

SKRIPSI

**IMPLEMENTASI SKEMA NVSS DENGAN MENGGUNAKAN
QR CODE SEBAGAI MEDIA TRANSMISI**



NI MADE RACHAEL APRILIA AWUY

NPM: 2013730037

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2017**

UNDERGRADUATE THESIS

**IMPLEMENTATION OF NVSS SCHEME WITH QR CODE AS
TRANSMISSION MEDIA**



NI MADE RACHAEL APRILIA AWUY

NPM: 2013730037

**DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND
SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2017**

LEMBAR PENGESAHAN

**IMPLEMENTASI SKEMA NVSS DENGAN MENGGUNAKAN
QR CODE SEBAGAI MEDIA TRANSMISI**

NI MADE RACHAEL APRILIA AWUY

NPM: 2013730037

Bandung, 22 Mei 2017

Menyetujui,

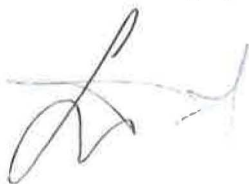
Pembimbing



Mariskha Tri Adithia, P.D.Eng



Ketua Tim Penguji



Husnul Hakim, M.T.

Anggota Tim Penguji



Vania Natali, 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:

IMPLEMENTASI SKEMA NVSS DENGAN MENGGUNAKAN QR CODE SEBAGAI MEDIA TRANSMISI

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 22 Mei 2017



Ni Made Rachael Aprilia Awuy
NPM: 2013730037

ABSTRAK

Skema *Visual Secret Sharing* (VSS) digunakan untuk menjaga kerahasiaan suatu gambar. Skema ini membagi suatu gambar rahasia menjadi beberapa bagian, yang disebut dengan *share*, dan untuk dapat merekonstruksi gambar rahasia kembali dibutuhkan penumpukan sejumlah *share*. *Share* yang dihasilkan merupakan gambar dengan piksel hitam putih acak yang tidak memiliki makna sehingga saat ditransmisikan dapat menimbulkan kecurigaan penyerang (*transmission risk*).

Skema *Natural-image-based Visual Secret Sharing* (NVSS) merupakan pengembangan dari skema konvensional VSS. Perbedaan skema NVSS dengan skema konvensional VSS terletak pada penggunaan gambar yang digunakan sebagai *share*. Skema (n, n) -NVSS menggunakan $n - 1$ gambar yang memiliki makna, disebut dengan *natural share*, dan satu gambar tidak bermakna, yang merupakan hasil proses enkripsi, sebagai *share* skema NVSS. Penggunaan gambar bermakna sebagai *share* bertujuan untuk mengurangi *transmission risk* yang muncul dalam proses transmisi.

Perangkat lunak dibangun untuk mengimplementasikan skema (n, n) -NVSS dengan menggunakan *QR Code* sebagai media transmisi. Jenis gambar yang akan digunakan merupakan gambar berwarna dengan panjang dan lebar yang sama. Pengujian eksperimental dilakukan untuk mencari ukuran maksimal gambar yang dapat disimpan di dalam *QR Code* dan menghitung kualitas *share* tidak bermakna yang dihasilkan menggunakan nilai *peak signal to noise ratio*.

Berdasarkan hasil pengujian, dapat disimpulkan bahwa implementasi skema (n, n) -NVSS dapat menghasilkan *share* tidak bermakna dengan kualitas yang baik serta terdapat ukuran maksimal gambar yang digunakan jika menggunakan *QR Code* sebagai media transmisi.

Kata-kata kunci: *Visual secret sharing, natural-imaged-based visual secret sharing, transmission risk, QR code, peak signal to noise ratio*

ABSTRACT

Visual Secret Sharing (VSS) scheme is used to protect the secrecy of an image. This scheme divides a secret image into some parts, which is called share, and to reconstruct the secret image, the stacking of a number of share(s) is needed. Share that is produced is an image with random black and white pixel which bears no meaning that could cause attacker's suspicion, which is called transmission risk.

Natural-image-based Visual Secret Sharing (NVSS) scheme is an improvement from the conventional VSS scheme. The difference between NVSS scheme and the conventional VSS scheme lies in the images that are used. (n, n) -NVSS scheme uses $n - 1$ meaningful image(s), which is called natural share(s), and one meaningless image, which is generated from encryption process, as NVSS scheme's shares. The purpose of using meaningful image(s) as shares is to decrease transmission risk in the transmission process.

A software is developed to implement (n, n) -NVSS scheme with the use of *QR Code* as transmission media. The formats of the pictures that are used are colorful images with the same width and height. Experimental test is conducted to find the maximum size of an image that can be hidden in QR Code and to calculate the resulting meaningless share's quality with the use of peak signal to noise ratio.

Based on the test results, it can be concluded that implementation of (n, n) -NVSS scheme can generate a meaningless share with good quality and that there is a size limit for the used image if QR Code is used as the transmission media.

Keywords: Visual secret sharing, natural-imaged-based visual secret sharing, transmission risk, QR code, peak signal to noise ratio

Dipersembahkan untuk Tuhan Yang Maha Esa, kedua orang tua dan kakak, Ibu Mariskha selaku dosen pembimbing, dan semua orang yang telah membantu pembuatan skripsi ini

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis berhasil menyelesaikan penyusunan skripsi yang berjudul "Implementasi Skema NVSS dengan Menggunakan *QR Code* sebagai Media Transmisi". Penulis menyadari bahwa penyelesaian penyusunan skripsi ini tidak terlepas dari bantuan berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terima kasih kepada:

1. Bu Mariskha atas bimbingannya selama satu tahun ini beserta dukungan dan motivasinya sehingga penulis bisa menyelesaikan penyusunan skripsi.
2. Kedua orang tua dan kakak penulis yang selalu memberikan motivasi dan kepercayaan kepada penulis.
3. Pak Husnul dan Ci Vania sebagai dosen penguji yang telah menguji dan memberikan masukan dalam penyusunan skripsi.
4. Rekan seperjuangan, Ijal, Dony Kurkur, Distra, dan Rashta, yang bersama-sama berjuang untuk menyelesaikan skripsi masing-masing.
5. Mesha, Gavriela, Caca, Vica, dan Glorya yang telah menemani dan memberikan dukungan sejak masuk perkuliahan sampai penyusunan skripsi selesai.
6. Keluarga UKM Aikido UNPAR yang selalu memberi hiburan kepada penulis.
7. Seluruh rekan dan sensei dari Aki No Sora, terutama rekan sekelas, Ii Sensei dan Aki Sensei atas dukungannya.
8. Rekan-rekan dari Jurusan Teknik Informatika UNPAR, terutama senior yang telah lulus terlebih dahulu dan membantu penulis dalam penyusunan skripsi.
9. Semua pihak yang tidak mungkin disebutkan satu-persatu yang sudah memberikan bantuan dan dukungan dalam pengerjaan penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna dan memohon maaf apabila terdapat kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini bermanfaat bagi pembaca yang sedang meneliti atau mempelajari topik yang berkaitan dengan skripsi ini.

Bandung, Mei 2017

Penulis

DAFTAR ISI

KATA PENGANTAR	xv
DAFTAR ISI	xvii
DAFTAR GAMBAR	xix
DAFTAR TABEL	xxi
1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan	3
1.4 Batasan Masalah	3
1.5 Metodologi	3
1.6 Sistematika Pembahasan	4
2 LANDASAN TEORI	5
2.1 Kriptografi	5
2.2 <i>Visual Secret Sharing</i>	6
2.3 <i>Natural Image Based Visual Secret Sharing Scheme</i>	7
2.4 Steganografi	11
2.5 <i>QR Code</i>	12
2.6 <i>ZXing Library</i>	14
2.7 <i>Peak Signal to Noise Ratio</i>	15
3 ANALISIS	17
3.1 Analisis Masalah	17
3.2 Studi Kasus Skema NVSS	18
3.3 Analisis Perangkat Lunak	23
3.3.1 Diagram Aliran Proses	23
3.3.2 Diagram Kelas	25
4 PERANCANGAN	29
4.1 Kebutuhan Masukan dan Keluaran	29
4.2 Perancangan Antarmuka	30
4.3 Diagram Kelas Lengkap	32
4.3.1 Diagram Kelas <i>Package Model</i>	33
4.3.2 Diagram Kelas <i>Package View</i>	40
4.3.3 Diagram Kelas <i>Package Controller</i>	41
5 IMPLEMENTASI DAN PENGUJIAN	45
5.1 Implementasi Antarmuka	45
5.2 Pengujian Fungsional	48
5.2.1 Rancangan Pengujian Fungsional	48

5.2.2	Hasil Pengujian Fungsional	49
5.2.3	Kesimpulan Pengujian Fungsional	50
5.3	Pengujian Eksperimental	50
5.3.1	Pengujian Eksperimental pada Nilai Blok Piksel	50
5.3.2	Pengujian Eksperimental pada Nilai Probabilitas Kemunculan <i>Noise</i>	51
5.3.3	Pengujian Eksperimental pada Ukuran Gambar	52
5.3.4	Pengujian Eksperimental pada Jenis Gambar	56
5.4	Kesimpulan Pengujian	57
6	KESIMPULAN DAN SARAN	59
6.1	Kesimpulan	59
6.2	Saran	60
	DAFTAR REFERENSI	61
A	HASIL PENGUJIAN EKSPERIMENTAL	63
A.1	Hasil Pengujian Eksperimental pada Nilai Blok Piksel	63
A.2	Hasil Pengujian Eksperimental pada Nilai Probabilitas Kemunculan <i>Noise</i>	63
A.3	Hasil Pengujian Eksperimental pada Jenis Gambar	64

DAFTAR GAMBAR

1.1	Skema (2, 2)-VSS [1]	2
2.1	Penumpukan dua <i>share</i> yang akan menampilkan gambar rahasia: (a) gambar rahasia, (b) <i>share</i> pertama, (c) <i>share</i> kedua, (d) hasil penumpukan kedua <i>share</i> ¹	7
2.2	Skema NVSS, (a) Proses enkripsi, (b) Proses dekripsi [2]	8
2.3	Proses persiapan gambar	9
2.4	Contoh gambar asli (a) dan gambar yang telah melalui proses persiapan gambar (b)	9
2.5	Hasil proses fitur ekstraksi. Gambar (a) menunjukkan hasil penjumlahan ketiga komponen warna. Gambar (b) menunjukkan hasil dari proses binerisasi dan stabilisasi. Gambar (c) menunjukkan hasil dari proses <i>chaos</i>	11
2.6	Proses steganografi	12
2.7	<i>Ean code</i> , salah satu tipe <i>barcode</i> satu dimensi ²	13
2.8	Perbandingan versi <i>QR Code</i>	13
3.1	Blok pertama pada <i>S1</i>	19
3.2	Hasil proses binerisasi pada blok pertama <i>S1</i>	19
3.3	Hasil proses <i>chaos</i> pada blok piksel pertama pada <i>S1</i>	20
3.4	Aliran proses enkripsi dalam implementasi skema (n, n) -NVSS	23
3.5	Aliran proses dekripsi dalam implementasi skema (n, n) -NVSS	25
3.6	Diagram kelas bagian <i>model</i>	26
4.1	Rancangan halaman Home	30
4.2	Rancangan halaman Encryption	31
4.3	Rancangan halaman Decryption	32
4.4	Diagram kelas memiliki tiga <i>package</i> , yaitu Model, View, dan Controller	33
4.5	Diagram kelas <i>package</i> Model	40
4.6	Diagram kelas <i>package</i> View	41
4.7	Diagram kelas <i>package</i> Controller	43
5.1	Antarmuka halaman Home	45
5.2	Antarmuka halaman Encryption	46
5.3	<i>Pop up QR Code</i> berhasil dibuat	46
5.4	Antarmuka halaman Decryption	47
5.5	<i>Pop up</i> pada akhir proses dekripsi	47
5.6	Gambar rahasia	48
5.7	<i>Natural share</i> pertama	48
5.8	<i>Natural share</i> kedua	49
5.9	<i>Share</i> tidak bermakna	49
5.10	<i>QR Code</i> hasil proses enkripsi perangkat lunak	49
5.11	Data yang tersimpan di dalam <i>QR Code</i>	50
5.12	Gambar hasil rekonstruksi	50
5.13	Gambar rahasia pengujian eksperimental pada nilai blok piksel	51
5.14	<i>Natural share</i> pertama pengujian eksperimental pada nilai blok piksel	51

5.15	<i>Natural share</i> kedua pengujian eksperimental pada nilai blok piksel	51
5.16	Gambar rahasia pengujian eksperimental pada nilai probabilitas kemunculan <i>noise</i> .	51
5.17	<i>Natural share</i> pengujian eksperimental pada nilai probabilitas kemunculan <i>noise</i> . .	52
5.18	<i>Natural share</i> pengujian eksperimental pada nilai probabilitas kemunculan <i>noise</i> . .	52
5.19	Gambar rahasia berukuran 6×6 piksel	52
5.20	<i>Natural share</i> dengan ukuran 6×6 piksel	52
5.21	<i>Natural share</i> dengan ukuran 6×6 piksel	53
5.22	Gambar rahasia dengan ukuran 10×10 piksel	53
5.23	<i>Natural share</i> dengan ukuran 10×10 piksel	53
5.24	<i>Natural share</i> dengan ukuran 10×10 piksel	53
5.25	Gambar rahasia berukuran 20×20 piksel	53
5.26	<i>Natural share</i> berukuran 20×20 piksel	53
5.27	<i>Natural share</i> berukuran 20×20 piksel	53
5.28	Gambar rahasia berukuran 24×24 piksel	53
5.29	<i>Natural share</i> berukuran 24×24 piksel	53
5.30	<i>Natural share</i> berukuran 24×24 piksel	54
5.31	Gambar rahasia berukuran 30×30 piksel	54
5.32	<i>Natural share</i> berukuran 30×30 piksel	54
5.33	<i>Natural share</i> berukuran 30×30 piksel	54
5.34	<i>QR Code</i> dengan gambar masukan berukuran 6×6 piksel	54
5.35	<i>QR Code</i> dengan gambar masukan berukuran 10×10 piksel	54
5.36	<i>QR Code</i> dengan gambar masukan berukuran 20×20 piksel	55
5.37	<i>QR Code</i> dengan gambar masukan berukuran 24×24 piksel	55
5.38	<i>QR Code</i> dengan gambar masukan berukuran 30×30 piksel	55
5.39	Gambar rahasia pengujian ke-4	56
5.40	<i>Natural share</i> pengujian ke-4	56
5.41	<i>Natural share</i> pengujian ke-4	56
5.42	<i>Natural share</i> pengujian ke-4	56
5.43	<i>Natural share</i> pengujian ke-4	56
5.44	<i>Natural share</i> pengujian ke-4	56
5.45	<i>Natural share</i> pengujian ke-4	57
A.1	<i>Share</i> dengan blok piksel 2	63
A.2	<i>Share</i> dengan blok piksel 4	63
A.3	<i>Share</i> dengan blok piksel 10	63
A.4	<i>Share</i> dengan probabilitas kemunculan <i>noise</i> 0.1	63
A.5	<i>Share</i> dengan probabilitas kemunculan <i>noise</i> 0.3	63
A.6	<i>Share</i> dengan probabilitas kemunculan <i>noise</i> 0.5	63
A.7	<i>Share</i> dengan probabilitas kemunculan <i>noise</i> 0.7	64
A.8	<i>Share</i> dengan probabilitas kemunculan <i>noise</i> 0.9	64
A.9	Hasil <i>share</i> menggunakan <i>natural share</i> dengan warna dominan gelap	64
A.10	Hasil <i>share</i> menggunakan <i>natural share</i> dengan warna dominan terang	64
A.11	Hasil <i>share</i> menggunakan <i>natural share</i> dengan warna dominan selain gelap dan terang	64

DAFTAR TABEL

2.1	Tabel Operasi <i>XOR</i>	8
2.2	Tabel persentase tingkat koreksi error	13
2.3	Tabel kapasitas penyimpanan <i>QR Code</i>	14
5.1	Tabel perhitungan <i>PSNR</i> untuk pengujian eksperimental pada nilai blok piksel . . .	51
5.2	Tabel perhitungan <i>PSNR</i> untuk pengujian eksperimental pada nilai blok probabilitas kemunculan <i>noise</i>	52
5.3	Tabel perhitungan <i>PSNR</i> untuk pengujian eksperimental dengan warna dominan yang berbeda	57

BAB 1

PENDAHULUAN

1.1 Latar Belakang

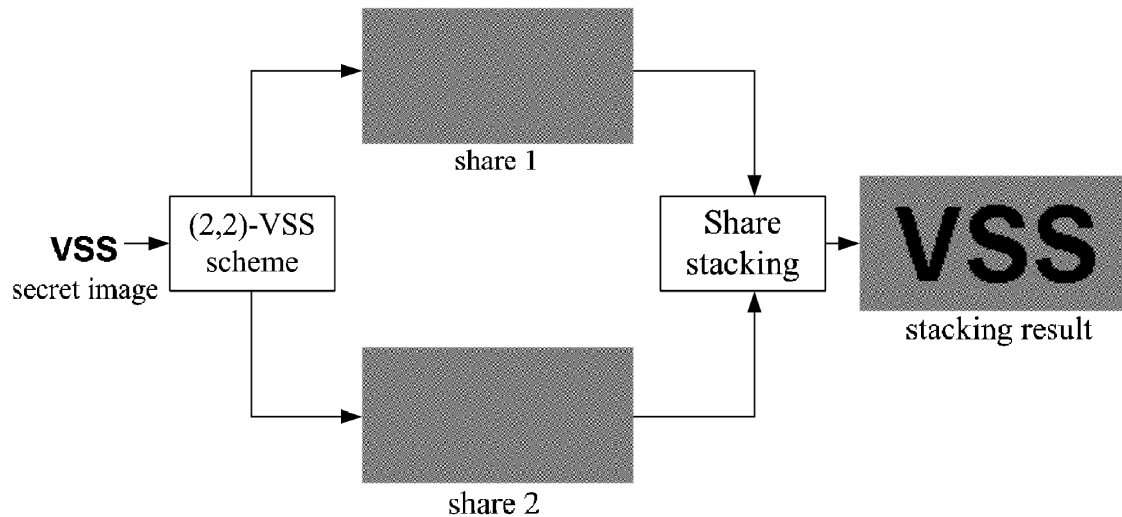
Manusia hidup pada masa di mana teknologi merupakan bagian yang penting dalam hidupnya. Sebagian besar kegiatan manusia melibatkan penggunaan teknologi di dalamnya, seperti penyimpanan informasi. Informasi yang dahulu memiliki bentuk fisik sekarang sudah memiliki bentuk digital di mana bentuk informasi digital dapat berupa teks, gambar, audio, atau video. Melalui teknologi, manusia dapat saling bertukar informasi digital dengan cepat dan mudah.

Banyak informasi yang bersifat publik, tetapi terdapat juga informasi bersifat rahasia yang hanya ditujukan untuk beberapa orang tertentu. Informasi bersifat publik dapat dengan mudah dikirimkan ke pihak lain karena tidak ada data rahasia yang harus disembunyikan sehingga jika informasi tersebut dilihat oleh banyak pihak tidak menjadi suatu masalah. Pengiriman informasi yang bersifat rahasia menjadi lebih sulit karena informasi tersebut tidak boleh dilihat oleh pihak lain selain dari pihak yang dituju. Informasi-informasi rahasia membutuhkan suatu metode pengamanan agar dapat dikirimkan ke pihak yang dituju dan pihak selain itu tidak dapat mengetahui informasi rahasia tersebut.

Salah satu cara menjaga kerahasiaan informasi adalah dengan mengenkripsi informasi. Proses enkripsi adalah proses mengubah informasi rahasia, yang disebut dengan *plaintext*, menjadi informasi yang tidak memiliki makna, yang disebut dengan *ciphertext*, dengan menggunakan kunci algoritma. *Ciphertext* tersebut kemudian dapat diubah kembali menjadi *plaintext* menggunakan kunci melalui proses dekripsi. Namun, pembuatan dan penyebaran kunci beserta proses enkripsi dan dekripsi dapat memakan waktu yang panjang. Apabila kunci hilang maka dekripsi tidak dapat dilakukan dan informasi rahasia tidak bisa diperoleh.

Metode lain yang dapat digunakan untuk informasi berupa gambar adalah *Visual Secret Sharing* (VSS). VSS merupakan salah satu metode *secret sharing* yang berfokus kepada informasi rahasia berupa gambar. Secara garis besar, *secret sharing* membagi suatu informasi rahasia menjadi beberapa bagian, yang disebut dengan *share*, dan untuk dapat merekonstruksi informasi rahasia kembali, dibutuhkan penumpukan sejumlah *share*. Skema (k, n) -VSS menunjukkan bahwa skema tersebut menghasilkan n buah *share* yang akan dibagikan ke n orang partisipan dan membutuhkan penumpukan k buah *share* untuk dapat merekonstruksi gambar rahasia. Masing-masing *share* tidak memiliki makna dan tidak akan memberikan petunjuk mengenai gambar rahasia kecuali sejumlah k *share* yang dibutuhkan ditumpuk [3]. Sifat tersebut membuat pihak yang memiliki *share* yang kurang dari k tidak dapat merekonstruksi gambar rahasia. Gambar 1.1 merupakan contoh skema $(2, 2)$ -VSS.

VSS menghasilkan *share* yang merupakan gambar dengan piksel acak seperti *noise* yang tidak memiliki arti sehingga saat ditransmisikan dapat menimbulkan kecurigaan penyerang. Risiko timbulnya kecurigaan penyerang disebut dengan *transmission risk*. *Transmission risk* dapat menyebabkan dicegatnya *share* saat ditransmisikan yang kemudian dapat mengekspos pihak-pihak yang terlibat. Selain itu, *share* yang dihasilkan bersifat tidak *user-friendly* karena tidak dapat dikenali oleh mata manusia. Salah satu pihak yang menerima gambar tidak dapat mengenali *share* miliknya ataupun membedakannya dengan *share* lain. Semakin banyak *share* yang digunakan,



Gambar 1.1: Skema (2, 2)-VSS [1]

maka semakin sulit juga pengelolaan *share* karena sifat *share* yang tidak *user-friendly*.

Extended Visual Cryptography Scheme, disingkat EVCS kemudian diajukan untuk mengatasi masalah pengelolaan *share*. Salah satu Skema EVCS, yang diajukan oleh G. Ateniese *et. al*, dapat menghasilkan *share* yang bersifat *user-friendly* [4]. *Share* bersifat *user-friendly* dapat dikenali oleh mata manusia, tetapi *share* yang dihasilkan tetap memiliki piksel-piksel seperti *noise* atau gambar dengan kualitas yang rendah. *Share* dengan piksel seperti *noise* atau gambar dengan kualitas rendah dapat dengan mudah dikenali oleh mata manusia sehingga pihak-pihak yang mentransmisikan *share* akan tetap dicurigai oleh penyerang.

Teknik steganografi juga dapat digunakan untuk menyembunyikan *share* yang bersifat tidak *user-friendly* [5]. *Share* tersebut disembunyikan di dalam suatu gambar yang disebut dengan *cover image* yang bersifat *user-friendly*. *Cover image* yang telah disisipi oleh *share* disebut dengan *stego-image*. *Stego-image* yang bersifat *user-friendly* dapat membantu masalah pengelolaan *share*, tetapi *stego-image* tetap dapat dideteksi dengan metode steganalisis¹ sehingga *transmission risk* masih ada.

Kai-Hui Lee dan Pei-Ling Chiu kemudian mengajukan skema *natural-imaged based VSS*, disingkat NVSS, untuk mengurangi *transmission risk* yang muncul dalam transmisi *share* [2]. Skema konvensional VSS menggunakan gambar yang tidak memiliki makna sebagai *share*, sedangkan skema ini menggunakan gambar bermakna sebagai *share*-nya, yang kemudian disebut dengan *natural share*. Skema ini tidak mengubah gambar bermakna yang digunakan sebagai *natural share* untuk mendapatkan gambar rahasianya, melainkan melakukan proses ekstraksi fitur untuk setiap *natural share*-nya. Gambar bermakna tersebut kemudian dikirim ke partisipan. Gambar bermakna yang tidak diubah bersifat tidak mencurigakan sehingga saat ditransmisikan, akan menurunkan tingkat *transmission risk* secara signifikan. Skema ini dapat mentransmisikan satu gambar rahasia melalui $n - 1$ *natural share* dan satu *share* seperti *noise* tidak bermakna yang dihasilkan oleh proses enkripsi dalam skema ini. *Share* tidak bermakna yang dihasilkan disembunyikan ke dalam suatu media untuk meningkatkan keamanan saat proses transmisi *share* dilakukan.

Dalam penelitian ini, akan dianalisis kinerja skema (n, n) -NVSS dengan cara membangun perangkat lunak yang dapat mengimplementasikan skema (n, n) -NVSS yang diajukan oleh Kai-Hui Lee dan Pei-Ling untuk gambar berwarna. Media yang digunakan untuk menyembunyikan *share* tidak bermakna hasil proses enkripsi dalam penelitian ini adalah *QR Code*.

¹Steganalisis merupakan seni dan ilmu untuk mendeteksi pesan rahasia yang disembunyikan menggunakan steganografi [6].

1.2 Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah penelitian ini adalah sebagai berikut:

1. Bagaimana cara kerja skema (n, n) -NVSS?
2. Bagaimana cara menyembunyikan *share* tidak bermakna ke dalam *QR Code*?
3. Bagaimana cara mengimplementasikan skema (n, n) -NVSS dan menyembunyikan *share* tidak bermakna ke dalam *QR Code*?

1.3 Tujuan

Berdasarkan identifikasi masalah, tujuan penelitian adalah sebagai berikut:

1. Mempelajari cara kerja skema (n, n) -NVSS.
2. Mempelajari cara untuk menyembunyikan *share* tidak bermakna ke dalam *QR Code*.
3. Mengimplementasikan skema (n, n) -NVSS dan penyembunyian *share* tidak bermakna ke dalam *QR Code*.

1.4 Batasan Masalah

Batasan-batasan masalah untuk penelitian ini adalah sebagai berikut:

1. Seluruh gambar masukan memiliki ukuran yang sama.
2. Seluruh gambar masukan memiliki ukuran panjang dan lebar yang sama. Ukuran panjang dan lebar yang sama bertujuan untuk mempermudah penentuan nilai yang digunakan sebagai ukuran blok piksel.

1.5 Metodologi

Metodologi yang digunakan dalam penyusunan penelitian ini adalah:

1. Melakukan studi literatur tentang skema (n, n) -NVSS, seperti cara kerja skema.
2. Melakukan studi literatur tentang *QR Code*.
3. Melakukan studi kasus skema (n, n) -NVSS.
4. Melakukan perancangan kelas untuk mengimplementasikan skema (n, n) -NVSS dan penyembunyian *share* tidak bermakna ke dalam *QR Code*.
5. Mengimplementasikan hasil perancangan kelas menggunakan bahasa pemrograman Java.
6. Melakukan pengujian terhadap perangkat lunak yang telah diimplementasikan.
7. Menganalisis hasil pengujian terhadap perangkat lunak.
8. Membuat kesimpulan berdasarkan hasil analisis.

1.6 Sistematika Pembahasan

Pembahasan dalam penelitian ini akan dilakukan dengan sistematis sebagai berikut:

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 kriptografi, VSS, NVSS, steganografi, *QR Code*, *Library ZXing*, dan *Peak Noise to Signal Ratio*.
3. Bab 3 Analisis
Bab ini berisi analisis masalah, studi kasus, diagram aliran proses, 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.