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

METERAI TEMPEL
6000
ENAM RIBU RUPIAH

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 nấŠ$k + 1$ 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 corelation with the form of shadow with the purpose to build a better scheme of VSS with Random Grids Technique and width 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

DAFTAR GAMBAR

DAFTAR TABEL

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.