JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

ALGORITMA DISCRETE COSINE TRANSFORM UNTUK PENGAMANAN CITRA DIGITAL DENGAN OTP BERBASIS WEB

Imam Budi Setiawan[1], Latif Fajar Pramukti[2], Ahmad Tri Hidayat[3]

[1]Universitas Teknologi Yogyakarta, Temanggung 56222
[2]Universitas Teknologi Yogyakarta, Pacitan 63561
[3]Universitas Teknologi Yogyakarta, Sleman 55285
** Email Korespondensi: imamsetiawan110@gmail.com*

INFO ARTIKEL

Sejarah Artikel:
Diterima Tgl. 28/12/2022
Diperbaiki Tgl. 19/01/2023
Disetujui Tgl. 25/01/2023
Tersedia daring tgl. 28/01/2023

e-ISSN 2961-9009
p-ISSN 2963-1289

DOI : 10.58290/jukomtek.v1i2.52

ABSTRAK

Ketiadaan pengamanan *file* citra digital yang tersebar luas menimbulkan kerugian bagi pemilik asli. Citra tersebut akan mudah dimanipulasi karena tidak ada hak cipta yang melindungi *file* citra digital. Untuk melindung *file* tersebut, maka gambar akan diolah terlebih dahulu dengan menyisipkan watermark di dalamnya. Metode pengamanan gambar yang dipakai adalah *Discrete Cosine Transform* karena tahan terhadap berbagai macam manipulasi terutama kompresi. Proses watermark dilakukan dengan menggunakan web. Proses tersebut mengharuskan pengguna untuk membuat akun atau log in terlebih dahulu. Setelah itu, pengguna dapat memilih watermark yang kemudian diunggah untuk diverifikasi terlebih dahulu agar watermark tersebut valid sehingga proses penyisipan watermark dapat dilakukan. Setelah memilih gambar dan watermark, sistem mengirimkan kode OTP ke email aktif pengguna. Pengguna kemudian memasukkan kode OTP yang jika valid proses penyisipan akan dilanjutkan dan gambar siap untuk diunduh. Begitu juga dengan proses ekstraksi yang membutuhkan kode OTP. Dengan demikian, gambar hasil proses watermark dapat terlindungi dikarenakan adanya identitas yang menunjukkan kepemilikan sah dari gambar digital tersebut.

Kata Kunci:
Citra Digital, *Discrete Cosine Transform*, OTP, Watermark

PENDAHULUAN

Informasi dalam bentuk media saat ini dapat tersebar dengan cepat dikarenakan perkembangan teknologi yang pesat. Hal ini menyebabkan kerentanan terhadap perubahan dan kesempatan kepada pihak yang tidak bertanggung jawab untuk melakukan tindak kejahatan seperti duplikasi dan pembajakan data tanpa mencantumkan informasi dari pemilik *file* media tersebut. Pemegang hak cipta *file* digital tersebut dapat merasa dirugikan karena adanya tindak kejahatan yang dilakukan.

Perlindungan hak cipta dari file digital tersebut dapat dilakukan dengan berbagai

e-ISSN 2961-9009
p-ISSN 2963-1289

upaya. Salah satunya menggunakan watermark agar hak cipta dapat terlindungi. Watermark dilakukan dengan menyisipkan informasi seperti data citra atau teks tertentu ke dalam *file* digital sehingga hak ciptanya dapat terlindungi. Penelitian ini dilakukan untuk membuat prototipe web yang dapat melakukan proses watermarking. Pengekstrakan ini menyebabkan citra digital kehilangan bit tetapi kerusakannya tidak akan terlihat dengan jelas. Namun berbeda dengan data teks yang akan berpengaruh secara signifikan saat diekstrak. Terdapat beberapa metode untuk watermark. Metode *Dicrete Cosine Transform* (DCT) dapat menjadi yang dapat melindungi hak cipta pada citra digital (Agustina & Asmara, 2017).

Pemilihan Algoritma DCT dikarenakan ketahanannya terhadap manipulasi citra terutama kompresi. Teknik tersebut merupakan teknik klasik dalam kompresi gambar. DCT memecah gambar ke dalam berbagai frekuensi seperti frekuensi rendah, tengah, dan tinggi (Indera Krisdianto et al., 2022). Gambar tersebut nantinya ditransformasikan dari domain spasial menjadi domain frekuensi untuk penyisipan gambar atau informasi lainnya. Transformasi DCT 2D dapat menentukan posisi pada gambar yang akan disisipi watermark (Meliala, 2017).

Penyisipan watermark ke dalam citra digital dapat dilakukan setelah menempatkan posisinya. Kemudian proses watermark juga diintegrasikan dengan algoritma OTP sebagai otentikasi. Dengan demikian, metode ini mampu untuk melindungi hak cipta apabila terjadi permasalahan terkait dengan duplikasi atau pembajakan yang menjadikan pemilik asli atau pemegang hak cipta dirugikan.

LANDASAN TEORI

Citra digital didapatkan dari gambar maupun video yang berupa dua dimensi dari hasil analog dua dimensi secara kontinu menjadi sebuah gambar melalui proses sampling (Gani & Setiyono, 2019). Pembagian gambar analog menjadi N baris dan M kolom (Andono et al., 2017). Citra digital dapat diolah oleh komputer karena disimpan dalam bentuk angka yang menunjukkan besarnya intensitas pada setiap piksel (Munantri et al., 2020).

Digital watermarking adalah teknik penyembunyian data di mana informasi tertentu di sisipkan dalam sebuah data asli untuk melindungi data dari duplikasi secara ilegal pada data digital yang di distribusikan di internet (Susanto, 2019). Proses digital watermarking dilakukan dengan penambahan kode identifikasi ke dalam data digital berupa teks, suara, gambar, atau video secara permanen sehingga tidak dapat dihilangkan (Kristianingrum et al., 2022) (Cox et al., 2007). Kode identifikasi tersebut harus memiliki ketahanan terhadap berbagai proses atau manipulasi seperti pengubahan, kompresi, enkripsi, dan sebagainya.

Discrete Cosine Transform (DCT) adalah sebuah teknik yang mengubah sinyal ke dalam komponen frekuensi dasar adalah algoritma yang digunakan untuk membuat kompresi (lossy compression) yaitu penempatan data di mana tidak ada satu byte pun data yang hilang sehingga data tersebut utuh dan disimpan sesuai dengan aslinya (Krasmala et al., 2017). DCT merepresentasikan citra dengan penjumlahan sinusoidal dari frekuensi dan magnitude yang berubah (Britanak et al., 2007).

PSNR (Peak Signal to Noise Ratio) adalah nilai untuk menentukan kualitas citra yang dihasilkan steganografi, untuk menghitung nilai PSNR akan dihitung nilai Mean Square Error (MSE) terlebih dahulu, MSE adalah rata-rata nilai selisih error antara piksel citra asli dan piksel citra steganografi. PSNR diukur dalam desible units (db), semakin besar nilai PNSR yang dihasilkan oleh citra maka semakin baik kualitas citra tersebut, sebaliknya semakin kecil nilai PSNR yang dihasilkan maka kualitas citra akan semakin buruk (Kusumah et al., 2022).

Kode OTP merupakan salah satu cara transaksi dalam dunia digital sekarang yang di fungsikan sebagai PIN untuk keamanan log in

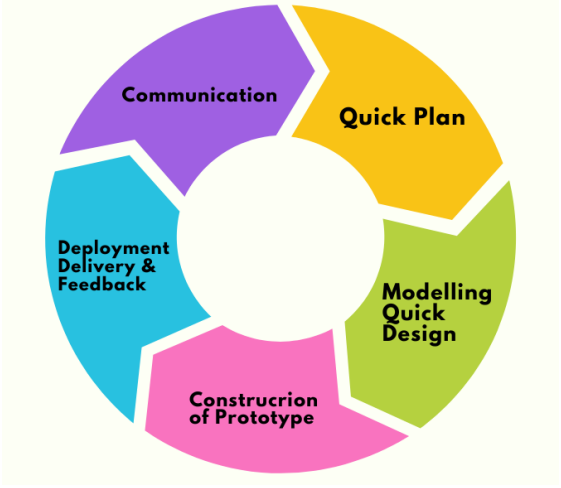
e-ISSN 2961-9009
p-ISSN 2963-1289

atau transaksi yang hanya digunakan untuk satu kali pemakaian (Fitriyansyah & Hazri, 2021). Biasanya Kode OTP atau PIN tersebut di kirim ke nomor telepon atau di hubungi ke telepon kita langsung. Teknologi ini adalah penambahan security untuk mengatasi pencurian informasi (Ungkawa et al., n.d.). Pada rancangan penelitian ini, proses watermarking diintegrasikan dengan OTP sehingga hak atas kepemilikan dan pengguna sebenarnya adalah pengguna yang sah dari sistem.

Flowchart merupakan langkah dan urutan prosedur dari suatu program yang digambarkan menggunakan grafik. Flowchart berguna dalam memecahkan masalah ke dalam banyak segmen yang kecil serta dapat menganalisis alternatif lain dalam memecahkan masalah ke dalam banyak segmen yang kecil serta dapat menganalisis alternatif lain dalam operasi (Ridlo, 2017).

METODE PENELITIAN

Penelitian ini mengimplementasikan metode prototipe. Metode pengembangan prototipe merupakan metode pengembangan perangkat lunak yang sering digunakan oleh pengembang agar dapat saling berinteraksi dengan pengguna selama waktu pembuatan sistem (Pressman, 2015). Gambar 1 berikut merupakan metode prototipe.



Gambar 1. Metode *Prototype*
Sumber: Ardiyansah et al., 2021

Langkah-langkah dari metode *prototype* adalah sebagai berikut:

Communication, penggalian informasi yang dilakukan oleh pengembang terhadap pengguna tentang berbagai kebutuhan agar sistem yang direncanakan dapat berjalan sesuai tujuan.

Quick Plan, perencanaan pembuatan prototipe dilakukan secara cepat dengan analisis. Langkah awal dalam perencanaan adalah mengidentifikasi kebutuhan dalam perancangan aplikasi. Langkah tersebut akan menentukan *input*, *output*, dan proses pada sistem sehingga sistem dapat menghasilkan *output* sesuai ekspektasi (Aditya et al., 2021).

Modeling Quick Design, tahapan ini merancang model dengan *tools* UML yang menjelaskan tentang alur, aktor, dan proses sistem pada aplikasi berbasis web.

Construction of Prototipe, perancangan *prototype* dibuat berdasarkan aspek yang terlihat pada representasi perangkat lunak. Rancangan ini terlihat oleh *end user* yang ditunjukkan oleh desain antarmuka.

Deployment Delivery & Feedback, evaluasi dan pengujian prototipe dilakukan menggunakan metode *black box*. Pengujian fungsionalitas sistem menjadi parameter yang menunjukkan kelayakan.

HASIL DAN PEMBAHASAN

Berdasarkan metode prototipe yang terdiri dari lima langkah yaitu *communicating, quick plan, modeling quick design, construction of prototype*, dan *deployment delivery & feedback*, penelitian ini membangun prototipe untuk proses watermark dengan OTP. Pembahasan membahas tentang bagaimana konsep, analisis, perencanaan, dan juga perancangan agar sistem dapat dibangun.

a. *Communication*

Informasi tentang kebutuhan sistem untuk proses penyisipan dan ekstraksi watermark serta pengiriman kode OTP melalui email. Dengan demikian sistem watermark

e-ISSN 2961-9009
p-ISSN 2963-1289

berbasis web dapat dibangun.

b. *Quick Plan*

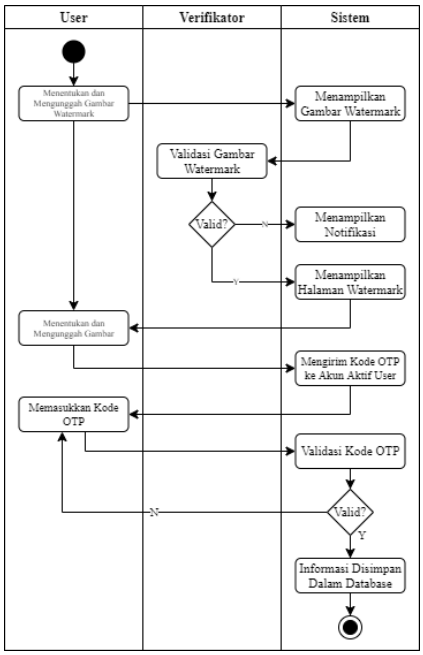
Perancangan sistem ini membutuhkan login, register, proses verifikasi watermark, proses watermarking, dan proses ekstraksi watermark.

1. Proses Login dan Register

Setiap pengguna diharuskan untuk memiliki akun. Jika pengguna belum memilikinya, maka pengguna diharuskan untuk melakukan register terlebih dahulu. *Input* yang dibutuhkan pada proses register adalah *username*, email, dan *password* sedangkan proses login *membutuhkan input username dan password*. Proses login dan register ditunjukkan pada Gambar 2.

2. Proses Watermarking

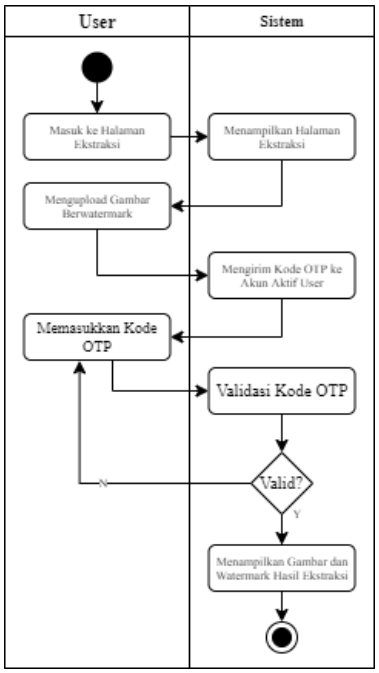
Pengguna menentukan gambar watermark untuk diunggah ke dalam sistem untuk dilakukan verifikasi. Jika pengguna sudah memiliki watermark yang ter-verifikasi maka proses watermarking dapat dilanjutkan. Sistem kemudian mengirim kode OTP setelah gambar dipilih. Kode OTP yang valid dimasukkan oleh pengguna sehingga proses watermarking dilakukan dan gambar dengan watermark dapat diunduh. Proses watermarking ditunjukkan pada Gambar 3.



Gambar 3. Proses Watermarking

3. Proses Ekstraksi

Jika pengguna sudah berada di halaman ekstraksi, pengguna diminta untuk mengunggah gambar untuk mendapat gambar watermark. Proses ini membutuhkan kode OTP yang dikirim melalui email. Jika *input* kode OTP yang valid maka gambar dan watermark akan ditampilkan. Gambar 4 menunjukkan proses ekstraksi.



Gambar 4. Proses Ekstraksi Watermark

Selain itu, terdapat kebutuhan fungsional dan kebutuhan non-fungsional.

1. Kebutuhan Fungsional

Kebutuhan fungsional merupakan kebutuhan yang berisi tentang proses-proses apa saja yang nantinya dilakukan oleh sistem. Kebutuhan fungsional juga berisikan tentang informasi-informasi apa saja yang harus ada dan dihasilkan oleh sistem. Berikut ini adalah kebutuhan fungsional dari sistem sebagai berikut:

a. Sistem dapat membaca masukan citra digital berupa foto dalam format JPG, PNG, dan BMP.
b. Sistem membaca watermark dalam bentuk citra grayscale.

e-ISSN 2961-9009
p-ISSN 2963-1289

c. Sistem mengirim Kode OTP sebelum melakukan proses watermark.
d. Sistem menghasilkan citra gambar yang telah di watermark.
e. Sistem dapat mendeteksi watermark yang ada pada citra gambar.
f. Sistem dapat melakukan pengekstrakan file citra yang sudah diberi watermark.

2. Kebutuhan Non-Fungsional

Pembangunan sistem ini didukung dengan perangkat keras dan perangkat lunak sehingga sistem dapat dirancang sebagai berikut:

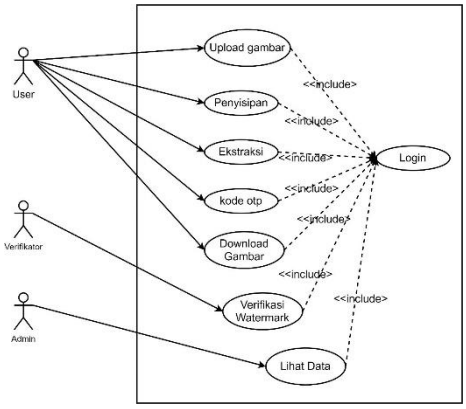
a. Kebutuhan perangkat keras,
   i. AMD Ryzen 5 3500U
   ii. RAM 8192 MB, 500 GB HDD
   iii. Radeon Vega 8 Graphics
b. Kebutuhan perangkat lunak
   i. Windows 10 Home
   ii. Draw.io
   iii. Microsoft Word
   iv. Sublime Text
   v. Google Chrome

c. *Modeling Quick Design*

Alur kerja dalam sistem dijelaskan menggunakan *Unified Modeling Language* (UML).

1. *Use Case*

Use case merupakan sudut pandang atau perspektif oleh pengguna yang menyatakan deskripsi fungsi sebuah sistem (Setiyani, 2021). Pada sistem watermark pengguna dapat melakukan beberapa proses yaitu unggah gambar, penyisipan dan ekstraksi watermark, mendapatkan kode OTP dan mengunduh gambar. *Use case* sistem ditunjukkan pada Gambar 5.



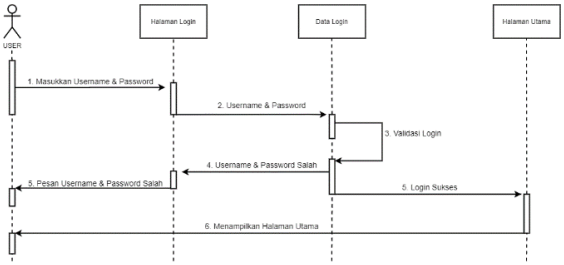
Gambar 5. *Use Case* Sistem Watermark

2. *Sequence Diagram*

Sequence diagram merupakan diagram yang menggambarkan interaksi yang terjadi antara objek antar elemen dari suatu *class* (Arianti et al., 2022).

a. *Sequence Diagram Login*

Alur sistem pada Gambar 6 pada saat pengguna melakukan *login* adalah dengan memasukkan *username* dan *password* kemudian divalidasi oleh sistem. Jika *login* sukses, sistem akan menampilkan halaman utama.

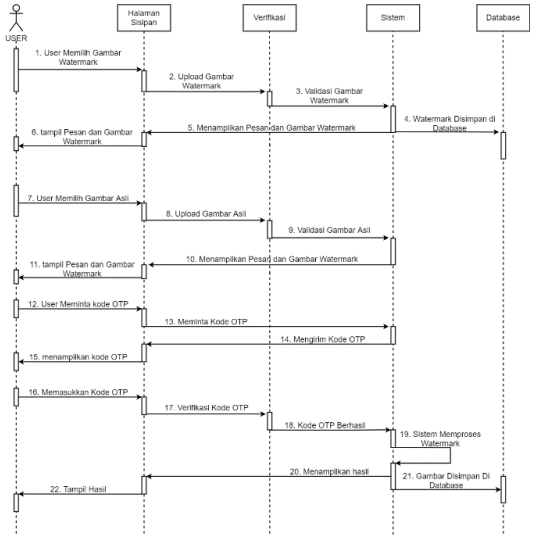


Gambar 6. *Sequence Diagram Login*

b. *Sequence Diagram* Penyisipan

Gambar 7 menunjukkan alur penyisipan watermark. Pengguna terlebih dahulu memilih watermark yang akan digunakan. Watermark tersebut divalidasi dan jika berhasil akan dimasukkan ke dalam *database*. Untuk proses watermark, pengguna memilih gambar asli kemudian memilih watermark yang akan disisipkan. Sistem akan otomatis mengirim kode OTP dan meminta pengguna untuk memasukkan kode tersebut. Jika kode valid maka proses akan dilanjutkan dan gambar ber-watermark dapat diunduh oleh pengguna.

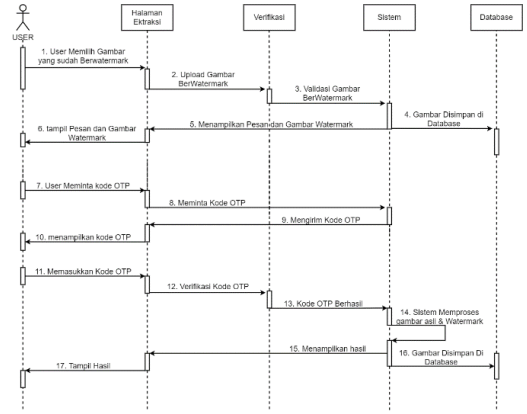
e-ISSN 2961-9009
p-ISSN 2963-1289



Gambar 7. *Sequence Diagram* Watermarking

c. *Sequence Diagram* Ekstraksi

Proses ekstraksi dilakukan pengguna dengan memilih gambar yang telah disisipkan watermark. Kemudian sistem akan mengirimkan kode OTP ke email pengguna dan pengguna diminta memasukkan kode tersebut. Jika kode valid maka proses ekstraksi akan dilakukan. Gambar 8 menunjukkan proses ekstraksi.

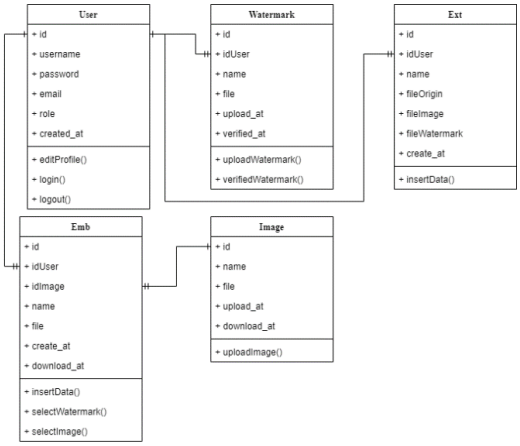


Gambar 8. *Sequence Diagram* Ekstraksi

3. *Class Diagram*

Class diagram merupakan sebuah spesifikasi dengan instansiasi yang menghasilkan objek dan merupakan inti dari pengembangan dan desain berorientasi objek (Arianti et al., 2022).

Pada sistem yang dibangun, terdapat beberapa *class*. *Class user* berhubungan dengan beberapa class yang lain. Hubungan dengan *class watermark* karena user dapat mengunggah beberapa watermark. User dapat melakukan penyisipan (*Class* Emb) dengan memilih gambar pada *class image* sehingga kedua class tersebut tentunya berelasi. *Class* ext (ekstraksi) memiliki hubungan dengan *class user* karena *user* dapat melakukan proses ekstraksi. *Class* diagram sistem watermarking ditunjukkan pada Gambar 9.



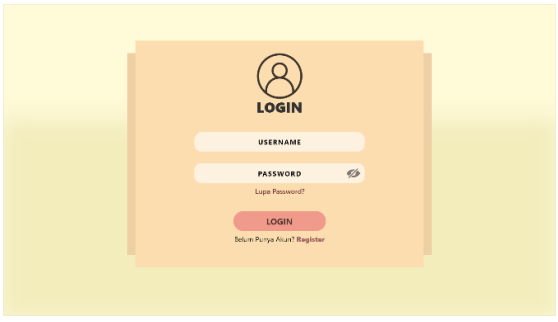
Gambar 9. *Class Diagram* Sistem Watermark

d. *Construction of Prototipe*

Konsep, analisis dan perencanaan yang telah dibuat kemudian diimplementasikan ke dalam bentuk rancangan tampilan aplikasi.

1. Halaman *Login*

Untuk masuk ke dalam sistem, pengguna diharuskan melakukan *login* terlebih dahulu. Pengguna mengisikan *username* dan *password* sehingga dapat masuk ke halaman *home*. Tampilan halaman *login* ditunjukkan pada Gambar 10.



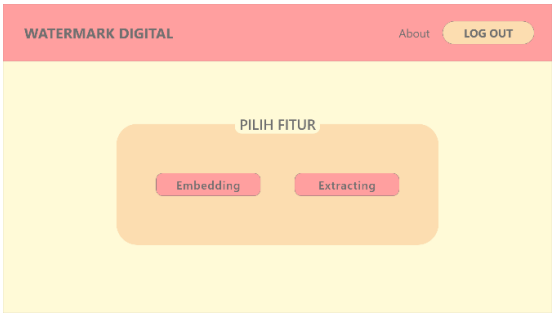
Gambar 10. Halaman Login

2. Halaman *Home*

Gambar 11 menunjukkan tampilan

e-ISSN 2961-9009
p-ISSN 2963-1289

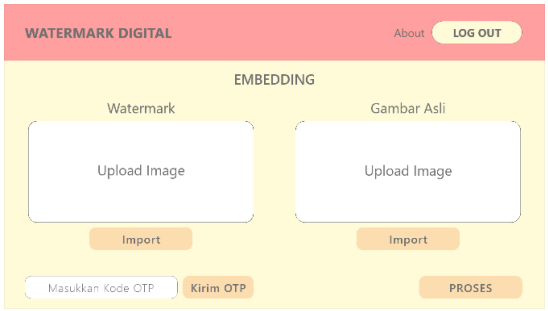
halaman *home*. Pada halaman ini pengguna dapat memilih proses *embedding* atau *extracting*. Masing-masing proses akan diarahkan ke halaman yang berbeda.



Gambar 11. Halaman *Home*

3. Halaman *Embedding*

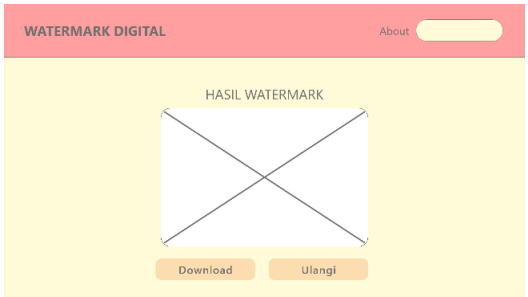
Proses watermark dilakukan pada halaman ini. Pengguna diharuskan untuk mengunggah gambar watermark dan gambar asli. Kemudian pengguna diminta untuk memasukkan kode OTP yang valid dari email.



Gambar 12. Halaman *Embedding*

4. Halaman Hasil Watermark

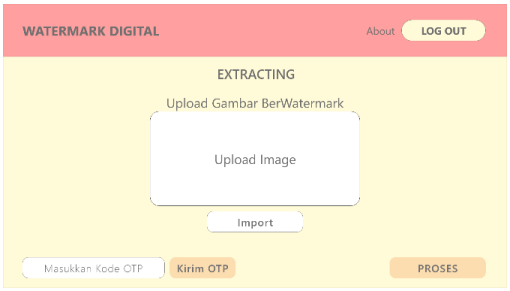
Halaman ini menampilkan gambar yang telah diberi watermark. Pengguna dapat mengunduh atau mengulangi proses dengan menekan tombol yang ada. Halaman hasil watermark ditunjukkan pada Gambar 13



Gambar 13. Halaman Hasil *Embedding*

5. Halaman Extracting

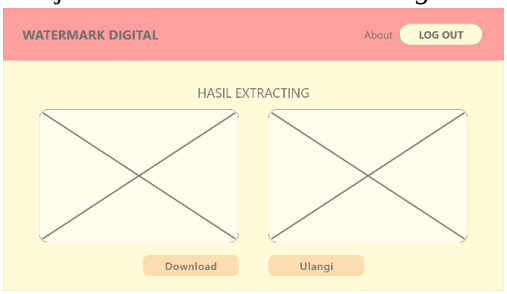
Pengguna memilih gambar dengan watermark di dalamnya yang akan diekstrak. Proses ini juga menggunakan kode OTP yang dikirim melalui email. Tampilan halaman *extracting* ditunjukkan pada Gambar 14.



Gambar 14. Halaman Ekstraksi

6. Halaman Hasil *Extracting*

Setelah pengguna menekan tombol proses pada halaman *extracting*, halaman hasil akan ditampilkan beserta watermark dan gambar tanpa watermark. Gambar 14 menunjukkan halaman hasil *extracting*.



Gambar 10. Halaman Hasil Ekstraksi

e. *Deployment Delivery & Feedback*

Evaluasi sistem dilakukan dengan menggunakan *black box* testing. Metode *black box* testing adalah pengujian yang melihat hasil eksekusi melalui data uji dan memastikan fungsi dari *software*. Metode *black box* testing mempunyai beberapa teknik pengujian, yaitu *Sample Testing*, *Boundary Value Analysis*, *Equivalence, Partitions* dan lain-lain (Febrian et al., 2020)

Tabel 1. Hasil Pengujian Metode *Black Box*

No.	Penguji-an	Hasil	Kesimpul an
1	*Usernam e* dan *password* diisi	Menampilkan halaman *home*	Valid

e-ISSN 2961-9009
p-ISSN 2963-1289

	dengan benar		
2	*Username* dan/atau *password* diisi dengan data yang salah	Muncul pesan kesalahan	Valid
3	Gambar watermark yang diunggah *grayscale*	Gambar masuk ke dalam sistem	Valid
4	Gambar watermark yang diunggah berwarna atau non-*grayscale*	Muncul pesan kesalahan	Valid
5	Kode OTP yang dimasukkan benar	Menampilkan hasil	Valid
6	Kode OTP yang dimasukkan salah	Muncul pesan kesalahan	Valid
7	Tombol *logout* ditekan	Menampilkan halaman *login*	Valid
8	Tombol *download* ditekan	Gambar diunduh dan tersimpan dalam *device*	Valid
9	Tombol ulangi ditekan	Menampilkan halaman awal proses	Valid
10	Gambar diimpor dengan menekan tombol impor	Menampilkan Windows Explorer untuk mencari *file* dan menampilkannya di halaman tersebut	Valid

KESIMPULAN

Kesimpulan yang didapatkan adalah sebagai berikut; Prototipe watermark berbasis web ini memudahkan dalam implementasi watermark ke dalam gambar yang ingin dilindungi hak cipta dan keasliannya.

OTP menjadikan sistem digunakan dengan email yang valid sehingga kepemilikan gambar menjadi jelas dan akurat.

Validasi watermark dilakukan setelah pengguna mengunggah gambar watermark sehingga gambar merupakan tanda kepemilikan bukan gambar sembarang sehingga sistem ini sangat berguna sebagai penyedia watermark yang valid.

ACKNOWLEDGEMENTS

Paper ini merupakan hasil dari penelitian seminar tematik mahasiswa Latif Fajar Pramukti dan Imam Budi Setiawan.

DAFTAR PUSTAKA

Aditya, R., Handrianus Pranatawijaya, V., & Bagus Adidyana Anugrah Putra, P. (2021). Rancang Bangun Aplikasi Monitoring Kegiatan Menggunakan Metode Prototype. *Jointecoms (Journal Of Information Technology And Computer Science)*, *1*(1).

Agustina, R., & Asmara, R. A. (2017). Penyisipan Watermark Menggunakan Metode Discrete Cosine Transform Pada Citra Digital. *Jurnal Informatika Polinema*, *2*(1), 29. Https://Doi.Org/10.33795/Jip.V2i1.51

Andono, P. N., Sutojo, T., & Others. (2017). *Pengolahan Citra Digital*. Penerbit Andi.

Ardiyansah, D., Pahlevi, O., & Santoso, T. (2021). Implementasi Metode Prototyping

e-ISSN 2961-9009
p-ISSN 2963-1289

Pada Sistem Informasi Pengadaan Barang Cetakan Berbasis Web. *Hexagon Jurnal Teknik Dan Sains*, *2*(2), 17–22.

Arianti, T., Fa'izi, A., Adam, S., Wulandari, M., & Aisyiyah Pontianak, P. '. (2022). Perancangan Sistem Informasi Perpustakaan Menggunakan Diagram Uml (Unified Modelling Language). In *Doi: …* (Vol. 1, Issue 1).

Britanak, V., Rao, K. R., & Yip, P. C. (2007). *Discrete Cosine And Sine Transforms*. Elsevier. Https://Doi.Org/10.1016/B978-0-12-373624-6.X5000-0

Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2007). *Digital Watermarking And Steganography*. Morgan Kaufmann.

Febrian, V., Ramadhan, M. R., Faisal, M., & Saifudin, A. (2020). Pengujian Pada Aplikasi Penggajian Pegawai Dengan Menggunakan Metode Blackbox. *Jurnal Informatika Universitas Pamulang*, *5*(1), 61–66.

Fitriyansyah, A. Y., & Hazri, M. (2021). *Analisis Security Web Login Mahasiswa Menggunakan Algoritma Two-Factor Time-Based One Time Password*. Yogyajakarta. Jurnal Penelitian Dan Pengkajian Sains Dan Teknologi.

Gani, S., & Setiyono, B. (2019). Teknik Invisible Watermarking Digital Menggunakan Metode Dwt (Discrete Wavelet Tarnsform). *Jurnal Sains Dan Seni Its*, *7*(2). Https://Doi.Org/10.12962/J23373520.V7i2.29845

Indera Krisdianto, Y., Agutina, M., & Jenderal Ahmad Yani No, J. (2022). *Watermarking Dengan Metode Discrete Cosine Transform (Dct) Untuk Menjaga Keamanan Citra Digital*.

Krasmala, R., Budimansyah, A., & Lenggana, U. T. (2017). Kompresi Citra Dengan Menggabungkan Metode Discrete Cosine Transform (Dct) Dan Algoritma Huffman. *Jurnal Online Informatika*, *2*(1), 1. Https://Doi.Org/10.15575/Join.V2i1.79

Kristianingrum, V., Faishal, M., & Yuda Irawan, A. S. (2022). Systematic Literature Review: Rancang Bangun Image Digital Watermarking. *Jbmi (Jurnal Bisnis, Manajemen, Dan Informatika)*, *19*(1), 48–60. Https://Doi.Org/10.26487/Jbmi.V19i1.20246

Kusumah, K. D., Pragantha, J., & Perdana, N. J. (2022). *Steganography Implementation Of Insertion Of Confidential Data On Digital Image Media With Bit-Plane Complexity Segmentation Method And Vigenere Cipher Extended Encryption Method*.

Meliala, B. O. (2017). *Implementasi Digital Watermarking Pada File Jpeg Dengan Metode Discrete Cosine Transform*. Universitas Kristen Duta Wacana.

Munantri, N. Z., Sofyan, H., & Florestiyanto, M. Y. (2020). Aplikasi Pengolahan Citra Digital Untuk Identifikasi Umur Pohon. *Telematika*, *16*(2), 97. Https://Doi.Org/10.31315/Telematika.V16i2.3183

Pressman, R. S. (2015). Rekayasa Perangkat Lunak: Pendekatan Praktisi Buku I. Yogyakarta. *Indonesia: Penerbit Andi*.

Ridlo, I. A. (2017). Panduan Pembuatan Flowchart. *Fakultas Kesehatan Masyarakat*, *11*(1), 1–27.

Setiyani, L. (2021). Desain Sistem: Use Case Diagram. *Prosiding Seminar Nasional Inovasi Dan Adopsi Teknologi (Inotek)*, *1*(1), 256–260.

Susanto, A. (2019). Uji Ketahanan Image Watermarking Dari Metode Chinese Remainder Theorem(Crt) Dengan Deteksi Tepi Canny Untuk Citra Rabbani. *Jurnal Teknik Elektro*, *12*(2), 100–106. Https://Doi.Org/10.26418/Elkha.V11i2.34793

Ungkawa, U., Amelia Dewi, I., & Ramadhan Putra, K. (N.D.). *Implementasi Algoritma Time-Based One Time Password Dalam Otentikasi Token Internet Banking*.