilkan. Ringkasan hasil dari penerapan enkripsi dapat dilihat pada tabel 1 Hasil perubahan enkripsi dan tabel 2 data hasil pengujian, sebagai berikut :

TABEL I
HASIL PERUBAHAN ENKRIPSI

Nama Citra	Citra Asli	
Citra1 (150x144)		
Citra Hasil Enkripsi (jumlah *Shares* = 5)	*Share* 1 (300x288)	*Share* 2 (300x288)
		

	Share 3 (300x288)	*Share* 4 (300x288)
		
	Share 5 (300x288)	
		
Citra2 (149x105)		
Citra Hasil Enkripsi (Jumlah *Shares* = 2)	*Share* 1 (298x210)	*Share* 2 (298x210)
		
Citra3 (98x125)		
Citra Hasil Enkripsi (jumlah *Shares* = 4)	*Share* 1 (196 x250)	*Share* 2 (196 x250)
		
	Share 3 (196 x250)	*Share* 4 (196 x250)
		

	Share 3 (300x288)	*Share* 4 (300x288)
		
	Share 5 (300x288)	
		
Citra4 (144 x 150)		
Citra Hasil Enkripsi (jumlah *Shares* = 3)	*Share* 1 (296x300)	*Share* 2 (296x300)
		
	Share 3 (296x300)	
		
Citra5 (140 x 140)		
Citra Hasil Enkripsi (jumlah *Shares* = 5)	*Share* 1 (280x280)	*Share* 2 (280x280)
		
	Share 3 (280x280)	*Share* 4 (280x280)

	Share 3 (300x288)	*Share* 4 (300x288)
		
	Share 5 (300x288)	
		
		
	Share 5 (280x280)	
		

TABEL II
DATA HASIL PENGUJIAN

Nama Citra	**Ukuran Awal**	**Ukuran Enkripsi**	**Isi Gambar**	**Jumlah *Share***	**Ket.**
Citra1	150 x 144	300 x 288	Tidak Terlihat	5	Berhasil
Citra2	149 x 105	298 x 210	Tidak Terlihat	2	Berhasil
Citra3	98 x 125	196 x 250	Tidak Terlihat	4	Berhasil
Citra4	144 x 150	296 x 300	Tidak Terlihat	3	Berhasil
Citra5	150 x 47	300 x 94	Tidak Terlihat	5	Berhasil

Pada tabel 1 dan tabel 2 dapat menunjukan perubahan yang terjadi pada citra asli setelah mengalami enkripsi dengan metode kriptografi visual. Perubahan terlihat pada ukuran piksel yang menjadi lebih besar dikarenakan adanya ekspansi sub-piksel sehingga menyebabkan citra hasil enkripsi memiliki ukuran 2 kali lebih besar dari citra aslinya. Kemudian citra hasil enkripsi isi/maksud dari citra tersebut tidak mampu dilihat oleh mata secara langsung, hal ini yang membuat proses enkripsi dari kriptografi visual skema (2,n) dapat dinyatakan berhasil.

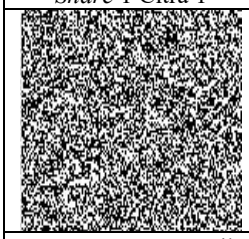
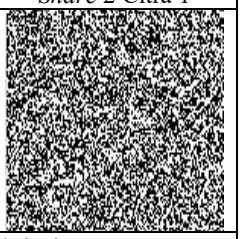
B. *Hasil Uji Dekripsi*

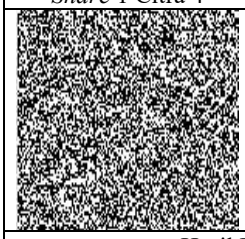
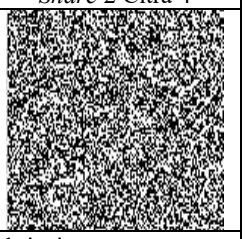
Pengujian untuk mengetahui hasil dari penggabungan meliki dua tipe, yang pertama dengan citra awal yang sama, yang kedua dengan berbeda citra awal. Dengan hasil sebagai berikut :

1. Hasil uji dekripsi dengan citra awal yang sama

   Untuk pengujian dekripsi pertama ketika proses dekripsi dengan kedua *shares* bersumber dari citra awal yang sama maka hasil dari dekripsinya menampilkan citra yang sama dengan citra awal seperti pada tabel 3.

TABEL III
CITRA HASIL DEKRIPSI PERTAMA

Citra Awal (Citra 1)	
	
Share 1 Citra 1	*Share* 2 Citra 1
	
Hasil Dekripsi	
	
Citra Awal (Citra 4)	
	

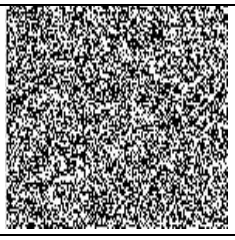
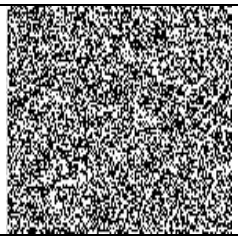
Share 1 Citra 4	*Share* 2 Citra 4
	
Hasil Dekripsi	
	

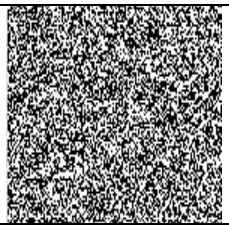
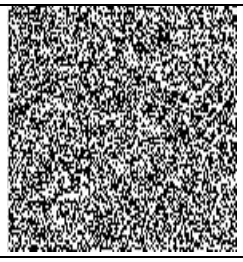
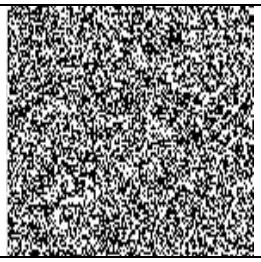
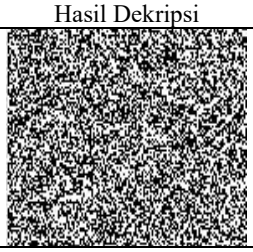
Dengan hasil dekripsi memiliki citra yang sama dengan citra awal dinyatakan pengujian ini berhasil.

2. Hasil uji dekripsi dengan citra awal yang berbeda

Untuk pengujian dekripsi kedua ketika proses dekripsi dengan kedua *shares* bersumber dari citra awal yang berbeda maka hasil dari dekripsinya menampilkan citra yang sama dengan citra awal seperti pada tabel 4.

TABEL IV
CITRA HASIL DEKRIPSI KEDUA

Citra Awal (Citra 5)	
	
Share 1 Citra 5	*Share* 2 Citra 3
	
Hasil Dekripsi	

	
Citra Awal (Citra 4)	
	
Share 1 Citra 4	*Share* 3 Citra 3
	
Hasil Dekripsi	
	

Dengan hasil dekripsi memiliki citra yang berbeda dengan citra awal dinyatakan pengujian ini berhasil.

Pada proses dekripsi dapat dilihat bahwa ketika *Share* yang digabungkan berasal dari citra awal yang sama maka citra hasil dari dekripsi dapat menghasilkan citra yang sama atau mirip dengan citra awalnya. Sedangkan apabila *Share* yang digabungkan berasal dari citra yang berbeda maka citra hasil dekripsi dari *Share* tersebut tidak dapat menunjukan citra yang mirip dengan citra awal ayng diinginkan. Sehingga proses dari dekripsi dapat dikatakan berhasil.

V. PENUTUP

A. *Kesimpulan*

Berdasarkan hasil pengujian terhadap penerapan fungsi *XOR* dan ekspansi sub-piksel kedalam kriptografi visual skema (2,n), didapatkan hasil bahwa penerapan tersebut sebagai berikut :

1. Pada proses enkripsi baik pada citra awal yang hitam putih maupun berwarna menghasilkan jumlah *shares* yang dihasilkan sesuai keinginan dan pada tiap *shares* gambar yang ditampilkan sangat berbeda dengan citra awal.
2. Pada proses dekripsi pertama ketika *shares* dengan sumber citra awal yang sama dapat menghasilkan kembali citra hasil dekripsi yang sama citra awal baik citra berwarna maupun citra yang hitam putih.
3. Pada proses dekripsi kedua ketika kedua *shares* dengan sumber citra awal yang berbeda tidak dapat menghasilkan kembali citra hasil dekripsi yang sama ataupun mirip dengan citra awal, hal ini berlaku untuk citra berwarna maupun hitam putih.

B. *Saran*

Beberapa hal yang dapat penulis sarankan untuk penelitian selanjutnya sebagai berikut :

1. seperti yang sudah penulis sebutkan sebelumnya ekspansi subpiksel memberikan sedikit dampak buruk berupa peningkatan dari ukuran tiap *Share* dan citra hasil dekripsi. Sehingga perlu pengembangan lagi agar ukuran dari citra hasil dekripsi dapat sama dengan ukuran dari citra awal/aslinya.
2. Citra yang dihasil dari penelitian ini ada citra biner atau hitam putih, sehingga perlu dikembangkan lebih banyak lagi agar nantinya ketika citra awalnya adalah citra berwarna hasilnya dari dekripsinya adalah citra berwarna pula agar isi dari citra tidak jauh berkurang dan lebih bermanfaat lagi.
3. Penelitian ini masih memiliki banyak hal untuk dikembangkan baik dari sisi skema yang digunakan dapaat diperluas atau dapat ditambahkan lebih banyak lagi fungsi atau algoritma lain yang bertujuan menyempurnakan dan meningkatan hasil dari *Share* ataupun hasil dari proses enkripsi dan dekripsi.

UCAPAN TERIMAKASIH

Puji syukur penulis haturkan kepada Allah SWT, yang telah memberikan rahmat dan kemudahan serta telah membimbing dan mengizinkan penelitian ini berjalan dengan lancar dan banyak memberikan pengetahuan baru.rasa bangga dan bersyukur disampaikan oleh penulis untuk seluruh pihak yang telah memberikan bantuan berupa apapun secara sadar maupun tidak penulis sampaikan terima kasih sebesar besarnya.

REFRENSI

[1] Hakim, L. (2014). “aplikasi dan implementasi secret sharing menggunakan kriptografi visual pada citra biner. Universitas Brawijaya, 1-8.

[2] Munir, I. (2004). Pengantar Kriptografi. Bandung : ITB.

[3] Munir, R., & Baratha, A. (1998). Studi Dan Implementasi Clustering Penerima Kunci Dengan Metode Shamir Secret Sharing Advanced. Laboratorium Ilmu dan Rekayasa Komputasi , 1-5.

[4] Naor, M., & Shamir, A. (1994). Visual Cryptography. Eurocrypt, 1-12. https://doi.org/10.1007/BFb0053419. Corpus ID: 5471098

[5] Menezes, A. J., Oorscot, P. v., & Vanstone, S. A. (1997). Handbook Of Apllied of Cryptography. United Kingdom: CRC Press Inc.

[6] Vizcarra, E. M., & Farias, C. M. (2019). A (2,2) *XOR*-based visual cryptography scheme without pixel expansion. Elsevier, 1-10. https://doi.org/10.1016/j.jvcir.2019.102592. Corpus ID: 201254554

[7] Singh, P., Raman, B., & Misra, M. (2018). A (n, n) Threshold Non-expansible *XOR* based Visual Cryptography with Unique Meaningful *Shares*. Signal Processing, 1-47. DOI: 10.1016/j.sigpro.2017.06.015. Corpus ID: 46716165

[8] Yan, B., Xiang, Y., & Hua, G. (2019). Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach. IEEE Transactions on Image Processing, 28, 896-911. DOI:10.1109/TIP.2018.2874378. Corpus ID: 52939206

[9] Orlowski, A., & Chmielewski, L. (2019). Generalized visual cryptography scheme with completely random shares. APPIS '19. DOI:10.1145/3309772.3309805. Corpus ID: 196458496

[10] Jia, X., Wang, D., Chu, Q., & Chen, Z. (2018). An efficient XOR-based verifiable visual cryptographic scheme. Multimedia Tools and Applications, 78, 8207-8223. DOI:10.1007/s11042-018-6779-6. Corpus ID: 53085420