

Perancangan Aplikasi Watermarking Citra Digital Menggunakan Algoritma Playfair Dan Algoritma Dynamic Cell Spreading (Dcs)

Digital Image Watermaking Application Design Using Playfair Algorithm And Dynamic Cell Spreading Algorithm (Dcs)

Khalid Arifin Harahap ^{a,1}, Heri Gunawan ^{b,2}

^{a,b}Program Studi Informatika

Universitas Potensi Utama, K.L. Yos Sudarso KM 6,5 No. 3A Tj. Mulia - Medan

e-mail: kalidarifin97@gmail.com¹, herigunawan@gmail.com²

ABSTRAK

Steganografi dan Kriptografi merupakan salah satu teknik yang digunakan untuk menjaga keamanan data. Steganografi adalah seni yang digunakan untuk menyisipkan pesan rahasia kedalam media, dimana pesan rahasia hanya disisipkan pada sebuah citra digital tanpa merubah bentuknya, sehingga orang lain tidak menyadari bahwa di dalam citra digital terdapat pesan rahasia. Cabang dari ilmu steganografi adalah digital watermarking. Digital watermarking merupakan salah satu solusi yang digunakan untuk melindungi hak cipta dengan menggunakan teknik penyisipan informasi ke dalam media data digital seperti video, audio, teks dan citra secara rahasia. Untuk meningkatkan keamanannya pada penelitian ini juga menggunakan teknik kriptografi dimana watermark akan disandikan terlebih dahulu sebelum di sisipkan kedalam citra digital. Pada penelitian ini untuk melindungi kepemilikan sebuah citra digital proses tersebut akan dilakukan menggunakan algoritma playfair dan algoritma dynamic cell spreading (DCS). Dimana teks watermark akan disandikan terlebih dahulu menggunakan algoritma playfair kemudian teks yang sudah disandikan kemudian disisipkan pada citra digital menggunakan algoritma dynamic cell spreading (DCS).

Kata Kunci : Steganografi, Kriptografi, Algoritma Dynamic Cell Spreading(DCS) dan Algoritma Playfair

ABSTRACT

Steganography and Cryptography are techniques used to maintain data security. Steganography is an art that is used to insert a secret message into the media, where the secret message is only inserted into a digital image without changing its shape, so that other people do not realize that in the digital image there is a secret message. The branch of steganography is digital watermarking. Digital watermarking is one of the solutions used to protect copyright by using techniques to insert information into digital data media such as video, audio, text and images in a confidential manner. To increase security, this research also uses cryptographic techniques where the watermark will be encoded before being inserted into the digital image. In this study, to protect the ownership of a digital image, the process will be carried out using the Playfair algorithm and the dynamic cell spreading (DCS) algorithm. Where the watermark text will be first encoded using the Playfair algorithm, then the encoded text is then inserted into the digital image using the dynamic cell spreading (DCS) algorithm.

Keywords : Steganography, Cryptography, Dynamic Cell Spreading Algorithm (DCS) and Playfair Algorithm

Info Artikel :

Disubmit: 10 Des 2022

Direview: 8 Jan 2023

Diterima : 30 Jan 2023

Copyright © 2023 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Saat ini keamanan merupakan hal yang sangat penting pada sistem informasi. Karena pesatnya perkembangan teknologi dan ilmu pengetahuan sehingga memungkinkan munculnya teknik baru yang salah satunya digunakan sehingga dapat mengancam keamanan sistem informasi tersebut. Maka dari itu timbul suatu gagasan yakni membuat suatu sistem keamanan yang dapat digunakan untuk

menjaga dan melindungi data penting dengan cara menyandikan data sehingga pihak-pihak lain sulit untuk mendeteksi data tersebut.

Perlindungan hak cipta memiliki beberapa pendekatan salah satunya yaitu digital *watermarking*, digital *watermarking* menjadi salah satu solusi yang digunakan untuk melindungi data dengan teknik penyisipan (*embedding*) maksudnya yaitu menyisipkan media yang tidak terlihat pada sebuah citra. Nantinya dari citra tersebut dapat terlihat apakah data tersebut telah disalahgunakan oleh pihak lain tanpa izin. Banyaknya teknik yang dilakukan untuk menjaga keamanan data dan informasi salah satunya Steganografi dan Kriptografi. Steganografi merupakan seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara ke dalam suatu media tanpa mengubah bentuknya, sehingga orang lain atau pihak lain tidak dapat mengetahui bahwa di dalam citra digital tersebut terdapat pesan rahasia. Penelitian ini juga menerapkan teknik kriptografi yang digunakan untuk meningkatkan keamanan, dimana watermark akan disandikan terlebih dahulu sebelum disisipkan pada citra digital.

Berdasarkan penelitian Sri Wahyuningsih, et. al., 2016. Penelitian tersebut menghasilkan sebuah aplikasi watermarking yang terlihat pada citra digital. Sedangkan pada penelitian yang dilaksanakan ini watermark yang akan diterapkan tidak kasat mata pada citra digital. [1]

Berdasarkan penelitian Dedek Dwi Santoso, 2018. Hasil dari penelitian tersebut yaitu merancang aplikasi yang digunakan untuk melakukan *enkripsi* dan *dekripsi* sebuah file teks dengan *Algoritma Rijndael* menggunakan penyandian kunci dengan *Algoritma Playfair*. Sedangkan penelitian yang akan dibuat, yaitu menggunakan *Algoritma Playfair* akan digunakan untuk menyandikan teks *watermark*. [2]

Berdasarkan penelitian Wamiliana, et. al., 2017. Penelitian tersebut menghasilkan sebuah aplikasi berbasis *website* untuk membandingkan hasil steganografi antara metode *DCS* dengan *Spread Spectrum*. Sedangkan penelitian yang dilakukan ini adalah algoritma *DCS* yang digunakan dalam proses watermarking citra digital. [3]

Berdasarkan penelitian Marthin dan Taronisokhi, 2016. Penelitian tersebut menghasilkan sebuah aplikasi untuk menyisipkan teks pada sebuah citra digital. Sedangkan pada penelitian yang dilaksanakan algoritma *DCS* akan dikombinasikan dengan *algoritma Playfair* agar pesan disandikan terlebih dahulu sebelum disisipkan pada citra digital. [4]

Berdasarkan penelitian Rivaldi Kristianto Hondro, 2020. Hasil dari penelitian tersebut yaitu membuat sebuah aplikasi yang digunakan untuk melakukan *enkripsi* dan *dekripsi* teks menggunakan *algoritma Playfair*. Adapun perbedaan dari penelitian sebelumnya, yaitu pada penelitian yang akan dilaksanakan *Algoritma Playfair* akan dikombinasikan dengan *algoritma DCS* untuk memberi *watermark* tak terlihat pada citra digital. [5]

Berdasarkan penelitian Yemima Kristiana Br. Simbolon, 2019. Hasil dari penelitian ini yaitu membuat sebuah aplikasi untuk mengamankan *file PDF* menggunakan *algoritma Playfair*. Yang menjadi perbedaan dengan penelitian ini adalah pada penelitian ini algoritma *Playfair* akan digunakan untuk mengamankan teks *watermark*. [6]

Pada penelitian ini untuk melindungi dan mengamankan kepemilikan sebuah citra digital akan digunakan algoritma *Playfair* dan algoritma *Dynamic Cell Spreading (DCS)*. Dimana teks *watermark* akan disandikan terlebih dahulu menggunakan algoritma *Playfair* dan selanjutnya teks yang telah disandikan akan disisipkan pada citra digital menggunakan algoritma *Dynamic Cell Spreading (DCS)* tanpa mengubah bentuk dari citra tersebut.

Oleh sebab itu akan dibangun sebuah aplikasi yang dapat digunakan untuk melindungi hak kepemilikan atas sebuah citra digital, untuk menyisipkan media tak kasat mata ke dalam sebuah citra digital menggunakan kombinasi algoritma *Playfair* dan algoritma *Dynamic cell spreading (DCS)*. Untuk itu penelitian ini akan menarik sebuah judul “Perancangan Aplikasi Watermarking Citra Digital Menggunakan *Algoritma Playfair* dan *Algoritma Dynamic Cell Spreading (DCS)*”

2. METODE

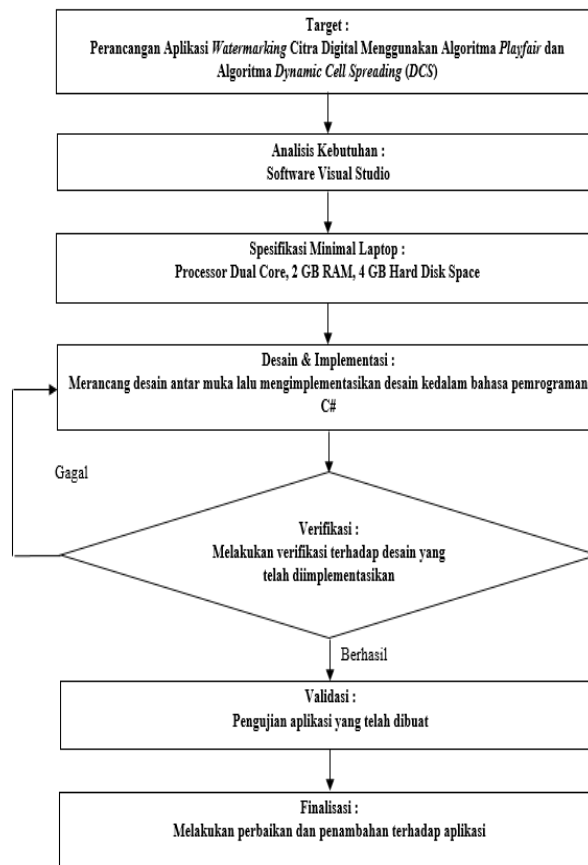
Untuk dapat mengimplementasikan sistem, maka secara garis besar digunakan beberapa metode sebagai berikut :

A. Metode Pengumpulan Data

- 1) Studi Literatur, dengan cara mempelajari acuan dan literatur yang berhubungan dengan materi dalam penulisan skripsi. Acuan yang digunakan umumnya adalah tentang cara penyusunan skripsi pada Universitas Potensi Utama dan juga jurnal-jurnal tentang studi pustaka yang digunakan dalam penulisan skripsi.
- 2) Pengamatan, yaitu melakukan pengamatan langsung dengan cara melihat beberapa contoh aplikasi berbasis desktop seperti *script* program bahasa pemrograman yang selanjutnya akan dituangkan kedalam bahasa pemrograman C#. kemudian simpulkan data dan informasi yang didapat..

B. Metode Perancangan Sistem

Untuk mencapai tujuan sebaiknya perhatikan beberapa langkah pada gambar 1.



Gambar 1. Prosedur Perancangan

Keterangan Gambar :

1. Analisis Kebutuhan

Setelah melewati tahapan perancangan, langkah berikutnya yaitu menganalisa kebutuhan. Untuk membangun aplikasi ada beberapa yang harus diperlukan seperti perangkat lunak, perangkat keras. Adapun untuk perancangan aplikasi, yang dibutuhkan seperti komputer, laptop dan visual studio.

2. Spesifikasi

Penelitian ini menggunakan perangkat keras dan perangkat lunak yang memiliki spesifikasi sebagai berikut :

a. Perangkat Keras (Hardware)

Spesifikasi perangkat keras yang dapat digunakan yaitu :

- 1) Laptop : Dual Core
- 2) RAM 2 GB

- 3) *Hard disk* : 4 GB
- b. Perangkat lunak (Software)

Spesifikasi Software yang digunakan untuk merancang aplikasi ini yaitu :

 - 1) Visual Studio
 - 2) Sistem operasi minimal Windows 7
3. Desain dan Implementasi

Pada tahap ini dirancang sebuah desain antar muka dari aplikasi *watermarking* citra digital menggunakan algoritma *Playfair* dan algoritma *Dynamic Cell Spreading (DCS)*. Bagaimana desain yang akan digunakan pada antarmuka perangkat dekstop. Setelah melakukan perancangan desain aplikasi tahap berikutnya yaitu melakukan implementasi terhadap desain yang telah dirancang kedalam bahasa pemrograman.
4. Verifikasi

Verifikasi dilakukan untuk pengecekan ulang apakah aplikasi yang dibuat sesuai dengan apa yang dirancang sebelumnya. Apakah desain yang dirancang dapat diimplementasikan kedalam bahasa pemrograman.
5. Validasi

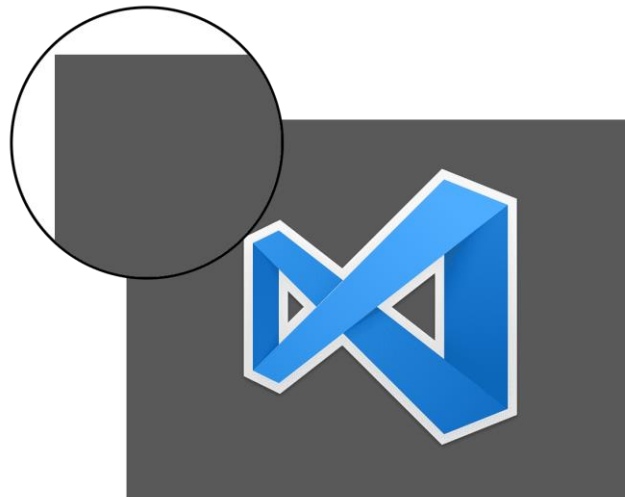
Pada tahap ini dilakukan pengujian aplikasi *watermarking* citra digital menggunakan algoritma *playfair* dan algoritma *dynamic cell spreading (DCS)* secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan aplikasi. Pengujian fungsional dilakukan untuk mengetahui bahwa aplikasi *watermarking* citra digital menggunakan algoritma *playfair* dan algoritma *dynamic cell spreading (DCS)* telah berjalan dengan sesuai dengan perancangan. Pengujian ketahanan merupakan kemampuan aplikasi untuk berjalan dengan baik pada spesifikasi minimum komputer atau laptop sesuai dengan yang telah dicantumkan.
6. Finalisasi

pada saat melakukan tahapan validasi dapat dilihat apakah aplikasi yang dihasilkan ini perlu dilakukan perbaikan dan pengembangan. Jika masih terdapat kesalahan- kesalahan maka perlu dilakukan perbaikan, sedangkan pengembangan dapat dilakukan apabila aplikasi yang dihasilkan dapat berjalan secara optimal saat memproses *watermarking* citra digital.
- a. Studi Kasus

Pada penelitian ini akan diterapkan kombinasi algoritma *Playfair* dan algoritma *Dynamic Cell Spreading (DCS)* untuk menanamkan dan mengekstrak *watermark* tak kasat mata pada citra digital. Kombinasi kedua algoritma tersebut dalam proses *watermarking* dapat dilihat sebagai berikut :

Teks *watermark* : KHALID
 Kunci : CITRA

Citra digital yang akan digunakan untuk proses *watermarking* adalah sebagai berikut :



- Tahap pertama adalah mengambil nilai piksel dari bagian kiri atas ke kanan sebanyak yang dibutuhkan untuk digunakan sebagai media penyisipan pesan.

- Dari gambar tersebut di dapat nilai RGB dari piksel adalah R = 89, G = 89, B = 89.
- Selanjutnya sebagian piksel dari citra digital tersebut di konversikan ke dalam bentuk biner untuk menanamkan teks *watermark* di dapatkan nilainya sebagai berikut :

R	G	B	R	G	B	R	G	B
01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001
01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001
01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001
01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001
01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001
01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001

1. Proses Watermarking

- Tambahkan kunci ke dalam tabel kunci bujur sangkar dengan ketentuan sebagai berikut :
 - Buang huruf J jika ada dan huruf-huruf yang berulang, agar menjadi : CITRA.
 - Tambahkan huruf-huruf yang belum ada kecuali huruf J, yang akan menjadi : CITRABDEFGHKLMNOPQRSUVWXYZ.
 - Memasukkan kunci tersebut ke dalam tabel kunci bujur sangkar.

Tabel 1. Tabel Kunci Bujur Sangkar

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

- Ubah teks *watermark* dengan cara melakukan proses enkripsi ke dalam bentuk pasangan menjadi : KH AL ID.
 - Pasangan huruf pertama **KH** menjadi **LK** dapat dilihat pada tabel III.2.

Tabel 2. Enkripsi Pasangan Huruf Pertama

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

Enkripsi KH menjadi LK dikarenakan posisi pasangan huruf plainteks berada pada baris yang sama sehingga cipherteks dihasilkan dengan mengambil pasangan huruf sebelah kanan KH ke arah kiri disesuaikan dengan pasangan huruf KH sehingga di dapat cipherteks LK.

- Pasangan huruf kedua **AL** menjadi **TN** dapat dilihat pada tabel III.3.

Tabel 3. Enkripsi Pasangan Huruf Kedua

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N

O	P	Q	S	U
V	W	X	Y	Z

Enkripsi AL menjadi TN di dapat sesuai dengan persilangan panah yang terdapat pada tabel.

- 3) Pasangan huruf ketiga **ID** menjadi **DK** dapat dilihat pada tabel III.4.

Tabel 4. Enkripsi Pasangan Huruf Ketiga

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

Enkripsi ID menjadi DK dapat dilihat berdasarkan tanda panah merah yang mewakili plainteks dan tanda panah biru yang mewakili cipherteks. Teks *watermark* **KHALID** menjadi **LKTNDK** setelah melalui proses enkripsi menggunakan algoritma *Playfair*.

- c. Selanjutnya teks *watermark* hasil enkripsi menggunakan algoritma *Playfair* di tanamkan pada sebuah citra digital menggunakan algoritma *Dynamic Cell Spreading (DCS)* sebagai berikut :
- 1) Langkah pertama ubah teks *watermark* yang telah di enkripsi ke dalam bentuk biner sebagai berikut :

L	=	0	1	0	0	1	1	0	0
K	=	0	1	0	0	1	0	1	1
T	=	0	1	0	1	0	1	0	0
N	=	0	1	0	0	1	1	1	0
D	=	0	1	0	0	0	1	0	0
K	=	0	1	0	0	1	0	1	1

- 2) Langkah selanjutnya adalah mengganti setiap bit ke 8, 16 dan 24 setiap piksel dengan nilai piksel teks *watermark* sehingga di hasilkan :

R	G	B	R	G	B	R	G	B
01011000	01011001	01011000	01011000	01011001	01011001	01011000	01011000	01011000
01011001	01011000	01011000	01011001	01011000	01011001	01011001	01011000	01011001
01011000	01011001	01011000	01011001	01011000	01011000	01011000	01011001	01011000
01011000	01011001	01011001	01011001	01011000	01011000	01011001	01011000	01011000
01011000	01011001	01011000	01011000	01011000	01011001	01011000	01011000	01011001
01011000	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001

Nilai piksel pada gambar yang berubah hanyalah pada bit paling akhir sehingga tidak mengubah citra digital secara kasat mata.

2. Proses Ekstraksi

Proses ekstraksi dilakukan untuk menampilkan identitas pemilik yang terdapat pada citra digital. Dalam proses ekstraksi, langkah pertama yang dilakukan adalah ekstraksi menggunakan algoritma *Dynamic Cell Spreading (DCS)*.

- a. Proses ekstraksi menggunakan algoritma *Dynamic Cell Spreading (DCS)* dapat dilihat sebagai berikut :

Nilai piksel citra digital :

R	G	B	R	G	B	R	G	B
01011000	01011001	01011000	01011000	01011001	01011001	01011000	01011000	01011000
01011001	01011000	01011000	01011001	01011000	01011001	01011001	01011000	01011001
01011000	01011001	01011000	01011001	01011000	01011000	01011000	01011001	01011000
01011000	01011001	01011001	01011001	01011000	01011000	01011001	01011000	01011000
01011000	01011001	01011000	01011000	01011000	01011001	01011000	01011000	01011001
01011000	01011001	01011001	01011001	01011001	01011001	01011001	01011001	01011001

Proses ekstraksi dilakukan dengan mengambil nilai setiap bit ke 8, 16 dan 24 pada citra digital yang memiliki watermark dan mengubah setiap 8 bit yang di dapat ke dalam nilai ASCII sehingga di dapatkan teks watermark sebagai berikut :

0	1	0	0	1	1	0	0 = L
0	1	0	0	1	0	1	1 = K
0	1	0	1	0	1	0	0 = T
0	1	0	0	1	1	1	0 = N
0	1	0	0	0	1	0	0 = D
0	1	0	0	1	0	1	1 = K

Dari proses ekstraksi watermark di dapatkan teks watermark **LKTNDK**.

- b. Tahap selanjutnya melakukan proses dekripsi menggunakan algoritma *Playfair* untuk menampilkan informasi asli dari watermark yang di dapat dalam proses ekstraksi.

Teks watermark : LKTNDK

Kunci : CITRA

- 1) Tabel kunci bujur sangkar akan dimasukkan kunci dengan ketentuan sebagai berikut :
 - a) Buang huruf J jika ada dan juga huruf-huruf yang berulang, agar menjadi : CITRA.
 - b) Tambahkan semua huruf-furuf yang belum ada, kecuali huruf J, kemudian akan menjadi : CITRABDEFGHKL MNOPQSU VWXYZ.
 - c) Memasukkan kunci tersebut ke dalam tabel kunci bujur sangkar.

Tabel 5. Tabel Kunci Bujur Sangkar

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

- 2) Lakukan proses dekripsi dengan cara mengubah teks watermark ke dalam bentuk pasangan menjadi : LK TN DK.

- a) Pasangan huruf pertama **LK** menjadi **KH** dapat dilihat pada tabel III.6.

Tabel 6. Dekripsi Pasangan Huruf Pertama

C	I	T	R	A
B	D	E	F	G
H ←	K ←	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

b) Pasangan huruf kedua **TN** menjadi **AL** dapat dilihat pada tabel III.7.

Tabel 7. Dekripsi Pasangan Huruf Kedua

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

c) Pasangan huruf ketiga **DK** menjadi **ID** dapat dilihat pada tabel III.8.

Tabel 8. Dekripsi Pasangan Huruf Ketiga

C	I	T	R	A
B	D	E	F	G
H	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

Setelah melakukan proses dekripsi menggunakan algoritma *Playfair* di dapat informasi asli dari pemilik citra digital adalah **KHALID**.

3. HASIL DAN PEMBAHASAN

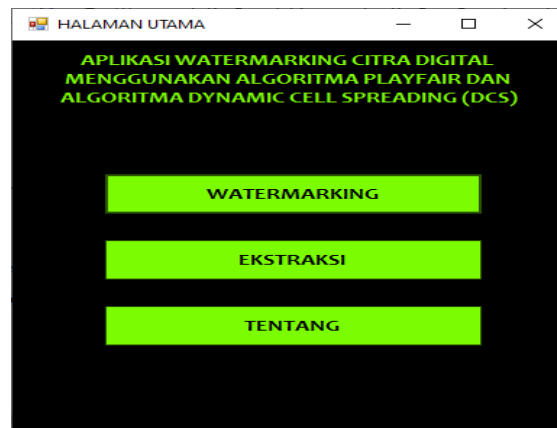
Adapun hasil dari pengujian yang dilakukan pada laptop adalah aplikasi yang dibuat atau dirancang sebagai berikut :

A. Hasil

Pada bab ini akan dijelaskan tampilan hasil dari aplikasi yang telah dibuat, yang digunakan untuk memperjelas tentang tampilan-tampilan yang ada pada aplikasi *watermarking* citra digital menggunakan algoritma *Playfair* dan algoritma *Dynamic Cell Spreading (DCS)*. Sehingga hasil implementasinya dapat dilihat sesuai dengan hasil program yang telah dibuat. Dibawah ini akan dijelaskan tiap-tiap tampilan yang ada pada program.

1. Tampilan Halaman Utama

Tampilan ini merupakan halaman yang akan tampil pertama kali saat aplikasi dijalankan. Pada halaman ini terdapat tombol *menu watermarking*, *menu ekstraksi*, dan tombol *menu Tentang*.



Gambar 2. Tampilan Halaman Utama

2. Tampilan *Form Watermarking*

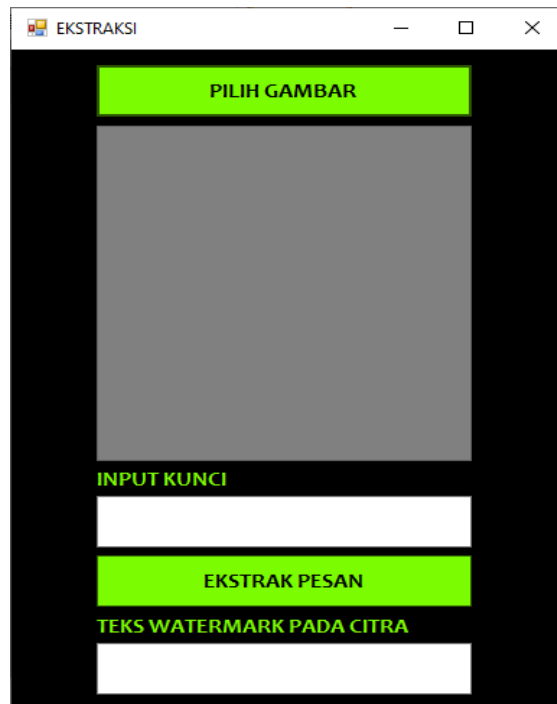
Halaman tambah *watermark* digunakan untuk proses penambahan teks *watermak* ke dalam sebuah citra atau gambar.



Gambar 3. Tampilan *form Watermarking*

3. Tampilan *Form Ekstraksi*

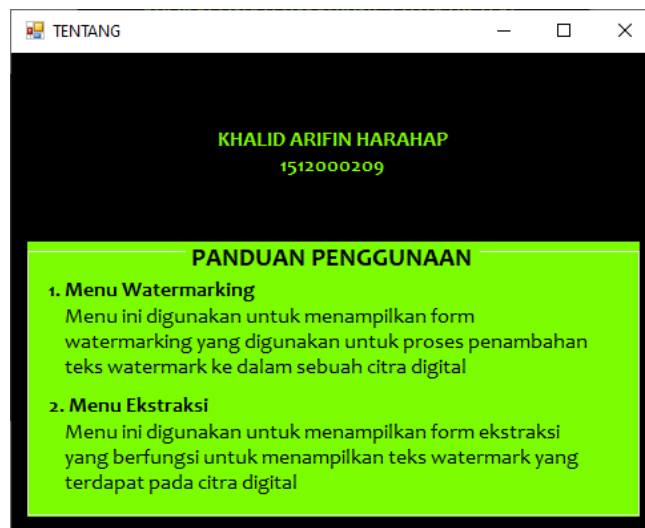
Halaman ekstraksi *watermark* digunakan untuk melakukan ekstraksi teks yang terdapat pada citra atau gambar



Gambar 4. Tampilan Halaman Ekstraksi Watermark

4. Tampilan *Form* Tentang

Halaman panduan digunakan untuk menampilkan informasi tentang peneliti dan tentang aplikasi yang dihasilkan pada penelitian ini.



Gambar 5. Tampilan Halaman Panduan

B. Pembahasan

1. Kelebihan dan Kekurangan

Kelebihan dan kekurangan dari hasil rancangan tentang aplikasi *watermarking* citra digital menggunakan algoritma *Playfair* dan algoritma *Dynamic Cell Spreading (DCS)* yang telah dibangun dapat penulis simpulkan sebagai berikut :

a. Kelebihan Aplikasi

Yang menjadi kelebihan dari aplikasi yang dihasilkan pada penelitian ini adalah sebagai berikut :

- 1) Aplikasi yang dihasilkan dapat digunakan untuk melakukan proses *watermarking* dan ekstraksi teks *watermarking* pada citra digital menggunakan algoritma *Dynamic Cell Spreading (DCS)*.
- 2) Pada aplikasi juga diterapkan algoritma *Playfair* untuk menyandikan teks *watermark* yang akan disisipkan pada citra digital.

b. Kekurangan Aplikasi

Aplikasi yang dirancang pada penelitian ini tidak terlepas dari beberapa kekurangan antara lain :

- 1) Aplikasi yang dihasilkan dikembangkan menggunakan bahasa pemrograman #C (C Sharp) sehingga hanya dapat digunakan pada perangkat desktop dan tidak dapat digunakan pada perangkat *mobile* seperti *smartphone*.
- 2) Tidak ada menu yang dapat digunakan untuk menyimpan kata kunci yang digunakan dalam proses *watermarking* sehingga pengguna harus selalu mengingat kata kunci yang digunakan dalam proses *watermarking*.

4. KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba aplikasi yang telah dilakukan dalam melakukan proses *watermarking* dan ekstraksi, dapat disimpulkan :

1. Hasil dari aplikasi yang dibuat dari penelitian ini dapat digunakan untuk menambahkan teks *watermark* tak kasat mata pada sebuah citra digital.
2. Aplikasi yang dihasilkan juga dapat digunakan untuk proses ekstraksi teks *watermark* yang telah ditambahkan pada citra digital.
3. Proses *watermarking* dan ekstraksi pada aplikasi dilakukan menggunakan algoritma *Playfair* dan algoritma *Dynamic Cell Spreading (DCS)*.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada Universitas Potensi Utama yang telah membantu penulis dalam menyelesaikan laporan penelitian ini.

DAFTAR PUSTAKA

- [1] Wahyuningsih, Sri, Pandex, Theodora. V.d, & Stefanny. V. (2016). *Implemetasi Visible Watermarking Dan Steganografi Least Significant Bit* pada File Citra Digital. *Jurnal Telematika MIKOM Vol.8*
- [2] Santoso, Dedek. D. (2018). *Penerapan Algoritma Playfair Cipher Sebagai Penyandian Kunci Dalam Pengamanan File Teks Dengan Algoritma Rijndael*, Jurnal Pelita Informatika, Vol. 17, No. 1, Hal. 59-64.
- [3] W. Wamiliana, Hijriani. A, Ningtyas.P.U. (2017). Perbandingan Metode *Dynamic Cell Spreading (DCS)* dan *Spread Spectrum* Pada Steganografi Berbasis Aplikasi Web. *Jurnal Komputasi*, Vol.5, (1)
- [4] Marthin dan Taronisokhi, 2016, *Penerapan Metode Dynamic Cell Spreading(DCS) Untuk Menyembunyikan Teks Tersandi Pada Citra*, Prosiding Seminar Nasional Inovasi dan Teknologi Informasi, Hal. 766-770.
- [5] Hondro, Rivalri.K. (2020). Modifikasi Platform Kunci Algoritma *Playfair* Untuk Meningkatkan Nilai *Confusion* Pada *Ciphertext*. *Jurnal Of Computer System And Informatics*. Vol. 1 (2)
- [6] Br. Simbolon. Y.K. (2019). Perancangan Aplikasi Pengamanan File PDF Menggunakan Algoritma *Playfair Cipher*. *Jurnal Informasi dan Teknologi Ilmiah*