SKRIPSI

VISUAL SECRET SHARING DENGAN *AUTOSTEREOGRAM*

Glenn Reysan

NPM: 2015730025

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

UNDERGRADUATE THESIS

VISUAL SECRET SHARING WITH AUTOSTEREOGRAM

Glenn Reysan

NPM: 2015730025

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

LEMBAR PENGESAHAN

VISUAL SECRET SHARING DENGAN *AUTOSTEREOGRAM*

Glenn Reysan

NPM: 2015730025

Bandung, 22 April 2019

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji	Anggota Tim Penguji
Pascal Alfadian, M.Comp.	Husnul Hakim, 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:

VISUAL SECRET SHARING* DENGAN *AUTOSTEREOGRAM

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 April 2019

Meterai
Rp. 6000

Glenn Reysan
NPM: 2015730025

ABSTRAK

Skema *visual secret sharing* merupakan sebuah metode *secret sharing* yang mengubah sebuah gambar rahasia menjadi beberapa gambar yang hanya terlihat sebagai kumpulan piksel acak yang disebut *share* yang tidak memiliki arti sama sekali. Untuk mendapatkan informasi mengenai gambar rahasia maka harus dilakukan penumpukan dari sejumlah *share*. Proses penumpukan ini tidak membutuhkan perhitungan komputasi namun hanya menggunakan sistem pengelihatan manusia. *Share* yang dihasilkan dapat menimbulkan kecurigaan pihak-pihak tidak berwenang karena hanya berisi kumpulan piksel acak, maka dari itu pada penulisan skripsi ini akan dipelajari sebuah metode yang dapat menghasilkan *share* yang bukan hanya berisi kumpulan piksel acak namun juga mengandung informasi tiga dimensi. *Autostereogram* merupakan gambar dua dimensi yang dapat dilihat sebagai gambar tiga dimensi dengan arah pandangan mata konvergen atau divergen.

Visual secret sharing dan *autostereogram* menggunakan sistem pengelihatan manusia untuk mendapatkan suatu informasi. Dalam penulisan skripsi ini akan dilakukan penelitian dengan menggabungkan algoritma untuk membangun *visual secret sharing* dan *autostereogram* dengan cara mengambil nilai warna pada suatu piksel yang terdapat pada *autostereogram* dan menyisipkan nilai warna tersebut pada saat membangun *share*.

Pada penelitian skripsi ini akan digabungkan algoritma untuk membangun *visual secret sharing* dan *autostereogram* agar dapat menghasilkan *share* yang dapat melindungi informasi rahasia dan juga mengandung informasi tiga dimensi sehingga tidak menimbulkan kecurigaan bagi pihak tidak berwenang.

Share yang dihasilkan dapat melindungi informasi rahasia serta mengandung informasi tiga dimensi. Namun *share* yang dihasilkan memiliki perbedaan antara skema *visual secret sharing* untuk gambar biner, *grayscale*, berwarna, dan CMYK. Berdasarkan hasil survey dan pengujian, skema *visual secret sharing* untuk gambar *grayscale* dapat menghasilkan penumpukan *share* yang lebih baik jika dibandingkan dengan skema lainnya, sedangkan skema *visual secret sharing* CMYK menghasilkan penumpukan *share* yang kurang baik.

Kata-kata kunci: *Visual Secret Sharing, Share, Autostereogram*

ABSTRACT

Visual secret sharing scheme is a secret sharing method which transform a secret image into several image that only can be seen as a set of random pixels, do not have a piece of information from the original secret image, and do not have any meaning which we call it as a share. To retrieve the piece of information from the original secret image several share must be overlaid. The overlaying process does not need any computational calculation yet only use human visual system. Share which produced could raises suspicion for unauthorized party when found that a person or party keep an image which contain random pixels. Therefore this thesis will discuss about a method which could produce a share that could protect secret information and contain a three dimensional information at the same time. An autostereogram is a two dimensional image which can be seen as three dimensional image, depending on proper eye convergence or divergence.

Visual secret sharing and autostereogram, both rely on human visual system to get some information. This undergraduate thesis will discuss a method to combine algorithm to create visual secret sharing and autostereogram. This method take a color value from a particular pixel in autostereogram and put the color value in the process of creating share.

In this thesis writer will combine two algorithm to create visual secret sharing and autostereogram so the method could produce a share that could protect secret information as well as containing three dimensional information at the same time so that would not raise suspicion from unauthorized party.

This combined method to create visual secret sharing with autostereogram could produce shares that will could be seen not only a set of random pixel but also contain a three dimensional image as well as hiding information from the secret image. Shares which was created are different between visual secret sharing scheme for binary, grayscale, colored, and CMYK image. Based on testing and survey visual secret sharing scheme for grayscale image could produce a better reconstructed image while visual secret sharing scheme for CMYK image produce the least good reconstructed image.

Keywords: Visual Secrret Sharing, Share, Autostereogram

kepada kalian yang ingin tahu lebih mengenai topik ini.

KATA PENGANTAR

Puji syukur kepada Tuhan atas seluruh berkat yang telah diberikan kepada penulis selama penulisan skripsi sehingga skripsi dengan judul *Visual Secret Sharing* dengan *Autostereogram* dapat diselesaikan tepat pada waktunya. Penulis juga mengucapkan terima kasih kepada pihak-pihak yang telah membantu penulis dalam proses penulisan dan penyelesaian skripsi, yaitu:

- Keluarga yang selalu memberi dukungan kepada penulis.
- Ibu Mariskha Tri Adithia selaku dosen pembimbing yang telah membimbing penulis selama penulisan skrips ini dari awal hingga akhir.
- Alvin Kurniawan, Jeremias Jason Joeng, Nicholas Steven, Reinardi Wilyanto, dan William Renaldo yang telah membuat penulis kerepotan dengan Ceritera Coffee Brunch and Culture yang dibuka bersamaan dengan pengambilan Skripsi 1.
- Teman-teman Teknik Informatika Unpar terutama Adrian Stefanus, Kevin Pratama, Matthew Alvredo, Stephen Senjaya, Vincent Joel Sinatra, dan Yosua yang telah membantu dan memberikan saran kepada penulis dalam penulisan dokumen skripsi maupun dalam penulisan perangkat lunak.

Bandung, April 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Informasi yang bersifat rahasia memerlukan suatu sistem yang dapat menjaga kerahasiaan, sehingga tidak dapat dibaca atau diubah oleh pihak yang tidak berwenang, baik pada saat proses pengiriman data maupun pada saat data tersebut tersimpan di dalam sebuah komputer.

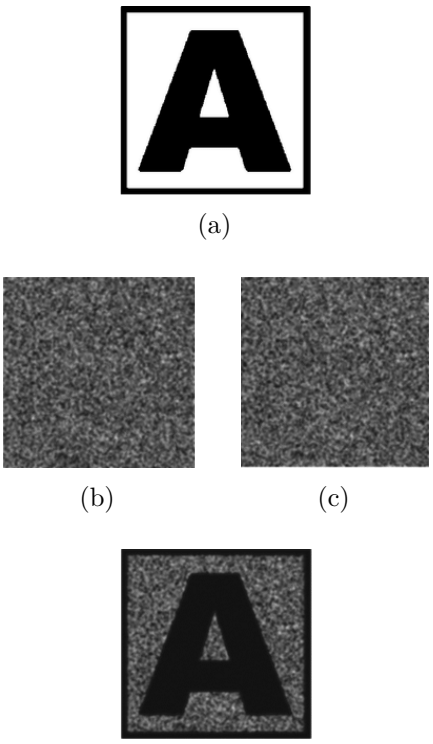
Salah satu metode yang digunakan untuk mengamankan dan menjaga kerahasiaan suatu informasi adalah enkripsi dan dekripsi. Enkripsi merupakan suatu metode yang dilakukan untuk menyembunyikan data yang terdapat di dalam informasi sehingga informasi tersebut akan sulit dan memakan waktu lama bagi orang yang tidak berwenang untuk mendapatkan informasi tersebut. [1] Gambar **??** merupakan contoh gambar dari enkripsi. Sedangkan dekripsi adalah proses yang dilakukan untuk mengubah informasi acak yang dihasilkan dalam proses enkripsi menjadi bentuk awal sebelum informasi tersebut melalui proses enkripsi. Dalam perkembangannya, proses enkripsi dan dekripsi memerlukan kunci rahasia yang tepat, namun jika kunci rahasia itu hilang atau diketahui oleh orang yang tidak berwenang, maka keamanan dan kerahasiaan informasi tersebut juga akan hilang atau diketahui oleh orang yang tidak berwenang.

Metode enkripsi dan dekripsi yang relatif aman membutuhkan teknik komputasi yang rumit, maka dari itu komputer sangat dibutuhkan dalam proses enkripsi dan dekripsi. Metode enkripsi dan dekripsi dapat diterapkan pada informasi yang berbentuk teks maupun gambar atau citra. Selain itu, jika kunci rahasia hilang atau diketahui oleh pihak yang tidak berwenang maka kerahasiaan informasi tersebut akan hilang. Pada penulisan skripsi ini akan dibahas metode-metode yang dapat mengatasi kelemahan metode enkripsi tersebut, yaitu dengan menggunakan metode yang disebut *secret sharing*.

Secret sharing adalah sebuah metode yang digunakan untuk menjaga kerahasiaan informasi dengan membanginya menjadi beberapa bagian. [2] Skema *secret sharing* (k, n), merupakan suatu skema di mana informasi rahasia akan dibagi menjadi n buah bagian yang disebut sebagai *share*, dan untuk mendapatkan kembali informasi rahasia maka diperlukan setidaknya k buah *share*.

Visual secret sharing (VSS) adalah sebuah skema *secret sharing* pada citra atau gambar rahasia yang membagi informasi rahasia menjadi n buah bagian berbeda yang dikenal sebagai *share* atau *shadow*. *Share* tersebut hanya berisi piksel acak sehingga tidak akan menampilkan informasi apapun mengenai citra rahasia. Konstruksi *share* dilakukan dengan cara memanipulasi piksel pada citra rahasia menjadi n buah *share*. Pada proses rekonstruksi, jika k buah *share* ditumpukkan, maka akan membentuk citra rahasia tersebut. Pada skema *Visual Secret Sharing* (k,n), citra rahasia dibagi menjadi n buah *share*. Setiap *share* akan dibagikan kepada partipisan yang berwenang. Penumpukkan minimal sebanyak k buah *share* dibutuhkan untuk melakukan rekonstruksi citra rahasia.

Share yang dihasilkan oleh *visual secret sharing*, tidak mengandung informasi rahasia karena *share* tersebut hanyalah sekumpulan piksel acak hasil enkode sebuah citra rahasia. Namun hal ini menimbulkan kecurigaan pada saat diketahui bahwa seseorang menyimpan citra yang hanya berisi kumpulan piksel acak. Untuk mencegah hal tersebut, Feng Yi, Daoshun Wang, dan Yiqi Dai pada [3] memperkenalkan sebuah skema yang bernama *Visual Secret Sharing with Autostereogram*,



(a) (b) (c)

Gambar 1.1: (a) Gambar awal atau gambar rahasia, (b) *share* 1, (c) contoh *share* 2, (c) Hasil rekonstruksi *share*

yang merupakan pengembangan dari skema *visual secret sharing* tradisional.

Autostereogram adalah suatu gambar dua dimensi (2D) yang dapat dilihat sebagai suatu gambar tiga dimensi (3D) pada saat diamati dengan pandangan mata konvergen atau divergen. *Visual Secret Sharing with Autostereogram* merupakan sebuah skema yang enkode pada citra rahasia menjadi n buah *share*, namun *share* yang dihasilkan bukanlah kumpulan piksel acak tapi merupakan *autostereogram*. Proses rekonstruksi *share* yang berbentuk *autostereogram* dilakukan dengan cara menumpukkan k buah *share*.

Dalam skripsi ini penulis akan mempelajari *visual secret sharing with autostereogram*, serta membangun perangkat lunak yang dapat menggabungkan skema *visual secret sharing* dengan *autostereogram*. Perangkat lunak yang dibangun makan menerima gambar rahasia dalam bentuk gambar *depth map* dan gambar rahasia dengan ukuran yang sama sebagai masukan. Proses rekonstruksi gambar rahasia dengan menumpukkan sejumlah *share* akan dilakukan dengan menggunakan komputer. Pengujian yang akan dilakukan terhadap perangkat lunak yang akan dibangun dilakukan dengan menggunakan pengujian fungsional, eksperimental, dan kualitatif. Pada pengujian eksperimental akan dilakukan percobaan terhadap seluruh skema dengan gambar masukan yang berbeda-beda serta jumlah ekspansi piksel yang berbeda-beda. Pengujian kualitatif akan menggunakan survei untuk mengetahui apakah *visual secret sharing* yang dikembangkan menghasilkan *share* yang dapat menyembunyikan informasi rahasia namun dapat menunjukan informasi mengenai gambar tiga dimensi, dan gambar hasil penumpukan *share* yang cukup jelas.

1.2 Rumusan Masalah

Rumusan masalah yang akan dibahas dalam penulisan skripsi ini adalah sebagai berikut:

1. Bagaimana cara membangun *autostereogram*?
2. Bagaimana menerapkan *autostereogram* pada *visual secret sharing scheme*?

3. Bagaimana menerapkan *visual secret sharing scheme* dengan *autostereogram* pada perangkat lunak?

1.3 Tujuan

Tujuan dari penulisan skripsi ini adalah sebagai berikut:

1. Mempelajari algoritma untuk membangun *autostereogram*.
2. Mempelajari *visual secret sharing scheme* dengan *autostereogram*.
3. Membangun perangkat lunak yang dapat menggabungkan *visual secret sharing scheme* dengan *autostereogram*.

1.4 Batasan Masalah

Batasan-batasan masalah yang digunakan dalam penelitian ini adalah:

- Masukan gambar untuk membangun *autostereogram* harus berupa gambar *depthmap*.
- Masukan gambar *depthmap* harus memiliki ukuran yang sama dengan gambar rahasia.
- Proses rekonstruksi gambar rahasia disimulasikan dengan menggunakan komputer. Penumpukan *share* dengan komputer dilakukan dengan tujuan untuk mendapatkan hasil yang optimal, karena proses penumpukan *share* dengan menggunakan kertas transparansi memiliki kekurangan pada kemampuan mesin percetakan yang digunakan dan proses penumpukan yang dilakukan. Dengan menggunakan komputer setiap piksel dapat dengan tepat ditumpukan dengan piksel yang terdapat pada gambar lainnya.

1.5 Metodologi

Metodologi yang dilakukan dalam penulisan skripsi ini adalah:

- Melakukan studi literatur mengenai landasan teori *autostereogram*, *Visual Secret Sharing* (VSS), VSS Naor dan Shamir pada gambar biner, VSS Probabilistik, VSS probabilistik untuk gambar *grayscale*, dan VSS probabilistik untuk gambar berwarna.
- Melakukan studi literatur mengenai *Visual Secret Sharing* dengan *autostereogram*.
- Mengembangkan *Visual Secret Sharing* dengan *autostereogram* sehingga tidak terjadi perubahan *aspect ratio*.
- Membuat perancangan diagram kelas dan perancangan antar muka.
- Membangun perangkat lunak sesuai dengan perancangan yang telah dibuat.
- Melakukan pengujian terhadap perangkat lunak yang telah dibangun.
- Menarik kesimpulan berdasarkan penelitian yang telah dilakukan.

1.6 Sistematika Pembahasan

Sistematika pembahasan dalam penelitian skripsi ini adalah sebagai berikut:

- Bab 1 Pendahuluan
  Bab ini berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan yang digunakan dalam penelitian skripsi ini.
- Bab 2 Landasan Teori
  Bab ini berisi teori-teori dasar mengenai kriptografi, *secret sharing*, *autostereogram*, dan VSS.
- Bab 3 Analisis
  Bab ini berisi analisis masalah dan solusi, studi kasus, pengembangan skema VSS, dan perancangan perangkat lunak.
- Bab 4 Perancangan
  Bab ini berisi perancangan antarmuka dan diagram kelas lengkap.
- Bab 5 Implementasi dan Pengujian
  Bab ini berisi implementasi antarmuka perangkat lunak, implementasi skema VSS, dan rancangan beserta hasil pengujian terhadap skema *visual secret sharing* dengan *autostereogram*.
- Bab 6 Kesimpulan dan Saran
  Bab ini berisi kesimpulan dari awal hingga akhir penelitian serta saran yang dapat digunakan untuk penelitian selanjutnya.