SKRIPSI

IMPLEMENTASI KRIPTOGRAFI VISUAL UNTUK MENJAGA PRIVASI WAJAH

Distra Vantari

NPM: 2012730060

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

UNDERGRADUATE THESIS

VISUAL CRYPTOGRAPHY FOR FACE PRIVACY IMPLEMENTATION

Distra Vantari

NPM: 2012730060

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

LEMBAR PENGESAHAN

IMPLEMENTASI KRIPTOGRAFI VISUAL UNTUK MENJAGA PRIVASI WAJAH

Distra Vantari

NPM: 2012730060

Bandung, 12 Desember 2017

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Rosa De Lima, M.Kom.

Anggota Tim Penguji

Pascal Alfadian, M.Comp.

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 KRIPTOGRAFI VISUAL UNTUK MENJAGA PRIVASI WAJAH

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 12 Desember 2017

Distra Vantari
NPM: 2012730060

ABSTRAK

Visual Cryptography adalah suatu metode yang digunakan untuk menjaga kerahasiaan dari suatu informasi berupa gambar. Skema yang paling banyak digunakan pada *Visual Cryptography* adalah *Visual Cryptography Scheme* (VCS). Pada VCS (k, n) gambar rahasia akan dibagi menjadi gambar lain yang disebut shadow sebanyak n. Masing-masing partisipan akan memiliki satu buah *shadow* yang berbeda-beda. Gambar rahasia dapat direkonstruksi dengan menumpukkan minimal k buah *shadow*.

Hasil pembentukan *shadow* yang dihasilkan VCS merupakan gambar yang berisikan sekumpulan piksel acak yang dapat menimbulkan kecurigaan bagi pihak yang tidak berwenang, maka dari itu digunakanlah *Gray-level Extended Visual Cryptography Scheme* (GEVCS) untuk mengatasi masalah tersebut. Masukkan dari skema GEVCS adalah tiga gambar natural yaitu satu gambar rahasia dan dua gambar natural lainnya. Dua gambar natural tersebut kemudian akan dibentuk menjadi *shadow*, di mana untuk merekonstruksi gambar rahasia, partisipan harus menumpukkan kedua shadow tersebut. Hasil rekonstruksi gambar rahasia menggunakan shadow disebut gambar target.

Perangkat lunak dibuat untuk mengimplementasikan privasi gambar wajah menggunakan GEVCS. Karena terdapat tingkat *error* yang tinggi ketika bentuk wajah tidak cocok, maka digunakanlah teknik sederhana untuk memilih wajah yang cocok dengan gambar rahasia.

Berdasarkan hasil pengujian, hasil shadow yang dibentuk belum terlalu optimal. Gambar target yang direkonstruksi dengan cara menumpukan kedua shadow belum mirip dengan gambar rahasia.

Kata-kata kunci: *Gray-level Extended Visual Cryptography Scheme*

ABSTRACT

Visual Cryptography is a method that is used to keep a secrecy of an information in a form of an image. The most used scheme in Visual Cryptography is Visual Cryptography Scheme (VCS). In VCS (k, n), a secret image will be divided into n number of another images which are called shadow . Every participant will have one different shadow. A secret image could be reconstructed by stacking minimum of k number of shadow.

The result of forming a shadow which is generated by VCS is an image contains a set of random pixels that can arouse suspicion for unauthorized parties, so Gray-level Extended Visual Cryptography Scheme (GEVCS) is used to resolve the issue. The input from GEVCS scheme are three natural images, which are one secret image and two other natural pictures. The two natural images will then be shaped into a shadow, in which to reconstruct the secret image, the participant must stack the two shadows. The results of the reconstruction of a secret image using a shadow is called the target image.

A software is created to implement face image privacy using GEVCS. Because of the high error rate when the face shape does not match, then a simple technique is used to choose a face that matches the secret image.

Based on the test result, the shadow results that are formed are not too optimal, the target images that are reconstructed by stacking both shadows is not yet similar to the secret image.

Keywords: Gray-level Extended Visual Cryptography Scheme

Dipersembahkan untuk Eyang, kedua orang tua saya dan Ibu Mariskha Tri Adithia selaku dosen pembimbing

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Kuasa atas segala rahmat yang telah diberikanNya, sehingga penulis dapat menyelesaikan skripsi yang berjudul Implementasi Kriptografi Visual untuk Menjaga Privasi Wajah.

Tujuan dari penyusunan skripsi ini guna memenuhi salah satu syarat untuk bisa menempuh sarjana pendidikan pada fakulas Teknologi Informasi dan Sains (FTIS) Program Studi Informatika di Universitas Parahyangan (UNPAR).

Pengerjaan skripsi ini telah melibatkan banyak pihak yang sangat membantu dalam banyak hal. Oleh sebab itu, di sini penulis sampaikan rasa terima kasih sebanyak-banyaknya kepada:

1. Ibu Mariskha Tri Adithia, S.Si, M.Sc, PDEng, Selaku Ketua Program Studi Informatika Universitas Parahyangan (FTIS UNPAR) serta Dosen pembimbing yang telah memberikan izin penelitian dan membimbing dalam penyusunan penelitian ini dari awal hingga selesai. 2. Ivan Lukman dan Avita Nadhilah Puteri, Selaku rekan yang banyak membantu memahami penelitian ini serta membantu pengecekan EYD penulisan dokumen penelitian ini. 3. Orang tua tercinta yang telah banyak memberikan doa dan dukungan kepada penulis secara moril maupun materil hingga skripsi ini dapat selesai. 4. Sahabat dan rekan seperjuangan tercinta yang tiada henti memberi dukungan dan motivasi kepada penulis. 5. Semua pihak yang telah banyak membantu dalam penyusunan skripsi ini yang tidak bisa penulis sebutkan semuanya.

Bandung, Desember 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Kerahasiaan informasi sudah menjadi salah satu kebutuhan yang diutamakan di bidang ilmu Teknik Informatika. Banyak informasi yang bersifat rahasia seperti kata sandi, foto dan pesan, sampai saat ini hanya disimpan dalam bentuk *plaintext* atau sebuah teks biasa, sehingga banyak orang yang menyalahgunakan informasi tersebut. Informasi yang bersifat rahasia masih sulit untuk dilindungi dari pihak-pihak yang tidak berwenang.

Metode yang paling banyak digunakan untuk melindungi informasi yang dirahasiakan tersebut adalah dengan melakukan enkripsi dan dekripsi. Enkripsi adalah proses penerapan algoritma pada sebuah informasi, proses yang dilakukan adalah mengacak data di dalam informasi tersebut sehingga akan sulit dan memakan waktu lama bagi orang yang tak berwenang untuk mendapatkan infomasi tersebut. Dekripsi adalah hal sebaliknya, yaitu proses transformasi data dalam infomasi yang sudah diacak melalui proses enkripsi, kembali ke bentuk awal sebelum proses enkripsi dilakukan. Dalam pengembangannya, proses enkripsi dan dekripsi memerlukan kunci rahasia. Artinya, tanpa kunci rahasia yang tepat, proses enkripsi dan dekripsi tidak dapat dilakukan.

Proses enkripsi dan dekripsi yang relatif aman, melibatkan teknik komputasi yang teralu rumit untuk dilakukan oleh manusia. Oleh karena itu, komputer sangat dibutuhkan dalam proses enkripsi dan dekripsi. Selain itu, apabila kunci rahasia hilang atau diketahui oleh orang lain yang tidak berwenang, maka kerahasiaan informasi tersebut akan hilang.

Skripsi ini akan banyak membahas metode yang dapat mengatasi kelemahan metode enkripsi dimana informasi yang digunakan berupa gambar, salah satu metode terbaik untuk melindungi informasi pada gambar adalah dengan menggunakan *Visual Cryptography Scheme*(VCS) Naor dan Shamir, sebuah skema yang dapat melakukan enkode kepada gambar rahasia menjadi n buah bagian berbeda yang dikenal sebagai *shadow*. *Shadow* yang dihasilkan tersebut tidak akan menampilkan informasi apapun mengenai gambar rahasia, cara melakukan konstruksi *shadow* adalah dengan memanipulasi piksel pada gambar rahasia menjadi n buah *shadow* sehingga jika k buah *shadow* ditumpukkan, maka akan akan membentuk gambar rahasia. *shadow* yang direkonstruksi dari manipulasi piksel tersebut sama sekali tidak menampilkan informasi apapun mengenai gambar rahasia, komputasi yang dilakukan juga cenderung lebih mudah dibandingkan melakukan enkripsi dan dekripsi, hal ini membuat metode VCS merupakan metode terbaik untuk melindungi informasi rahasia dalam gambar. Pada VCS (k, n), gambar awal akan dibagi ke dalam n buah *shadow*, lalu setiap *shadow* akan dibagikan kepada partisipan, yaitu entitas yang berwenang. Penumpukkan minimal sebanyak k buah *shadow* dibutuhkan untuk proses dekripsi atau rekonstruksi gambar rahasia.

Walaupun *shadow* pada VCS tidak memperlihatkan informasi rahasia sama sekali. *Shadow* yang direkonstruksi pada skema VCS hanyalah sekumpulan *pixel* acak yang dihasilkan dari proses enkode sebuah gambar rahasia, hal ini dapat menimbulkan kecurigaan oleh interseptor dengan mempercayai bahwa adanya informasi rahasia dibalik *shadow* tersebut. Untuk mencegah hal ini Nakajima dan Yamaguchi mengenalkan sebuah skema yang merupakan sebuah pengembangan dari VCS. skema itu adalah *Gray-Level Extended Visual Cryptography Scheme* (GEVCS), GEVCS merupakan skema

yang menggunakan dua gambar natural atau gambar yang sudah ada dan sebuah gambar yang akan dirahasiakan sebagai masukan yang kemudian akan diolah untuk menghasilkan dua buah *shadow* yang sesuai dengan dua gambar natural tersebut. Hasil penumpukan kedua *shadow* tersebut akan menampilkan gambar ketiga yang dinamakan *target*.

Gambar yang digunakan pada skripsi untuk gambar natural ataupun gambar yang akan dirahasiakan merupakan gambar wajah sehingga, untuk mengurangi tingkat kegagalan saat membentuk *shadow* akan dilakukan proses pemilihan wajah yang dianggap paling cocok dengan gambar rahasia. Gambar yang terpilih akan menjadi gambar natural yang kemudian akan dibentuk menjadi *shadow*. Selain terdapat pemilihan wajah yang paling cocok dengan gambar rahasia, pada skripsi ini masukan gambar akan selalu berukuran $300x300$ piksel dengan format *jpg*.

Dalam skripsi ini, penulis akan mempelajari GEVCS Nakajima dan Yamaguchi terhadap gambar rahasia yang berupa gambar wajah. Gambar wajah yang akan menjadi masukan pada skema ini adalah dua gambar wajah yang terdapat pada sebuah basis data dan sebuah gambar wajah yang akan dirahasiakan dengan masing-masing derajat keabuan sebanyak 4 dan ekspansi piksel sebanyak 9 yang berarti warna pada piksel ketiga gambar masukkan hanya memiliki 4 warna abu yang berbeda, dan setiap piksel pada gambar akan dipecah menjadi $3x3$ subpiksel. Basis data yang digunakan adalah basis data yang terdiri dari beberapa gambar wajah. Hasil akhir dari skripsi ini adalah sebuah perangkat lunak yang mampu memilih gambar wajah dari basis data, dan mampu memroses gambar-gambar masukan dari pengguna berdasarkan GEVCS Nakajima dan Yamaguchi untuk memberikan sebuah keluaran berupa dua buah *shadow*. Pengguna dapat mendapatkan sebuah *target* dengan menumpukan kedua *shadow*.

1.2 Rumusan Masalah

Rumusan masalah penelitian adalah sebagai berikut:

- Bagaimanakah menerapkan GEVCS pada gambar *grayscale*?
- Bagaimanakah menerapkan GEVCS pada perangkat lunak penjaga privasi wajah?
- Bagaimanakah perangkat lunak penjaga privasi wajah dapat memilih wajah paling cocok dari basis data?

1.3 Tujuan

Berdasarkan identifikasi masalah, tujuan penelitian sebagai berikut:

- Mempelajari GEVCS pada gambar *grayscale*.
- Membuat perangkat lunak penjaga privasi wajah yang menerapkan GEVCS berdasarkan gambar wajah yang dimasukan pengguna.
- Mempelajari teknik untuk memilih wajah pada basis data.

1.4 Batasan Masalah

Batasan-batasan masalah untuk penelitian ini adalah sebagai berikut:

- Nilai ekspansi piksel yang digunakan pada penelitian ini adalah 9. Nilai ekspansi piksel adalah nilai yang digunakan untuk mencegah terjadinya perubahan aspek rasio.
- Nilai derajat keabuan yang digunakan pada penelitian ini adalah 4. Nilai ini cocok dengan nilai ekspansi piksel 9, dimana akan menghasilkan 3 perbedaan subpiksel pada setiap piksel dengan keabuan yang berbeda.

- Ukuran panjang dan lebar setiap gambar harus sama, baik itu gambar yang akan dimasukkan kedalam basis data atau gambar yang akan dirahasiakan. Hal ini bertujuan agar proses enkripsi atau dekripsi dapat dilakukan secara optimal.
- Masukan gambar harus berukuran sama dengan gambar yang ada pada basis data yaitu berukuran 300x300 piksel. Dimana semua gambar harus berupa *jpg*.
- Penumpukan kedua shadow yang didapat akan dilakukan pada komputer. Hal ini dilakukan untuk mendapatkan hasil yang optimal pada proses penumpukan kedua shadow tersebut. Karena proses penumpukan pada komputer dengan proses penumpukan yang dilakukan menggunakan kertas transparansi. Salah satu yang membuat perbedaannya adalah kemampuan mesin percetakannya, dan pada proses penumpukannya, celah kecil dapat ditimbulkan saat penumpukkan tersebut yang mengakibatkan tidak optimalnya proses penumpukkan kedua shadow tersebut.

1.5 Metodologi

Metodologi yang digunakan dalam penyusunan skripsi adalah:

- Melakukan studi literatur tentang dasar-dasar *Visual Cryptography Sharing* (VCS), VCS Naor dan Shamir pada gambar biner, VCS probabilistik untuk gambar *grayscale*, dan VCS probabilistik.
- Melakukan studi literatur tentang dasar-dasar *Gray-level Extended Visual Cryptography Scheme* (GEVCS).
- Melakukan studi literatur mengenai *library* milik *OpenCV*.
- Melakukan studi kasus mengenai pembentukan *shadow* menggunakan skema VCS.
- Melakukan studi kasus mengenai pembentukan *shadow* menggunakan skema GEVCS.
- Merancang langkah-langkah untuk pemilihan wajah paling cocok dengan gambar rahasia.
- Merancang langkah-langkah untuk merekonstruksi *shadow* dari gambar natural yang sudah dipilih menggunakan skema GEVCS.
- Mengimplementasikan langkah-langkah merekonstruksi *shadow* dari gambar natural menggunakan skema GEVCS.
- melakukan pengujian terhadap perangkat lunak yang telah diimplementasi.
- menarik kesimpulan berdasarkan hasil pengujian.

1.6 Sistematika Pembahasan

Pembahasan dalam penelitian ini dilakukan secara sistematis sebagai berikut:

- Bab 1 Pendahuluan
  Berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan.
- Bab 2 Dasar Teori
  Berisi teori-teori dasar tentang kriptografi, *Secret Sharing*, dan *Visual Secret Sharing*, skema VCS.

- Bab 3 Analisis
  Berisi analisis masalah dan solusi, studi kasus, pengembangan skema VCS, dan perancangan perangkat lunak.

- Bab 4 Perancangan
  Berisi perancangan antarmuka dan diagram kelas lengkap.

- Bab 5 Implementasi dan Eksperimen
  Berisi implementasi antarmuka perangkat lunak, implementasi skema VCS, dan rancangan beserta hasil eksperimen terhadap skema VCS untuk gambar grayscale.

- Bab 6 Kesimpulan dan Saran
  Berisi kesimpulan dari awal hingga akhir penelitian dan saran untuk pengembangan selanjutnya.