SKRIPSI

PERLINDUNGAN HAK MILIK GAMBAR DIJITAL DAN INTEGRITASNYA DENGAN MENGGUNAKAN *WATERMARKING*

Christofer Indra Sinarya

NPM: 2013730042

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

UNDERGRADUATE THESIS

DIGITAL IMAGE WATERMARKING FOR COPYRIGHT PROTECTION

Christofer Indra Sinarya

NPM: 2013730042

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

LEMBAR PENGESAHAN

PERLINDUNGAN HAK MILIK GAMBAR DIJITAL DAN INTEGRITASNYA DENGAN MENGGUNAKAN *WATERMARKING*

Christofer Indra Sinarya

NPM: 2013730042

Bandung, 23 07 2019

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji	Anggota Tim Penguji
Rosa De Lima, M.Kom.	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:

PERLINDUNGAN HAK MILIK GAMBAR DIJITAL DAN INTEGRITASNYA DENGAN MENGGUNAKAN *WATERMARKING*

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 23 07 2019

Meterai
Rp. 6000

Christofer Indra Sinarya
NPM: 2013730042

ABSTRAK

Tanda air atau yang lebih dikenal orang dengan *watermark*, sudah banyak digunakan untuk melindungi hak cipta pada gambar dijital. Namun penggunaan *watermark* yang banyak digunakan adalah watermark yang terlihat, dimana sebuah gambar menjadi sangat mudah diidentifikasi apakah menggunakan *watermark* atau tidak. Hal ini membuat gambar yang diberi *watermark* terjamin hak ciptanya karena sebuah *watermark* yang terlihat sangat sulit untuk dihapus atau dihilangkan. Namun masalah yang muncul adalah menjadi berkurangnya nilai estetika atau keindahan dari gambar yang diberi *watermark* tersebut.

Disinilah *watermark* yang tidak terlihat menjadi solusi untuk mengatasi masalah tersebut diatas, tanpa mengurangi keamanan gambar dari segi hak cipta. Karena pada dasarnya *watermark* yang terlihat maupun tidak memiliki fungsi yang sama yaitu untuk melindungi hak cipta. Pada perkembangan skripsi ini juga digunakan *Advanced Encryption Standard* untuk mengenkripsi *digest* hasil dari fungsi *hash* SHA-256 yang didapat dari pesan rahasia pemilik gambar. Sedangkan untuk pembuatan *watermark* yang tidak terlihat sendiri digunakan *Least Significant Bit* untuk menyisipkan *watermark* pada bit-bit pada gambar. Pada skripsi ini juga dikembangkan suatu proses yang digunakan untuk menjaga integritas dari gambar yang disisipi *watermark*, yaitu dengan menghitung *digest* dengan fungsi *hash* SHA-256 dengan gambar sebagai masukannya. *Digest* ini kemudian ikut disisipi ke dalam gambar.

Verifikasi gambar dilakukan untuk memastikan kepemilikan dari gambar tersebut, dimana verifikasi hanya dapat dilakukan oleh orang yang memberi *watermark* pada gambar. Integritas gambar juga dapat dibuktikan apakah gambar ber-*watermark* mengalami modifikasi atau tidak. Berdasarkan beberapa pengujian yang dilakukan, penggunaan *watermark* tidak terlihat ini dapat dengan baik menjaga hak cipta dari gambar yang diberi *watermark*.

Kata-kata kunci: Tanda Air, *Digest, Advanced Encryption Standard, Least Significant Bit*, Enkripsi, Dekripsi, Hak Cipta, Integritas, Verifikasi, Kerahasiaan

ABSTRACT

Watermark have been widely used to protect copyright in digital images. But mostly is visible watermark, where an image is easily identified whether using watermark or not. This makes the image that is given watermark guaranteed protected because visible watermark is difficult to delete or remove. However, the problem that arises is that there are reduction in the aesthetic value or beauty of the image itself.

It's where invisible watermark seem to be the solution to overcome the above problem, without reducing image security in terms of copyright. Because basically visible and invisible watermark have the same function, it's to protect copyright. In the development of this thesis also used the Advanced Encryption Standard to encrypt digest results from SHA-256 hash function that obtained from the image owner's secret message. As for making invisible watermark, it uses Least Significant Bit to embed the watermark on the bits of the image. In this paper a process is also used to maintain image integrity by counting digest using SHA-256 hash function with the image as its input. The digest then inserted into the image along with the watermark.

Image verification is done to ensure ownership of the image, where verification can only be done by the person who gave the watermark into the image. Image integrity can also be proven whether the image has been modified of not. Based on several tests carried out, the use of invisible watermark can properly protect the copyright of the image.

Keywords: Watermark, Digest, Advanced Encryption Standard, Least Significant Bit, Encryption, Decryption, Copyright, Verification, Confidentiality, Integrity

Dipersembahkan untuk Teknik Informatika, Fakultas Teknologi Informasi dan Sains, Universitas Katolik Parahyangan, keluarga tercinta, teman-teman, dan diri sendiri.

KATA PENGANTAR

Puji dan syukur kepada Tuhan Yang Maha Esa atas seluruh berkat yang telah diberikan kepada penulis sehingga dapat menyelesaikan skripsi dengan judul **Perlindungan Hak Cipta Dengan Menggunakan *Watermark*** ini dengan baik dan tepat waktu. Penulis juga ingin mengucapkan terima kasih kepada seluruh pihak yang telah mendukunga dan memberikan bantuan kepada penulis dalam mengerjakan skripsi ini hingga selesai. Penulis mengucapkan terima kasih kepada:

1. Kedua orang tua penulis, Bapak Ir. Paulus Suprapto Sinarya dan Ibu Ignatia Muljani yang selalu memberikan semangat dan dukungan sejak awal, dalam pengerjaan, hingga skripsi ini selesai.

2. Kedua kakak penulis, dr. Vita Victoria Sinarya dan dr. Regine Rosaline Sinarya yang juga memberi semangat serta menghibur selama mengerjakan skripsi ini.

3. Ibu Mariskha Tri Adithia, PDEng sebagai dosen pembimbing yang tidak pernah berhenti membimbing penulis hingga skripsi ini selesai.

4. Agustine Mia Permata, S.IlKom yang selalu memberi semangat sejak awal penulisan skripsi dan Priambodo Pangestu, S.Kom yang telah membantu memberi segala informasi seputar pengerjaan skripsi yang dibutuhkan oleh penulis.

5. Teman-teman Teknik Informatika UNPAR yang telah membantu dan mendukung dalam pengerjaan skripsi ini.

6. Pihak-pihak lain yang telah membantu dalam penulisan skripsi ini, yang terus memberikan doa dan semangat kepada penulis.

Akhir kata, penulis berharap semoga skripsi ini dapat memberikan manfaat kepada yang membacanya di kemudian hari serta yang akan melakukan penelitian berdasarkan skripsi ini.

Bandung, 07 2019

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 . . . 1
- 1.3 Tujuan . . . 2
- 1.4 Batasan Masalah . . . 2
- 1.5 Metodologi . . . 2
- 1.6 Sistematika Pembahasan . . . 3

2 Landasan Teori 5
- 2.1 Hash Function . . . 5
- 2.2 Advanced Encryption Standard . . . 6
  - 2.2.1 Desain . . . 6
  - 2.2.2 Ronde . . . 7
  - 2.2.3 Ekspansi Kunci . . . 10
  - 2.2.4 Enkripsi dan Dekripsi . . . 12
- 2.3 Least Significant Bit . . . 13
- 2.4 Galois Field / GF(2^8) Pada AES . . . 14

3 Analisis 17
- 3.1 Analisis Masalah . . . 17
- 3.2 Studi Kasus . . . 18
  - 3.2.1 Fungsi *Hash* SHA-256 . . . 18
  - 3.2.2 Enkripsi Dan Dekripsi AES . . . 18
  - 3.2.3 Penyisipan Dan Ekstraksi LSB . . . 20
- 3.3 Analisis Perangkat Lunak . . . 20
  - 3.3.1 Diagram Aktivitas . . . 20
  - 3.3.2 Diagram Kelas Awal . . . 23
- 3.4 Kebutuhan Masukan dan Keluaran . . . 25

4 Perancangan Perangkat Lunak 27
- 4.1 Rancangan Antarmuka . . . 27
- 4.2 Diagram Kelas Lengkap . . . 30
- 4.3 Rincian Diagram Kelas . . . 32
  - 4.3.1 Kelas MenuUtama . . . 32
  - 4.3.2 Kelas MenuBuatWatermark . . . 33

4.3.3 Kelas MenuBuatPembuktian . . . 34
4.3.4 Kelas World . . . 35
4.3.5 Kelas Converter . . . 36
4.3.6 Kelas FungsiHash . . . 37
4.3.7 Kelas LSB . . . 38
4.3.8 Kelas Penyisipan . . . 39
4.3.9 Kelas Ekstraksi . . . 40
4.3.10 Kelas AES . . . 42
4.3.11 Kelas Enkripsi . . . 46
4.3.12 Kelas Dekripsi . . . 47

5 Implementasi dan Pengujian **49**
5.1 Implementasi . . . 49
5.1.1 Lingkungan Implementasi . . . 49
5.1.2 Implementasi Antarmuka . . . 49
5.2 Pengujian Fungsional . . . 52
5.3 Pengujian Eksperimental . . . 55
5.3.1 Pengujian Eksperimental Terhadap Gambar *Watermark* . . . 56
5.3.2 Pengujian Eksperimental Terhadap Masukan untuk Verifikasi . . . 63

6 Kesimpulan dan Saran **67**
6.1 Kesimpulan . . . 67
6.2 Saran . . . 67

Daftar Referensi **69**

A Kode Program **71**

DAFTAR GAMBAR

2.1 Desain *Advanced Encryption Standard* . . . 7
2.2 Ronde *Advanced Encryption Standard* . . . 7
2.3 Ekspansi kunci . . . 11
2.4 Desain orijinal . . . 13

3.1 Contoh gambar dengan *watermark* yang terlihat . . . 17
3.2 Diagram Aktivitas untuk Proses Penyisipan . . . 21
3.3 Diagram Aktivitas untuk Proses Ekstraksi . . . 22
3.4 Diagram kelas awal . . . 24

4.1 Antarmuka menu halaman utama . . . 28
4.2 Rancangan antarmuka pembuatan *watermark* . . . 28
4.3 Rancangan antarmuka verifikasi *watermark* . . . 29
4.4 Diagram kelas . . . 30
4.5 Kelas MenuUtama . . . 32
4.6 Kelas MenuBuatWatermark . . . 33
4.7 Kelas MenuBuatPembuktian . . . 34
4.8 Kelas World . . . 35
4.9 Kelas Converter . . . 36
4.10 Kelas FungsiHash . . . 38
4.11 Kelas LSB . . . 39
4.12 Kelas Penyisipan . . . 39
4.13 Kelas Ekstraksi . . . 41
4.14 Kelas AES . . . 42
4.15 Kelas Enkripsi . . . 46
4.16 Kelas Dekripsi . . . 47

5.1 Antarmuka menu utama . . . 50
5.2 Antarmuka pembuatan *watermark* . . . 50
5.3 Antarmuka verifikasi *watermark* . . . 51
5.4 Penanganan pesan kosong . . . 51
5.5 Penanganan kunci kosong . . . 52
5.6 Penanganan kunci salah ukuran . . . 52
5.7 Penanganan gambar kosong . . . 52
5.8 Contoh hambar asli . . . 53
5.9 Seluruh masukan sudah terisi . . . 53
5.10 Notifikasi pembuatan *watermark* berhasil . . . 54
5.11 Hasil pembuatan *watermark* . . . 54
5.12 Gambar *watermark* . . . 55
5.13 Seluruh masukan sudah terisi . . . 56
5.14 Notifikasi verifikasi *watermark* berhasil . . . 56
5.15 Contoh gambar *watermark* . . . 57
5.16 Gambar dengan piksel yang sudah dimodifikasi . . . 58

5.17 Masukan untuk gambar menggunakan gambar baru 58
5.18 Hasil akhir pengujian *digest* 59
5.19 Gambar dengan piksel yang sudah dimodifikasi 60
5.20 Masukan untuk gambar menggunakan gambar baru 60
5.21 Hasil akhir pengujian *watermark* 61
5.22 Gambar dengan piksel yang sudah dimodifikasi 62
5.23 Masukan untuk gambar menggunakan gambar baru 62
5.24 Hasil akhir pengujian di luar bagian *digest* dan *watermark* 63
5.25 Gambar *watermark* 63
5.26 Masukan pesan yang salah 64
5.27 Hasil pengujian kesalahan masukan pesan 65
5.28 Masukan kunci yang salah 65
5.29 Hasil pengujian kesalahan masukan kunci 66

DAFTAR TABEL

2.1 Tabel SBOX 8
2.2 Tabel inverse SBOX 9
2.3 Tabel Word 11
2.4 Tabel Rcon 12

5.1 Tabel perubahan nilai piksel 57
5.2 Modifikasi piksel pada bagian *watermark* 59
5.3 Modifikasi piksel diluar bagian *digest* dan *watermark* 61

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Digital watermarking adalah suatu proses penyisipan data seperti tanda air, tanda tangan, label, atau tanda pada sebuah objek multimedia seperti gambar atau audio atau video yang dapat diekstrak untuk verifikasi kepemilikan ataupun keperluan otentikasi. Berdasarkan jenisnya, *digital watermarking* dapat dibagi menjadi 2, yaitu *visible watermark* dan *invisible watermark*. *visible watermark* adalah *watermark* yang dapat dilihat secara kasat mata dan umumnya digunakan untuk keperluan verifikasi hak cipta. Sedangkan *invisible watermark* adalah tanda air yang disisipkan dalam piksel-piksel gambar sehingga tidak terlihat secara kasat mata dan umumnya digunakan untuk keperluan otentikasi dan menjaga integritas gambar yang disisipi *watermark*.

Pada jurnal yang dibuat oleh Shankar Thawkar, diusulkan penggunaan *invisible watermarking* sebagai upaya untuk menjaga hak cipta dan integritas dari suatu gambar. *Watermark* disisipkan ke dalam piksel-piksel gambar dan dapat diekstraksi untuk membuktikan kepemilikan gambar. Digunakan pula komputasi fungsi *hash* untuk menghasilkan *digest* dari suatu gambar yang juga disisipkan ke dalam gambar untuk menjaga integritas gambar. Dengan disisipkannya *digest* ke dalam gambar, perubahan yang terjadi pada gambar dapat dideteksi dengan menghitung *digest* dari gambar dan dibandingkan dengan digest yang disisipkan dalam gambar. Jika gambar sudah mengalami perubahan, maka hasil perbandingan kedua digest pasti berbeda, sehingga integritas dari gambar dapat dibuktikan.

Pada skripsi ini, dibahas skema *invisible watermarking* di mana *watermark* yang berupa suatu teks/kalimat sebagai *plaintext* terlebih dahulu dienkripsi dengan *Advanced Encryption Standard* menjadi *ciphertext*, sehingga kepemilikan gambar dapat diverifikasi dengan mendekripsi *ciphertext* menggunakan metode yang sama yaitu *Advanced Encryption Standard*. Setelah dienkripsi, *ciphertext* yang kemudian disebut *watermark* disisipkan ke dalam gambar dengan metode *Least Significant Bit*(LSB) beserta dengan *digest* yang sudah dihitung sebelumnya sehingga menghasilkan *watermark image*. *Watermark image* dapat diekstraksi untuk mendapatkan kembali *digest* untuk membuktikan integritas gambar, serta *watermark* untuk verifikasi kepemilikan gambar tersebut. Pada skripsi ini juga dibangun sebuah perangkat lunak untuk mengimplementasikan bahasan skema diatas.

1.2 Rumusan Masalah

Adapun rumusan masalah ini dapat diuraikan dalam bentuk pertanyaan sebagai berikut:

1. Bagaimana cara kerja perlindungan hak milik dijital dan integritasnya dengan penandaan tanda air?
2. Bagaimana metode penyisipan data terenkripsi dengan metode LSB?
3. Bagaimana mengimplementasikan penyisipan data terenkripsi dengan metode LSB?

1.3 Tujuan

Berdasarkan rumusan masalah yang sudah diuraikan diatas, diharapkan dapat dicapai tujuan sebagai berikut:

1. Mempelajari metode perlindungan hak milik dijital dan integritasnya dengan penandaan tanda air.
2. Mempelajari langkah-langkah penyisipan data terenkripsi dengan metode LSB.
3. Membangun perangkat lunak penyisipan data terenkripsi dengan metode LSB.

1.4 Batasan Masalah

Batasan masalah yang dibuat terkait dengan pengerjaan skripsi ini adalah sebagai berikut:

- Perangkat lunak menerima masukan gambar dengan format JPEG atau PNG dengan batasan resolusi minimal 23x23 piksel sebagai media untuk penyisipan *watermark*.
- Perangkat lunak menerima kalimat/*string* yang panjangnya tidak dibatasi sebagai masukan pesan rahasia untuk dijadikan *watermark*.
- Perangkat lunak menerima kalimat/*string* dengan ukuran maksimal 16 karakter yang dapat berupa alfabet maupun numerik sebagai kunci rahasia.
- Untuk proses pembuatan *watermark*, perangkat lunak hanya menghasilkan sebuah gambar dengan format PNG, memiliki resolusi yang sama dengan gambar sebagai masukan dan sudah memiliki *watermark*.
- Untuk proses verifikasi *watermark*, perangkat lunak hanya menghasilkan dua baris kalimat hasil verifikasi.

1.5 Metodologi

Metodologi yang dilakukan dalam pengerjaan skripsi ini adalah sebagai berikut:

1. Studi literatur mengenai :
   - *Advanced Encryption System* sebagai algoritma yang digunakan untuk mengenkripsi *watermark* sebelum disisipkan dan mendekripsi *watermark* sesudah diekstraksi.
   - *Hash function SHA-256* khususnya pada *java library* sebagai algoritma yang digunakan untuk menghitung digest yang digunakan sebagai watermark dan perlindungan integritas gambar.
   - *Least Significant Bit* sebagai algoritma yang digunakan untuk penyisipan *watermark* maupun *digest*.
   - *Galois Field / GF(2^8)* sebagai teknik perhitungan yang digunakan dalam *MixColumn* pada proses enkripsi maupun dekripsi *Advanced Encryption Standard*.
   - Beberapa *java library* yang digunakan dalam membangun perangkat lunak seperti *BufferedImage*, *BufferedReader*, dll.
2. Membuat *flowchart* untuk proses pembuatan *watermark* dan proses verifikasi *watermark*.
3. Membuat diagram kelas sebagai bagian dalam perancangan perangkat lunak.

4. Membangun *engine* perangkat lunak yang berfungsi melakukan segala proses seperti enkripsi, dekripsi, penyisipan, ekstraksi, dll.
5. Membangun antarmuka perangkat lunak dan menggabungkannya dengan *engine*.
6. Melakukan eksperimen dan pengujian untuk mencari masalah yang mungkin terjadi.
7. Melakukan penanganan pada perangkat lunak untuk mengatasi masalah yang terjadi.

1.6 Sistematika Pembahasan

Setiap bab dalam skripsi ini memiliki sistematika penulisan [1] yang dijelaskan ke dalam poin-poin sebagai berikut:

1. Bab 1 : Pendahuluan
   Membahas latar belakang, rumusan masalah, tujuan, batasan masalah, metode penelitian, dan sistematika penulisan.
2. Bab 2 : Dasar Teori
   Membahas seluruh teori-teori yang diperlukan dalam penelitian ini. Berisi tentang *Advanced Encryption System*, *Hash function SHA-256*, *Least Significant Bit*, *Galois Field / GF(2^8)*, dan beberapa *java library*.
3. Bab 3 : Analisis
   Membahas mengenai analisis masalah dan solusi serta pengembangannya, penjabaran diagram aktivitas, dan penjabaran diagram kelas awal.
4. Bab 4 : Perancangan
   Membahas mengenai kebutuhan masukan dan keluaran, perancangan antarmuka, dan penjelasan diagram kelas akhir yang digunakan untuk implementasi perangkat lunak.
5. Bab 5 : Implementasi dan Pengujian
   Membahas mengenai implementasi antarmuka, pengujian fungsional dan pengujian eksperimental yang telah dilakukan.
6. Bab 6 : Kesimpulan dan Saran
   Membahas hasil kesimpulan dari keseluruhan penelitian ini dan saran-saran yang dapat diberikan untuk penelitian berikutnya.