Robust Digital Watermarking Dengan Metode LSB

Yusak Yuwono Awondatu
Program Studi Teknik Informatika
Institut Teknologi Bandung
Bandung, Indonesia
yusak.awondatu@gmail.com

***Abstract*—Keamanan informasi sangatlah penting seiring dengan berkembangnya internet yang dapat diakses siapapun. Salah satu keamanan informasi yang harus dilindungi adalah hak cipta terhadap gambar digital yang disebarkan di internet karena gambar dapat di-*download* dan di-*upload* ulang oleh siapapun sehingga kehilangan jejak atas siapa pemilik aslinya dan hal ini menjadi maslaah bagi pekerjaan banyak orang. Salah satu cara perlindungan gambar adalah dengan Robust Steganography. Teknik ini akan menempelkan identitas pembuatnya kedalam gambar dan identitas tersebut akan tetap bertahan(robust) meskipun gambar mengalami sejumlah serangan seperti *cropping*, *resize*, dan *editing*.**

Keywords—Digital Watermark, LSB

I. PENDAHULUAN

Internet sebagai media informasi kini berkembang dengan sangat cepat dan perkembangan ini membuatnya dapat diakses oleh siapapun juga. Kemudahan ini juga merupakan ancaman terhadap keamanan informasi karena banyaknya pihak yang bisa saja menginterferensi penyaluran data dan mencuri atau mengubah data tersebut.

Namun masalah keamanan informasi tidak sebatas interferensi oleh pihak ketiga saja. Kepemilikan/ hak cipta atas informasi juga merupakan masalah terhadap keamanan informasi. Setiap orang yang mengakses internet bisa saja men-*download* dan meng-*upload* ulang, atau melakukan copy dan paste terhadap data yang mereka temukan di internet kemudian mengklaim data tersebut sebagai milik mereka.

Salah satu data yang rentan terhadap klaim pihak ketiga adalah gambar digital. Ada banyak pekerjaan yang melibatkan pembuatan gambar secara digital seperti fotografer, illustrator atau desain grafis. Dan karena pekerjaan ini kini dilakukan secara online, seniman mau tidak mau menggunakan internet sebagai media penyaluran data kepada klien. Data digital ini tentunya akan rentan terhadap penggandaan. Pihak ketiga dapat men-download dan meng-upload, atau *copy paste* gambar tersebut dan mengklaimnya sehingga akan merugikan pihak pencipta aslinya.

Oleh karena itu identitas pencipta perlu diselipkan kedalam karyanya sehingga tidak bisa diklaim dengan mudah. Biasanya hal ini diwujudkan dengan gambar air(*watermark*). *Watermark* berupa nama, tanda tangan atau gambar symbol unik sebagai penanda identitas penciptanya dibubuhkan ke atas gambar yang telah dibuat.

Namun sekarang ada banyak *tools* untuk memanipulasi gambar yang membuat *watermark* dapat dihilangkan dengan mudah sehingga gambar yang ada tetap dapat dicuri dan diklaim orang. Oleh karena itu diperlukan teknik *watermark* baru, salah satu cara alternative yaitu dengan *steganography watermark*. *Watermark* yang dibuat tidak lagi dibubuhkan keatas gambar seperti cap, namun diselipkan secara digital kedalam gambar secara *steganography* sehingga gambar tampak tidak mengandung apa-apa, namun sebenarnya mengandung *watermark* yang dapat dikeluarkan kapan saja. dengan cara seperti ini, seniman dapat membubuhkan identitas yang lebih tahan manipulasi dibandingkan dengan *watermark* stempel tanpa merusak gambar yang mereka buat. Selain itu seniman dapat mengklaim kembali gambar milik mereka yang digunakan atau dimanipulasi orang lain.

Gambar yang diberikan *watermark* selain dapat diambil kembali sebagai bukti kepemilikan, diharapkan juga dapat memiliki ketahanan (*robust*) terhadap manipulasi sekalinya ada pihak luar yang bermaksud mencoba untuk mengutak-atik gambar yang diberi watermark.

Gambar 1. *Watermark* stempel berupa tanda tangan

Gambar 2. *Watermark* di hilangkan dengan tools untuk manipulasi gambar

II. DASAR TEORI

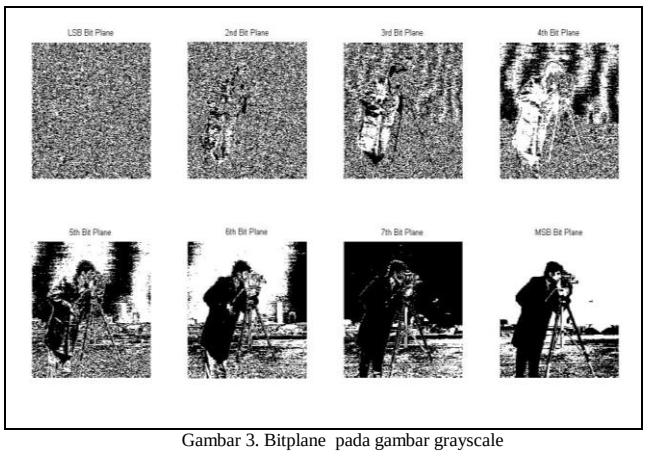
A. Steganography

Steganography adalah teknik untuk menyembunyikan dan mengambil kembali pesan rahasia diatas pesan yang tidak rahasia.

Dalam teknologi kuno, *steganography* dilakukan dengan banyak cara seperti tato yang ditutupi rambut, ukiran yang ditutupi dengan lilin, tinta tembus pandang, gulungan benang yang diikat sesuai kode morse, tulisan mikroskopis pada gambar, dan bermacam macam cara lainnya.

Dalam teknologi digital, *steganography* diterapkan dengan cara menyelipkan pesan rahasia kedalam bit pesan yang tidak rahasia(umumnya data multimedia seperti gambar, suara, atau video) dengan berbagai macam algoritma. Hasilnya, pesan tidak rahasia ketika ditampilkan tidak memiliki perubahan yang begitu nampak meskipun telah diselipi pesan rahasia.

B. Bitplane dan Least Significant Bit(LSB)

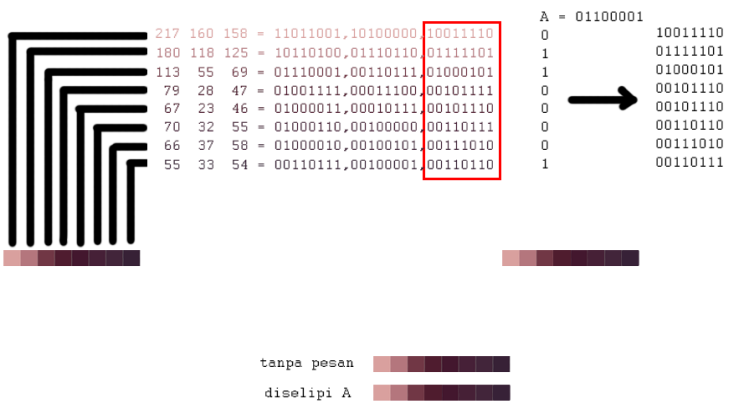


Gambar 3. Bitplane pada gambar grayscale

Salah satu metode penyelipan pesan rahasia kedalam gambar adalah dengan metode Bitplane dan LSB.

Bitplane adalah proyeksi bit ke n dari setiap pixel gambar. Seperti yang dapat dilihat pada Gambar 3, suatu gambar grayscale setiap pixelnya memiliki 8 bit dan jika setiap bit tersebut dikelompokkan kedalam satu bitplane, akan menghasilkan 8 sub gambar. Dari 8 bitplane yang dihasilkan, dapat dilihat bahwa semakin kecil bit gambar, semakin menghasilkan gambar yang tidak begitu signifikan terhadap gambar secara keseluruhan sehingga dapat dimaanfaatkan untuk menyembunyikan pesan dengan metode LSB. Untuk gambar dengan detail yang lebih tinggi seperti gambar full color yang memiliki 24 atau 32 bit per pixelnya, akan semakin banyak informasi yang bisa diselipkan kedalamnya. Metode LSB seperti namanya, yaitu menyembunyikan pesan pada least significant bit. Seperti yang terlihat pada gambar 3, bitplane bit yang semakin kecil tidak begitu memiliki perubahan signifikan terhadap gambar sehingga dapat dimaniuplasi untuk menyembunyikan informasi. Salah informasi yang dapat disembunyikan juga ada adalah gambar sehingga metode ini dapat digunakan untuk menyelipkan *watermark* pembuatnya.

Dalam metode LSB, menyelipkan pesan teks dapat dilakukan dengan memecah teks menjadi bit, lalu diselipkan kedalam bit gambar. Perubahan bit yang kecil per pixelnya tidak akan memberikan perubahan warna yang besar pada gambar secara keseluruhan sehingga tidak akan mencurigakan.



Gambar 4. Implementasi LSB steganografi untuk teks

Sebagai contoh pada gambar 4, 8 pixel gambar full color 24 bit akan diselipi informasi berupa huruf A. huruf A diproses menjadi nilai binary, yaitu 01100001, kemudian 8 bit ini disebarkan kedalam 8 pixel gambar pada salah satu bitplanenya (dalam gambar dipilih LSB bagian Blue), kemudian nilai 01100001 diselipkan kedalam bitplane tersebut. Jika biplane digabungkan kembali menjadi pixel warna, maka dapat dilihat akan menghasilkan warna yang tidak begitu berbeda dengan warna pixel sebelum penyelipan pesan.

Untuk penerapan metode LSB pada gambar *watermark*, gambar *watermark* dapat disebarkan kedalam gambar utama yang besar. Namun hal ini akan membuat gambar utama harus berukuran lebih besar dibandingkan gambar *watermark* sesuai tipe gambar yang digunakan. Agar pixelnya dapat diselipkan.

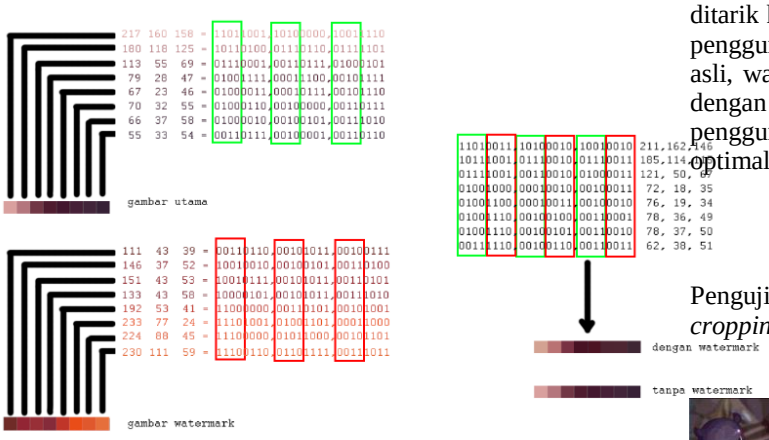
Selain itu jika menggunakan teknik LSB seperti ini, gambar *watermark* memang tidak dapat dilihat sama sekali, namun gambar tidak akan bertahan terhadap serangan yang mengubah ukuran gambar seperti stretching, rotation, ataupun *cropping*.

Untuk itu akan digunakan Bitplane yang lebih tinggi untuk diisi dengan gambar *watermark* agar *watermark* tetap dapat diekstrak. bitplane yang digunakan akan berkisar dari 1 sampai 4 layer tergantung dari *watermark* yang akan digunakan apakah bitplane(cukup 1 bitplane gambar utama), grayscale (1-2 bitplane gambar utama), atau full color (3-4 bitplane gambar utama).

III. IMPLEMENTASI DAN PENGUJIAN

Pada implementasi LSB untuk steganografi, akan menggunakan 4-4 bitplane, 4 bitplane gambar asli MSB(Most Significant Bit) + 4 bitplane MSB dari *watermark* yang dimasukkan kedalam 4 bitplane LSB gambar asli seperti yang ditunjukkan pada Gambar 5. Hasil akan dibandingkan dengan hasil steganografi jika menggunakan 4-4 MSB, 5-3 MSB, dan 6-2MSB bitplane

gambar asli-gambar *watermark*, selain itu hasil steganografi akan diuji terhadap beberapa macam serangan.



Gambar 5. Penerapan 4 bitplane *watermark* steganografi

Pengujian dengan 4-4, 5-3, dan 6-2 bitplane dari gambar *watermark*

(gambar kiri adalah gambar asli setelah diembed *watermark*, gambar kanan adalah *watermark* yang ekstrak dari gambar asli)

Gambar 6. Perbandingan penggunaan 4-4, 5-3, 6-2 bitplane

Melalui perbandingan hasil ekstraksi *watermark*, dapat dilihat bahwa jika menggunakan 3 bitplane (gambar kedua) ataupun 2 bitplane (gambar ketiga) *watermark* hampir tidak mengubah gambar asli meskipun *watermark* adalah gambar full color, namun hanya 2 dan 3 bitplane masih tidak cukup untuk dapat mengekstrak gambar *watermark* dengan cukup jelas sehingga lebih direkomendasikan menggunakan 4-4 MSB. Dengan 4 bitplane, *watermark* dapat dimasukkan dan ditarik kembali tanpa merusak *watermark*, namun sayangnya penggunaan 4-4 akan sedikit mengubah warna dari gambar asli, watermark akan masih dapat terlihat di bagian gambar dengan noise yang rendah. Namun secara keseluruhan penggunaan 4-4 MSB bitplane memberikan hasil paling optimal dibandingkan perbandingan lain gambar lain.

Pengujian terhadap transformasi gambar, pemutaran, *cropping*, *resize* besar, kecil dan *resize* besar.

Gambar 7. Perbandingan pengujian pemutaran, *cropping*, dan *resize*

Melalui pengujian, dapat dilihat bahwa meskipun gambar asli diputar(gambar kedua), dapat tetap mempertahankan bentuk dan warna *watermark*nya secara keseluruhan meskipun tampak beberapa tambahan garis akibat algoritma pemutaran gambar.

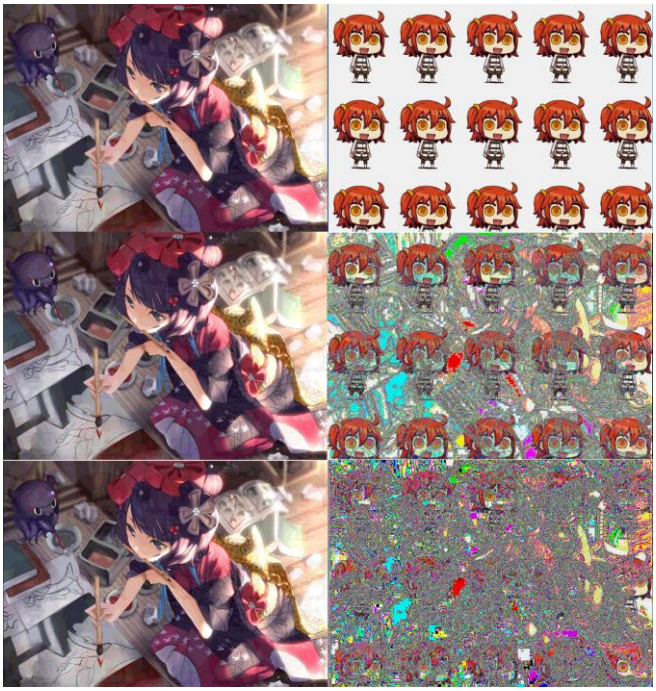
W*atermark* juga tetap utuh meskipun dilakukan *cropping* (gambar ketiga dan keempat). *Watermark* juga tetap bertahan terhadap *resize* baik diperkecil ataupun diperbesar.

Pengujian yang ke tiga adalah ketahanan terhadap editing baik penghapusan atau penambahan objek dalam gambar

Gambar 8. Perbandingan pengujian terhadap editing

Hasil ekstraksi watermark menunjukkan bahwa watermark tetap utuh meskipun mengalami manipulasi, gambar kedua mengalami penghilangan objek dan gambar ketiga mengalami penambahan objek. Pengubahan pada sebagian area dari gambar tidak akan memberikan pengaruh terhadap area lainnya. Watermark hanya akan rusak seluruhnya jika gambar mengalami *editing* dalam jumlah besar

pengujian yang ke empat adalah ketahanan terhadap serangan compression JPEG/JPG (lossy compression) dan *snapshot*(pengambilan gambar melalui layar pengguna, tidak melalui *download* image) secara berulang terhadap gambar utama yang bertipe PNG (tidak *lossy*). Gambar dengan lossy compression memiliki algoritma untuk menghemat file size dengan menghilangkan detail detail pada pixelnya sehingga umumnya gambar digital yang diselipi informasi tidak bisa menggunakan format JPEG/JPG karena sedikit pengubahan pada gambar seperti compression akan membuat informasi yang diselipkan didalamnya tidak dapat diambil kembali. Namun dengan algoritma yang digunakan, gambar berwatermark akan memiliki beberapa ketahanan terhadap compression.



Gambar 9. Perbandingan pengujian terhadap compression dan snapshot

Dapat dilihat bahwa dengan snapshot yang memakai kompresi JPEG pertama (gambar kedua), *watermark* masih dapat terlihat dengan jelas meskipun mulai terdapat banyak noise.

Namun untuk snapshot dari snapshot pertama (gambar ketiga), *watermark* mulai pudar dan tidak jelas bentuknya. Hal ini dikarenakan display dari perangkat biasanya menggunakan compression agar kinerja tidak berat saat menampilkan gambar. Perangkat baru menampilkan pixel lebih detail jika gambar di *zoom.* Oleh karena itu, kompresi ganda melalui snapshot akan membuat gambar kehilangan kualitasnya sehingga watermark bisa mulai pudar. Terlebih lagi jika gambar menggunakan snapshot dari snapshot yang lainnya.

Dengan sejumlah pengujian dan manipulasi terhadap gambar, maka dapat dinyatakan bahwa steganografi *watermark* yang diberikan cukup *robust*.

IV. KESIMPULAN

Steganography watermarking dapat dilakukan dengan menggunakan beberapa bitplane pada gambar asli untuk diselipi dengan *watermark* sebagai penanda identitas pembuatnya.

Algoritma 4-4 bitplane memiliki ketahanan terhadap manipulasi gambar berupa pemutaran, *resizing*, *cropping*, *editing*, dan kompresi gambar yang tidak beruntun.

Penggunaan digital watermarking dapat memberikan keamanan atas identitas pembuatnya sehingga membantu orang-orang yang bekerja di bidang digital image.

REFERENSI

[1] Steganografi. http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Steganografi-(2018).pdf diakses pada 16 Mei 2018.

[2] Steganography: Hiding an image inside another. https://towardsdatascience.com/steganography-hiding-an-image-inside-another-77ca66b2acb1 diakses pada 16 Mei 2018

[3] Steganography: Hiding Data Within Data https://www.garykessler.net/library/steganography.html diakses pada 16 Mei 2018

[4] Sumber gambar ilustrasi untuk pengujian oleh つーはん https://www.pixiv.net/member_illust.php?mode=medium&illust_id=68405015

[5] Sumber gambar sebagai watermark http://typemoon.wikia.com/wiki/File:Female_Protagonist_Riyo.png

Bandung 17 Mei 2018

Yusak Yuwono Awondatu