e-ISSN 2549-7472
Edumatic: Jurnal Pendidikan Informatika
Vol. 5 No. 2, Desember, 2021, **Hal. 204-213**
DOI: 10.29408/edumatic.v5i2.3901

Analisis Digital *Watermarking* untuk Otentikasi pada Citra Manipulasi Menggunakan Metode *Least Significant Bit*

Ardhi Fadlika Satria[*1], Riza Ibnu Adam [2], Carudin [3]

[1,2,3] Program Studi Teknik Informatika, Universitas Singaperbangsa Karawang
email : ardhi.fadlika17059@student.unsika.ac.id *[1], riza.ibnu@staff.unsika.ac.id [2], carudin@staff.unsika.ac.id [3]

(Received: 6 Agustus 2021/ Accepted: 20 Agustus 2021/ Published Online: 20 Desember 2021)

Abstrak

Penggunaan platform digital memiliki efek positif dan efek negatif. Banyak pelaku kejahatan yang melakukan manipulasi citra untuk kepentingan pribadi, sehingga dapat merugikan pemegang hak cipta (ownership) dari citra tersebut. Tujuan penelitian ini adalah untuk mendeteksi citra palsu yang dihasilkan oleh teknik *copy-move, splicing*, dan *retouching*. Metode yang digunakan merupakan metode *Least Significant Bit* (LSB) sebagai teknik *watermarking* dan fitur pendeteksiannya. Proses penyisipan dilakukan pada citra *watermark* kedalam citra *cover* sebagai media penampungnya. Pemilik citra dapat melakukan otentikasi (*temper proofing*) untuk membuktikan keaslian citra tersebut saat proses ekstraksi dilakukan, citra manipulasi berhasil di deteksi karena mengalami kerusakan. Hasil pengujian menunjukkan teknik *digital watermarking* dengan metode *Least Significant Bit* ini mampu melindungi dan membuktikan keaslian citra tersebut. Disimpulkan bahwa hasil perbandingan ekstraksi *watermark* pada citra asli dan citra manipulasi terlihat perbedaan yang sangat signifikan dari segi visual dan perhitungan dengan parameter *MSE*, *RMSE*, dan *PSNR*.

Kata kunci: *Digital Watermarking, Least Significant Bit (*LSB*),* Manipulasi citra.

Abstract

The use of digital platforms has both positive and negative effects. Many criminals who manipulate images for personal gain, so as to harm the copyright holder (ownership) of the image. The purpose of the study was to detect false imagery generated by copy-move, splicing, and retouching techniques. The method used is the Least Significant Bit (LSB) method as a watermarking technique and its detection features. The insertion process is carried out on watermark images into the cover image as the container media. Image owners can authenticate to prove the originality of the image when the extraction process is done, the image manipulation is successfully detected because it is damaged. The test results showed that the digital watermarking technique with the Least Significant-Bit method is able to protect and prove the authenticity of the image. It was concluded that the results of comparison of watermark extraction on the original image and manipulation image saw a very significant difference in terms of visual and calculation with MSE, RMSE, and PSNR parameters.

Keywords: *Digital Watermarking, Least Significant Bit (LSB), Image Manipulation.*

PENDAHULUAN

Pesatnya perkembangan dunia digital saat ini memiliki berbagai dampak positif, seperti kemudahan akses citra digital dan banyaknya *platform* yang mendukung pemrosesan citra digital tersebut. Selain menunjukkan efek positif tersebut, perkembangan dunia digital juga membawa dampak negatif. Penggunaan *platform* digital yang berdampak negatif dapat berdampak pada masyarakat yang nantinya mengakses citra digital tersebut sebagai sumber informasi. Pemanfaatan ilmu komputer dapat dengan mudah mewujudkan kemajuan dunia digital yang mendukung pengolahan citra. Namun banyak pelaku kejahatan yang melakukan

manipulasi citra untuk kepentingan pribadi atau bahkan untuk menyebarkan informasi yang menyesatkan (*hoax*) sehingga dapat menimbulkan perselisihan dan merugikan pemegang hak cipta (*ownership*) dari sebuah citra tersebut (Faroek et al., 2020).

Di era digital sekarang ini, sangat memungkinkan untuk manipulasi citra digital. Ini karena sejumlah besar peralatan foto digital dan aplikasi pengolah gambar telah dikembangkan, sehingga orang dapat dengan mudah mengambil dan memodifikasi gambar digital tanpa meninggalkan jejak yang dapat dilacak (Wijaya et al., 2017).

Manipulasi citra terbagi menjadi tiga kategori, yaitu *image splicing*, manipulasi gambar *copy-move* dan *image retouching* (Sari et al., 2016). Citra digital (foto atau gambar) termasuk karya yang secara otomatis akan dilindungi hak cipta begitu terwujud (Rahmaniar et al., 2019). Hal ini mengacu pada Pasal 12 Ayat 1 Undang-undang Hak Cipta (UUHC). Hak cipta memberi sejumlah hak eksklusif kepada pencipta gambar untuk melaksanakan perbanyakan, perubahan, dan melarang orang lain melaksanakan tindakan-tindakan tersebut tanpa seizinnya (Setiadi et al., 2018).

Metode *Least Significant Bit* (LSB) pada *digital watermarking* bisa dilakukan dengan menyisipkan data ke dalam gambar yang diinginkan (Deeba et al., 2020; Febriani & Irawati, 2017). Proses yang terjadi adalah bit data tersebut dimasukkan ke dalam bit citra digital sehingga bit data tersebut akan disembunyikan di bit citra digital (*cover*) (Ardiansyah & Kurniasih, 2018; Deeba et al., 2020). Dengan menggunakan metode *digital watermarking* dan *Least Significant Bit* (LSB), data dapat disembunyikan dan kemudian diambil kembali untuk dibaca oleh pemilik data, namun tidak dijelaskan apakah teknik *digital watermarking* ini dapat mendeteksi manipulasi pada citra atau tidak.

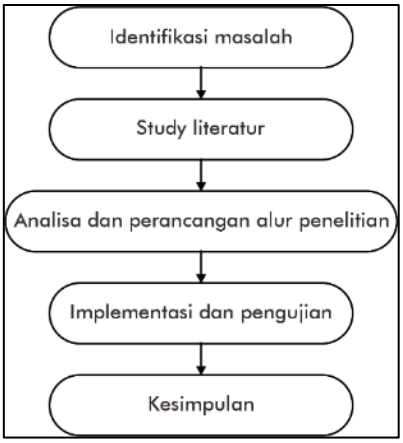
Oleh karena itu dengan adanya berbagai teknik pemalsuan, maka sangat diperlukan metode untuk melindungi hak cipta dari sebuah citra dan pendeteksian yang cukup baik untuk mendeteksi citra manipulasi yang terjadi. Menurut (Zulfan et al., 2016) secara umum, metode pendeteksian yang dikembangkan ada dua yaitu metode aktif dan pasif. Metode aktif merupakan metode deteksi dengan cara memanfaatkan *watermarking* dan *digital signature* yang dimasukkan ke dalam citra pada saat sebuah citra diciptakan. Metode pasif merupakan metode deteksi yang tidak menggunakan informasi tambahan yang dimasukkan ke citra karena pendeteksian dilakukan dengan mengindentifikasi perubahan fitur.

Penelitian ini menggunakan metode aktif dan fitur yang digunakan untuk pendeteksian adalah metode *Least Significant Bit* (LSB) yang merupakan metode dengan cara memanfaatkan *digital watermarking* yang dimasukkan ke dalam citra digital sebagai medianya pada saat sebuah citra diciptakan. Kemudian *digital watermarking* ini juga dapat di ekstrak kembali untuk nantinya membuktikan keaslian sebuah citra digital.

Penelitian yang dilakukan saat ini bertujuan untuk menganalisis *digital watermarking* yang telah mengalami manipulasi citra dengan teknik *splicing*, *copy*-move, dan *retouching* sehingga menghasilkan citra palsu yang berdampak pada berita tidak benar (*hoax*) dan pelanggaran hak cipta. Tujuan dari *digital watermarking* ini adalah sebagai perlindungan hak cipta citra digital, serta menggunakan metode *Least Significant Bit* (LSB) sebagai fitur pendeteksian.

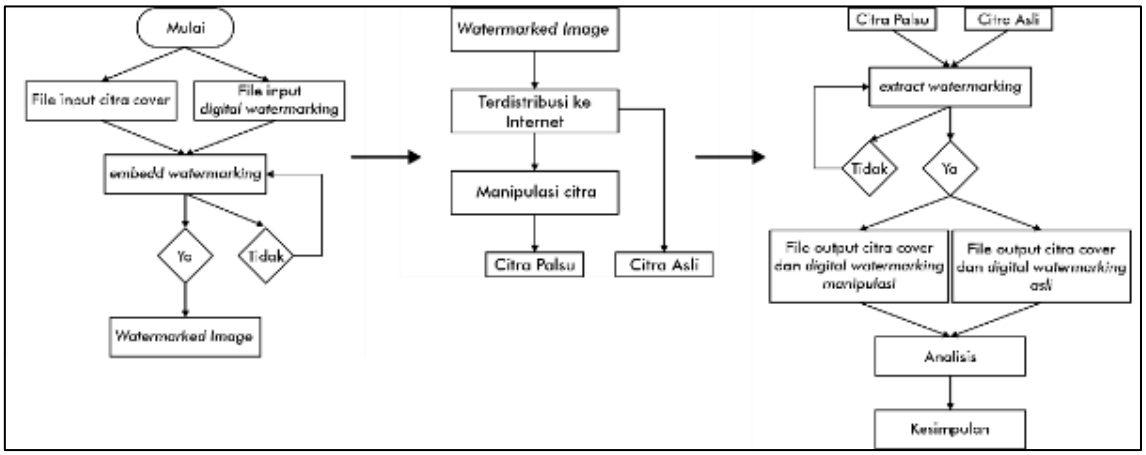
METODE

Penelitian ini menggunakan metode *Least Significant Bit* (LSB). Dengan metode *Least Significant Bit* (LSB) ini ada tahapan-tahapan dalam membantu proses mendeteksi *digital watermarking* pada citra digital yang telah mengalami pemalsuan dengan tahapan disajikan pada gambar 1.



Gambar 1. Rencana penelitian

Pada tahap analisa dan perancangan penelitian melakukan analisis kebutuhan dengan mengidentifikasi kebutuhan dari proses analisis menggunakan metode *Least Significant Bit* (LSB). Untuk menganalisa bagaimana cara kerja algoritma *Least Significant Bit* (LSB) yang terdiri dari proses *embedd* (penyisipan) dan proses *extract* (ekstraksi) (Kurniadi & Ariyus, 2020). Diantara proses penyisipan dan ekstraksi akan disimulasikan citra yang sudah ber-*watermark* mengalami manipulasi/pemalsuan dengan teknik *splicing*, *copy*-move, dan *retouching*. Alur kegiatan dapat dilihat pada gambar 2.



Gambar 2. Alur Kegiatan Penelitian

Untuk memastikan kualitas citra setelah proses penyisipan dan ekstraksi berhasil dilakukan, maka perlu adanya perhitungan kualitas citra. Kualitas citra ber-*watermark* dapat dinilai secara visual, apakah bagus, cukup bagus, rusak, sedikit rusak, dan lain-lain (Pamungkas, 2017). Namun, penilaian itu cenderung subyektif. Alternatifnya digunakanlah perhitungan kualitas citra dengan menggunakan parameter *Mean Square Error (MSE), Root Mean Squared Error* (*RMSE*), dan *Peak Signal-to-Noise Rasio* (*PSNR*) (Kaur & Kaur, 2016). *MSE* dan *RMSE* tidak memiliki satuan sedangkan satuan dari PSNR adalah desibel. Semakin mirip kedua citra maka nilai *MSE* dan *RMSE* nya semakin mendekati nilai nol. Sedangkan pada *PSNR*, jika nilai $\geq$ 30 dB masih dapat dianggap berkualitas bagus, tetapi jika *PSNR* < 30 dikatakan kualitas citra sudah terdegradasi secara signifikan. Parameter ini sering digunakan untuk membandingkan hasil pengolahan citra dengan citra awal atau citra asli (Munir, 2019). Persamaan yang digunakan untuk menghitung ketiga paramater tersebut adalah dapat dilihat pada persamaan (1), (2), dan (3).

$$MSE = \frac{1}{m \times n} + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2 \quad (1)$$

$$RMSE = \sqrt{\frac{1}{m \times n} + \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2} \quad (2)$$

$$PSNR = 10\log_{10} \frac{255^2}{MSE} \quad (3)$$

HASIL DAN PEMBAHASAN

Hasil

Hasil penelitian yang telah dilakukan pada penelitian ini adalah tentang bagaimana mendeteksi manipulasi citra dengan teknik *splicing*, *copy*-move, dan *retouching* sehingga menghasilkan citra palsu dan akan dilakukan pendeteksian menggunakan metode *Least Significant Bit* (LSB) sebagai fitur pengamanan. Kasus yang diteliti merupakan sebuah kasus simulasi kasus pelanggaran hak cipta dimana pelaku sudah merubah atau mengedit sebuah citra digital dari aslinya. Dalam penelitian ini dilakukan beberapa skenario yang dijadikan sebagai objek penelitian.

Tabel 1 Objek Gambar Penelitian (Citra Cover)

Nama File	Dimensi	Format	Ukuran	Objek gambar
Citra_Anak1	512x512px	.jpg	768 KB	
Citra_Anak2	1080x720px	.jpg	2220 KB	

Objek yang di teliti adalah citra yang terdiri dari dua citra *cover* dan dua citra *watermark*. Untuk memudahkan peneilitian dilakukanlah skenario penelitian sesuai alur kegiatan yang telah dibuat dan dapat dilihat pada tabel 1 dan tabel 2. Pada tabel 1 merupakan citra digital yang dijadikan objek penelitian sebagai citra *cover*. Citra tersebut terdiri dari citra yang memiliki ukuran file dan dimensi yang berbeda dan ekstensi format file .jpg. Sementara itu, pada tabel 2 merupakan citra digital yang dijadikan objek penelitian sebagai citra *watermark*. Citra tersebut terdiri dari citra yang memiliki ukuran file dan dimensi yang berbeda dan ekstensi format file .jpg.

Tabel 2 Objek Gambar Penelitian (Citra *Watermark*)

Nama File	Dimensi	Format	Ukuran	Objek gambar
WM1	512x512px	.jpg	768 KB	
WM2	1080x720px	.jpg	2220 KB	

Pada tahap selanjutnya, dilakukan proses penyisipan *digital watermarking* pada beberapa citra yang memiliki resolusi berbeda. Proses penyisipan ketika *digital watermarking* telah dipecah kedalam bit-bit kemudian disisipkan kedalam bit citra yang menjadi *cover* menggunakan metode *Least Significant Bit* (LSB). Ketika proses ini selesai akan dihasilkan sebuah citra yang sudah memiliki *watermark* (*watermarked image*). Proses ini menggunakan sebuah aplikasi yang di buat pada program Matlab 2019a. Pada tahap ini ada syarat tertentu yang harus dipenuhi agar prosesnya berhasil, yaitu citra *cover* dan citra *watermark* harus memiliki resolusi yang sama. Jika resolusi citra *cover* 512x512px maka citra *watermark* juga harus 512x512px, hasil ini dapat dilihat pada gambar 3, begitupun seterusnya.

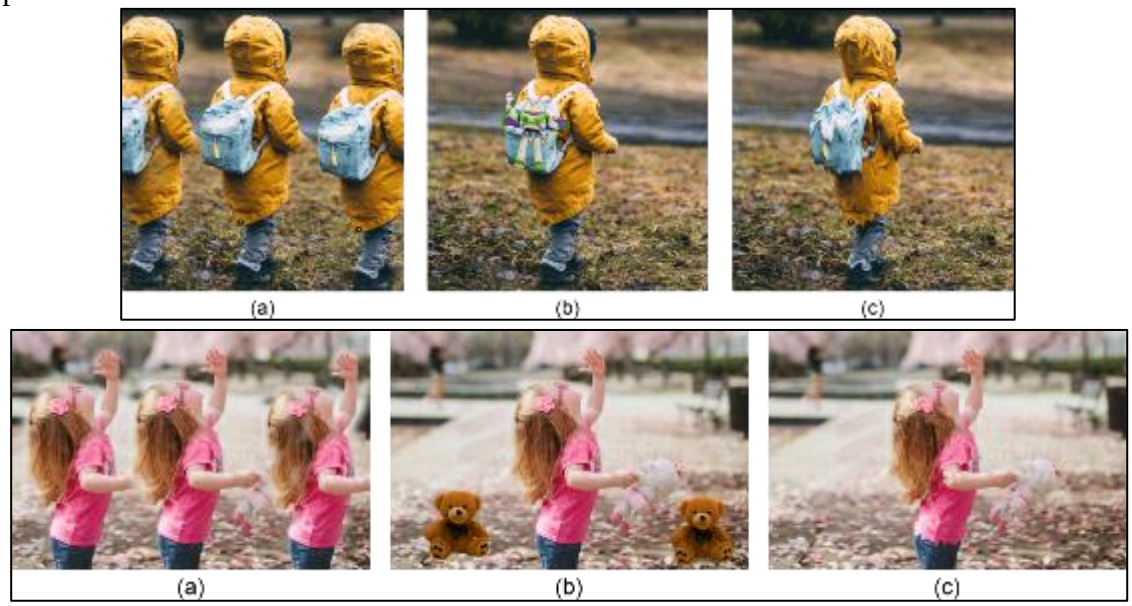
Gambar 3. Proses Penyisipan (a) citra 512x512px (b) citra 1080x720px

Berdasarkan perhitungan yang dilakukan dapat disimpulkan bahwa proses penyisipan/*embedd watermarking* yang telah dilakukan hanya sedikit mengalami perubahan. Kesimpulan ini berdasarkan hasil nilai pada *MSE*, *RMSE*, dan *PSNR*. Untuk hasilnya dapat dilihat pada Tabel 3. Terlihat pada Tabel 3, bahwa nilai dari hasil hitung kualitas citra setelah penyisipan tidak mengalami perubahan yang signifikan. Ditunjukan dengan nilai *MSE* dan *RMSE* yang mendekati nol, dan juga nilai *PSNR* yang ≥ 30. Itu artinya kualitas citra hanya sedikit mengalami perubahan.

Tabel 3. Hasil Hitung Kualitas Citra Setelah Penyisipan

Nama file	Nilai *MSE*	Nilai *RMSE*	Nilai *PSNR*
Citra_Anak1	0.0513458	0.226596	61.0597
Citra_Anak2	0.576134	0.759035	50.5596

Pada tahap proses simulasi manipulasi citra ini, citra yang telah disisipi *watermark* di *upload* (*distributed*) ke *internet* (sosial media) oleh pemilik. Simulasi serangan terjadi ketika citra sudah berada di *intenet* dengan membandingkan citra yang ber-*watermark* asli dan citra yang sudah di manipulasi. Citra sudah mengalami perubahan dari bentuk aslinya dan mengalami serangan berupa manipulasi dengan teknik *copy-move*, *splicing*, dan *retouching.* Dapat dilihat pada gambar 4 merupakan perubahan yang terjadi pada citra asli yang sudah di manipulasi.

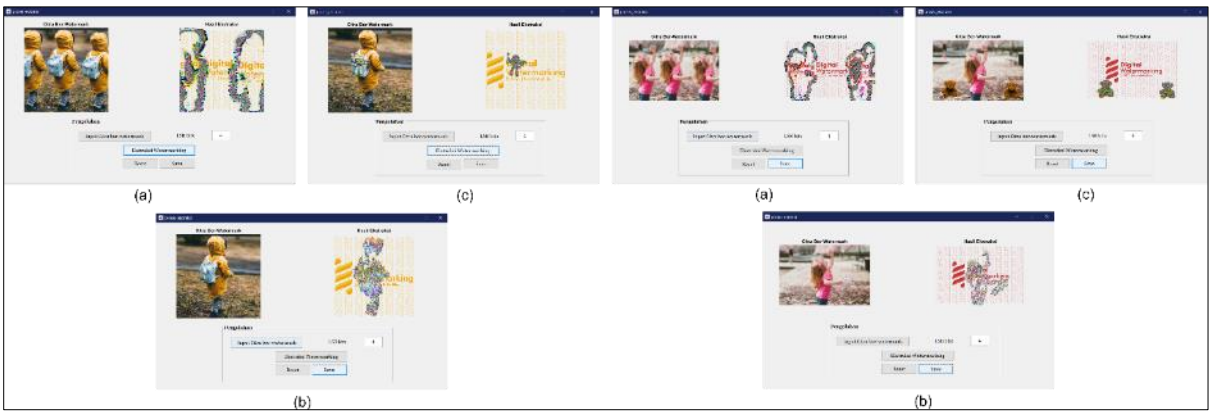


Gambar 4. Perubahan pada Citra Manipulasi (a) *copy-move*, (b) *splicing*, (c) *retouching*

Setelah proses manipulasi dilakukan, selanjutnya dilakukan proses ekstraksi. Pada tahap ini citra asli ber-*watermark* dan citra yang sudah dimanipulasi akan di ekstrak dengan tujuan untuk mengeluarkan kembali citra *watermark* yang ada di dalam citra *cover*. Untuk *watermark* yang telah berhasil di ekstrak, akan dilakukan perbandingan antara hasil ekstrak citra asli dan hasil ekstrak citra manipulasi.

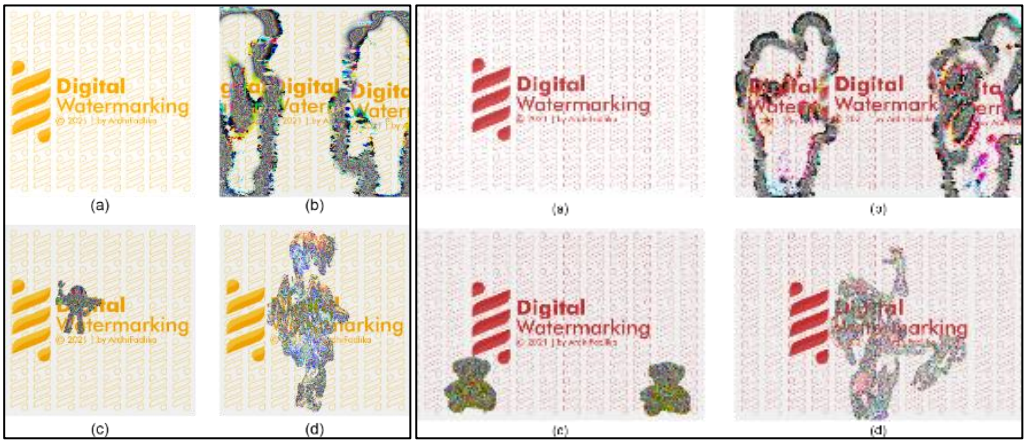
Gambar 5. Proses Ekstraksi Citra Asli

Pada Gambar 5 merupakan proses ekstraksi yang telah berhasil dilakukan dengan hasil *watermark* yang masih utuh tanpa kerusakan sedikit pun. Sedangkan pada Gambar 6 hasil ekstraksi dari citra yang telah dimanipulasi sebelumnya mengalami perubahan.



Gambar 6. Proses Ekstraksi Citra Manipulasi

Tahap implementasi dan Pengujian, dilakukan beberapa pengujian terhadap *watermark* hasil ekstraksi pada citra asli dan citra yang sudah dimanipulasi. Namun, agar lebih objektif dalam pengambilan kesimpulan ada beberapa parameter yang digunakan untuk menentukan apakah citra tersebut asil atau bukan. Selanjutnya, perbandingan citra *watermark* asli dan citra *watermark* hasil manipulasi dapat terlihat dengan jelas perbedaanya. Terlihat pada Gambar 7(a), merupakan *watermark* hasil ekstraksi pada citra asli. Pada Gambar 7(b) merupakan *watermark* hasil ekstraski pada citra manipulasi dengan teknik *copy*-move, Gambar7(c) *splicing*, Gambar7(d) *retouching*. Untuk hasil perbandingan dapat dilihat pada Gambar 7.



Gambar 7 Perbandingan Citra *Watermark* Asli dan Manipulasi (a) Asli (b) *Copy-Move* (c) *Splicing* (d) *Retouching*

Tahap selanjutnya adalah dilakukan pengujian dengan parameter *RMSE*, *MSE*, *PSNR* untuk membandigkan citra *watermark* yang asli dan citra *watermark* yang sudah dimanipulasi. Berdasarkan hasil perhitungan yang tertera pada tabel 4, dapat disimpulkan bahwa citra *watermarking* yang sudah di manipulasi mengalami perubahan yang cukup signifikan. Kesimpulan ini berdasarkan hasil nilai pada *MSE*, dan *RMSE* yang tidak mendekati nol, juga *PSNR* yang kurang dari sama dengan 30 dB.

Tabel 4. Hasil Perhitungan Kualitas pada Citra Watermak Termanipulasi

	Citra_Anak1			Citra_Anak2		
	MSE	***RMSE***	***PSNR***	***MSE***	***RMSE***	***PSNR***
Copy-move	211.175	14.5508	24.9071	208.9	14.4534	24.9654
Splicing	194.445	13.9444	25.2768	201.993	14.2124	25.1114
Retouching	200.759	14.1689	25.1381	202.606	14.234	25.0983

Seluruh kegiatan yang sudah dilakukan, dapat dirangkum hasilnya bahwa citra yang sudah termanipulasi dapat di deteksi dengan adanya kerusakan pada citra *watermark* yang sudah di ekstraksi dan hasil hitung kualitas citra dengan parameter *MSE, RMSE*, dan *PSNR* menunjukan bahwa kemiripannya sangat jauh ditunjukan dengan nilainya *MSE* dan *RMSE* yang tidak mendekati nol, dan nilai *PSNR* yang kurang dari 30 db.

Pembahasan

Syarat untuk bisa mendeteksi manipulasi citra pada simulasi ini harus dilakukan proses penyisipan/*embedd watermarking* pada citra yang akan dijadikan *cover* sebelum disebarkan dan digandakan. Proses ini dilakukan menggunakan metode LSB dengan cara memasukan citra *watermark* kedalam setiap bit pada citra *cover*, itulah mengapa dimensi citra *watermark* harus sama dengan dimensi citra *cover* agar prosesnya berhasil. Untuk memastikan bahwa proses ini berhasil, tidak boleh adanya perubahan yang signifikan pada citra *cover* sebeleum dan sesudah penyisipan. Maka dilakukan perhitungan kualitas citra dengan parameter nilai *MSE, RMSE,* dan *PSNR.*

Citra yang telah berhasil dilakukan penyisipan *watermark* telah siap disberkan dan digandakan. Maka dilakukan simulasi manipulasi pada citra tersebut dengan menggunakan *tools Adobe Photoshop.* Teknik manipulasi yang dilakukan adalah manipulasi *copy-move, splicing,* dan *retouching.* Saat proses ekstraksi dilakukan citra *watermark* yang asil tidak ada kerusakan sama sekali, sedangkan citra *watermark* yang sudah di manipulasi terdapat beberapa kerusakan pada bagian tertentu di dalam citra tersebut sesuai dengan serangan manipulasinya. Citra *watermark* asli dan citra *watermark* manipulasi dilakukan perhitungan kualitas citra dengan parameter yang sama saat proses *embedd watermarking* atau penyisipan, yaitu *MSE, RMSE,* dan *PSNR*. Dan hasilnya menunjukkan bahwa rata-rata nilai dari parameter *MSE* dan *RMSE* tidak mendekati nol sama sekali, begitu juga dengan nilai *PSNR* yang memiliki rata-rata <30 dB.

Penyisipan pesan tersembunyi berupa data dapat dilakukan ke dalam wadah citra digital berformat JPEG dan format citra digital lainnya, kemudian dapat mengekstraksi kembali data tersembunyi tersebut dari dalam citra digital (Hafiz, 2019). Sejalan dengan penelitian Kurniadi & Ariyus, (2020) yang melakukan watermarking media gambar dengan implementasi kombinasi Kriptografi dan Steganografi pada Teks Pesan menggunakan Algoritma Vigenere Cipher untuk pengamanan hak cipta. Aplikasi pada penelitian sebelumnya dapat digunakan untuk mengamankan gambar digital dengan penyisipan *watermark* berupa teks atau gambar ke dalam *file* gambar digital menggunakan metode *Least Significant Bit (LSB)* telah berhasil dilakukan (Putro & Febriani, 2017). Implementasi pada penelitian sebelumnya bahwa aplikasi penyembunyian pesan pada citra digital dengan menggabungkan algoritma *hill cipher* dan metode *least significant bit* (LSB) hasilnya aman dan tidak diketahui secara kasat mata, (Sari et al., 2017).

Pada penelitian ini merupakan penelitian simulasi dari sebuah kasus pelanggaran hak cipta yang dapat menyebabkan penyebaran hoaks pada citra manipulasi, dan dapat dilakukan otentikasi (*temper proofing*) oleh pemilik citra setelah proses ekstraksi dilakukan. Hal ini mengacu pada Pasal 12 Ayat 1 Undang-undang Hak Cipta (UUHC).

SIMPULAN

Berdasarkan penelitian yang sudah dilakukan sebelumnya, maka diketahui bahwa proses analisis manipulasi citra dapat dilakukan dengan baik menggunakan metode *Least Significant Bit.* Citra yang sudah dimanipulasi terdapat keruskan pada citra *watermark* saat proses ekstraksi dilakukan. Sehingga pemilik citra dapat melakukan otentikasi terhadap citra asli yang sudah di ekstrak. Namun penelitian ini masih harus dikembangkan dengan menggunakan objek digital lain seperti video, suara, dan lain-lain. Serta parameter yang digunakan bisa diganti dengan perhitungan yang lebih akurat.

REFERENSI

Ardiansyah, A., & Kurniasih, M. (2018). Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganograpi Menggunakan Metode Least Significant Bit. *Respati*, *13*(3), 96–101. https://doi.org/https://doi.org/10.35842/jtir.v13i3.258

Deeba, F., Kun, S., Dharejo, F. A., & Memon, H. (2020). Digital image watermarking based on ANN and least significant bit. *Information Security Journal: A Global Perspective*, *29*(1), 30–39.

Faroek, D. A., Umar, R., & Riadi, I. (2020). Deteksi Keaslian Citra Menggunakan Metode Error Level Analysis (ELA) dan Principal Component Analysis (PCA). *Format : Jurnal Ilmiah Teknik Informatika*, *8*(2), 132–137. https://doi.org/10.22441/format.2019.v8.i2.006

Febriani, S. R., & Irawati, D. C. (2017). Implementasi Digital Watermarking pada Citra Menggunakan Metode Least Significant Bit. *Jurnal Ilmiah Informatika Komputer*, *21*(3), 8–18.

Hafiz, A. (2019). Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, *17*(1), 194–198.

Kaur, R., & Kaur, S. (2016). Comparison of contrast enhancement techniques for medical image. *Conference on Emerging Devices and Smart Systems (ICEDSS)*, 155–159. Namakkal, India: IEEE.

Kurniadi, A., & Ariyus, D. (2020). Metode Pengamanan Hak Cipta Dengan Kriftografi Klasik Dan Kombinasi Teknik Digital Watermarking Menggunakan Metode Least Significant Bit (LSB). *Prosiding Seminar Nasional Teknologi Informasi Dan Komunikasi (SENATIK)*, *3*(1), 559–569.

Munir, R. (2019). *Kriptografi* (Vol. 2). Bandung: Informatika.

Pamungkas, A. (2017). *Cara Menghitung Nilai MSE, RMSE, dan PSNR pada Citra Digital*. Pemrogramanmatlab.Com. https://pemrogramanmatlab.com/2017/06/04/cara-menghitung-nilai-mse-rmse-dan-psnr-pada-citra-digital

Putro, B. W. A., & Febriani, F. (2017). Aplikasi Watermarking Dengan Metode Least Significant Bit Menggunakan Matlab. *Jurnal Ilmiah Informatika Komputer*, *21*(3), 1–7. https://www.ejournal.gunadarma.ac.id/index.php/infokom/article/view/1521

Rahmaniar, M., Saptono, H., & Njatrijani, R. (2019). Perlindungan Hak Cipta pada Karya Fotografi Produk Online Shop atas Tindakan Penggunaan Tanpa Izin untuk Kepentingan Komersial. *Diponegoro Law Journal*, *8*(3), 2177–2185.

Sari, J. I., Sulindawaty, & Sihotang, H. T. (2017). Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma HILL Cipher Dan Metode Least Significant BIT (LSB). *Jurnal Mantik Penusa*, *1*(2), 1–8.

Sari, T., Riadi, I., & Fadlil, A. (2016). Forensik Citra untuk Deteksi Rekayasa File Menggunakan Error Level Analysis. *Annual Research Seminar: Computer Science and Information and Communications Technology*, *2*(1), 133–138. https://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/821

Setiadi, D. R. I. M., Jatmoko, C., Rachmawanto, E. H., & Sari, C. A. (2018). Kombinasi DCT

dan Beaufort Chiper Untuk Peningkatan Keamanan Hak Cipta Citra Digital. *JST (Jurnal Sains Dan Teknologi)*, *7*(2), 188–197. https://doi.org/10.23887/jst-undiksha.v7i2.13795

Wijaya, A. Y., Al Musayyab, S., & Studiawan, H. (2017). Pengembangan Metode Block Matching Untuk Deteksi Copy-Move Pada Pemalsuan Citra. *JUTI J. Ilm. Teknol. Inf*, *15*(1), 84–94.

Zulfan, Arnia, F., & Muharar, R. (2016). Deteksi Pemalsuan Citra dengan Teknik Copy-Move Menggunakan Metode Ordinal Measure dari Koefisien Discrete Cosine Transform. *Jurnal Nasional Teknik Elektro*, *5*(2), 165–174.