Penggunaan Digital Watermarking pada Karya Citra NFT dan Analisis Kerentanan Terhadap Serangan

Rahmat Rafid Akbar - 13520090
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail) : 13520090@std.stei.itb.ac.id

***Abstract*— Karya NFT adalah aset digital unik yang menggunakan teknologi blockchain. Namun, masalah pemalsuan dan hilangnya keaslian karya digital menjadi tantangan bagi pembuat karya. Oleh karena itu, digital watermarking digunakan untuk menyisipkan tanda tangan digital yang unik pada karya NFT guna melindungi keaslian dan hak cipta. Sertifikat digital juga diberikan kepada pembuat karya sebagai bukti otentikasi dan kepemilikan karya. Makalah ini mengulas konsep digital watermarking, implementasinya dalam karya NFT, serta manfaatnya.**

***Keywords*— NFT; Sertifikat Digital; Tanda Tangan; Digitalisasi; Digital Watermarking; Karya Digital; Kriptografi;**

I. Latar Belakang

Perkembangan teknologi telah membawa kehidupan manusia satu tingkat lebih baik dari sebelumnya. Teknologi yang dikembangkan menghasilkan perangkat-perangkat yang memudahkan manusia dalam suatu urusuan dan pekerjaan. Salah satu teknologi yang paling berguna saat ini adalah perangkat elektronik. Perangkat elektronik memungkinkan kita menembus batasan dunia nyata dengan menggunakan jaringan internet. Manusia dapat berinteraksi satu sama lain tanpa memandang jarak dan waktu. Menyesuaikan dengan perkembangan teknologi yang makin mumpuni, banyak orang yang juga mengembangkan berbagai macam fitur-fitur yang ada di dunia nyata agar dapat diakses melalui perangkat elektronik seperti Handphone dan Komputer. Tak terlepas pula pada dampaknya terhadap perekonomian.

Saat ini, perekonomian tidak hanya terpusat dalam bentuk uang yang diterbitkan (uang riil). Sejak berkembangnya teknologi, pemegang kekuasaan cenderung melakukan investasi kekayaannya dalam bentuk digital seperti saham dan kriptocurrency. Hal ini dinilai untuk melakukan penyebaran dan pengembaganan kekeayaannya dalam segala sektor, termasuk sektor teknologi. Salah satu dampak pemakaian kekayaan terhadap aset digital adalah pada aset NFT yang baru-baru ini marak diperbincangkan di publik. Hal ini dikarenakan nilai jual-beli dari NFT ini sangat mencengangkan dan membuat banyak orang tergiur untuk ikut melakukan publikasi karya mereka sendiri.

NFT atau Non-Fungible Token sendiri adalah aset digital yang menggunakan teknologi blockchain untuk memberikan kepemilikan dan dan otentikasi yang unik terhadap suatu item digital, seperti gambar, video, atau karya seni. Namun, salah satu tantangan yang dihadapi oleh pembuat karya NFT adalah masalah tentang pemalsuan, pencurian, dan hilangnya keaslian karya digital mereka. Karya digital dapat dengan mudah disalin atau digandakan tanpa seizin pembuat aslinya. Ini dapat merugikan pembuat karya secara finansial dan merusak integritas serta nilai karya mereka.

Untuk mengatasi masalah ini, konsep digital watermarking dapat diterapkan dalam karya NFT. Digital watermarking adalah teknik yang digunakan untuk menyisipkan informasi tersembunyi ke dalam suatu file digital, seperti gambar atau video, tanpa mengganggu tampilan atau fungsionalitasnya. Watermark digital ini berfungsi sebagai tanda tangan digital atau cap khusus yang mengidentifikasi pembuat asli dan memberikan bukti otentikasi atas karya tersebut. Dengan menyisipkan watermark digital yang unik ke dalam karya NFT, setiap kali karya tersebut dipublikasikan, dibeli, atau ditransfer, tanda tangan digital akan tetap melekat pada karya tersebut. Ini memungkinkan untuk melakukan pelacakan dan verifikasi otentikasi terhadap karya NFT serta melacak asal usulnya.

Memang karya digital yang telah diberikan token NFT akan terjamin keasliannya dalam forum komunikasi terkait. Namun, apabila karya digital digunakan secara masif dan terhadap orang awam yang tidak paham akan NFT, maka tentunya akan terjadi tindak kriminal seperti pemalsuan dan lainnya.

II. Teori Dasar

A. Digital Watermarking

Digital watermarking adalah teknik yang digunakan untuk menyematkan informasi tersembunyi ke dalam data digital, seperti gambar, audio, video, atau dokumen lainnya. Tujuan utama dari digital watermarking adalah untuk memberikan keaslian, integritas, dan perlindungan hak cipta (copy right) atau kepemilikan terhadap konten digital. Selain itu dengan melakukan watermarking, karya digital juga dapat terhindar dari manipulasi atau penggunaan tanpa izin dari pemilik (dapat dilacak pemakaiannya). Penyisipan informasi tersembunyi berupa watermark ini digunakan sebagai penanda keaslian dan kepemilikan. Watermark yang dibubuhkan dapat berupa tanda tangan, logo, ataupun data lainnya.

Prinsip utama dari Digital Watermaking adalah sebagai berikut:

1. Authentication

Digital watermarking digunakan untuk membuktikan keaslian suatu konten digital. Dalam konteks ini, watermark yang disematkan berfungsi sebagai tanda tangan digital yang memverifikasi sumber atau pencipta asli dari konten tersebut. Dengan menggunakan algoritma kriptografi yang kuat, digital watermarking dapat menyematkan informasi rahasia yang hanya diketahui oleh pencipta asli, sehingga membuktikan keaslian dan keaslian konten tersebut.

2. Integrity

Digital watermarking digunakan untuk memastikan integritas konten digital. Dalam hal ini, watermark digunakan untuk mendeteksi apakah konten digital telah mengalami perubahan atau modifikasi yang tidak sah. Dengan menyematkan watermark yang sensitif terhadap perubahan, perubahan apa pun pada konten dapat dideteksi dengan membandingkan watermark yang disematkan dengan konten yang diubah. Jika ada perbedaan, dapat diasumsikan bahwa konten telah mengalami perubahan yang tidak sah.

3. Copyright Protection

Digital watermarking digunakan untuk memberikan perlindungan hak cipta terhadap konten digital. Dengan menyematkan watermark yang berisi informasi hak cipta atau identifikasi pemilik, konten digital dapat diidentifikasi kembali ke pemiliknya. Jika konten tersebut ditemukan tersebar secara tidak sah, pemilik dapat menggunakan watermark untuk membuktikan kepemilikan dan melindungi hak ciptanya.

4. Robustness

Digital watermarking juga mencakup ketahanan terhadap berbagai serangan atau transformasi yang dapat mempengaruhi kemampuan deteksi atau ekstraksi watermark. Digital watermarking harus mampu bertahan terhadap serangan seperti kompresi, perubahan format, cropping, rotasi, dan manipulasi lainnya, tetapi tetap dapat dipulihkan dengan akurasi yang tinggi.

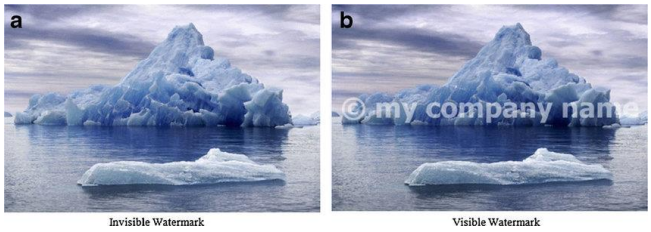
5. Capacity

Dalam digital watermarking, *capacity* mengacu pada jumlah informasi yang dapat disematkan dalam konten digital tanpa mengganggu kualitas visual atau audio yang signifikan. Tujuan dari digital watermarking adalah untuk menyematkan watermark seefektif mungkin tanpa mengorbankan kualitas atau mempengaruhi pengalaman pengguna.

B. *Image Watermarking*

Digital watermaking dalam konteks file citra mengharuskan watermark untuk disisipkan sebagai bagian dari gambar. Penyisipan ini sendiri dapat terlihat secara langsung dengan mata manusia (visible) maupun tersembunyi secara visual namun dapat diambil menggunakan metode tertentu (invisible).

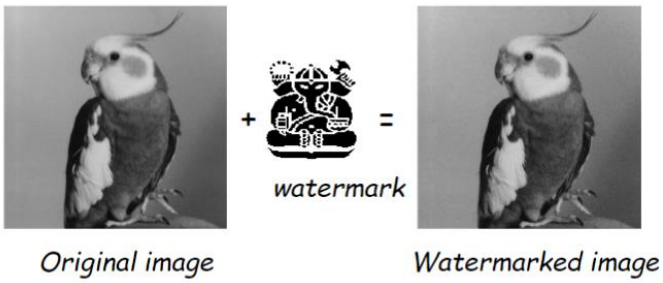
1. Visible watermaking



Gambar 2.1. Contoh Citra dengan Visible Watermark

Watermark jenis ini dapat terlihat secara langsung pada file citra. Penyisipan ini dilakukan dengan tujuan untuk menunjukkan kepada pemakai bahwa citra yang diambil memiliki hak cipta dan tidak bisa sembarangan dipakai tanpa izin pencipta. Selain itu, teknik ini dapat digunakan untuk identifikasi maupun branding sebuah produk/ jasa. Visible watermarking biasanya digunakan dalam industri seperti fotografi, penerbitan, atau distribusi konten digital yang membutuhkan identifikasi yang jelas dan tampak untuk melindungi hak cipta.

2. Invisible watermaking



Gambar 2.2. Contoh Citra dengan Invisible Watermark

Penyisipan ini dilakukan dengan tujuan untuk mengetahui keaslian, integritas, ataupun penelusuran atas pemakaian konten (jejak digital). Teknik ini menyisipkan watermark secara tak kasat mata namun tidak merusak koten dari gambar yang dapat ditangkap oleh mata manusia. Teknik ini dicapai dengan cara khusus baik untuk penyematan maupun ekstraksi watermark. menunjukkan kepada pemakai bahwa citra yang diambil memiliki hak cipta dan tidak bisa sembarangan dipakai tanpa izin pencipta. Watermark dapat terlihat secara langsung pada file citra. Invisible watermarking biasanay digunakan dalam bidang forensik digital, perlindungan hak cipta, atau manajemen hak digital, di mana keberadaan watermark tidak boleh terdeteksi oleh orang lain yang tidak berwenang.

Terdapat 2 kategori impementasi invisible watermarking berdasarkan tujuan pemakaiannya, yakni:

1. Fragile Watermarking (*rentan*)

Fragil watermarking digunakan untuk mengecek keaslian citra. Apabila dilakukan manipulasi pada file citra, maka watermark yang diberikan akan berubah dan tidak lagi sesuai dengan yang asli. Hal ini ditujukan untuk menjaga keaslian dan keabsahan data dan agar file citra tidak diedit dan digunakan untuk isu disinformasi.

Jenis metode yang dapat digunakan dalam implementasi fragil watermarking adalah **Metode Domain Spasial**. Metode ini langsung menyisipkan watermark ke dalam ruang piksel dari gambar asli. Salah satu metode yang umum digunakan adalah metode **LSB** (***Lease Significant Bit***), yang menggunakan perubahan bit-bit terakhir dari piksel gambar untuk menyimpan informasi watermark. Hal ini didasari bahwa tingkat kepekaan mata manusia tidak mengharuskan memiliki tingkat presisi tinggi untuk mengenali suatu warna.

2. Robust Watermarking (*tahan banting*).

Robust watermarking digunakan untuk mengklaim hak cipta sebagai penanda kepemilikan asli/ asal dari citra yang tersebar di publik. Watermark yang ditanamkan tidak dapat dihapus/ dihilangkan walaupun dilakukan manipulasi terhadap file citra. Hal ini ditujukan agar file citra tahan akan serangan seperti kompresi, pemotongan, penambahan, penghapusan, maupun pengeditan lainnya. Sehingga walaupun telah diedit sedemikian rupa, jejak digital (asal) citra dapat ditemukan.

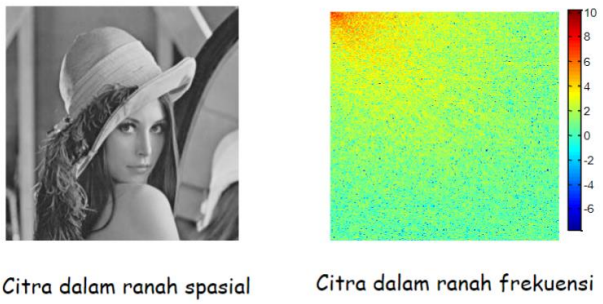
Jenis metode yang dapt digunakan dalam implementasi robust watermarking adalah **Metode Transformasi Domain**. Metode ini melibatkan transformasi domain gambar, seperti *Fourier Transformation* atau *Discrete Cosine Transform* (DCT), untuk menyematkan watermark. Dalam metode ini, domain frekuensi gambar digunakan untuk menyisipkan watermark, yang dapat menjadi lebih tahan terhadap serangan seperti kompresi.

C. Penggunaan Domain Transformation Method

Transformasi dilakukan menggunakan teknik *Discrete Cosine Transform* (DCT) dan menggunakan metode *Discrete Wavelet Transform* (DWT)

1. *Discrete Cosine Transform* (DCT)

Discrete Cosine Transform (DCT) adalah teknik untuk mengubah sebuah citra dari ranah spasial (setiap piksel merepresentasikan lokasi pada citra) ke ranah frekuensi (intensitas warna) dari bit gambar.



Gambar 2.3. Ilustrasi Domain Transform (domain spasial ke domain frekuensi)

Rumus yang dipakai untuk melakukan transformasi *encoding* (penyisipan) adalah sebagai berikut:

$$C(u,v) = a_u a_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} F(x,y) \cdot \cos\left(\frac{\pi(2x+1)u}{2M}\right) \cdot \cos\left(\frac{\pi(2y+1)v}{2N}\right)$$

$$dengan,$$

$$a_u = \begin{cases} \frac{1}{\sqrt{M}} & ,u = 0 \\ \sqrt{\frac{2}{M}}, & 1 \le u \le M-1 \end{cases} \quad dan \quad a_v = \begin{cases} \frac{1}{\sqrt{N}} & ,v = 0 \\ \sqrt{\frac{2}{N}}, & 1 \le v \le N-1 \end{cases}$$

Sementara untuk mendapatkan kembali watermark yang telah disisipkan melalui proses ekstraksi, digunakan rumus:

$$F(x,y) = a_u a_v \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} C(u,v) \cdot \cos\left(\frac{\pi(2x+1)u}{2M}\right) \cdot \cos\left(\frac{\pi(2y+1)v}{2N}\right)$$

III. RANCANGAN SOLUSI DAN IMPLEMENTASI

Rancangan implementasi digital watermaking pada citra NFT menggunakan algoritma modifikasi DCT dengan terlebih dahulu mengkonversi file citra. Berikut detail proses masing-masing bagian:

A. Embedding/ Watermaking

Berikut proses embedding watermark menggunakan algoritma modifikasi DCT:

1. Gambar asli dikonversikan ke dalam domain spasial (nilai RGB). Setiap piksel gambar akan memiliki nilai intensitas warna yang mewakili bagian dari gambar.

2. Bagi hasil konversi gambar menjadi blok-blok kecil, dalam hal ini menjadi NxN piksel (N = ukuran gambar/2/2piksel). Blok ini akan digunakan untuk melakukan transformasi DCT pada setiap blok.

3. Terapkan transformasi DCT pada setiap blok gambar. Transformasi DCT mengubah blok piksel menjadi koefisien-koefisien DCT yang mewakili frekuensi yang berbeda pada blok tersebut. Koefisien DCT yang paling signifikan umumnya mewakili frekuensi rendah, sedangkan koefisien yang kurang signifikan mewakili frekuensi tinggi.

4. Masukkan watermark (gambar) yang dikonversikan dalam ranah spasial ke dalam blok-blok gambar dengan memanipulasi beberapa koefisien DCT yang kurang signifikan. Operasi yang dapat dilakukan adalah penambahan atau pengurangan sejumlah kecil nilai koefisien DCT yang dipilih secara acak untuk mewakili bit-bit watermark.

5. Rekontruksi ulang gambar dengan melakukan inverse transformasi DCT pada semua blok gambar yang telah

dimodifikasi untuk mendapatkan gambar yang telah di-watermarking. Hasilnya adalah gambar baru yang berisi watermark yang telah disisipkan

Berikut adalah *source code* pada proses *embedding* pada kelas *DCT_Watermark*:

```
class DCT_Watermark():
    def __init__(self):
        self.Q = 10
        self.size = 2
        sig_size = 100

    @staticmethod
    def __gene_signature(wm, size):
        wm = cv2.resize(wm, (size, size))
        wm = np.where(wm < np.mean(wm), 0, 1)
        return wm

    def inner_embed(self, B: np.ndarray, signature):
        sig_size = self.sig_size
        size = self.size

        w, h = B.shape[:2]
        embed_pos = [(0, 0)]
        if w > 2 * sig_size * size:
            embed_pos.append((w-sig_size*size, 0))
        if h > 2 * sig_size * size:
            embed_pos.append((0, h-sig_size*size))
        if len(embed_pos) == 3:
            embed_pos.append((w-sig_size*size, h-sig_size*size))

        for x, y in embed_pos:
            for i in range(x, x+sig_size * size, size):
                for j in range(y, y+sig_size*size, size):
                    v = np.float32(B[i:i + size, j:j + size])
                    v = cv2.dct(v)
                    v[size-1, size-1] = self.Q * \
                        signature[((i-x)//size) * sig_size + (j-y)//size]
                    v = cv2.idct(v)
                    maximum = max(v.flatten())
                    minimum = min(v.flatten())
                    if maximum > 255:
                        v = v - (maximum - 255)
                    if minimum < 0:
                        v = v - minimum
                    B[i:i+size, j:j+size] = v
        return B

    def embed(self, cover, wm):
        B = None
        img = None
        signature = None

        if len(cover.shape) > 2:
            img = cv2.cvtColor(cover, cv2.COLOR_BGR2YUV)
            signature = self.__gene_signature(wm, self.sig_size).flatten()
            B = img[:, :, 0]

        if len(cover.shape) > 2:
            img[:, :, 0] = self.inner_embed(B, signature)
            cover = cv2.cvtColor(img, cv2.COLOR_YUV2BGR)
        else:
            cover = B
        return cover
```

B. *Extraction*

Pada proses ekstraksi, citra yang telah disisipkan watermark diperlakukan mirip dengan proses embedding. Perbedaannya adalah pengambilan nilai pada bit-bit dengan koefisien yang termodifikasi. Berikut proses ekstraksinya:

1. Gambar watermarked dikonversikan ke dalam domain spasial (nilai RGB). Setiap piksel gambar akan memiliki nilai intensitas warna yang mewakili bagian dari gambar.

2. Bagi hasil konversi gambar tersebut menjadi blok-blok kecil, sama seperti dalam proses embedding/ watermarking.

3. Terapkan transformasi DCT pada setiap blok gambar yang telah di-watermarking yang nantinya menghasilkan koefisien-koefisien DCT untuk setiap blok.

4. Lakukan pengidentifikasian koefisien-koefisien yang digunakan untuk watermark. Proses pencarian berdasarkan pola *v[size-1, size-1] > self.Q / 2*. Pola ini merupakan modifikasi yang sesuai dengan pembagian blok gambar. Hal ini juga nantinya ditentukan dengan nilai signifikansi dari koefisien DCT.

5. Lakukan ekstraksi watermark dengan mengkodekan semua bit-bit sisipkan pada koefisien DCT mengubahnya menjadi domain spasian dan menjadi bit-bit watermark.

6. Terakhir, rekonstruksi citra watermark dengan menggabungkan tiap piksel spasial menjadi gambar watermark utuh.

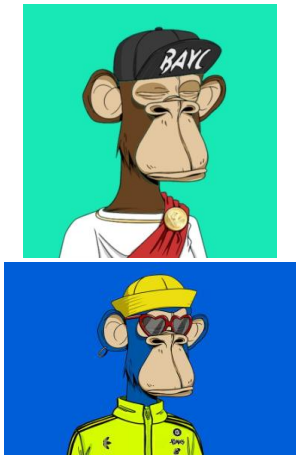
Berikut adalah *source code* pada proses *extraction* sebagai lanjutan kelas *DCT_Watermark*:

```
def inner_extract(self, B):
        sig_size = 100
        size = self.size

        ext_sig = np.zeros(sig_size**2, dtype=np.int)

        for i in range(0, sig_size * size, size):
            for j in range(0, sig_size * size, size):
                v = cv2.dct(np.float32(B[i:i+size, j:j+size]))
                if v[size-1, size-1] > self.Q / 2:
                    ext_sig[(i//size) * sig_size + j//size] = 1
        return [ext_sig]

def extract(self, wmimg):
        B = None
        if len(wmimg.shape) > 2:
            (B, G, R) = cv2.split(cv2.cvtColor(wmimg,
cv2.COLOR_BGR2YUV))
        else:
            B = wmimg
        ext_sig = self.inner_extract(B)[0]
        ext_sig = np.array(ext_sig).reshape((self.sig_size, self.sig_size))
        ext_sig = np.where(ext_sig == 1, 255, 0)
        return ext_sig
```

IV. PENGUJIAN DAN ANALISIS

Pengujian dilakukan untuk proses embedding, extraction, dan *attack abuse*. File yang digunakan dalam pengujian berupa NFT file citra yang dapat diambil dari situs https://opensea.io/. Namun perlu diingat bahwa file citra ini *tidak gratis* dan dapat dibeli dengan menggunakan

cryptocurrency. Untuk pengujian kali ini, terdapat beberapa file citra NFT yang telah diambil yakni:

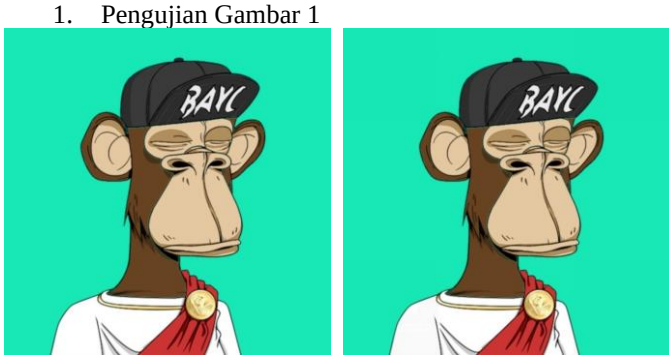


Gambar 4.1. File-File Citra NFT yang Diuji

Untuk file citra watermark yang akan digunakan adalah citra berikut:

Gambar 4.2. File Citra Watermark yang Diuji

1. Pengujian Gambar 1



58KB 88KB

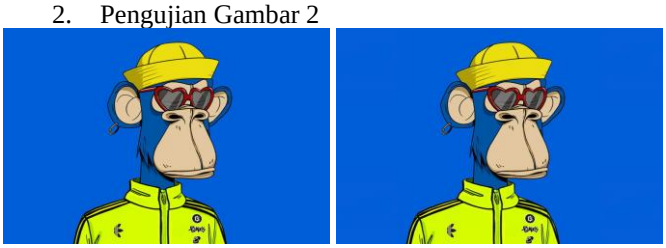
Gambar 4.3. Pengujian Watermarking 1

Dari hasil pengujian, terlihat bahwa ukuran file citra setelah watermarking (kanan) menjadi lebih besar dari citra orisinil (kiri) akibat penyisipan citra watermark. Namun, dapat dilihat pula bahwa kedua citra sama persis apabila dilihat dengan mata telanjang.

Gambar 4.4. Pengujian Extraction 1

Dari hasil pengujian, terlihat bahwa file citra watermark yang diekstraksi mirip dengan citra watermark awal. Perubaham minor yang terjadi akibat toleransi error dari teknik DCT.

2. Pengujian Gambar 2



57KB 109KB

Gambar 4.5. Pengujian Watermarking 2

Dari hasil pengujian, terlihat bahwa ukuran file citra setelah watermarking (kanan) menjadi lebih besar dari citra orisinil (kiri) akibat penyisipan citra watermark. Namun, dapat dilihat pula bahwa kedua citra sama persis apabila dilihat dengan mata telanjang.

Gambar 4.4. Pengujian Extraction 2

Dari hasil pengujian, terlihat bahwa file citra watermark yang diekstraksi mirip dengan citra watermark awal. Perubaham minor yang terjadi akibat toleransi error dari teknik DCT. Namun, perubahan yang terjadi berbeda dengan pengujian pada kasus 1, hal ini dikarenakan file orisinil berpengaruh terhadap koefisien-koefisien DCT.

3. Pengujian Serangan

Pengujian serangan dilakukan pada file citra pertama, serangan yang dilakukan adalah pemotongan bagian atas file citra sebanyak 10 pixel.

88KB 67KB

Gambar 4.7. Pengujian Attack Abuse pada Watermarked Image

Dari hasil pengujian, terlihat bahwa ukuran file citra setelah pemotongan (kanan) menjadi lebih kecil dari citra hasil watermarking awal. Namun, dapat dilihat pula bahwa kedua citra sama persis apabila dilihat dengan mata telanjang.

Gambar 4.4. Pengujian Extraction 1

Dari hasil pengujian, terlihat bahwa file citra watermark yang diekstraksi mirip dengan citra watermark awal. Perubaham minor yang terjadi akibat toleransi error dari teknik DCT. Namun, perubahan yang terjadi berbeda dengan pengujian pada kasus 1, hal ini dikarenakan file hasil serangan berpengaruh terhadap ektraksi koefisien-koefisien DCT, walaupun tidak mengubahnya secara masif.

V. Kesimpulan & Saran

Digital watermarking adalah sebuah teknik yang digunakan untuk menandai sebuah file digital baik berupa gambar, suara, video, maupun data lainnya. Dalam konteks Image Watermarking, terdapat banyak jenis watermarking berdasarkan tujuan penggunaannya seperti menjaga keaslian data ataupun menjaga hak cipta dari karya.

Salah satu teknik image watermarking adalah menggunakan metode Discrete Cosine Transform (DCT) yang mentransformasikan domain asli citra (domain spasial) ke domain baru (domain frekuensi). Berdasarkan hasil pengujian yang dilakukan pada citra NFT di atas, terbukti bahwa modifikasi algoritma DCT berhasil melakukan embedding/ watermaking hingga melakukan extraction. Tak terlepas pula saat diuji kerentananya. Ketika file citra hasil watermarking dipotong, watermark yang diekstrak terjaga.

Pembuatan program digital watermarking pada citra NFT diperlukan untuk citra yang disebarluaskan di luar platform jual belinya. Hal ini dapat menjadi indikator keabsahan bahwa citra tersebut asli ataupun tidak.

Namun, pengujian serangan belum dilakukan untuk semua testcase yang ada dan tipikal cover-image yang digunakan juga tidak lah beragam karena terbatas pada penggunaan cintra NFT. Program yang dirancang dapat sewaktu-waktu tidak bekerja pada file cover ataupun watermark tertentu sehingga diperlukan pengujian lebih lanjut dengan banyak sample data.

Semoga kedepannya dengan melakukan banyak pengujian kasus, program ini mempunyai cakupan yang lebih luas.

VI. Ucapan Terima Kasih

Penulis ingin mengucapkan terima kasih sebesar-besarnya kepada beberapa pihak yang telah berperan besar dalam penyelesaian makalah ini :

1. Tuhan Yang Maha Esa karena berkat dan rahmat-Nya, makalah ini dapat terselesaikan dengan baik tanpa kurang satu bagian pun.
2. Dr. Ir. Rinaldi, M.T. sebagai dosen kelas K1 karena telah membimbing penulis selama pembelajaran Kriptografi (IF-S1). Makalah IF4020 Kriptografi (IF-S1), – Sem. 2 Tahun 2022/2023
3. Teman-teman seangkatan karena telah memberikan dukungan selama perkuliahan sehingga penulis dapat menulis makalah ini dengan baik.

VII. References

[1] https://opensea.io/ (Diakses pada 28 Mei 2023)
[2] https://www.geeksforgeeks.org/digital-watermarking-and-its-types/ (Diakses pada 28 Mei 2023)
[3] https://www.geeksforgeeks.org/discrete-cosine-transform-algorithm-program/ (Diakses pada 28 Mei 2023)
[4] https ://www.elprocus.com/cryptography-and-its-concepts/ (Diakses pada 28 Mei 2023)
[5] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/10-Digital-watermarking-2023.pdf (Diakses pada 28 Mei 2023)

VIII. Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 28 Mei 2023

Rahmat Rafid Akbar—13520090