PERANCANGAN PERANGKAT LUNAK KRIPTOGRAFI VISUAL TANPA EKSPANSI PIKSEL DAN ALGORITMA RLE

Dhina Bangkit Kumalasari

Jurusan Teknik Elektro, Fakultas Teknik, Universitas Kristen Maranatha

Jl. Prof.Drg.Suria Sumantri, MPH no. 65, Bandung, Indonesia

dhina_kumalasari@hotmail.de

ABSTRAK

Kriptografi visual diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1995. Kriptografi visual digunakan pada media yang dapat dicetak, misalkan citra. Pada skema (n,n), sebuah citra rahasia akan diubah menjadi n buah citra enkripsi yang dicetak dalam bentuk transparansi. Untuk mendekripsinya tidak membutuhkan komputasi matematis, tetapi dilakukan dengan menumpuk n buah citra terenkripsi dengan tepat dan dilihat dengan pandangan mata. Pada tugas akhir ini penumpukan dilakukan menggunakan logika OR. Untuk jumlah citra kurang dari n, maka tidak ada informasi apapun yang dapat diperoleh mengenai citra rahasia.

Pada tugas akhir ini skema yang digunakan adalah kriptografi visual (3,3), yaitu sebuah citra rahasia akan diubah menjadi 3 citra terenkripsi. Citra yang digunakan adalah citra biner. Prosesnya adalah dengan mengubah citra tersebut menjadi 3 citra terenkripsi, kemudian matriks dari 3 citra *share* tersebut akan diproses dengan algoritma metode RLE. Untuk proses dekripsinya matriks-matriks share yang telah diproses dengan algoritma RLE akan diproses kembali menjadi matriks semula kemudian didekripsi menggunakan logika OR sehingga didapatkan citra semula.

Pengujian dilakukan dengan 6 citra berbeda yang memiliki ukuran piksel yang berbeda. Hasil pengujian yang didapatkan yaitu program penyembunyian citra rahasia menggunakan Visual Kriptografi (3,3) tanpa ekspansi piksel menggunakan *software* MATLAB berhasil direalisasikan, citra hasil dekripsi pada citra rahasia yang bergaris tipis tidak dapat dikenali, r*elative difference* (α) yang menunjukkan seberapa baik kontras citra hasil dekripsi dengan *additional basis* yaitu sekitar 0,375 lebih besar daripada kontras citra hasil dekripsi tanpa *additional basis* yaitu

sekitar 0,25, nilai PSNR (*Peak Signal to Noise Ratio*) dan MOS (*Mean Opinion Score*) yang didapatkan kecil.
Kata Kunci : Kriptografi, Kriptografi Visual

ABSTRACT

Visual cryptography was introduced by Moni Naor and Adi Shamir in 1995. Visual Cryptography is used in the media that can be printed, eg image. In scheme (n, n), a secret image will be converted into n pieces of encrypted image is printed in the form of transparency. To decrypt it does not require mathematical computation, but is done by stacking n encrypted image. With the right image, secret image will be seen or use logic OR . In this final project stacking performed using a logical OR. For the number of images is less than n, then there is no any information that can be obtained about the secret image.

In this final assignment used scheme of a visual cryptography (3.3), which is the secret image will be converted into 3 encrypted image. The image used are binary image. The process is to convert the image into 3 encrypted image, then the matrix of 3 share images will be processed with RLE algorithm. For decryption process share matrices that has been processed with RLE algorithm will be processed back into matrix before processed with RLE algorithm and decrypted using a logical OR to obtain the original image.

Tests carried out with 6 different images that have different levels of detail and different pixel size. The test result were obtained that the program of a secret image hiding using visual cryptography (3.3) without pixel expansion using MATLAB software successfully realized, the decrypted image of thin striped secret image can not be recognized, the relative difference (α) which indicates how well the contrast of the image of the decryption with additional basis about 0.375 more than contrast image of the decryption without additional basis about 0.25, the value of PSNR (Peak Signal to Noise Ratio) and MOS (Mean Opinion Score) are small.

keywords : cryptography, visual cryptography

1. PENDAHULUAN

Kriptografi visual adalah sebuah teknik kriptografi yang memungkinkan penyembunyian informasi visual atau citra (enkripsi) sehingga tidak bermakna. Teknik ini diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam jurnal *Eurocrypt'94*. Teknik ini dilakukan dengan membagi citra plainteks menjadi beberapa share yang merupakan hasil enkripsinya. Dari beberapa hasil enkripsi tadi, proses dekripsi dilakukan dengan menumpuk share yang ada dengan benar sehingga terlihat makna dari citra tersebut.

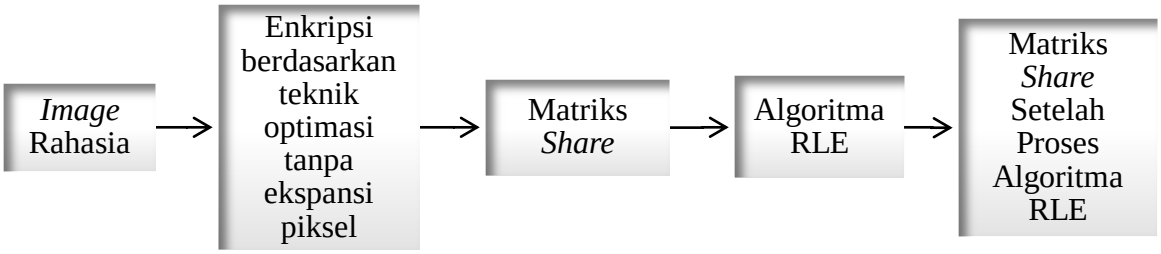
Ekspansi piksel merupakan istilah untuk perbesaran atau perluasan suatu piksel. Perbesaran yang dimaksud disini adalah setiap piksel pada citra awal diekspansi atau direpresentasikan menjadi *m* buah piksel untuk citra baru. Hal ini mengakibatkan citra baru tersebut akan mengalami perbesaran sesuai dengan perbesaran tiap pikselnya. Oleh karena itu, dibutuhkan kriptografi visual tanpa ekspansi piksel agar tidak terjadi perbesaran jumlah piksel dari citra semula maupun setelah proses enkripsi dan dekripsi (jumlah piksel tetap sama). Sedangkan kompresi RLE (*Run Length Encoding*) bertujuan untuk mengkodekan matriks citra hasil enkripsi atau *share*.

2. PERANCANGAN DAN REALISASI

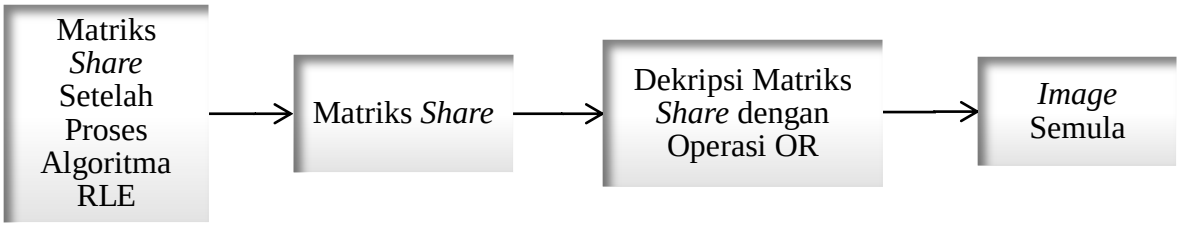
2.1 Perancangan Perangkat Lunak

Perancangan perangkat lunak terbagi dalam dua bagian utama yaitu perancangan pada proses enkripsi citra rahasia dan proses dekripsi.

Proses Enkripsi



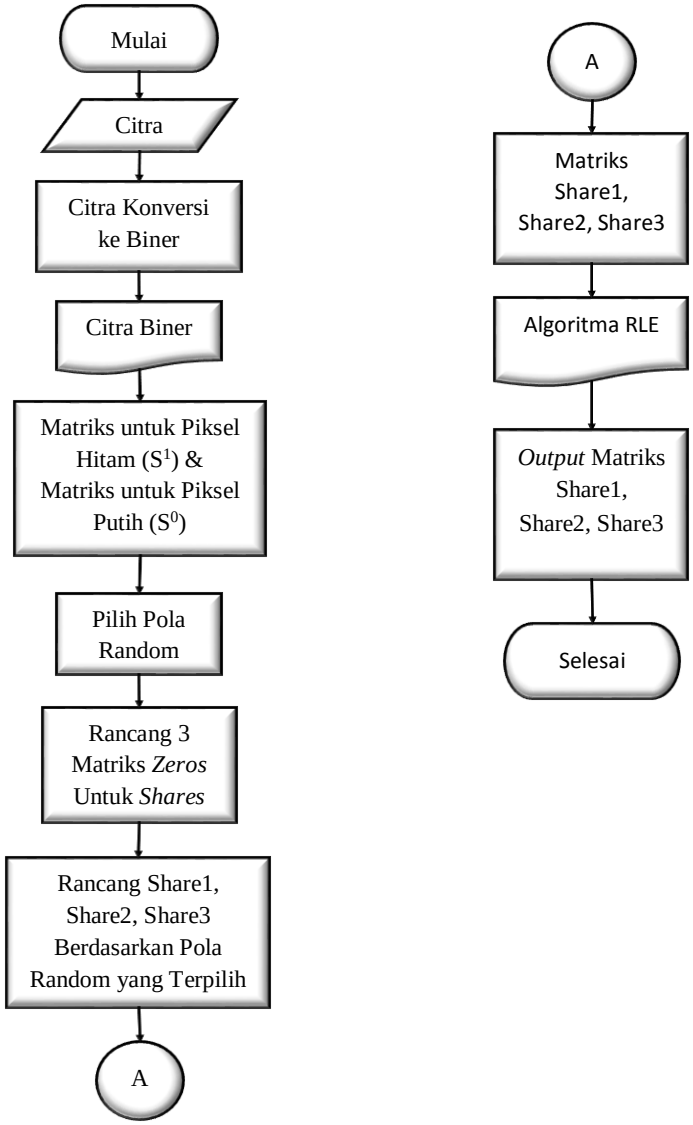
Proses Dekripsi



Gambar 1. Diagram Blok Proses Enkripsi dan Dekripsi

Untuk lebih jelasnya, blok diagram proses enkripsi dan dekripsi pada Gambar 1 akan dijelaskan dalam bentuk diagram alir seperti berikut.

Diagram Alir Proses Enkripsi tanpa *Additional Basis*



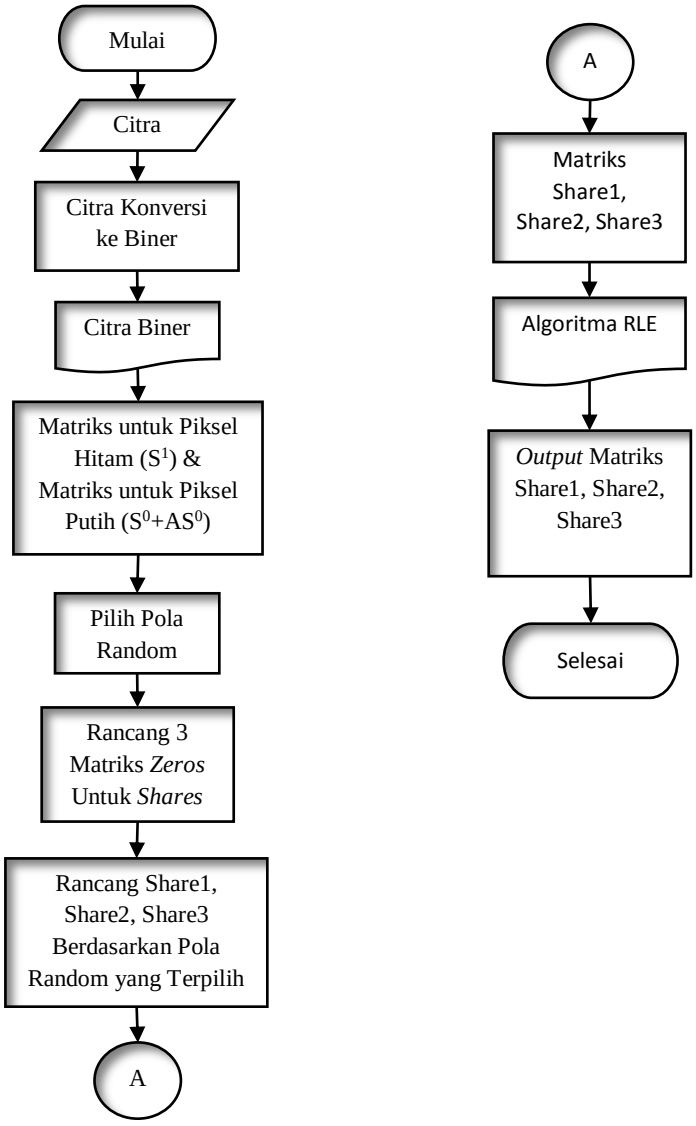
Gambar 2. Diagram Alir Proses Enkripsi tanpa *Additional Basis*.

Diagram alir dari proses enkripsi tanpa *Additional Basis* ditunjukkan pada Gambar 2 dan proses yang terjadi adalah sebagai berikut:

1. Masukkan citra yang akan di proses.
2. Konversi citra tersebut menjadi biner.
3. Mendefinisikan basis matriks untuk piksel hitam (S^1) dan basis matriks untuk piksel putih (S^0) kemudian dipilih satu kolom secara acak dari masing-masing matriks.
4. Membuat 3 matriks *zeros* untuk *shares* yang ukurannya sama dengan matriks *input*.

5. Masukkan pola acak yang terpilih pada matriks *zeros* untuk *share* yang telah dirancang.
6. Matriks *shares* yang telah didapatkan dikodekan dengan algoritma RLE (*Run Length Encoding*) sehingga menghasilkan output matriks shares.

Diagram Alir Proses Enkripsi dengan *Additional Basis*



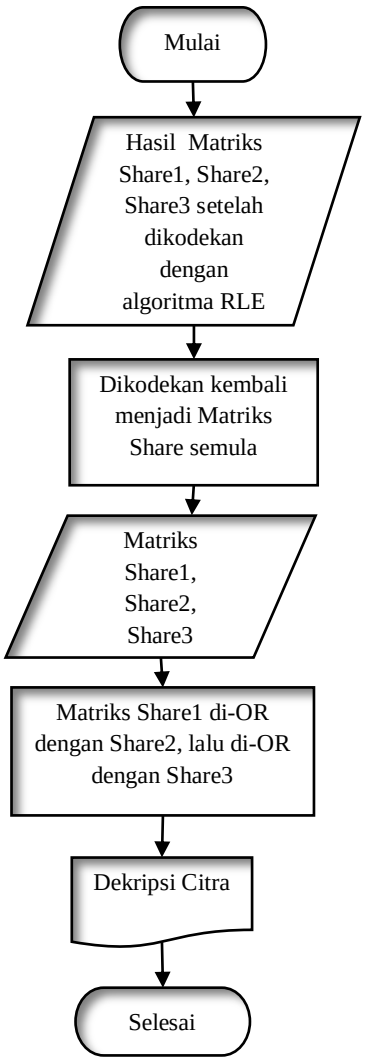
Gambar 3. Diagram Alir Proses Enkripsi dengan *Additional Basis*.

Diagram alir dari proses enkripsi dengan *Additional Basis* ditunjukkan pada Gambar 3 dan proses yang terjadi adalah sebagai berikut:

1. Masukkan citra yang akan di proses.
2. Konversi citra tersebut menjadi biner.

3. Mendefinisikan basis matriks untuk piksel hitam (S^1) dan basis matriks untuk piksel putih (S^0) ditambahkan denga *Additional Basis Matrix* (AS^0) kemudian dipilih satu kolom secara acak dari masing-masing matriks.
4. Membuat 3 matriks *zeros* untuk *shares* yang ukurannya sama dengan matriks *input*.
5. Masukkan pola acak yang terpilih pada matriks *zeros* untuk *share* yang telah dirancang.
6. Matriks *shares* yang telah didapatkan dikodekan dengan algoritma RLE (*Run Length Encoding*) sehingga menghasilkan output matriks shares.

Diagram Alir Proses Dekripsi



Gambar 4. Diagram Alir Proses Dekripsi.

Pada prosedur dekripsi yang dilakukan untuk hasil matriks share yang diproses tanpa *additional basis matrix* AS^0 untuk piksel putih sama dengan untuk hasil matriks share yang diproses dengan *additional basis matrix* AS^0.

Diagram alir dari proses dekripsi ditunjukkan pada Gambar 4 dan proses yang terjadi adalah sebagai berikut:

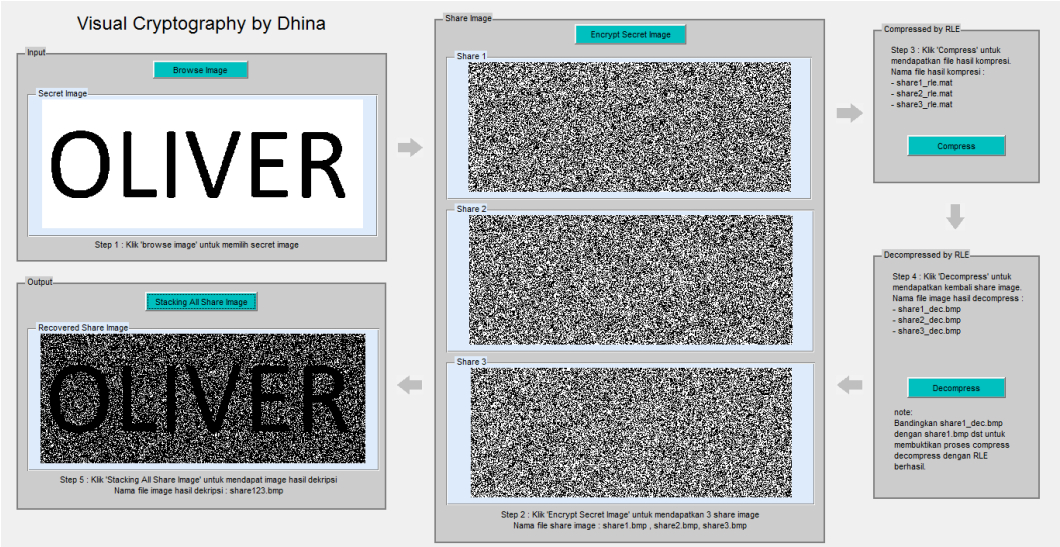
1. Proses dekripsi pertama dilakukan proses algoritma pada matriks *share* 1, *share* 2 dan *share* 3 yang sebelumnya matriks dari *share-share* tersebut telah dikodekan dengan metode RLE, supaya menjadi matriks *share* semula yang diinginkan.
2. Matriks *Share* 1, *share* 2, dan *share* 3 yang telah diproses akan didekripsi dengan menggunakan algoritma OR untuk mendapatkan hasil dekripsi.

3. DATA PENGAMATAN DAN ANALISIS

Berikut adalah data dari 2 contoh citra rahasia yang dilakukan pada program kriptografi visual (3,3) tanpa *additional basis matrix* AS^0 pada *software* MATLAB.

Data 1

Gambar 5 merupakan hasil dari percobaan dengan citra rahasia 1 pada GUI MATLAB R2012a.

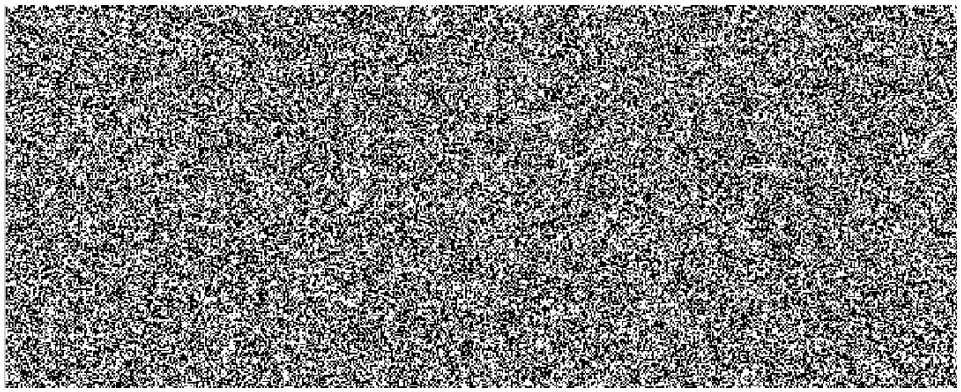


Gambar 5. Percobaan 1

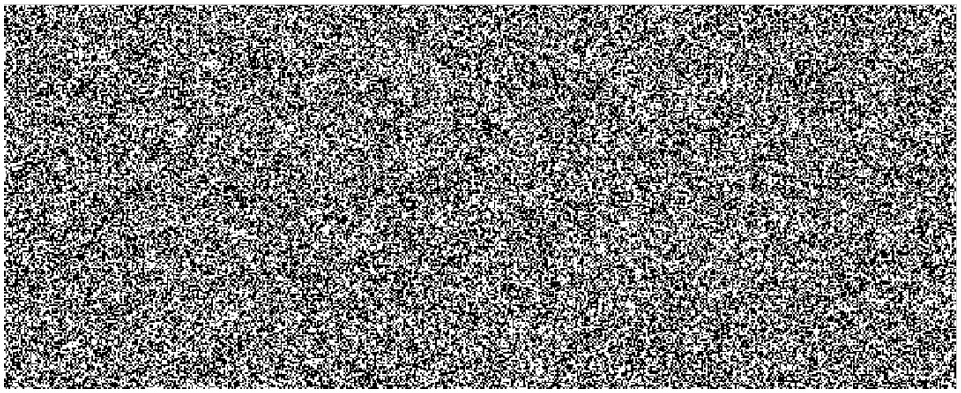
Gambar 6 yaitu citra rahasia 1 yang digunakan pada percobaan 1 kriptografi visual (3,3) tanpa *additional basis matrix* AS^0.

Gambar 6. Citra Rahasia 1

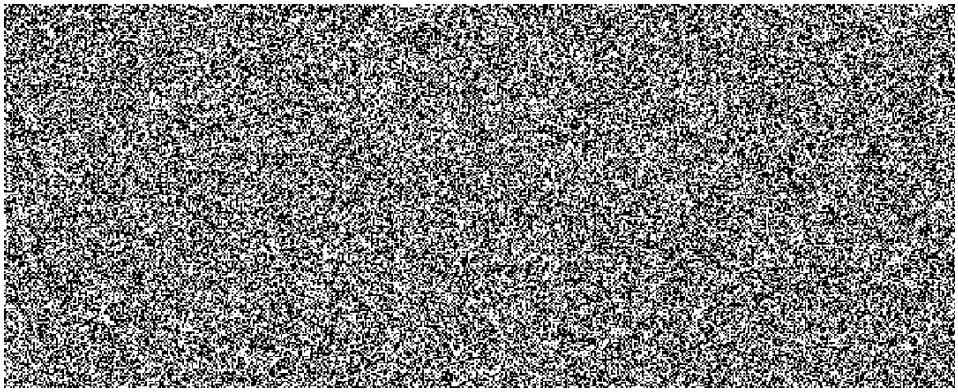
Dari citra rahasia 1 akan didapatkan hasil enkripsi (*share*) sebagai berikut



Gambar 7. *Share* 1

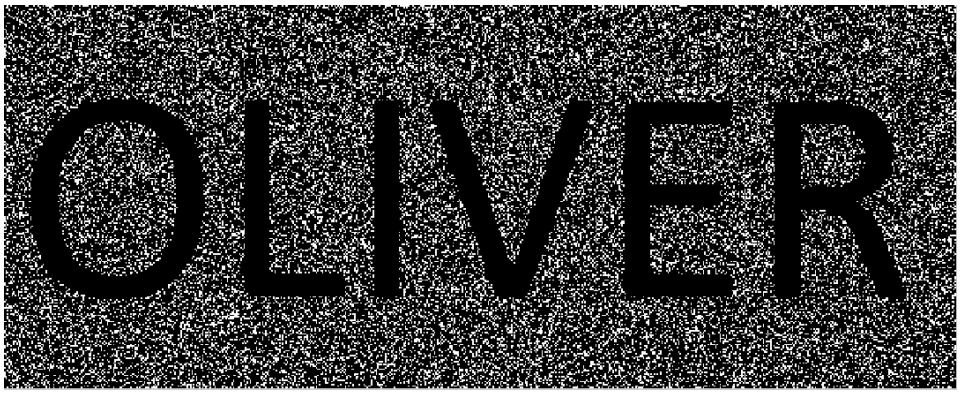


Gambar 8. *Share* 2



Gambar 9. *Share* 3

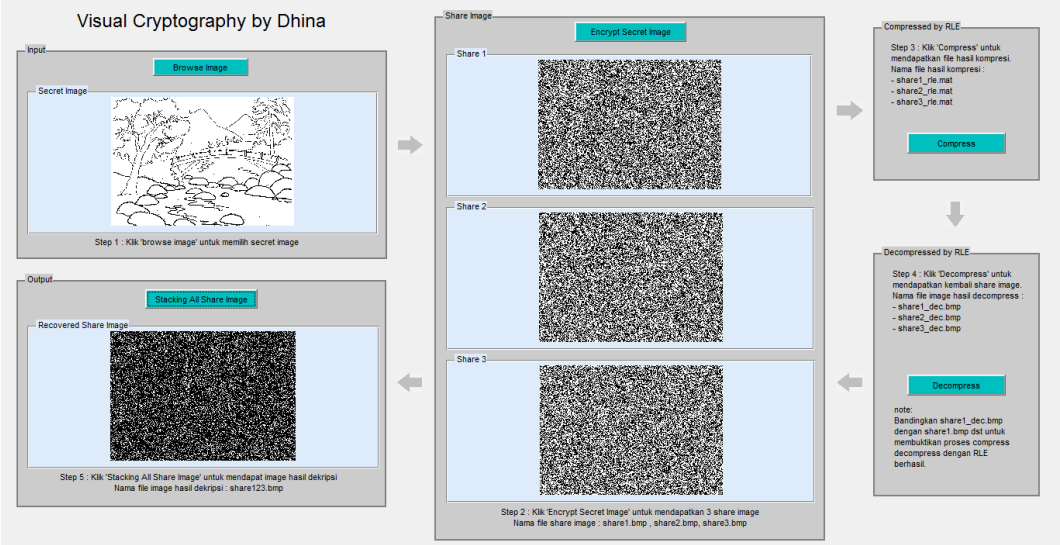
Hasil dekripsi dari share 1, share 2 dan share 3 dapat dilihat sebagai berikut



Gambar 10. *Share* 1 di-OR *Share* 2 di-OR *Share* 3

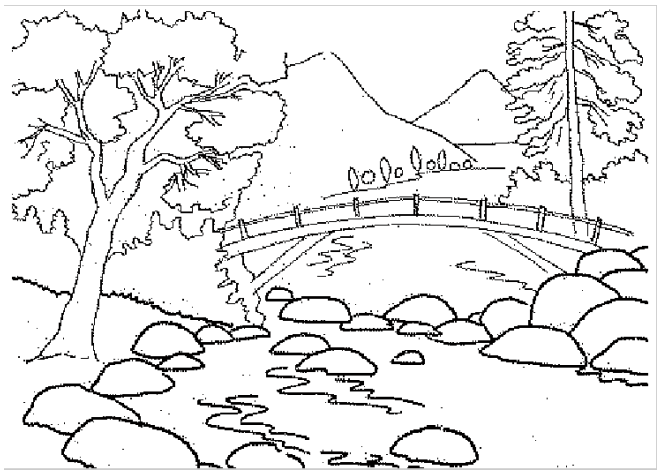
Data 2

Gambar 11 merupakan hasil dari percobaan dengan citra rahasia 2 bergaris tipis pada GUI MATLAB R2012a.



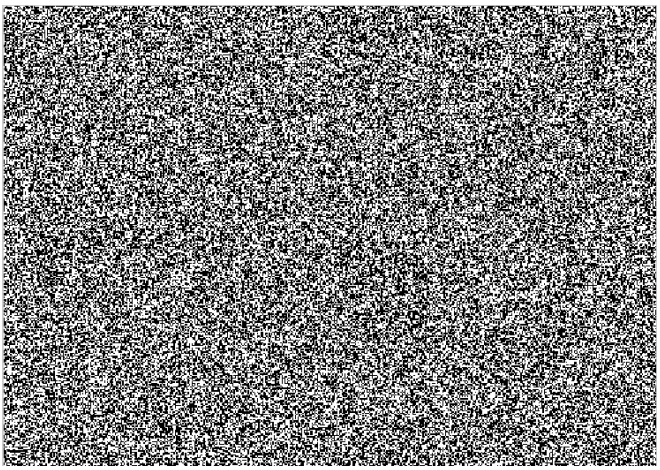
Gambar 11. Percobaan 2

Gambar 12 yaitu citra rahasia 2 yang digunakan pada percobaan 2 kriptografi visual (3,3) tanpa *additional basis matrix* AS^0.

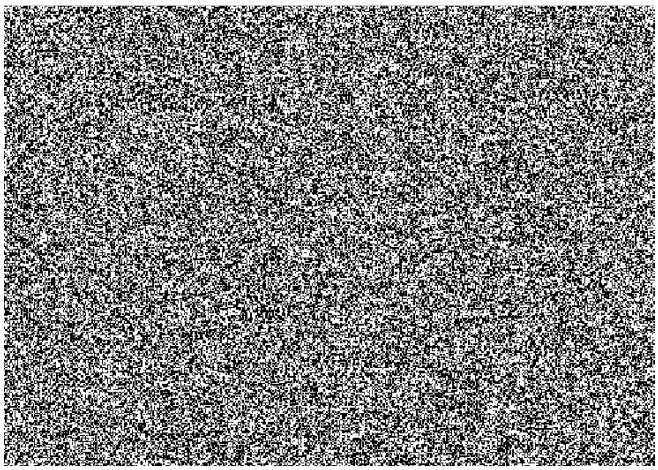


Gambar 12. Citra Rahasia 2

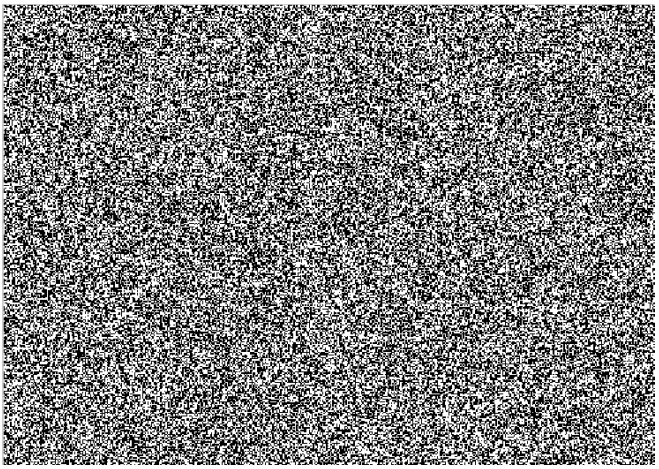
Dari citra rahasia 2 akan didapatkan hasil enkripsi (*share*) sebagai berikut



Gambar 13. *Share* 1

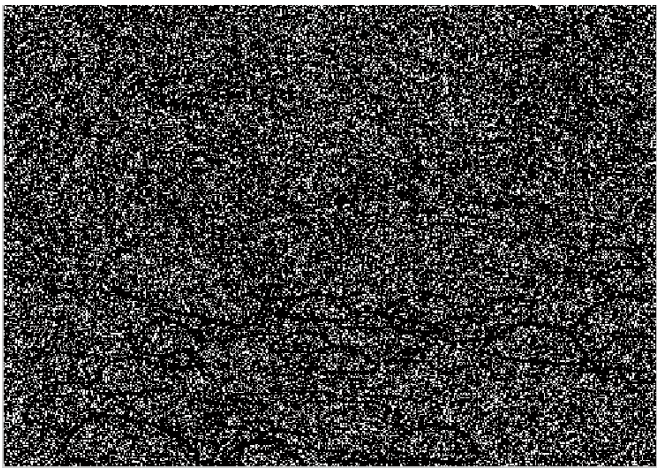


Gambar 14. *Share* 2



Gambar 15. *Share* 3

Hasil dekripsi dari share 1, share 2 dan share 3 dapat dilihat sebagai berikut

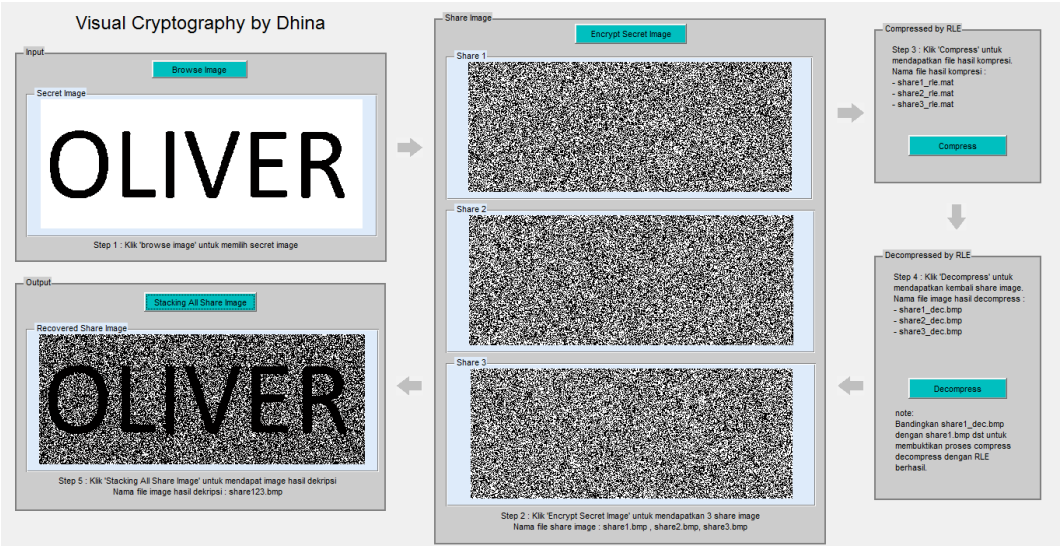


Gambar 16. *Share* 1 di-OR *Share* 2 di-OR *Share* 3

Berikut adalah data dari 2 contoh citra rahasia yang dilakukan pada program kriptografi visual (3,3) dengan *additional basis matrix* AS^0 pada *software* MATLAB.

Data 3

Gambar 17 merupakan hasil dari percobaan dengan citra rahasia 1 pada GUI MATLAB R2012a.

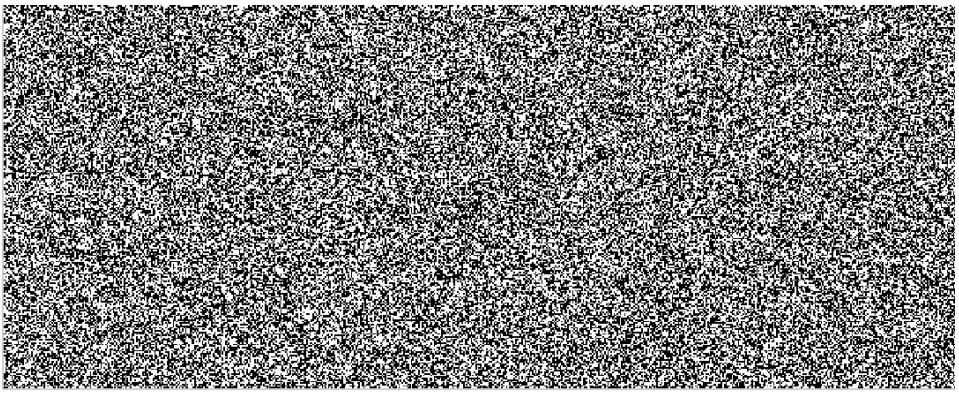


Gambar 17. Percobaan 3

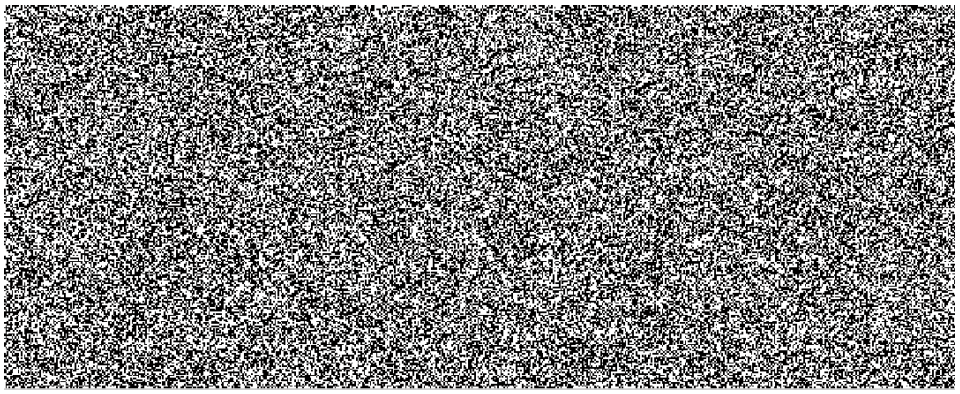
Gambar 18 yaitu citra rahasia 1 yang digunakan pada percobaan 3 kriptografi visual (3,3) dengan *additional basis matrix* AS^0.

Gambar 18 Citra Rahasia 1

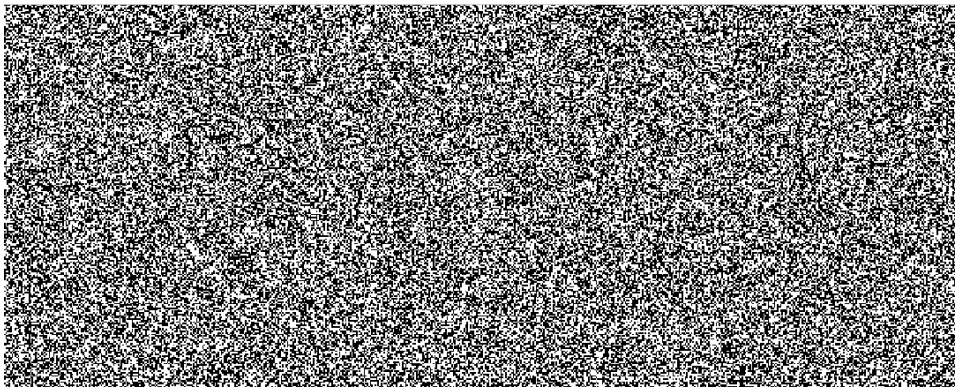
Dari citra rahasia 1 akan didapatkan hasil enkripsi (*share*) sebagai berikut



Gambar 19. *Share* 1

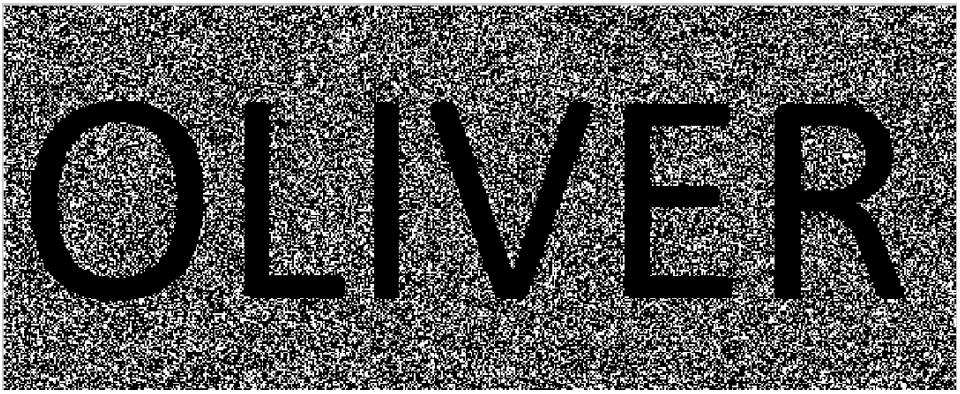


Gambar 20. *Share* 2



Gambar 21. *Share* 3

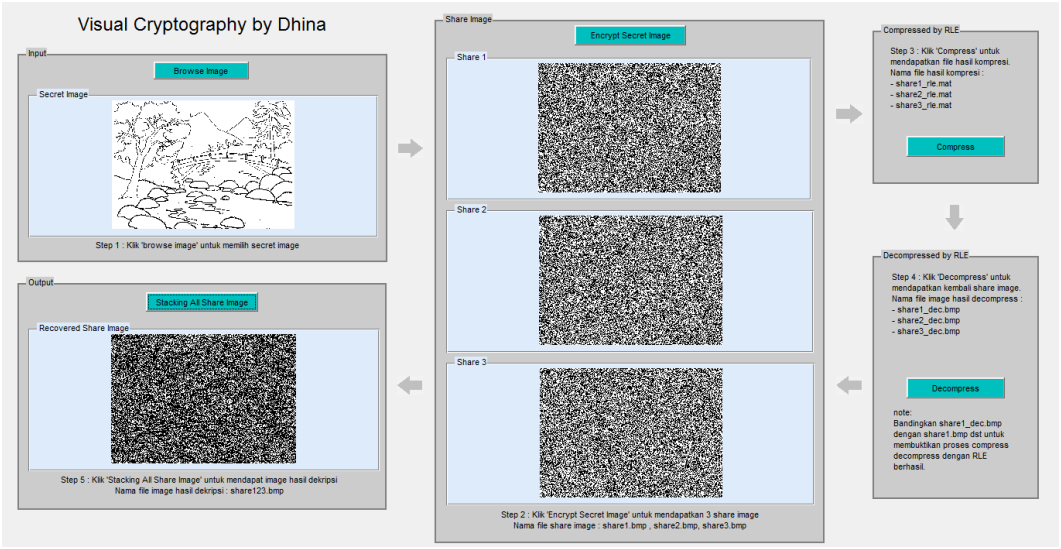
Hasil dekripsi dari share 1, share 2 dan share 3 dapat dilihat sebagai berikut



Gambar 22. *Share* 1 di-OR *Share* 2 di-OR *Share* 3

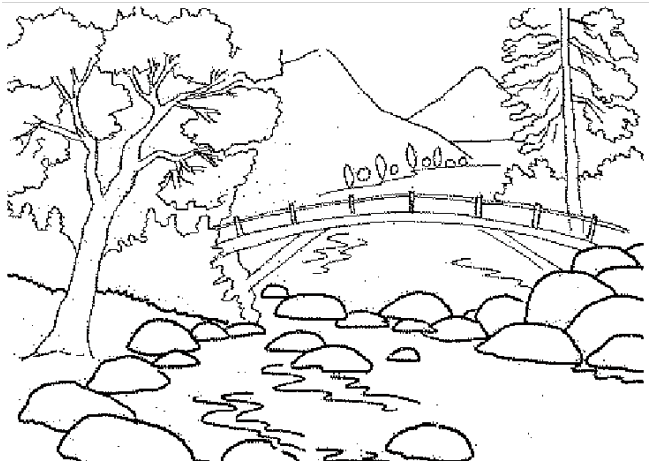
Data 4

Gambar 23 merupakan hasil dari percobaan dengan citra rahasia 2 bergaris tipis pada GUI MATLAB R2012a.



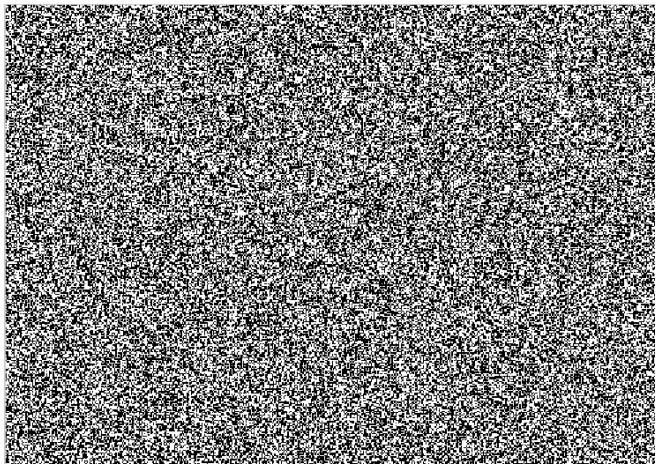
Gambar 23. Percobaan 4

Gambar 24 yaitu citra rahasia 2 yang digunakan pada percobaan 4 kriptografi visual (3,3) dengan *additional basis matrix* AS^0.

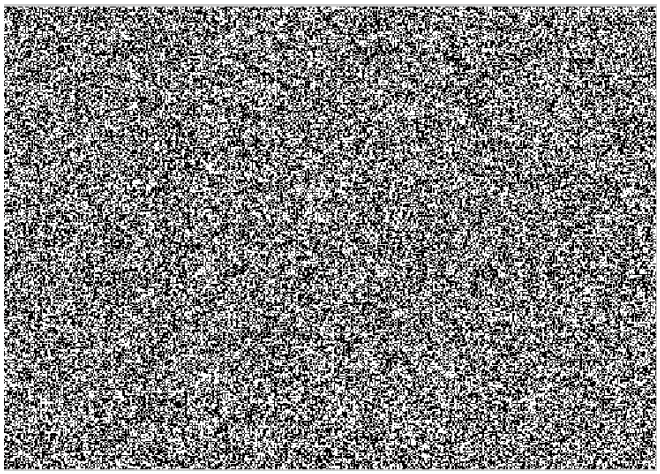


Gambar 24. Citra Rahasia 2

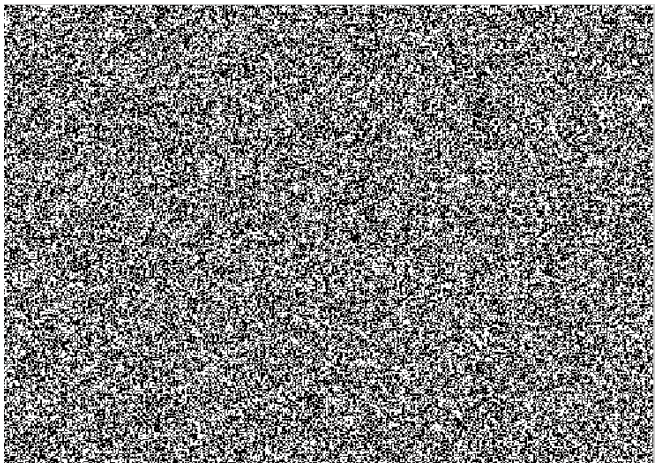
Dari citra rahasia 2 akan didapatkan hasil enkripsi (*share*) sebagai berikut



Gambar 25. *Share* 1

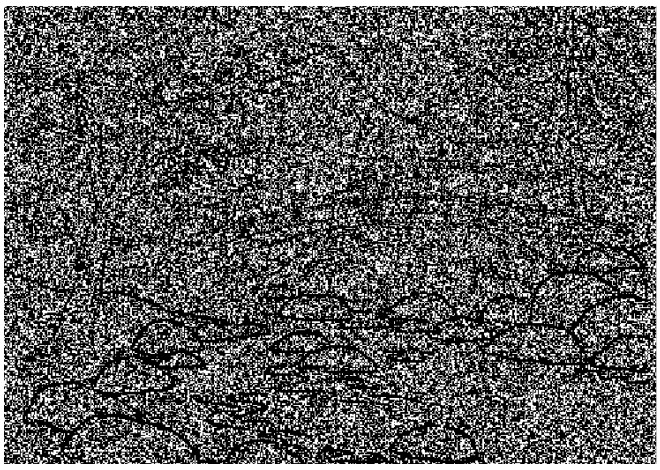


Gambar 26. *Share* 2



Gambar 27. *Share* 3

Hasil dekripsi dari share 1, share 2 dan share 3 dapat dilihat sebagai berikut



Gambar 28. *Share* 1 di-OR *Share* 2 di-OR *Share* 3

Analisa Data

Percobaan dilakukan sebanyak dua kali untuk mengetahui perbedaan jumlah piksel hitam dan putih pada citra rahasia, *share* 1, *share* 2, *share* 3 dan hasil dekripsi dari ketiga *share* tersebut dikarenakan teknik basis kolom acak yang dilakukan pada proses enkripsi. Setelah melakukan percobaan pada 2 citra rahasia didapatkan hasil pada tabel sebagai berikut.

Tabel 1 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 tanpa *Additional Basis Matrix* AS^0

(Percobaan 1)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	620	250	23988	131012	155000
Share 1	620	250	77349	77651	155000
Share 2	620	250	77537	77463	155000
Share 3	620	250	77660	77340	155000
Share 1or2or3	620	250	122243	32757	155000
Relative difference, α = 32757 / 131012 = 0,25003					
PSNR = 1,9678					

Tabel 2 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 tanpa *Additional Basis Matrix* AS^0

(Percobaan 2)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	620	250	23988	131012	155000
Share 1	620	250	77570	77430	155000
Share 2	620	250	77309	77691	155000
Share 3	620	250	77611	77389	155000
Share 1or2or3	620	250	122261	32739	155000
Relative difference, α = 32739 / 131012 = 0,24989					

PSNR = 1,9698

Tabel 3 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 yang merupakan citra bergaris tipis tanpa *Additional Basis Matrix* AS^0

(Percobaan 1)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	500	355	17173	160327	177500
Share 1	500	355	88832	88668	177500
Share 2	500	355	88609	88891	177500
Share 3	500	355	88910	88590	177500
Share 1or2or3	500	355	137523	39977	177500
Relative difference, α = 39977 / 160327 = 0,24935					
PSNR = 1,6875					

Tabel 4 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 yang merupakan citra bergaris tipis tanpa *Additional Basis Matrix* AS^0

(Percobaan 2)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	500	355	17173	160327	177500
Share 1	500	355	89099	88401	177500
Share 2	500	355	89026	88474	177500
Share 3	500	355	88514	88986	177500
Share 1or2or3	500	355	137672	39828	177500
Relative difference, α = 39828 / 160327 = 0,24842					
PSNR = 1,6821					

Tabel 5 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 dengan *Additional Basis Matrix* AS^0

(Percobaan 1)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	620	250	23988	131012	155000
Share 1	620	250	77437	77563	155000
Share 2	620	250	77486	77514	155000
Share 3	620	250	77690	77310	155000
Share 1or2or3	620	250	105925	49075	155000
Relative difference, α = 49075 / 131012 = 0,37458					
PSNR = 2,7753					

Tabel 6 Hasil Detail Jumlah Piksel Pada Citra Rahasia 1 dengan *Additional Basis Matrix* AS^0

(Percobaan 2)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	620	250	23988	131012	155000
Share 1	620	250	77405	77595	155000
Share 2	620	250	77362	77638	155000
Share 3	620	250	77486	77514	155000
Share 1or2or3	620	250	105779	49221	155000
Relative difference, α = 49221 / 131012 = 0,3757					
PSNR = 2,7745					

Tabel 7 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 yang merupakan citra bergaris tipis dengan *Additional Basis Matrix* AS^0

(Percobaan 1)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	500	355	17173	160327	177500
Share 1	500	355	88820	88680	177500
Share 2	500	355	88842	88658	177500
Share 3	500	355	88668	88832	177500
Share 1or2or3	500	355	117501	59999	177500
Relative difference, α = 59999 / 160327 = 0,37423					
PSNR = 2,4778					

Tabel 8 Hasil Detail Jumlah Piksel Pada Citra Rahasia 2 yang merupakan citra bergaris tipis dengan *Additional Basis Matrix* AS^0

(Percobaan 2)

Image	Jumlah Kolom Pada *Image*	Jumlah Baris Pada *Image*	Jumlah Piksel Hitam Pada Image	Jumlah Piksel Putih Pada Image	Jumlah piksel Pada Image
Citra rahasia	500	355	17173	160327	177500
Share 1	500	355	88464	89036	177500
Share 2	500	355	88196	89304	177500
Share 3	500	355	88442	89058	177500
Share 1or2or3	500	355	117007	60493	177500
Relative difference, α = 60493 / 160327 = 0,37731					
PSNR = 2,4992					

4. KESIMPULAN

Kesimpulan yang dapat diambil dari Tugas Akhir ini adalah sebagai berikut:

1. Program penyembunyian citra rahasia menggunakan Visual Kriptografi (3,3) tanpa ekspansi piksel menggunakan *software* MATLAB berhasil direalisasikan.
2. *Relative difference* (α) yang menunjukkan seberapa baik kontras citra hasil dekripsi dengan *additional basis matrix* AS^0 yaitu sekitar 0,375 lebih besar daripada kontras citra hasil dekripsi tanpa *additional basis matrix* AS^0 yaitu sekitar 0,25.
3. Citra hasil dekripsi pada citra rahasia bergaris tipis (citra rahasia 2) tidak dapat dikenali.
4. PSNR yang didapatkan dari citra hasil dekripsi tanpa *additional basis* tidak bagus pada citra rahasia 1 yaitu 1,9678 dB dan 1,9698 dB, pada citra rahasia 2 yaitu 1,6821 dB dan 1,6875 dB.
5. PSNR yang didapatkan dari citra hasil dekripsi dengan *additional basis* juga tidak bagus pada citra rahasia 1 yaitu 2,7745 dB dan 2,7753 dB, pada citra rahasia 2 yaitu 2,4778 dB dan 2,4992 dB.
6. MOS (*Mean Opinion Score*) yang didapatkan dari hasil dekripsi citra rahasia 1 yaitu 1,6-2, pada citra rahasia 2 yaitu 1.

5. DAFTAR PUSTAKA

1. Manimurugan. S, Ramajayam. N. *"Visual Cryptography Based On Modified RLE Compression without Pixel Expansion"* International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, Issue 3, September 2012.

2. Thomas month and babu anto p. *"Achieving Optimal Contrast in Visual Cryptography Schemes without Pixel Expansion"* International journal of recent trends in engineering, vol. 1, no. 1, may 2009.

3. S. Kirkpatrick et al. *"Optimization by Simulated Annealing"* Science, 13 May 1983, vol. 220, no. 4598.