Jurnal SimanteC
Vol. 6, No. 3 Juni 2018 ISSN 2088-2130;e-ISSN 2502-4884

RANCANG BANGUN APLIKASI MANAJEMEN HAK CIPTA CITRA DIGITAL MENGGUNAKAN DES DAN LSB

Paulus Lucky Tirma Irawan[1], Budi Purnomo[2], Oesman Hendra Kelana[3]
[1,2,3] Prodi Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Ma Chung
Jl. Villa Puncak Tidar N-01, Tidar, Malang
E-mail : [1]paulus.lucky@machung.ac.id, [2]311010009@student.machung.ac.id,
[3]oesman.hendra@machung.ac.id

ABSTRAK

Kasus pencurian data digital merupakan sebuah contoh nyata dimana kemajuan teknologi juga dapat membawa potensi ancaman yang merugikan banyak pihak bila tidak ditangani dengan baik. Dalam penelitian ini akan dikembangkan sebuah aplikasi untuk membantu melindungi hak karya cipta berupa data citra digital melalui penambahan *watermark* yang dihasilkan dari kombinasi teknik keamanan data steganografi *Least Significant Bit* (LSB) dan teknik kriptografi Data *Encryption Standard* (DES). Kode informasi rahasia yang disisipkan sebagai watermark pada data citra digital akan terlebih dahulu di enkripsi menggunakan teknik kriptografi DES sebelum disematkan menggunakan teknik penyisipan data steganografi LSB. Penggunaan teknik keamanan data berlapis ditujukan untuk mendapatkan tingkat keamanan data yang lebih baik. Dalam pengujian tingkat kemiripan antara citra asli dan citra stegano yang sudah dilakukan menggunakan uji nilai *Mean Squared Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR), didapatkan nilai rerata dari pengujian MSE terhadap citra stegano adalah sebesar 0,371. Sementara untuk komponen nilai PNSR didapatkan rerata nilai sebesar 121,045.

Kata kunci : Citra Digital, DES, Karya Cipta, LSB

ABSTRACT

The case of digital data theft is one of example where technological advances can also bring potential threats to the detriment of many parties if not handled properly. In this research an application will be developed to help protect copyright in the form of digital image data through the addition of watermarks resulting from a combination of Least Significant Bit (LSB) steganography techniques and the Data Encryption Standard (DES) cryptographic techniques. The confidential information code that is inserted as a watermark on the digital image data will be encrypted using DES cryptographic techniques before embedding using LSB steganographic data insertion technique. The use of layered data security techniques is aimed at obtaining a better level of data security. In testing the level of similarity between the original image and stegano image that has been done using the test of Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR), value obtained from the test of MSE to stegano image is 0.371. While the value of PNSR obtained average value of 121,045.

Keywords : *Digital Image, DES, Copyrights, LSB*

PENDAHULUAN

Pemanfaatan teknologi sebagai media penyimpanan data digital sudah menjadi hal yang lumrah saat ini. Dalam sebuah artikel yang diterbitkan pada tahun 2012 diketahui telah terjadi peningkatan yang sangat signifikan terhadap penjualan media penyimpanan digital sebanyak 129% dibandingkan tahun sebelumnya. Hal ini merupakan salah satu hal yang mengindikasikan bahwa popularitas penggunaan media penyimpanan data digial seperti *flash disk*, SSD, *hard disk* eksternal terus mengalami peningkatan [1]. Beberapa keuntungan yang didapat dari penggunaan media penyimpanan digital ini antara lain kemudahan dalam melakukan menajemen data, kemudahan untuk melakukan penyuntingan, rekayasa, penggandaan, serta penyebaran data yang tidak akan dijumpai pada model penyimpanan data konvensional.

Berbagai kemudahan yang didapat dari penggunaan data digital tidak jarang dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab sehingga dapat merugikan orang lain. Beberapa kasus pencurian data digital mulai dari data pribadi pengguna yang disimpan di media sosial hingga pencurian karya cipta dalam bentuk data digital adalah beberapa contoh potensi ancaman keamanan yang akan dihadapi pengguna di masa mendatang.

Beberapa teknik pengamanan data saat ini sudah cukup memberikan solusi untuk mengatasi potensi pencurian data-data digital yang ada saat ini. teknik keamanan data yang sering digunakan adalah teknik kriptografi, teknik steganografi atau gabungan dari kedua teknik tersebut. Pada penelitian sebelumnya (2012) telah dilakukan penerapan teknik kriptografi untuk pengamanan data digital dalam bentuk pesan SMS [2] dan pada basis data MySQL [3]. Kombinasi teknik kriptografi dan steganografi juga sudah dilakukan untuk memberikan solusi pengamanan data citra digital yang akan dikirimkan melalui perangkat bergerak. Hasil pengujian terhadap kualitas citra stegano yang dihasilkan juga menunjukkan hasil yang sangat baik [4], [5].

Dalam penelitian ini akan dilakukan perancangan dan pengembangan sebuah aplikasi untuk melakukan manajemen data dalam bentuk citra digital. Aplikasi ini ditujukan untuk memberikan perlindungan terhadap hak karya cipta melalui pemberian serangkaian informasi terenkripsi yang disisipkan menggunakan gabungan teknik kriptografi dan steganografi. Penelitian kemudian dilanjutkan dengan melakukan pengujian terhadap kualitas citra stegano yang dihasilkan setelah dilakukan penyisipan watermark menggunakan komponen uji parameter MSE dan PSNR. Dalam penelitian ini lingkup permasalahan yang akan diselesaikan akan dibatasi pada objek karya cipta berupa citra digital dalam format bitmap, PNG dan JPG serta implementasi teknik kriptografi DES dan teknik steganografi LSB. Aplikasi yang dikembangkan akan menggunakan platform desktop untuk pertimbangan performa dan efisiensi jalannya algoritma.

METODE

Penelitian dilakukan dalam 3 tahapan utama. Tahap pertama adalah pengenalan terhadap struktur file citra digital. Pada penelitian ini, objek citra digital yang akan digunakan hanyalah yang memiliki format penyimpanan Bitmap (BMP), Portable Network Graphics (PNG), dan Joint Photographic Group (JPG). Pengenalan susunan bit serta struktur dari citra digital penting untuk diketahui sehingga operasi manipulasi bit yang nantinya akan dilakukan tidak merusak citra yang tersimpan dalam file citra digital tersebut.

Pada tahapan selanjutnya adalah implementasi teknik *Data Encryption Standard* (DES) untuk melakukan enkripsi maupun dekripsi terhadap *secret information* yang disisipkan kedalam citra (*watermark*). Adapun *secret information* yang disisipkan adalah sebuah kode yang terdiri dari 8 *Byte* karakter, dimana pada kode tersebut akan mewakili informasi mengenai nama pemilik citra digital serta tanggal dan jam dilakukannya proses *watermarking*.

Pada tahap terakhir akan dilakukan implementasi metode *Least Significant Bit* (LSB) terhadap citra digital dengan *secret information* berupa kode yang sudah lebih dulu dienkripsi menggunakan DES. Teknik LSB akan diaplikasikan untuk menyisipkan maupun mangambil *secret information* ke/dari dalam citra digital tadi.

A. Tahapan Pengenalan Struktur File

Sebuah *file* citra digital umumnya tersusun dari 3 bagian yakni, *header, image data*, dan *footer*. Pada *header* biasanya tersimpan bit-bit berisi informasi metadata dari sebuah *file* citra. Sedangkan pada *image data* tersimpan bit-bit yang merepresentasikan sebuah citra analog. Sedangkan pada *footer*, berisikan kumpulan bit akhir yang digunakan untuk menandakan sebuah akhir dari *file*.

Masing-masing jenis *file* citra digital memiliki bentuk *header*, *footer*, serta metode penyimpanan yang berbeda-beda. Pada penelitian ini citra digital yang digunakan terbatas pada citra digital dengan format penyimpanan Bitmap (BMP), Portable Network Graphics (PNG) dan Joint Photographic Group (JPG). Pengenalan struktur file ditujukan agar proses manipulasi bit yang akan dilakukan tidak merusak struktur bawaan yang sudah ada yang lebih jauh dapat memberikan dampak pada rusaknya *file* citra digital.

B. Citra Digital

Sebuah citra digital dapat mewakili sebuah matriks dengan ukuran N baris dan M kolom. Perpotongan antara kolom dan baris tersebut kemudian dinamakan pixel. Dengan kata lain pixel sendiri merupakan titik penyusun gambar yang berkumpul dan bergabung membentuk seperti mozaik yang memanipulasi mata sehingga pada jarak pandang tertentu akan tampak kesan gambar utuh. Dari pixel yang terkumpul inilah yang kemudian membentuk sebuah citra analog yang menyerupai objek tertentu. Dari citra analog tersebut, kemudian dihasilkan citra digital.

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek [6]. Citra terbagi 2 yaitu ada citra yang bersifat analog dan ada citra yang bersifat digital. Citra analog adalah citra yang bersifat kontinu seperti gambar pada monitor televisi, foto sinar X, hasil CT Scan, dan sebagainya. Sedangkan pada citra digital adalah citra yang dapat diolah oleh komputer.

Secara umum citra digital merupakan suatu gambar yang tersusun dari pixel, dimana tiap pixel mewakili warna pada suatu titik pada gambar. Citra digital adalah gambar dua dimensi yang ditampilkan pada layar monitor sebagai himpunan berhingga (*discrete*) nilai digital yang disebut dengan piksel [7]. Citra digital dihasilkan dari citra analog (*continue*) melalui digitalisasi. Digitalisasi citra analog terdiri atas penerokan (*sampling*) dan kuantisasi (*quantization*). Penerokan (*sampling*) adalah pembagian citra ke dalam elemen-elemen diskrit (*pixel*), sedangkan kuantisasi adalah pemberian nilai intensitas warna pada setiap piksel dengan nilai bilangan bulat.

C. Digital Watermarking

Steganografi dapat dibagi menjadi dua bagian berdasarkan tujuan penggunaannya yakni *protection against detection (data hiding)* dan *protection against removal (document marking). Watermarking* merupakan salah satu jenis dari *document marking*.

Watermarking secara umum merupakan teknik penyisipan data ke dalam elemen multimedia seperti citra, audio atau video. Sedangkan pengertian *digital watermarking* sendiri adalah pengaplikasian teknik *watermarking* pada media digital. Proses yang terjadi pada *watermarking* hampir sama dengan proses steganografi, yakni menyisipkan informasi ke dalam sebuah media. Media akan di-*encode* dengan menambahkan data rahasia dan kunci tertentu. Media yang sudah di-*encode*, selanjutnya dapat ditransfer melalui suatu jalur komunikasi dan jika

akan diperiksa keasliannya atau ingin mendapatkan media aslinya (*original cover*), maka dilakukan proses *decoder*. Proses *decode* menggunakan kunci yang sama pada proses *encode*.

D. Data Encryption Standard (DES)

DES adalah salah satu algoritma enkripsi yang paling banyak digunakan di dunia. Secara umum enkripsi data menggunakan algoritma DES dapat dikelompokkan ke dalam 3 kelompok, yakni pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit. DES termasuk ke dalam enkripsi simetris dan tergolong jenis blok kode [7]. Ciphertext memliki panjang 64 bit, sedangkan key memiliki panjang 56 bit, dan 8 bit parity [8].

Adapun skema dari algoritma DES adalah sebagai berikut [9]:

1. Bit dari plaintext (m) dipermutasi dengan initial permutation (IP) untuk menghasilkan m0 = IP(m). Ditulis m0 =L0R0, di mana L0 merupakan 32 bit pertama dari m0 dan R0 adalah 32 bit terakhir,
2. Untuk $1 \leq i \leq 16$, berlaku:
   $L_i = R_{(i\text{-}1)}$ (1)
   $R_i = L_{(i\text{-}1)}\ xor\ F(R_{(i\text{-}1)}, K_i)$ (2)
3. Setelah mendapatkan $R_{16}L_{16}$ kemudian dipermutasi dengan *inverse initial permutation* (IP^{-1}) menjadi blok ciphertext $C = IP^{-1}$ ($R_{16}L_{16}$).

Proses dekripsi DES dilakukan dengan membalik proses enkripsi menggunakan key yang dibalik (C_{16}, D_{16}). Perlu diketahui bahwa C_0, D_0 D_0 akan selalu bernilai sama dengan C_{16}, D_{16}. Oleh karena itu pada dekripsi C_{16}, D_{16} adalah C_0, D_0 (inputan *key* dari pengguna). Kemudian selanjutnya C_{15}, D_{15} didaptkan dengan melakukan *right shift* berdasarkan tabel rotasi key.

Pada penelitian ini algoritma DES digunakan untuk melakukan enkripsi/ dekripsi terhadap kode yang bernilai 8 *Byte*. *Key* untuk proses enkripsi/dekripsi berasal dari data masukan *password.* Pada proses penyisipan akan dilakukan proses enkripsi, yang hasilnya akan disisipkan ke dalam citra menggunakan metode LSB. Sedangkan pada proses pembacaan *watermark*, DES digunakan untuk mendekripsi informasi *chipertext* untuk menghasilkan kode, yang nantinya dari kode tersebut akan dicari dalam basis data aplikasi sehingga didapatkan data terkait data citra digital tersebut, termasuk di dalamnya nama pemilik serta informasi terkait penyematan *watermark* pada citra yang dimaksudkan.

E. Least Significant Bit (LSB)

Metode LSB merupakan salah satu metode watermarking yang bekerja dalam mode warna RGB [10]. Metode ini bekerja dengan cara menyisipkan informasi pada bit-bit paling kanan dari setiap elemen RGB. Perubahan bit paling kanan hanya menimbulkan perubahan nilai RGB sebesar 1 dari 256 warna yang ada sehingga perubahan tersebut hampir tidak dapat dideteksi dengan mata telanjang.

Pada metode LSB, bit-bit pesan disisipkan pada bit terakhir, atau bit paling kanan, dari piksel-piksel citra penampung. Sebagai contoh, misalnya diambil blok 4 titik dengan nilai sebagai berikut: 100110101 01100111 110110000 110011010. Kemudian akan disisipkan sebuah informasi: 1001. Maka hasil penyisipannya adalah: 100110101 01100110 110110000 110011011, di mana bit yang dicetak tebal merupakan informasi yang disisipkan ke dalam media citra digital.

Least Significant Bit (LSB) merupakan jenis *fragile watermark* di mana faktor robustness tidak diperhitungkan sebagai syarat karena watermark jenis ini memang digunakan untuk tujuan tertentu seperti untuk mendeteksi apakah citra yang telah di-watermark pernah di-edit atau tidak. Bilai faktor *robustness* dari LSB dapat diabaikan, maka sebalikya faktor keamanan (*secure*) dari *watermark* menggunakan metode LSB perlu diperhatikan. Oleh karena itu, data yang akan disisipkan terlebih dahulu diproses menggunakan metode enkripsi, sehingga

data rahasia tidak mudah terbaca. Hasil enkripsi menyebabkan data dalam kondisi acak, maka hal ini akan menyulitkan pendeteksian *watermark* pada media yang disisipi. Keberadaan *watermark* yang ada di dalam media akan semakin sukar untuk ditemukan, karena data yang disisipkan berbentuk data acak sehingga terkesan membaur dengan media citra penampungnya.

F. Alur Kerja Aplikasi

Alur dari aplikasi dibagi menjadi 2 bagian, yakni alur penyisipan watermark dan alur pembacaan *watermark*. Gambar 1 menjelaskan detil tahapan proses penyisipan *watermark*. Pada tahapan ini aplikasi akan terlebih dahulu akan meminta inputan atau masukan dalam bentuk citra digital, serta detil informasi terkait lainnya seperti nama pemilik dari citra, dan *password*. Aplikasi akan terlebih dahulu memastikan validitas data masukan yang diberikan apakah sudah sesuai dengan format gambar yang didukung aplikasi atau tidak. Apabila data yang dimasukkan oleh pengguna sudah dinyatakan valid, maka aplikasi akan membangkitkan sebuah kode unik yang mewakili identitas dari pemilik citra tersebut. Kode unik ini nantinya akan berisikan informasi tanggal dan waktu yang memberikan informasi kapan proses *watermarking* dilakukan. Tahapan proses selanjutnya adalah menyimpan data-data yang sudah dikumpulkan ke dalam *database* aplikasi. Adapun data yang dimasukkan ke dalam *database* adalah informasi nama pemilik citra, kode unik, tanggal dan jam *watermark*. Fungsi *database* di sini lebih kepada fungsi manajemen data (historikal).

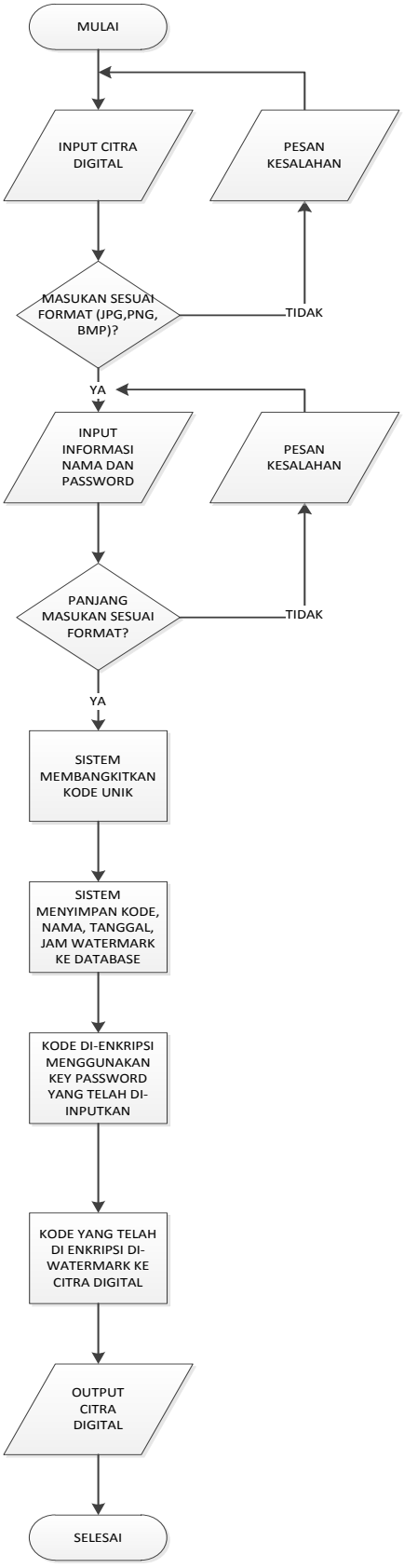
Setelah semua data selesai disimpan di dalam database, sistem akan melakukan enkripsi menggunakan *key* dari *password* yang sebelumnya telah diberikan oleh pengguna sebelum akhirnya dilakukan penyisipan menggunakan metode *Least Significant Bit* (LSB). Hasil dari penyisipan tersebut adalah sebuah citra digital baru yang menyerupai citra aslinya dan juga telah berisi informasi tambahan rahasia lain.

Pada gambar 2 dijelaskan detil tahapan proses pembacaan *watermark* diawali dengan meminta masukan berupa data citra digital yang akan dianalisa serta data *password*. *Password* inilah yang nantinya akan digunakan dalam proses dekripsi untuk mendapatkan kode unik yang nantinya akan dicocokan dengan data yang terdapat di dalam basis data aplikasi.

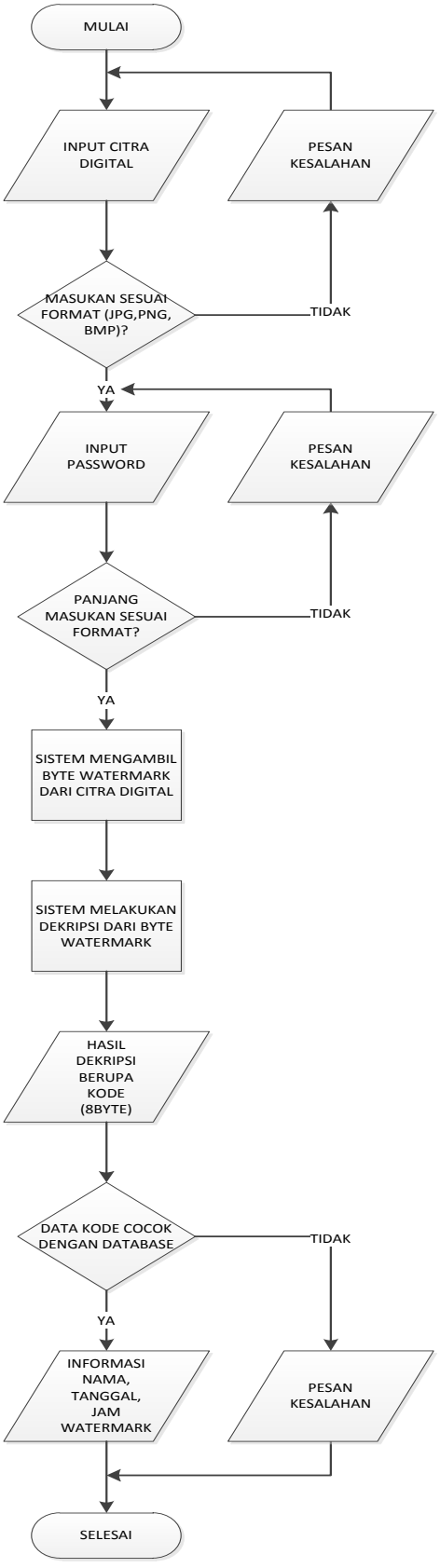
Apabila semua data masukan valid, maka aplikasi akan mengambil nilai dari tiap-tiap bit terwatermark pada citra yang di-inputkan. Nilai dari bit watermark tersebut kemudian akan dilakukan ekstraksi untuk kemudian disusun sehingga membentuk sebuah *ciphertext* 8 *byte*.

Proses dekripsi menggunakan metode DES terhadap ciphertext yang telah didapatkan dari proses sebelumnya juga akan dilakukan menggunakan *key password* yang sama sehingga menghasilkan sebuah *plaintext* 8 *byte*. *Plaintext* inilah yang akan dicocokkan dengan kumpulan kode yang telah disimpan di dalam basis data aplikasi untuk didapatkan informasi berupa nama pemilik dari citra, serta tanggal dan jam dilakukannya *watermark*.

Apabila hasil pencocokan kode tidak menghasilkan kesesuaian, maka aplikasi akan menampilkan pesan kesalahan yang memberitahukan pengguna bahwa sistem tidak menemukan kecocokan data hasil pembacaan *watermark* dengan data yang tersimpan di dalam basis data aplikasi.



Gambar 1. Diagram Alir Penyematan *Watermark*



Gambar 2. Diagram Alir Pembacaan *Watermark*

HASIL DAN PEMBAHASAN

Aplikasi manajemen hak cipta citra digital yang telah dihasilkan memberikan hasil kualitas yang tidak jauh berbeda dengan citra aslinya. pengujian hasil dilakukan dengan 3 cara, yakni melalui pengamatan langsung, maupun melalui penghitungan metode khusus MSE (*Mean Squared Error*) dan PNSR (*Peak Noise to Signal Ratio*).

Mean Squared Error (MSE) adalah metode yang digunakan untuk mengetahui nilai *error* dari citra *watermark* (*stego-image*). Adapun perumusan perhitungan MSE adalah sebagai berikut.

$$\boldsymbol{MSE} = \left[\frac{\sum_{X=1}^{M}\sum_{Y=1}^{N}[\boldsymbol{H}(\boldsymbol{X},\boldsymbol{Y})\text{-}\boldsymbol{F}(\boldsymbol{X},\boldsymbol{Y})]^{2}}{\boldsymbol{M}.\boldsymbol{N}}\right] \quad (3)$$

Besaran nilai MSE memiliki rentang nilai 0 samai dengan 1. Semakin kecil nilai MSE yang dihasilkan dari dua/lebih citra yang dibandingkan (mendekati nilai 0) maka kualitas citra tersebut dapat disimpulkan setara, namun jika nilai MSE yang dihasilkan sebaliknya maka citra digital yang dibandingkan tersebut berbeda atau secara kualitas tidak sama. Tabel 2 menunjukkan hasil pengujian MSE terhadap 5 data sampel dalam format JPG yang digunakan dalam penelitian ini.

Tabel 1. Hasil Pengujian MSE Data Sampel

Citra	Nama File	MSE
	autumn_leaves.jpg	0,374
	fish.jpg	0,369
	kiwi.jpg	0,370
	misty.jpg	0,383
	mountain.jpg	0,359
	Rata-Rata MSE	0,371

Sementara *Peak Signal to Noise Ratio* (PNSR) adalah metode yang digunakan untuk mengetahui perbedaan nilai puncak sinyal dengan *noise* [8]. *Noise* yang dimaksud adalah citra *watermark* (*stego-image*) sedangkan sinyal yang dimaksud adalah citra asli. Perhitungan PNSR dapat dirumuskan sebagai berikut. Besaran nilai PNSR dinyatakan dalam satuan dB (desibel). Adapun perumusan perhitungan PNSR adalah sebagai berikut.

$$\boldsymbol{NSR} = 20\log_{10}\frac{\boldsymbol{nilai\ max}}{\sqrt{\boldsymbol{MSE}}} \quad (4)$$

Adapun semakin besar nilai PNSR, maka kemiripan 2 buah citra digital yang dibandingkan akan semakin tinggi. Besaran nilai normal PNSR adalah > 50dB. Semakin kecil nilai PNSR maka akan semakin banyak *noise* pada citra. Semakin tinggi nilai PNSR maka *noise* akan semakin sedikit sehingga citra yang dibandingkan akan semakin serupa secara kualitas.

Tabel 2 menunjukkan hasil penghitungan nilai PNSR terhadap data sampel.

Tabel 2. Hasil Pengujian PNSR Data Sampel

Citra	Nama File	MSE
	autumn_leaves.jpg	121,039
	fish.jpg	121,050
	kiwi.jpg	121,049
	misty.jpg	121,035
	mountain.jpg	121,052
	Rata-Rata PNSR	121,045

Sementara Tabel 3 menunjukkan rata-rata nilai pengujian komponen MSE dan PNSR untuk masing-masing format data citra digital (.BMP, .JPG, .PNG). Pengujian dilakukan dengan menggunakan 5 data sampel citra digital.

Tabel 3. Hasil Pengujian MSE & PNSR

Format Citra	MSE	PNSR
BMP	0,331	121,121
PNG	0,346	121,102
JPG	0,371	121,052

SIMPULAN

Pembuatan aplikasi manajemen hak cipta citra digital dapat digunakan untuk memeberikan perlindungan hak kekayaan intelektual terhadap sebuah karya dalam bentuk data citra digital. Aplikasi manajemen hak cipta citra digital melalui pemberian *watermark* diterapkan dengan menggabungkan dua teknik keamanan data kriptografi DES dan steganografi LSB untuk menghasilkan sebuah citra watermarked (*stego-image*) dengan kualitas yang cukup baik. Hal ini dapat dilihat dari rerata nilai yang didapatkan dari pengujian komponen nilai MSE dan PNSR terhadap citra digital dengan format BMP 0,331(MSE) dan 121,121 (PNSR), PNG 0,346 (MSE) dan 121,102 (PNSR) dan JPG 0,371 (MSE) 121,052 (PNSR).

SARAN

Penelitian ini masih membuka celah kemungkinan untuk dilakukan penelitian lanjutan terutama untuk format objek karya cipta citra selain yang sudah digunakan dalam penelitian ini. Teknik kriptografi dan steganografi yang akan digunakan juga masih perlu dilakukan analisa yang lebih mendalam untuk mengetahui tingkat keamanan yang dihasilkan terhadap beberapa pola serangan yang mungkin terjadi. Pemilihan platform aplikasi mungkin dapat diubah ke dalam bentu API sehingga memudahkan pengembangan aplikasi pada multiplatform untuk alasan skalabilitas yang lebih baik sehingga tidak terbatas pada satu jenis platform tertentu saja.

DAFTAR PUSTAKA

[1] "Evolution of data storage industry accelerates," *SearchStorage*. [Daring]. Tersedia pada: https://searchstorage.techtarget.com/opinion/Evolution-of-data-storage-industry-accelerates. [Diakses: 06-Apr-2017].

[2] P. L. . Irawan dan M. Linggardjati, "Implementasi Algoritma Kriptografi Salsa20 Untuk Keamanan Pesan SMS Pada Telepon Seluler," dalam *Proceedings EECCIS*, 2012, hlm. E11(1)-E11(3).

[3] P. L. T. Irawan, "Implementasi Teknik Kriptografi Stream Cipher Salsa20 Untuk Pengamanan Basis Data," *SMATIKA J.*, vol. 5, no. 02, hlm. 88–92, 2015.

[4] P. L. T. Irawan, D. D. H. Santjojo, dan M. Sarosa, "Implementasi Kripto-Steganografi Salsa20 dan BPCS untuk Pengamanan Data Citra Digital," *J. EECCIS*, vol. 8, no. 2, hlm. 175–180, 2014.

[5] T. Sutojo, E. Mulyanto, V. Suhartono, dan O. D. NURHAYATI, "Teori Pengolahan Citra Digital," 2009.

[6] Fahmi, "Studi dan Implementasi Watermarking Citra Digital Dengan Menggunakan Fungsi Hash," Institut Teknologi Bandung, Bandung, Tugas Akhir, 2007.

[7] P. L. T. Irawan, D. D. H. Santjojo, dan M. Sarosa, "Implementasi Kripto-Steganografi Salsa20 dan BPCS untuk Pengamanan Data Citra Digital," *J. EECCIS*, vol. 8, no. 2, hlm. 175–180, 2014.

[8] W. Stallings, L. Brown, M. D. Bauer, dan A. K. Bhattacharjee, *Computer security: principles and practice*, Fifth Edition. Pearson Education, 2011.

[9] W. Trappe, *Introduction to cryptography with coding theory*. Pearson Education India, 2006.

[10] A. Dony, "Pengantar Ilmu Kriptografi," *Ed. Dua Yogyak. CV Andi Offset*, 2008.