

SKRIPSI

**SKEMA VISUAL SECRET SHARING DENGAN TEKNIK
RANDOM GRIDS**



Wahyu Hariadi Nugroho

NPM: 2014730061

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2019**

UNDERGRADUATE THESIS

**VISUAL SECRET SHARING SCHEME WITH RANDOM
GRIDS TECHNIQUE**



Wahyu Hariadi Nugroho

NPM: 2014730061

**DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2019**

LEMBAR PENGESAHAN



**SKEMA VISUAL SECRET SHARING DENGAN TEKNIK
RANDOM GRIDS**

Wahyu Hariadi Nugroho

NPM: 2014730061

Bandung, 13 Desember 2018

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Natalia, M.Si.

Anggota Tim Penguji

Chandra Wijaya, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng



PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

SKEMA VISUAL SECRET SHARING DENGAN TEKNIK RANDOM GRIDS

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 13 Desember 2018



Wahyu Hariadi Nugroho
NPM: 2014730061

ABSTRAK

Visual Secret Sharing (VSS) adalah metode untuk merahasiakan sebuah rahasia berupa gambar. Hal ini dilakukan dengan cara membagi gambar rahasia tersebut menjadi beberapa gambar lain yang disebut sebagai *shadow*. Pada skema VSS (k, n) , gambar akan dibagi menjadi n buah *shadow* dan untuk mendapatkan kembali gambar awal dibutuhkan penumpukan k buah *shadow*.

Pada skripsi ini, akan membahas mengenai Skema (k, n) -*Random Incrementing Visual Secret Sharing* (RIVSS) berbasis Teknik *Random Grids*. Skema (k, n) -*Random Incrementing Visual Secret Sharing* (RIVSS) berbasis Teknik *Random Grids* ini berarti sebuah gambar rahasia akan dibagi ke beberapa tingkat kerahasiaan dan dibagi menjadi n *shadow* berupa *random grids* di mana $t(k \leq t \leq n)$ *share* dapat digunakan untuk merekonstruksi bagian rahasia sampai dengan tingkat $t - k + 1$. Namun, tidak ada informasi mengenai gambar asli yang didapatkan oleh $k - 1$ atau lebih sedikit *share*. *Random Grids* sendiri adalah sebuah transparansi yang terdiri dari piksel bertipe array dua dimensi yang transparan atau buram yang ditentukan dengan cara yang benar-benar acak (*random*).

Skripsi ini akan dibangun perangkat lunak yang dapat mengimplementasikan VSS dengan skema $(2, n)$ -VSS Naor Shamir, $(3, n)$ -VSS Naor Shamir, $(2, 2)$ -Tradisional VSS *Random Grids*, (k, n) -RIVSS dengan Teknik *Random Grids*. Pada perangkat lunak diimplementasikan modifikasi dari cara pembagian *region* pada gambar rahasia dan hubungannya dengan pembentukan *shadow* dengan tujuan untuk membuat skema VSS dengan Teknik *Random Grids* menjadi lebih baik dan lebih luas implementasinya. Selain itu, dilakukan juga perhitungan Jarak Euclidean untuk hasil penumpukan *shadow* VSS yang menjadi ukuran perbandingan kualitas skema VSS untuk mencari tahu skema mana yang lebih baik.

Berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan bahwa perangkat lunak yang dibangun dapat mengimplementasikan $(2, n)$ -VSS Naor Shamir, $(3, n)$ -VSS Naor Shamir, $(2, n)$ -Tradisional VSS *Random Grids*, (k, n) -RIVSS dengan Teknik *Random Grids*.

Kata-kata kunci: *visual secret sharing, random grids, shadow, region, VSS Naor Shamir, Random Incrementing Visual secret Sharing Random Grids, Jarak Euclidean*

ABSTRACT

Visual Secret Sharing (VSS) is a method to conceal an image by dividing it into some other images called shadows printed on transparency paper. In the (k, n) -VSS scheme, the image will be divided into n shadows and to get back into secret/initial image, a stacking of k shadows is needed.

To construct a general (k, n) -RIVSS scheme for any $2 \leq k \leq n$, we utilize the concept of the random-grid based image sharing. In our scheme, the image A is partitioned into $n - k + 1$ regions of different secrecy levels, then it can be reconstructed by any k or more shadows.

In this undergraduate thesis, a software is developed to implement $(2, n)$ -VSS Naor Shamir scheme, $(3, n)$ -VSS Naor Shamir scheme, $(2, n)$ -Traditional VSS Random Grids scheme, (k, n) -RIVSS with Random Grids Technique scheme. In this software, it should implemented modification of dividing region in the secret image and the correlation with the form of shadow with the purpose to build a better scheme of VSS with Random Grids Technique and with the implementation. Furthermore, the better scheme will be decided by calculate the Euclidean Distance.

Based on the test done, it can be concluded that the software can implement $(2, n)$ -VSS Naor Shamir, $(3, n)$ -VSS Naor Shamir, $(2, n)$ -Traditional VSS *Random Grids*, (k, n) -RIVSS with *Random Grids* Technique.

Keywords: visual secret sharing, random grids, shadow, region, VSS Naor Shamir, Random Incrementing Visual secret Sharing Random Grids, Euclidean Distance

*Dipersembahkan kepada Tuhan Yesus Kristus, Amah, Omcil, Papa,
dan Mama.*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis berhasil menyelesaikan skripsi yang berjudul "*Visual Secret Sharing* dengan Teknik *Random Grids*". Penulis menyadari bahwa penyusunan skripsi ini tidak akan selesai tanpa bantuan dan dukungan berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terimakasih kepada:

- Amah, omcil, papa, dan mama atas dukungan dan kepercayaan serta motivasi untuk penulis sehingga mampu menyelesaikan skripsi ini.
- Ibu Mariskha atas motivasi, kritik, serta saran yang membantu penulis sehingga dapat menyelesaikan skripsi ini.
- Ibu Natali dan Pak Chandra atas masukan dan saran yang telah diberikan sebagai dosen penguji.
- Averina, Nathaniel, Enrico, serta Stephanie yang selalu setia mengerti dan menyemangati penulis agar skripsi ini dapat terselesaikan.
- Vica, Aldo, Ilham, Keenan, Abat, Walah, serta teman-teman seperjuangan yang selalu menjadi parameter dan dorongan bagi penulis untuk terus bisa berjuang menyelesaikan skripsi ini.
- Teruntuk Kabinet LKM SINERGI, terima kasih atas pengalaman dan semangat yang selalu ditularkan kepada penulis sehingga dapat menyelesaikan skripsi ini.
- Semua pihak yang tidak dapat disebutkan satu-persatu yang sudah memberikan bantuan dan dukungan sepanjang masa perkuliahan dan pengerjaan skripsi ini baik secara langsung maupun tidak langsung.

Semoga semua pihak diatas mendapatkan balasan dan berkat dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf apabila terdapat kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini berguna bagi semua pihak yang memerlukan.

Bandung, Januari 2019

Penulis

DAFTAR ISI

KATA PENGANTAR	xv
DAFTAR ISI	xvii
DAFTAR GAMBAR	xix
DAFTAR TABEL	xxiii
1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Batasan Masalah	2
1.5 Metodologi	3
1.6 Sistematika Pembahasan	3
2 LANDASAN TEORI	5
2.1 Secret Sharing	5
2.2 Visual Secret Sharing	5
2.2.1 $(2, n)$ -Visual Secret Sharing Naor Shamir	6
2.2.2 $(3, n)$ -Visual Secret Sharing Naor Shamir	7
2.2.3 $(2, 2)$ -Tradisional Visual Secret Sharing dengan Teknik Random Grids	8
2.2.4 Random Incrementing Visual Secret Sharing dengan Teknik Random Grids	9
2.2.5 Rekonstruksi <i>Shadow</i> menjadi Gambar Rahasia	9
2.3 Penentuan Segmen pada Gambar(Segmen Labeling)	10
2.4 Open CV	10
2.5 Euclidean Distance	12
3 ANALISIS	13
3.1 Analisis Masalah	13
3.2 Studi Kasus	16
3.3 Analisis Perangkat Lunak	20
3.3.1 Diagram Aktivitas	20
3.3.2 Diagram Kelas Awal	22
4 PERANCANGAN	27
4.1 Kebutuhan Masukan dan Keluaran	27
4.2 Perancangan Antarmuka	28
4.3 Diagram Kelas Lengkap	30
4.4 Rincian Metode	31
4.4.1 Kelas VSS	32
4.4.2 Kelas TVSSRG	36
4.4.3 Kelas RIVSSRG	37

4.4.4	Kelas VSSNS2N	40
4.4.5	Kelas VSSNS3N	42
4.4.6	Kelas Pixel	43
4.4.7	Kelas PixelComparator	44
4.4.8	Kelas SobelEdgeDetection	45
4.4.9	Kelas GUI	45
4.4.10	Kelas GUI2	45
4.4.11	Kelas GUI3	45
4.4.12	Kelas GUI4	45
4.4.13	Kelas GUI5	47
5	IMPLEMENTASI DAN PENGUJIAN	51
5.1	Implementasi Antarmuka	51
5.2	Pengujian Fungsional	52
5.3	Pengujian Eksperimental	55
5.3.1	Pengujian Eksperimental dengan Gambar Solid dengan Batas Gambar Tegas (Jumlah Segmen = 1)	55
5.3.2	Pengujian Eksperimental dengan Gambar Solid dengan Batas Gambar Tegas (Jumlah Segmen = 2)	59
5.3.3	Pengujian Eksperimental dengan Gambar Solid dengan Batas Gambar Tegas (Jumlah Segmen = 3)	65
5.3.4	Pengujian Eksperimental dengan Gambar Solid dengan Batas Gambar Tegas yang Berpola	71
5.3.5	Pengujian Eksperimental dengan Gambar Tidak Solid dengan Batas Gambar Tidak Tegas	80
6	KESIMPULAN DAN SARAN	89
6.1	Kesimpulan	89
6.2	Saran	90
	DAFTAR REFERENSI	91
	A KODE PROGRAM	93

DAFTAR GAMBAR

2.1 skema <i>Visual Secret Sharing</i>	6
2.2 <i>Shadow</i> untuk piksel putih	7
2.3 <i>Shadow</i> untuk piksel hitam	7
2.4 Hasil penumpukan <i>shadow</i> untuk piksel putih	7
2.5 Hasil penumpukan <i>shadow</i> untuk piksel hitam	8
3.1 Hasil Canny Edge Detection	14
3.2 Hasil Sobel Edge Detection	14
3.3 (a) segmen yang hanya terdiri dari piksel hitam, dan (b) segmen dengan kombinasi piksel hitam dan putih	15
3.4 Hasil Sobel Edge Detection	15
3.5 Contoh masukan gambar rahasia 5 x 5 piksel	16
3.6 Hasil pemberian label segmen	17
3.7 Hasil Pemberian Garis Tepi dengan Metode <i>Sobel Edge Detection</i>	17
3.8 Hasil Nilai Label Segmen setelah melalui Proses <i>Sobel Edge Detection</i>	17
3.9 Hasil Nilai <i>Region</i> tiap piksel	18
3.10 <i>Shadow</i> R1	19
3.11 <i>Shadow</i> R2	19
3.12 <i>Shadow</i> R3	19
3.13 <i>Shadow</i> R1 + R2	19
3.14 <i>Shadow</i> R1 + R3	19
3.15 <i>Shadow</i> R2 + R3	19
3.16 R1 + R2 + R3	20
3.17 Diagram aktivitas penyelesaian masalah VSS naor Shamir untuk perangkat lunak yang akan dibuat	21
3.18 Diagram aktivitas penyelesaian masalah RIVSS dengan Teknik <i>Random Grids</i> untuk perangkat lunak yang akan dibuat	23
3.19 Diagram Kelas Awal Perangkat Lunak RIVSS dengan Teknik <i>Random Grids</i>	24
4.1 Rancangan antarmuka proses memasukan gambar rahasia, memilih skema vss, menentukan nilai k dan n	28
4.2 Rancangan antarmuka proses penampilan <i>shadow</i> hasil VSS dan juga menampilkan penumpukan <i>shadow</i> , serta menampilkan nilai dari <i>euclidean distance</i>	29
4.3 Diagram Kelas Lengkap	31
4.4 Kelas VSS	32
4.5 Kelas Tradisional VSS <i>Random Grids</i>	36
4.6 Kelas <i>Random Incrementing VSS Random Grids</i>	39
4.7 Kelas VSS Naor Shamir $(2, n)$	41
4.8 Kelas VSS Naor Shamir $(3, n)$	42
4.9 Kelas Pixel	43
4.10 Kelas <i>Pixel Comparator</i>	44
4.11 Kelas <i>Sobel Edge Detection</i>	44
4.12 Kelas GUI	45

4.13	Kelas GUI 2	46
4.14	Kelas GUI3	46
4.15	Kelas GUI4	46
4.16	Kelas GUI5	47
5.1	Tampilan Antarmuka Proses Memasukan Gambar Rahasia	51
5.2	Tampilan Antarmuka Proses Menampilkan <i>Shadow</i> serta Melakukan Penumpukan <i>Shadow</i>	52
5.3	Gambar rahasia yang digunakan	52
5.4	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	53
5.5	Tampilan Hasil Pendeteksian Jumlah Segmen Awal dan Segmen Akhir beserta nilai Region	53
5.6	Tampilan Hasil Pemberian Garis Tepi yang disimpan di dalam Perangkat Keras	53
5.7	Tampilan Antarmuka ketika, (a) <i>Shadow 1</i> dipilih untuk ditampilkan, (b) <i>Shadow 2</i> dipilih untuk ditampilkan, (c) <i>Shadow 3</i> dipilih untuk ditampilkan.	54
5.8	Tampilan Antarmuka ketika, (a) Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan, (b) Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan, (c) Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	54
5.9	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1,2, dan 3</i> dipilih untuk ditampilkan	55
5.10	Gambar rahasia yang digunakan	55
5.11	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	56
5.12	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	56
5.13	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	56
5.14	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	57
5.15	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	57
5.16	Tampilan Hasil Pendeteksian Garis Tepi	57
5.17	Tampilan Hasil Pemberian Garis Tepi yang disimpan di dalam Perangkat Keras	58
5.18	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	58
5.19	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	58
5.20	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	59
5.21	Gambar rahasia yang digunakan	59
5.22	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	60
5.23	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	60
5.24	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	60
5.25	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	61
5.26	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	61
5.27	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan	61
5.28	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	61
5.29	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	62
5.30	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	62
5.31	Tampilan Hasil Pemberian Garis Tepi yang disimpan di dalam Perangkat Keras	62
5.32	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	63
5.33	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	63
5.34	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	63
5.35	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	64
5.36	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan	64

5.37	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	64
5.38	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	65
5.39	Gambar rahasia yang digunakan	65
5.40	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	66
5.41	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	66
5.42	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	66
5.43	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	67
5.44	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	67
5.45	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan	67
5.46	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	68
5.47	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	68
5.48	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	68
5.49	Tampilan Hasil Pemberian Garis Tepi yang disimpan di dalam Perangkat Keras . .	69
5.50	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	69
5.51	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	69
5.52	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	70
5.53	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	70
5.54	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan	70
5.55	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	70
5.56	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	71
5.57	Gambar rahasia yang digunakan	71
5.58	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	72
5.59	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	72
5.60	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	72
5.61	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	73
5.62	Tampilan Antarmuka ketika <i>Shadow 4</i> dipilih untuk ditampilkan	73
5.63	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	74
5.64	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	74
5.65	Tampilan Antarmuka ketika Penumpukan <i>Shadow 3 dan 4</i> dipilih untuk ditampilkan	74
5.66	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	75
5.67	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3 dan 4</i> dipilih untuk ditampilkan	75
5.68	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3 dan 4</i> dipilih untuk ditampilkan	76
5.69	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	76
5.70	Tampilan Hasil Pemberian Garis Tepi, segmen awal, region, dan segmen akhir . . .	77
5.71	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	77
5.72	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	77
5.73	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	78
5.74	Tampilan Antarmuka ketika <i>Shadow 4</i> dipilih untuk ditampilkan	78
5.75	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	78
5.76	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	79
5.77	Tampilan Antarmuka ketika Penumpukan <i>Shadow 3 dan 4</i> dipilih untuk ditampilkan	79

5.78	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	79
5.79	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3 dan 4</i> dipilih untuk ditampilkan	80
5.80	Gambar rahasia yang digunakan	80
5.81	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	81
5.82	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	81
5.83	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	81
5.84	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	82
5.85	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	82
5.86	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan	82
5.87	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	83
5.88	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	83
5.89	Tampilan Antarmuka proses Memasukan Gambar Rahasia, Pemilihan Skema VSS, dan Penentuan Nilai k dan n	84
5.90	Tampilan Hasil Pemberian Garis Tepi, segmen awal, region, dan segmen akhir	84
5.91	Tampilan Antarmuka ketika <i>Shadow 1</i> dipilih untuk ditampilkan	84
5.92	Tampilan Antarmuka ketika <i>Shadow 2</i> dipilih untuk ditampilkan	85
5.93	Tampilan Antarmuka ketika <i>Shadow 3</i> dipilih untuk ditampilkan	85
5.94	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2</i> dipilih untuk ditampilkan	85
5.95	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 3</i> dipilih untuk ditampilkan	86
5.96	Tampilan Antarmuka ketika Penumpukan <i>Shadow 2 dan 3</i> dipilih untuk ditampilkan	86
5.97	Tampilan Antarmuka ketika Penumpukan <i>Shadow 1 dan 2 dan 3</i> dipilih untuk ditampilkan	86

DAFTAR TABEL

2.1	Tabel Operasi XOR	10
2.2	Tabel Operasi OR	10

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan zaman dan teknologi menyebabkan kebutuhan akan kerahasiaan informasi semakin meningkat. Informasi yang dirahasiakan ini dapat berupa teks, suara, maupun gambar. Metode yang paling sering digunakan selama ini dalam merahasiakan informasi adalah metode enkripsi. Akan tetapi, metode enkripsi memiliki kelemahan yang cukup fatal, yaitu jika kunci enkripsi hilang atau dapat dibongkar maka kerahasiaan informasi di dalamnya tidak terjamin akan aman atau bahkan dapat hilang. Sehingga, dibutuhkan metode lain dalam menjaga kerahasiaan informasi agar dapat terjaga dengan baik.

Secret sharing adalah metode untuk merahasiakan sebuah pesan rahasia dengan membagi pesan rahasia tersebut pada suatu grup partisipan di mana masing-masing partisipan mendapatkan satu bagian (*share*) [1]. Dengan kata lain, Skema *Secret Sharing* ini dapat diartikan terdiri dari satu pengirim dan banyak/beberapa penerima. Skema (k, n) -*Secret Sharing* berarti pesan rahasia akan dibagi ke n penerima dan dibutuhkan minimal k (*threshold*) *share* sehingga dapat direkonstruksi ke pesan rahasia awal. Jika seseorang tersebut hanya memiliki $k - 1$ *share* maka ia tidak akan mendapatkan informasi apa-apa mengenai pesan rahasia.

Visual secret sharing (VSS) adalah pengembangan dari *Secret Sharing* yang digunakan untuk merahasiakan pesan rahasia berupa gambar [2]. Tipe-tipe gambar sendiri ada yang berupa gambar berwarna, gambar *grayscale*, dan gambar biner (hitam-putih). Skema (k, n) -*Visual Secret Sharing* berarti gambar rahasia akan dibagi menjadi n gambar berbeda yang disebut dengan *shadow* dan untuk merekonstruksi ke gambar asli dibutuhkan penumpukan minimal k *shadow*.

VSS yang kemudian dikenal sebagai kriptografi visual ini dikembangkan konsepnya oleh Moni Naor dan Adi Shamir dan diperkenalkan pertama kali pada *Eurocrypt'94* di Perugia, Italia. VSS-Naor Shamir sendiri adalah skema VSS yang paling populer. Skema ini akan membentuk matriks dasar dan kemudian memilih satu dari himpunan permutasi kolom matriks dasar tersebut untuk tiap piksel dari gambar tersebut. Kelebihan dari skema VSS ini adalah kemudahan dalam proses implementasi tetapi skema ini memiliki kelemahan yaitu besarnya ekspansi piksel yang bergantung pada banyaknya *shadow* yang dihasilkan. Ekspansi piksel sendiri adalah besarnya piksel tambahan yang digunakan dalam proses merahasiakan gambar rahasia.

Sebelumnya, pada tahun 1987, Oded Kafri dan Eliezer Keren mengusulkan skema VSS yang lain yaitu VSS yang menggunakan teknik *random grids* [3]. Skema ini memiliki kelebihan yaitu tidak memiliki ekspansi piksel dan tidak memerlukan *codebook requirement*. Mereka membuat tiga algoritma untuk membagi sebuah gambar biner rahasia menjadi dua *shadow* yang memiliki ukuran yang sama. Pada tahun 2009, Ran-Zan Wang memperkenalkan konsep *Random Incrementing in Visual Cryptography / (2, n)-RIVC* yang mampu memperluas pengaplikasian skema VSS ini [4]. Skema ini akan membagi gambar rahasia menjadi beberapa tingkatan *region* kerahasiaan dimana untuk setiap $t \geq 2$ *shadow* dapat digunakan untuk merekonstruksi *region* sampai dengan tingkatan ke $t - 1$. Skema ini digunakan untuk menyimpan lebih dari satu rahasia dalam sebuah gambar yang bisa dibagi ke beberapa tingkatan *region* kerahasiaan tersebut.

Skripsi ini membahas mengenai Skema (k, n) -*Random Incrementing Visual Secret Sharing*

(RIVSS) berbasis Teknik *Random Grids* [5]. RIVSS berbasis Teknik *Random Grids* ini merupakan pengembangan konsep dari VSS tanpa ekspansi piksel yang diciptakan oleh Kafri dan Keren. Skema (k, n) -*Random Incrementing Visual Secret Sharing* (RIVSS) berbasis Teknik *Random Grids* ini berarti sebuah gambar rahasia akan dibagi ke beberapa tingkat kerahasiaan dan dibagi menjadi n *shadow* berupa *random grids* di mana $t(k \leq t \leq n)$ *share* dapat digunakan untuk merekonstruksi bagian rahasia sampai dengan tingkat $t - k + 1$. Namun, tidak ada informasi mengenai gambar asli yang didapatkan oleh $k - 1$ atau lebih sedikit *share*. *Random Grids* sendiri adalah sebuah transparansi yang terdiri dari piksel bertipe array dua dimensi yang transparan atau buram yang ditentukan dengan cara yang benar-benar acak (*random*). RIVSS ini juga tidak memiliki ekspansi piksel seperti VSS Kafri dan Keren.

Skripsi ini membandingkan skema VSS Naor Shamir dengan VSS dengan Teknik *Random Grids*. Skema VSS Naor Shamir yang digunakan adalah $(2, n)$ -VSS Naor Shamir dan $(3, n)$ -VSS Naor Shamir. Sedangkan untuk skema VSS dengan Teknik *Random Grids* yang digunakan adalah skema $(2, 2)$ -Tradisional VSS dengan teknik *random grids* dan (k, n) -RIVSS dengan Teknik *Random Grids*. Skripsi ini juga memperlihatkan skema yang mana yang lebih baik diantara kedua skema ini.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas pada skripsi ini antara lain adalah:

1. Bagaimana skema RIVSS dengan teknik *random grids* bekerja?
2. Bagaimana mengimplementasikan skema RIVSS dengan teknik *random grids* pada perangkat lunak?

1.3 Tujuan

Tujuan yang ingin dicapai pada skripsi ini berdasarkan rumusan masalah yang sudah ditentukan adalah:

1. Mempelajari cara kerja skema RIVSS dengan teknik *random grids*.
2. Membangun perangkat lunak yang dapat mengimplementasikan metode RIVSS dengan *random grids*.

1.4 Batasan Masalah

Batasan-batasan masalah untuk penelitian ini adalah sebagai berikut:

1. Tipe gambar yang dimasukan hanya gambar biner. Selain gambar biner tidak ditangani dalam perangkat lunak.
2. Maksimal ukuran masukan gambar sebesar 400×600 . Batasan masalah ini dikarenakan karena VSS Naor Shamir memiliki nilai ekspansi yang besar dan menyesuaikan dengan layar perangkat lunak agar gambar hasil dapat terlihat dengan jelas.
3. Kombinasi nilai k dan n yang ditangani adalah $(2,2)$, $(2,3)$, $(2,4)$, $(2,5)$, $(3,3)$, $(3,4)$, $(3,5)$, $(4,4)$, $(4,5)$. Batasan masalah ini dikarenakan pembentukan matriks dasar VSS Naor Shamir yang kompleks dan besarnya ukuran *shadow* yang dihasilkan sehingga skema yang diimplementasikan hanya $(2, n)$ -VSS Naor Shamir dan $(3, n)$ -VSS Naor Shamir.

1.5 Metodologi

Metodologi yang digunakan dalam penyusunan penelitian ini adalah:

1. Melakukan studi literatur mengenai *secret sharing*, skema VSS, *random grids*, VSS Naor Shamir, RIVSS dengan teknik *random grids*, dan metode pemisahan *background* dan *foreground*.
2. Melakukan studi literatur mengenai *library* yang disediakan oleh *Open CV*.
3. Mengimplementasikan skema $(2, n)$ -VSS Naor Shamir, $(3, n)$ -VSS Naor Shamir, $(2, 2)$ -Tradisional VSS *Random Grids*, (k, n) -RIVSS dengan teknik *Random Grids* secara manual.
4. Melakukan analisis kebutuhan perangkat lunak termasuk diagram kelas dan diagram aktivitas.
5. Melakukan perancangan perangkat lunak.
6. Mengimplementasikan skema skema $(2, n)$ -VSS Naor Shamir, $(3, n)$ -VSS Naor Shamir, $(2, 2)$ -Tradisional VSS *Random Grids*, (k, n) -RIVSS dengan teknik *random grids* pada perangkat lunak dengan bahasa pemrograman *Java*.
7. Melakukan pengujian fungsional dan eksperimental terhadap perangkat lunak.
8. Melakukan penarikan kesimpulan berdasarkan hasil pengujian.

1.6 Sistematika Pembahasan

Skripsi ini tersusun dalam enam bab secara sistematis. Enam bab tersebut terdiri dari pendahuluan, dasar teori, analisis, perancangan, implementasi dan pengujian, dan kesimpulan. Berikut merupakan sistematika pembahasan dalam skripsi ini.

1. Bab 1 Pendahuluan
Bab ini berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan.
2. Bab 2 Dasar Teori
Bab ini berisi dasar teori tentang *secret sharing*, skema VSS, VSS Naor Shamir, RIVSS dengan teknik *random grids*, dan *library* yang disediakan oleh *Open CV*.
3. Bab 3 Analisis
Bab ini berisi analisis masalah dan solusi, studi kasus, diagram aktivitas, dan rancangan diagram kelas
4. Bab 4 Perancangan
Bab ini berisi perancangan perangkat lunak yang akan dibangun yang meliputi kebutuhan masukan dan keluaran perangkat lunak, perancangan antarmuka, dan diagram kelas lengkap.
5. Bab 5 Implementasi dan Penelitian
Bab ini berisi implementasi antarmuka perangkat lunak, pengujian fungsionalitas perangkat lunak, pengujian eksperimental perangkat lunak, dan kesimpulan dari pengujian.
6. Bab 6 Kesimpulan dan Saran
Bab ini berisi kesimpulan dari awal hingga akhir penelitian serta saran untuk pengembangan selanjutnya.