ANALISIS PERBANDINGAN DUA DAN EMPAT LEVEL *GRAYSCALE* SERTA ARUCO *MARKER* DALAM PENGEMBANGAN CDP PADA SQR

SKRIPSI

Disusun oleh:

Ade Firmansyah
19/440303/TK/48630

PROGRAM STUDI TEKNOLOGI INFORMASI
DEPARTEMEN TEKNIK ELEKTRO DAN TEKNOLOGI INFORMASI
FAKULTAS TEKNIK UNIVERSITAS GADJAH MADA
YOGYAKARTA
2023

HALAMAN PENGESAHAN

ANALISIS PERBANDINGAN DUA DAN EMPAT LEVEL *GRAYSCALE* SERTA ARUCO *MARKER* DALAM PENGEMBANGAN CDP PADA SQR

SKRIPSI

Diajukan Sebagai Salah Satu Syarat untuk Memperoleh
Gelar Sarjana Teknik
pada Departemen Teknik Elektro dan Teknologi Informasi
Fakultas Teknik
Universitas Gadjah Mada

Disusun oleh:

Ade Firmansyah
19/440303/TK/48630

Telah disetujui dan disahkan

Pada tanggal . . . . . .

Dosen Pembimbing I	Dosen Pembimbing II
Syukron Abu Ishaq Alfarozi, S.T., Ph.D.	**«Nama Dosen»**
1111 9920 5202 10 1 102	**«NIP xxxxxx»**

PERNYATAAN BEBAS PLAGIASI

Saya yang bertanda tangan di bawah ini :

Nama	:
NIM	:
Tahun terdaftar	:
Program Studi	:
Fakultas	: Teknik Universitas Gadjah Mada

Menyatakan bahwa dalam dokumen ilmiah Skripsi ini tidak terdapat bagian dari karya ilmiah lain yang telah diajukan untuk memperoleh gelar akademik di suatu lembaga Pendidikan Tinggi, dan juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang/lembaga lain, kecuali yang secara tertulis disitasi dalam dokumen ini dan disebutkan sumbernya secara lengkap dalam daftar pustaka.

Dengan demikian saya menyatakan bahwa dokumen ilmiah ini bebas dari unsur-unsur plagiasi dan apabila dokumen ilmiah Skripsi ini di kemudian hari terbukti merupakan plagiasi dari hasil karya penulis lain dan/atau dengan sengaja mengajukan karya atau pendapat yang merupakan hasil karya penulis lain, maka penulis bersedia menerima sanksi akademik dan/atau sanksi hukum yang berlaku.

Yogyakarta, tanggal-bulan-tahun

Materai Rp10.000

(Tanda tangan)

Nama Mahasiswa
NIM

HALAMAN PERSEMBAHAN

Tugas akhir ini kupersembahkan kepada kedua orang tuaku. Kupersembahkan pula kepada keluarga dan teman-teman semua, serta untuk bangsa, negara, dan agamaku.

[contoh]

KATA PENGANTAR

[SAMPLE]

Puji syukur ke hadirat Allah SWT atas limpahan rahmat, karunia, serta petunjuk-Nya sehingga tugas akhir berupa penyusunan skripsi ini telah terselesaikan dengan baik. Dalam hal penyusunan tugas akhir ini penulis telah banyak mendapatkan arahan, bantuan, serta dukungan dari berbagai pihak. Oleh karena itu pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. <isi dengan nama Kadep>
2. <isi dengan nama Sekdep>
3. <isi dengan nama Dosen Pembimbing>
4. Kedua Orang Tua, kakak, dan adik yang selalu memberikan arahan selama belajar dan menyelesaikan tugas akhir ini.
5. <isi dengan nama orang lainnya>

Akhir kata penulis berharap semoga skripsi ini dapat memberikan manfaat bagi kita semua, aamiin. [Contoh]

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN

[SAMPLE]

b	=	bias
$K(x_i, x_j)$	=	fungsi kernel
y	=	kelas keluaran
C	=	parameter untuk mengendalaikan besarnya pertukaran antara penalti variabel slack dengan ukuran margin
L_D	=	persamaan Lagrange dual
L_P	=	persamaan Lagrange primal
w	=	vektor bobot
x	=	vektor masukan
QR	=	Quick Response
SQR	=	Secure Quick Response Code
CDP	=	Copy Detection Pattern
ANFIS	=	Adaptive Network Fuzzy Inference System
ANSI	=	American National Standards Institute
DAG	=	Directed Acyclic Graph
DDAG	=	Decision Directed Acyclic Graph
HIS	=	Hue Saturation Intensity
QP	=	Quadratic Programming
RBF	=	Radial Basis Function
RGB	=	Red Green Blue
SV	=	Support Vector
SVM	=	Support Vector Machines

INTISARI

Intisari ditulis menggunakan bahasa Indonesia dengan jarak antar baris 1 spasi dan maksimal 1 halaman. Intisari sekurang-kurangnya berisi tentang latar belakang dan tujuan penelitian, metodologi yang digunakan, hasil penelitian, kesimpulan dan implikasi, dan Kata kunci yang berhubungan dengan penelitian.

Kata Kunci ditulis maksimal 5 kata yang paling berhubungan dengan isi skripsi. Silakan mengacu pada ACM / IEEE *Computing classification* jika Anda adalah mahasiswa Sarjana TI http://www.acm.org/about/class/ atau mengacu kepada IEEE keywords http://www.ieee.org/documents/taxonomy_v101.pdf jika Anda berasal dari Prodi Sarjana TE.

Kata kunci : Kata kunci 1, Kata kunci 2, Kata kunci 3, Kata kunci 4, Kata kunci 5

ABSTRACT

Abstract ditulis italic (miring) menggunakan bahasa Inggris dengan jarak antar baris 1 spasi dan maksimal 1 halaman. Abstract adalah versi Bahasa Inggris dari intisari. Abstract dapat ditulis dalam beberapa paragraf. Baris pertama paragraph harus menjorok ke dalam sekitar 1 cm. Tidak dsarankan menggunakan mesin penerjemah melainkan tulis ulang.

Keywords : Keyword 1, Keyword 2, Keyword 3, Keyword 4, Keyword 5

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pembajakan produk atau yang dikenal juga sebagai tindakan pemalsuan, merupakan suatu tindakan ilegal yang dilakukan dengan tujuan memperoleh keuntungan dengan cara meniru atau menyalin produk asli yang sudah dipatenkan atau memiliki hak cipta. Pembajakan produk semakin marak di era digital dan globalisasi, seiring dengan perkembangan teknologi. Di era digital, pembajakan produk semakin mudah dilakukan dengan memanfaatkan internet dan teknologi digital. Sementara itu, globalisasi mempermudah transportasi dan distribusi produk palsu dari satu negara ke negara lain. Pembajakan produk juga menyebabkan kerugian ekonomi yang signifikan bagi produsen dan pemilik hak merek, serta dapat membahayakan keselamatan konsumen. Hal ini terjadi karena pembajakan produk dapat merusak citra perusahaan, mengurangi pendapatan, serta merugikan konsumen yang membeli produk palsu yang seringkali berkualitas rendah dan dapat membahayakan diri secara langsung. [3]

Teknologi percetakan dan pemindai digital telah mengalami perkembangan yang pesat selama beberapa dekade terakhir. Namun, kemajuan ini tidak hanya digunakan untuk kegiatan positif juga dimanfaatkan oleh pelaku pembajakan untuk memproduksi produk-produk bajakan. Dengan kemampuan teknologi percetakan dan pemindai yang semakin canggih, pembajakan produk menjadi lebih mudah, lebih cepat, dan lebih murah. [4]

Printer 2D beresolusi tinggi dan Printer 3D, memungkinkan pembuat produk bajakan untuk membuat produk-produk dengan kualitas hampir sama dengan produk asli. Pemindai 3D juga pembuat produk bajakan untuk menyalin produk asli hingga detail terkecil dengan cepat dan mudah. Selain itu, teknologi digital seperti desain grafis dan software pemodelan juga memudahkan pelaku pembajakan dalam membuat desain dan cetakan produk tanpa harus membeli hak cipta atau paten produk tersebut. [5]

Kerugian dari praktik ilegal dan tidak etis ini diperkirakan mencapai $4,2 triliun per tahun, dan terus meningkat dengan sangat cepat. Beberapa cara yang dapat dilakukan untuk melawan pembajakan, antara lain melalui, komunikasi, pemerintah, hukum, kontak langsung, pelabelan, pemasaran proaktif, dan mempromosikan perlawanan terhadap pembajakan. Oleh karena itu, upaya preventif perlu dilakukan untuk meminimalisir dan melakukan perlawanan terhadap pembajakan produk. [6]

1.2 Rumusan Masalah

Dari masalah yang telah dijelaskan pada bagian latar belakang, yaitu semakin maraknya pembajakan dan pemalsuan produk seiring dengan berkembangnya teknologi perangkat pemindai digital dan juga teknologi percetakan, penulis mencoba untuk menerapkan CDP yang akan digunakan untuk mendeteksi pemalsuan produk. CDP yang didesain penulis dilengkapi dengan delapan marker disekitarnya untuk memudahkan pendeteksian objek CDP.

1.3 Batasan Penelitian

Beberapa batasan yang penulis gunakan dalam penelitian ini antara lain:

1. *Printer* yang digunakan untuk mencetak kumpulan data SQR seragam.
2. Pemotretan kumpulan data SQR dilakukan dalam kondisi pencahayaan yang baik yang berasal dari *flash* hp.
3. Kamera, konfigurasi kamera, sudut dan kondisi pengambilan gambar yang digunakan dalam melakukan pemotretan adalah tetap.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Mengukur nilai akurasi beberapa algoritme pembelajaran mesin dalam mendeteksi CDP asli dan palsu dalam SQR.
2. Mengukur performa yang didapatakan dalam pembuatan CDP dengan dua dan empat kuantisasi *grayscale*.
3. Mengetahui hasil deteksi objek CDP dalam SQR menggunakan delapan ArUco *marker* yang diletakkan di sekitar CDP.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini, pengembang SQR dua dimensi dapat menggunakan algoritme pembelajaran mesin dan jumlah kuantisasi grayscale yang memiliki akurasi klasifikasi biner terbaik. Selain itu, peletakan ArUco marker diharapkan mampu mendeteksi CDP dalam SQR yang nantinya akan diambil fiturnya dengan lebih cepat dan akurat. Bagi peneliti, penelitian ini dapat menambah wawasan, ilmu dan pengetahuan dalam pembuatan tulisan ilmiah, khususnya pada topik keamanan digital, pengolahan citra gambar, dan pembelajaran mesin. Bagi pelaku bisnis, penerapan SQR dapat membantu mereka dalam melindungi produk mereka dari pembajakan.

1.6 Sistematika Penulisan

BAB I : PENDAHULUAN

Pada bab ini dijelaskan latar belakang, rumusan masalah, batasan, tujuan, manfaat penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA DAN LANDASAN TEORI

Pada bab ini dijelaskan teori-teori dan penelitian terdahulu yang digunakan sebagai acuan dan dasar dalam penelitian.

BAB III : METODOLOGI PENELITIAN

Pada bab ini dijelaskan metode yang digunakan dalam penelitian meliputi langkah kerja, pertanyaan penilitian, alat dan bahan, serta tahapan dan alur penelitian.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan hasil penelitian dan pembahasannya.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini ditulis kesimpulan akhir dari penelitian dan saran untuk pengembangan penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

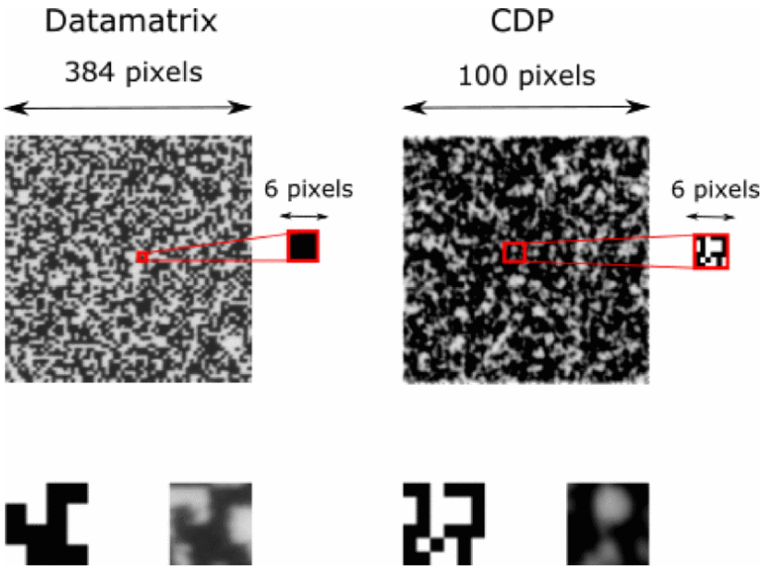
2.1.1 Apakah Pola Deteksi Duplikat (CDP) dapat Disalin

CDP dinilai dapat digunakan untuk mendeteksi pemalsuan, sehingga akhir-akhir ini mendapatkan banyak perhatian dari akademisi dan industri. Tingkat keamanan CDP dalam mendeteksi serangan pemalsuan yang canggih telah dipelajari secara teoritis dan praktis dalam beberapa penelitian, namun hasilnya masih belum sepenuhnya meyakinkan [1]. Kontribusi utama dari penelitian ini adalah untuk menyajikan kumpulan data CDP secara publik dan berbagai jenis contoh penyerangan terdapat CDP tersebut, sehingga kinerja CDP terhadap beberapa penyerangan dapat diketahui. Set data CDP tersebut terdiri dari lebih dari 27.500 gambar CDP dan merupakan set data CDP terbesar hingga saat ini [1]. Kontribusi selanjutnya adalah meneliti tentang kinerja detektor CDP dalam mendeteksi CDP asli ataupun salinan. Verifikasi dari CDP dapat dilakukan dengan perangkat seluler, tanpa harus menggunakan pemindai khusus [7], [8]. Dengan dataset dan detektor yang dibuat, peneliti sebelumnya ingin menguji validitas hipotesis bahwa CDP yang dicetak berulang kali akan terdegradasi kualitasnya dan dapat dideteksi sebagai CDP palsu [1]. Kontibusi terakhir dari penelitian ini adalah beberapa metode yang dapat dilakukan untuk meningkatkan performa klasifikasi dari model.

Gambar 2.1. Contoh dari CDP a) CDP original hasil *generate* dari program I b) CDP yang telah terdegradasi kualitasnya akibat dari beberapa kali penyetakan dan pemindaian $\widetilde{I}$ [1]

2.1.1.1 Prinsip Degradasi Informasi

Prinsip dari deteksi CDP palsu dilakukan berdasarkan hilangnya informasi, yang mana muncul dari proses pemindaian dan penyetakan [9]. Proses *Print-and-Scan* (P&S) merupakan proses stokastik (mempunyai unsur peluang atau kebolehjadian) [10], yang menyebabkan perubahan struktur dan kualitas gambar pada CDP, seperti yang ditampilkan pada Gambar 2.1 *Noise* yang dihasilkan dari P&S CDP sulit untuk dikarakterisasi [11] karena setiap printer dan pemindai memiliki karakteristiknya sendiri.



Gambar 2.2. Perbandingan dari CDP dengan data-matriks: Data-matriks memiliki ukuran unit komponen yang lebih besar, sehingga degradasi informasi tidak berdampak signifikan pada struktur kode [1]

CDP sering dibandingkan dengan kode batang dua dimensi seperti data-matriks karena kemiripan visualnya. Namun, seperti yang diilustrasikan pada Gambar 2.2, unit elemen data-matriks jauh lebih besar dibandingkan unit elemen CDP. Oleh karena itu, prinsip kehilangan atau degradasi informasi tidak berdampak pada struktur data-matriks. Sebagai contoh, korelasi antara data-matriks digital *template* hasil *generate* dengan versi rusak P&S bisa lebih dari $0,9$, sedangkan korelasi antara CDP digital *template* hasil *generate* dengan versi rusak P&S-nya hanya sekitar $0,45 - 0,55$ tergantung pada pemindai dan penyetaknya. Oleh karena itu, ukuran dari unit elemen pola CDP, yaitu uxu piksel seperti yang ditampilkan pada Gambar 2.2, ukuran pola keseluruhan juga sangat mempengaruhi proses otentikasi dan kemampuan pemalsu dalam mereproduksi pola. Pada praktiknya, ukuran unit elemen pada CDP adalah $1x1$ piksel atau $2x2$ piksel agar bisa memanfaatkan prinsip kehilangan atau degradasi informasi secara maksimal.

2.1.1.2 Definisi Teoritis dari Sistem Autentikasi CDP

Autentikasi dari CDP terdiri dari dua langkah utama. Langkah pertama adalah langkah registrasi di mana pola dihasilkan kemudian dicetak dengan penyetak untuk menghasilkan CDP asli. Langkah kedua adalah verifikasi CDP, menggunakan sebuah perangkat pemindai yang telah terotentikasi (perangkat selular dengan kamera), CDP dipindai dan dilewatkan ke tes autentikasi (dengan parameter-parameter peminadaian tertentu). Jika tes tersebut positif, item dianggap autentik.

Upaya penyerangan yang paling sering terjadi oleh pembajak adalah sebagai berikut: Pembajak melakukan pemindaian CDP pada sebuah item menggunakan pemindai beresolusi tinggi, mengestimasi pola asli dari CDP, kemudian mencetak pola yang te-

lah diestimasi menggunakan penyetak beresolusi tinggi. Pada skenario ini I merupakan CDP digital hasil *generate* dari *template*, kemudian $\Pi(I)$ merupakan hasil *generate* CDP *template* yang dicetak, dengan $\Pi(\cdot)$ *noise* yang dihasilkan dalam proses penyetakan menggunakan penyetak yang telah terautentikasi. Selanjutnya, proses autentikasi dapat dirumuskan sebagai uji hipotesis berikut ini:

$$\begin{aligned} \mathcal{H}_0 &: \tilde{I} \sim \Sigma(\Pi(I)), \\ \mathcal{H}_1 &: \tilde{I} \not\sim \Sigma(\Pi(I)), \end{aligned} \tag{2-1}$$

di mana $\widetilde{I}$ adalah gambar CDP *grayscale* yang diterima oleh pusat autentikasi. $\widetilde{I}$ dapat berupa CDP asli (i.e. $\Sigma(\Pi(I))$) atau CDP palsu (i.e. $\Sigma(\Pi'(\hat{I}))$). Metriks yang digunakan untuk membandingkan CDP asli dengan palsu adalah koefisien jarak ataupun korelasi [12].

2.1.1.3 Komponen dari Detektor

Hasil menunjukkan bahwa autentikasi menggunakan CDP *raw grayscale* lebih efisien dibandingkan dengan CDP yang telah di-*thresholding* [10]. Kemudian, secara umum, ada beberapa langkah yang dilakukan untuk melakukan autentikasi CDP, antara lain:

- Melakukan *resizing* pada *template* CDP menggunakan faktor skala tertentu.
- Menggunakan teknik pencocokan *template* dengan mengambil sub-bagian dari CDP.
- Menggunakan *high pass filtering* (seperti *unsharp masking*) sebelum melakukan penyekoran korelasi.

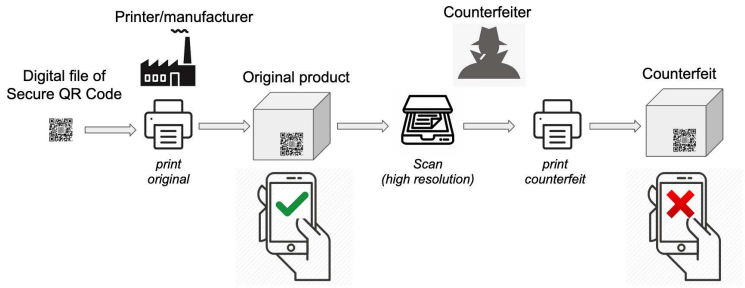
2.1.2 Detekti Pembajakan menggunakan SQR

Pendekatan keamanan tradisional pada produk sebelumnya sudah diimplementasikan melalui *taggant*, hologram, dan tinta keamanan.Beberapa metode tersebut memang mudah diimplementasikan, mudah diverifikasi, dan murah. Namun, dalam sebuah Kode QR metode-metode tersebut belum dapat diimplementasikan. Produk yang ditempeli oleh kode QR palsu biasanya masih dapat dipindai dan mengembalikan keluaran sama dengan produk asli. Penelitian yang dilakukan oleh Justin Picard, Paul Landry, dan Michael Bolay ini membahas tentang bagaimana mengimplementasikan CDP ke dalam SQR untuk mendeteksi pembajakan [2].

Pada Gambar 2.3 terlihat bahwa sangat sulit untuk membedakan antara kode QR asli dan replika, apabila jika tidak ada pembandingnya. Skenario yang dapat dilakukan

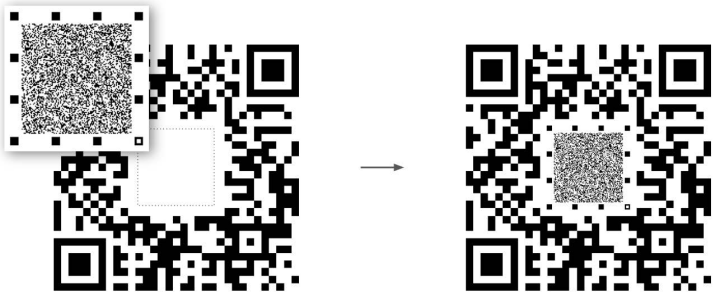
Gambar 2.3. Perbandingan dari kode QR asli dan palsu, keduanya menyimpan informasi yang sama dan sama-sama dapat dipindai [2]

oleh pembajak dalam menerbitkan kode QR palsu dapat dilihat pada Gambar 2.4. Kode QR palsu dipindai dengan perangkat beresolusi tinggi, kemudian dicetak ulang. Harapannya dengan CDP yang diletakkan pada kode QR, kode QR palsu yang dipindai untuk autentikasi dapat terdeteksi sebagai kode QR palsu, lihat pada Gambar 2.4.



Gambar 2.4. SQR diharapkan dapat mendeteksi kode QR palsu pada saat diautentikasi oleh pengguna [2]

2.1.2.1 Struktur dari SQR



Gambar 2.5. Struktur SQR secara umum [2]

Secara umum, CDP akan diletakkan di tengah-tengah dari kode QR. CDP nantinya akan digunakan untuk proses autentikasi. Di sekitar CDP diletakkan beberapa *markers* untuk memudahkan program dalam mendeteksi dan mendapatkan objek CDP. CDP

mungkin ditempelkan di tengah-tengah kode QR karena adanya fitur koreksi kesalahan dalam kode QR. Ada empat jenis koreksi kesalahan pada kode QR: L, M, Q, dan H, yang secara teoritis memiliki kemampuan untuk memulihkan informasi yang hilang sebesar 7%, 15%, 25%, dan 30% kerusakan pada kode QR. Pada penelitian ini, area yang dirusak untuk meletakkan CDP adalah sebesar 1/9 dari ukuran awal kode QR. Aplikasi yang digunakan untuk melakukan autentikasi pada perangkat pemindai (perangkat seluluer) hanya mengambil objek CDP saja, hal tersebut memiliki beberapa keuntungan, area yang digunakan untuk autentikasi menjadi lebih spesifik, sehingga kecepatan deteksi akan lebih cepat, fokus dari kamera juga relatif akan lebih baik karena mengambil objek yang lebih kecil dan terfokus, selain itu karena sistem autentikasi berada di *remote server* yang mana data akan dikirim dari perangkat seluler pemindai, maka semakin kecil area yang dikirimkan, semakin hemat *bandwith* yang digunakan.

2.1.2.2 Pembuatan dan Pencetakan SQR

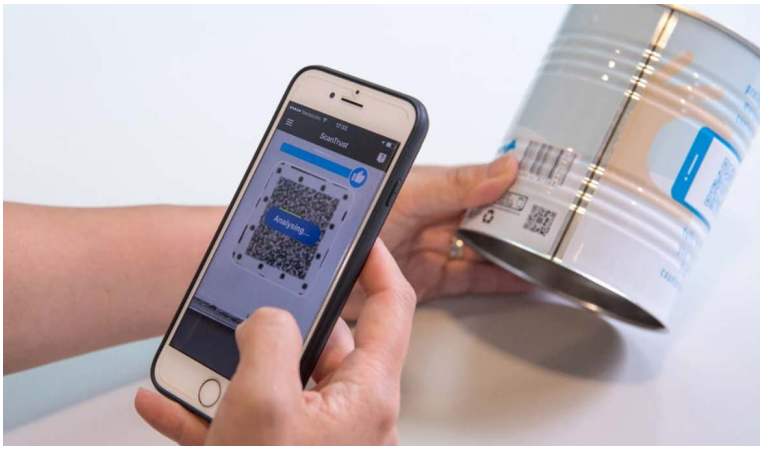
CDP yang digunakan dalam penelitian ini menggunakan dua kuantisasi *grayscale* atau biner. Resolusi mesin *printer* yang digunakan adalah 812,8 ppi dengan merek HP Indigo. CDP di-*generate* menggunakan *pseudo-random number generator*, menggunakan *seed* tertentu. CDP dapat dibuat unik untuk setiap kode QR ataupun sama pada sekelompok kode QR tertentu. Dalam melakukan penyetakan dan pemindaian SQR, perangkat pencetak dan pemindai akan diverifikasi terlebih dahulu dengan konfigurasi dan parameter tertentu untuk menjamin kualitas dari pencetakan.

2.1.2.3 Autentikasi SQR

Perangkat pemindai QR biasa sudah pasti dapat melakukan *decode* informasi dari kode QR, namun untuk melakukan autentikasi terhadap CDP, tentunya diperlukan aplikasi khusus. Aplikasi khusus ini berjalan di perangkat seluler, secara umum proses pemindaian yang dilakukan oleh aplikasi khusus tersebut adalah sebagai berikut:

- Aplikasi akan melakukan pemindaian per-*frame* dari kamera hingga mendapatkan kode QR.
- Kode QR akan di-*decode* untuk mengekstrak informasi dalam kode QR.
- Indeks kualitas pemindaian akan dikalkulasi berdasarkan *frame* yang didapatkan.
- Jika indeks kualitas pemindaian dinilai cukup tinggi, area CDP akan dideteksi, dipotong, dan dikirim ke *remote server* bersamaan dari informasi dari kode QR yang telah ter-*decode* untuk autentikasi.

Setelah *server* mendapatkan CDP yang telah dipotong beserta informasi data kode QR, autentikasi yang dilakukan di *server* adalah sebagai berikut:



Gambar 2.6. Perangkat seluler melakukan pemindaian menggunakan aplikasi khusus [2]

- *Identifier* unik akan diekstrak dari informasi kode QR yang didapatkan yang mana dibutuhkan sebagai parameter autentikasi.
- Template CDP digital akan di-*generate*.
- Matriks similaritas akan dikalkulasi dari perbandingan antara CDP yang dikirimkan dari hasil pemindaian dengan CDP *template* yang di-*generate*.
- Penyesuaian lain seperti, ketajaman gambar, filter akan dilakukan untuk memperoleh hasil terbaik.
- Normalisasi nilai akan dilakukan.
- Keluaran berupa CDP "asli", "palsu", atau "pemindaian buruk" akan dikeluarkan oleh *server* (pemindaian buruk bisa disebabkan oleh hasil gambar yang blur).

2.1.3 Autentikasi Digital menggunakan CDP

2.1.4 Pencetakan Variasi CDP

2.1.5 Autentikasi CDP menggunakan Perangkat Seluler

2.2 Dasar Teori

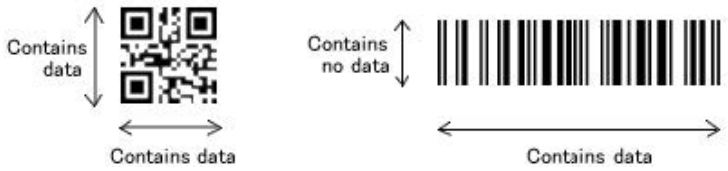
2.2.1 Kode QR

Kode QR (Quick Response) adalah sebuah kode matriks dua dimensi (2-D) yang dapat dibaca oleh komputer. Kode QR dua dimensi dapat menyimpan data yang lebih banyak dibandingkan dengan kode satu dimensi (barcodes) dengan ruang yang lebih kecil. Selain itu, kode QR memiliki fitur koreksi kesalahan pembacaan dan beberapa fitur unik lainnya [13].

Seperti bahasa tertulis lainnya, kode batang atau *barcode* merupakan representasi visual dari informasi. Namun, berbeda dengan bahasa yang dapat dibaca oleh manusia,

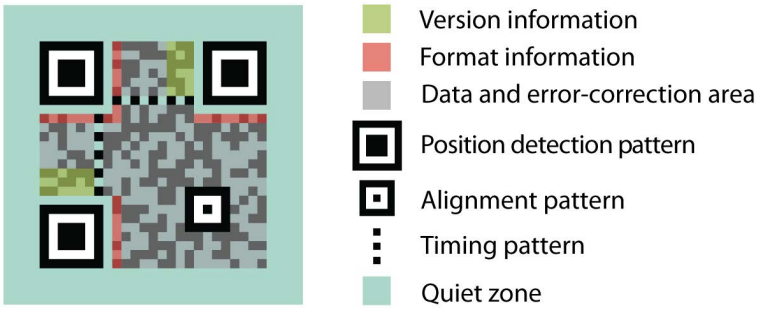
kode batang dirancang untuk dibaca dan dipahami oleh komputer atau mesin. Menggunakan sistem penglihatan dari mesin berupa pemindai laser optik ataupun kamera dan perangkat lunak yang dapat menginterpretasikan kode batang. Aturan bagaimana *barcode* dikonstruksikan disebut sebagai *grammar*, sedangkan set karakter yang digunakan (alfabet) disebut *symbology* [13].

2.2.1.1 Bagaiamana Kode QR Bekerja



Gambar 2.7. Perbandingan 1-D dengan 2-D *barcodes*

Tidak seperti kode batang satu dimensi, kode QR adalah matriks 2-D yang menyimpan informasi dalam tiap modul di baris dan kolomnya yang memiliki gelap dan terang tertentu.



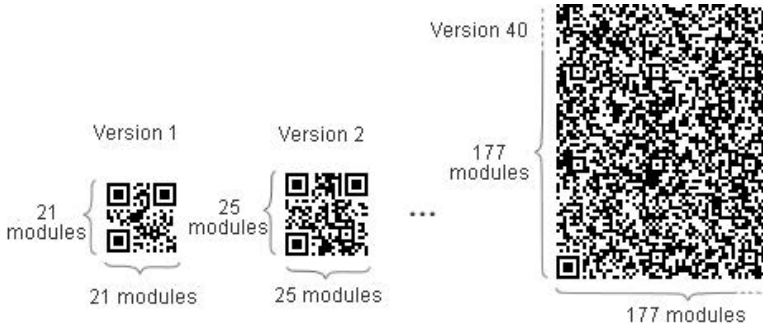
Gambar 2.8. Struktur modul pada kode QR dua dimensi

Setiap modul dalam kode QR memiliki fungsi-fungsi tertentu. Beberapa modul berisi tentang informasi yang tersimpan dalam kode QR itu sendiri, dengan lainnya dibagi menjadi beberapa grup berdasarkan fungsinya. Untuk memastikan kode QR dapat dipindai dari berbagai sisi, ada tiga modul *position detection pattern* yang terletak di ketiga sudut yang memungkinkan kode QR untuk dipindai dari 360°.

2.2.1.2 Versi Kode QR

Kode QR dapat di-*generate* dari 40 versi yang berbeda, dari yang berukuran $21x21$ modul (versi 1) hingga $177x177$ modul (versi 40).

Setiap kenaikan satu versi, maka akan ada penambahan 4 modul, sehingga dapat memuat data atau informasi yang lebih banyak. Jumlah maksimum data yang dapat disimpan tergantung pada versi kode QR, tipe karakter, dan besar toleransi kesalahan.



Gambar 2.9. Jumlah modul berdasarkan versi kode QR

2.2.1.3 Koreksi Kesalahan Kode QR

Koreksi kesalahan kode QR mengimplementasikan *Reed-Solomon codes*, yang mana merupakan salah satu metode koreksi kesalahan matematis yang banyak digunakan. Hal ini memungkinkan kode QR tetap dapat dibaca walaupun dalam kondisi kotor ataupun rusak dengan batasan tertentu. Ada empat tipe koreksi kesalahan standar yang ada dalam kode QR. Semakin tinggi level koreksi kesalahan, semakin besar toleransi terhadap kerusakan kode QR, namun semakin besar juga versi kode QR-nya.

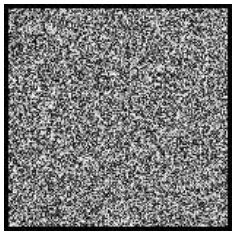
Tabel 2.1. Tabel perbandingan level koreksi kesalahan dengan persentase toleransi kesalahannya

Level Koreksi Kesalahan	Besar Toleransi Kesalahan
L	7%
M	15%
Q	25%
H	30%

Dalam memilih level koreksi kesalahan, sebaiknya disesuaikan dengan kondisi lingkungan di mana kode QR tersebut digunakan. Misalnya dalam kondisi lingkungan yang bersih, level L (7%) dapat digunakan. Secara umum, level yang paling sering digunakan adalah level M (15%).

2.2.2 Deteksi Pola Duplikat (CDP)

Pola deteksi duplikat (CDP) adalah sebuah gambar berpola dengan entropi tinggi yang dibuat menggunakan kode rahasia (*secret key*). CDP memanfaatkan konsep dari "*information loss principle*" dari proses P&S pada dokumen. Biasanya, CDP digunakan di dalam gambar digital yang dicetak ataupun langsung ke dalam dokumen digitalnya. CDP tidak didesain untuk dideteksi menggunakan mata telanjang. Namun, CDP dapat bekerja secara maksimal pada pendeteksian otomatis pada gambar yang dipindai. CDP akan sangat bermanfaat saat digunakan dalam memverifikasi dokumen dalam jumlah besar [9], [14], [].



Gambar 2.10. Salah satu contoh CDP

CDP telah dicoba untuk dicetak menggunakan berbagai variasi *printers*: *Printer* kantor seperti *inkjet* dan *laser*, *printer offset* dan *digital offset*, dan juga *printer* termal. Hasil percobaan dari pencetakan menggunakan beberapa jenis *printer* tadi, semua CDP salinan dapat dibedakan dengan CDP asli dengan margin yang cukup nyaman [9], [14].

CDP sebaiknya tidak dianggap sebagai pesaing untuk perangkat keamanan optik lainnya, namun dijadikan sebagai alternatif yang lebih murah pada kasus-kasus tertentu. Dengan memanfaatkan konsep degradasi gambar dan informasi yang tidak terancam oleh perkembangan perangkat pemindai dan pencetak digital, CDP menjadi alternatif yang paling murah dalam memroteksi dokumen [9], [14], [15].

2.2.3 Lokalisasi Objek dengan Pengenalan Pola

Lokalisasi objek adalah proses mengidentifikasi posisi dan orientasi objek atau pola tertentu pada sebuah gambar menggunakan teknik pengolahan citra dan visi komputer. Proses ini melibatkan deteksi objek atau pola dalam gambar serta mengestimasi lokasi dan orientasi yang tepat relatif terhadap kamera [16], [17].

Berbagai teknik telah diusulkan untuk melakukan lokalisasi objek atau gambar dengan pengenalan pola, termasuk deteksi fitur, pencocokan *template*, dan metode berbasis pembelajaran mesin. Teknik-teknik ini telah digunakan dalam berbagai aplikasi, seperti *augmented reality*, robotika, dan pelacakan objek.

2.2.4 ArUco *Marker*

ArUco *marker* adalah jenis *marker* fidusial yang biasa digunakan untuk estimasi pose kamera dan pelacakan dalam pengolahan citra dan visi komputer. ArUco *marker* terdiri dari kisi-kisi kotak hitam dan putih dengan pola unik yang mudah dideteksi dan dikenali oleh algoritma visi komputer. ArUco *marker* banyak digunakan dalam aplikasi robotika, realitas tambahan, dan pelacakan objek karena kesimpelannya, akurasi deteksi yang tinggi, dan biaya komputasi yang rendah.

Marker fidusial adalah objek berpola yang digunakan ke dalam sebuah gambar atau tempat tertentu untuk memudahkan sistem visi komputer menentukan posisi dan orientasi objek atau *scene* dengan akurasi yang tinggi. *Marker* fidusial biasanya didesain

dengan pola atau bentuk yang unik dan mudah dikenali, sehingga dapat dideteksi dan dilacak oleh algoritme pendeteksian objek visi komputer, yang memungkinkan estimase pose dan pelacakan yang akurat. *Marker* fidusial banyak digunakan dalam berbagai aplikasi seperti *augmented reality*, robotika, dan pendeteksian objek.

2.2.5 Koefisien Jarak

Koefisien jarak merupakan ukuran atau besaran yang menggambarkan seberapa dekat atau jauh dua objek dalam ruang atau dimensi tertentu. Koefisien jarak dapat digunakan untuk mengukur kesamaan atau perbedaan antara dua objek yang diamati. Ada beberapa koefisien jarak yang sering digunakan, antara lain:

2.2.5.1 Koefisien Jarak Euclidean

Jarak Euclidean adalah ukuran jarak yang paling umum digunakan dalam matematika dan ilmu komputer untuk mengukur jarak antara dua titik dalam ruang Euclidean n-dimensi. Jarak Euclidean dihitung sebagai akar kuadrat dari jumlah kuadrat perbedaan koordinat antara dua titik. Secara formal, jarak Euclidean antara dua vektor $\mathbf{u}$ dan $\mathbf{v}$ dalam ruang Euclidean n-dimensi didefinisikan sebagai:

$$d(\mathbf{u}, \mathbf{v}) = \sqrt{\sum_{i=1}^{n} (u_i - v_i)^2} \tag{2-2}$$

di mana n adalah jumlah dimensi dalam *vector space*, dan u_i dan v_i merepresentasikan komponen ke-i pada vektor.

2.2.5.2 Koefisien Jarak Korelasi

Koefisien jarak korelasi adalah suatu ukuran kemiripan atau perbedaan antara dua vektor, berdasarkan korelasi antara komponen-komponennya. Nilai dari jarak korelasi dinormalisasi antara 0 dan 1, di mana 0 menunjukkan korelasi positif sempurna sedangkan 1 menunjukkan korelasi negatif sempurna.

Untuk menghitung jarak korelasi antara dua vektor u dan v, dapat dituliskan dengan:

$$d = 1 - \frac{(u - \bar{u}) \cdot (v - \bar{v})}{\|(u - \bar{u})\|_2 \|(v - \bar{v})\|_2} \tag{2-3}$$

di mana d adalah jarak korelasi antara u dan v, $\bar{v}$ adalah rata-rata elemen dari vektor v, dan $x \cdot y$ adalah *dot product* dari x dan y. Jarak korelasi sering digunakan dalam algoritma pengelompokan dan klasifikasi untuk mengukur perbedaan antara sampel, terutama ketika vektor memiliki banyak komponen dan data sangat berkorelasi.

2.2.5.3 Koefisien Jarak Kosinus

Koefisien jarak kosinus adalah sebuah metode untuk mengukur kemiripan antara dua vektor dalam ruang n-dimensi [18], [19]. Metode ini mengukur sudut antara dua vektor dan menghasilkan nilai berkisar antara 0 dan 1, di mana 0 menunjukkan bahwa vektor tersebut saling tegak lurus, sedangkan 1 menunjukkan bahwa vektoor tersebut saling sejajar. Semakin kecil nilai koefisien jarak kosinus, semakin mirip kedua vektor tersebut. Jarak kosinus antara dua vektor u dan v dapat dituliskan sebagai berikut:

$$1 - \frac{u \cdot v}{\|u\|_2 \|v\|_2} \tag{2-4}$$

di mana $u \cdot v$ adalah hasil *dot product* antara vektor u dan v, sedangkan $\|u\|_2$ dan $\|v\|_2$ adalah panjang dari vektor u dan v.

2.2.5.4 Koefisien Jarak Canberra

Jarak Canberra adalah salah satu metode mengukur jarak antara dua vektor dalam ruang n-dimensi. Metode ini mengevaluasi perbedaan proporsional antara nilai-nilai pada setiap elemen vektor. Metode ini sering digunakan dalam analisis data untuk mengukur kemiripan antara dua set data numerik [20], [21]. Secara formal, perhitungan jarak canberra antara dua vektor u dan v adalah:

$$d(u, v) = \sum_i \frac{|u_i - v_i|}{|u_i| + |v_i|} \tag{2-5}$$

2.2.6 Transformasi Homografi

Transformasi homografi adalah sebuah transformasi geometri pada ruang n-dimensi yang memetakan setiap titik pada bidang ke titik yang sesuai pada bidang lainnya, dengan menerapkan konsep persamaan linier homogen. Transformasi homografi dapat mengubah ukuran, rotasi, dan persepektif dari gambar atau objek pada bidang ruang n-dimensi.

Transformasi homografi biasanya dilakukan dalam ruang koordinat *homogeneous*, yang merupakan ruang n+1 dimensi dengan koordinat homogen yang memungkinkan dilakukannya transformasi perspektif. Dalam ruang koordinat *homogeneous*, sebuah titik pada bidang n-dimensi dinyatakan dalam bentuk vektor homogen (x, y, z, w), di mana x, y, dan z adalah koordinat euclidean, dan w adalah koordinat homogen. Sebuah matriks homografi H juga dinyatakan dalam bentuk matriks homogen:

$$\begin{bmatrix} x' \\ y' \\ w' \end{bmatrix} = H \begin{bmatrix} x \\ y \\ w \end{bmatrix} \tag{2-6}$$

2.2.7 Pembelajaran Mesin

Pembelajaran mesin adalah sebuah cabang dari kecerdasan buatan yang memungkinkan sistem komputer untuk belajar dari data, mengidentifikasi pola, dan melakukan prediksi dalam menyelesaikan permasalahan. Secara umum, pembelajaran mesin mencoba untuk menemukan pola tersembunyi dalam data dan mempergunakan informasi tersebut untuk menghasilkan hasil yang lebih baik dalam setiap iterasinya [22], [23], [24].

Sistem pembelajaran mesin dilatih dengan menggunakan data masukan dan berbagai teknik pemrosesan data untuk menghasilkan output yang diharapkan. Proses pembelajaran ini melibatkan pembuatan model matematis dan analisis data. Dalam pembelajaran mesin, data digunakan untuk melatih model atau algoritma, sehingga sistem dapat belajar dan meningkatkan kinerjanya dalam memecahkan masalah atau menyelesaikan tugas tertentu. Secara umum, ada tiga jenis pembelajaran mesin, yaitu *supervised learning*, *unsupervised learning*, dan *reinforcement learning*. *Supervised learning* melibatkan penggunaan data yang telah dilabeli atau dikategorikan sebelumnya untuk melatih model atau algoritma. *Unsupervised learning* melibatkan penggunaan data yang belum dilabeli atau dikategorikan sebelumnya untuk menemukan pola atau struktur yang terdapat dalam data. Sedangkan *reinforcement learning* melibatkan penggunaan sistem *reward* dan *punishment* untuk melatih model atau algoritma.

Dalam praktiknya, pembelajaran mesin sering digunakan dalam berbagai aplikasi bisnis, seperti analisis data, personalisasi produk, dan deteksi kecurangan. Dalam kehidupan sehari-hari, pembelajaran mesin juga diterapkan dalam pengenalan suara, identifikasi gambar, dan pengembangan sistem kendali otomatis.

2.3 Analisis Perbandingan Metode

BAB III
METODE PENELITIAN

Bab ini menjelaskan metode atau cara yang digunakan dalam penelitian ini untuk mencapai maksud dan tujuan seperti yang tertulis dalam sub-bab 1.3 [jika diinginkan, kalian dapat menuliskan Kembali tujuan penelitian yang ingin dicapai di sini].

3.1 Alat dan Bahan Tugas akhir (Opsional)

3.1.1 Alat Tugas akhir

Alat-alat yang digunakan pada tugas akhir ini berupa perangkat keras maupun perangkat lunak sebagai sarana pendukung antara lain. Kemukakan secara detail sesuai dengan kebutuhan tugas akhir dan juga tambahkan spesifikasi minumum sehingga peneliti lain yang hendak melakukan hal yang sama bisa melakukannya :

1. *Notebook* dengan spesifikasi minumum sistem operasi Windows 8, *processor* Intel Core i3 2330M CPU @ 2,2 GHz, memori 4GB DDR3, grafis NVIDIA GeForce GT 610 (4GB), hardisk 500GB. Pada tugas akhir ini digunakan Windows 10, Intel Core i7 4570M CPU, Memori 4GB DDR 3, grafis Intel HD4300.
2. *Smartphone* dengan spesifikasi tipe minimum, OS Android OS v4.1.2 (Jelly Bean),CPU Dual-core 800 MHz, GPU Mali-400, Internal 4 GB, 768 MB RAM. Pada tugas akhir ini digunakan ....
3. *Game creation platform* versi 3.3.2 untuk Stencyl dan Construct2.
4. CORELDRAW X7, Tiled dan GIMP 2

3.1.2 Bahan Tugas akhir

Bahan tugas akhir adalah segala sesuatu yang bersifat fisik atau digital yang digunakan untuk kebutuhan tugas akhir. Bahan tugas akhir dapat berupa:

1. Bahan habis pakai. Bahan yang digunakan untuk tugas akhir. Sebagai contoh mungkin dibutuhkan kertas transparansi, baterai, atau yang lain
2. Bahan yang berupa data atau informasi yang menjadi dataset tugas akhir. Dataset tugas akhir dapat berupa:
    - Dataset pihak lain yang diperoleh dengan izin atau dalam lisensi yang diizinkan untuk digunakan secara langsung
    - Dataset pihak pertama yang disusun sendiri melalui quisioner, observasi, atau interview

- Dokumen panduan yang mengacu pada standar, hasil tugas akhir, atau artikel yang disitasi dan digunakan.

3.2 Metode yang Digunakan

Bagian ini membahas metode atau cara yang akan digunakan dalam penelitian, tahapan penerapan metode, dan desain penelitian (misalnya apakah penelitian akan menggunakan eksperimen di Laboratorium atau di lapangan, misalkan saja penelitian biomedis atau penelitian alat ukur hama yang dapat dilakukan di laboratorium ataupun di lapangan, atau menggunakan metode survei (misalnya untuk teknologi Informasi), studi kasus, atau analisis dengan perangkat lunak (ETAP, LTSpice, dst), atau *prototyping* (pembuatan perangkat keras).

Bagian ini juga membahas bagaimana data [akan] dianalisis, apakah dengan membandingkan keluaran beberapa alat ukur, membandingkan dengan standar atau bagaimana.

3.3 Alur Tugas Akhir

Menguraikan prosedur yang akan digunakan dan jadwal atau alur penyelesaian setiap tahap. Alur penelian ini dapat disajikan dalam bentuk diagram. Diagram dapat disusun dengan aturan yang baik semisal menggunakan *flowchart*. Aturan dan tutorial pembuatan *flowchart* dapat dilihat di http://ugm.id/flowcharttutorial. Setelah menggambarkannya, penulis wajib menjelaskan langkah-langkah setiap alur tugas akhir dalam sub bab tersendiri sesuai dengan kebutuhan.

3.4 Etika, Masalah, dan Keterbatasan Penelitian (Opsional))

Bagian ini membahas pertimbangan etis penelitian dan [potensi] masalah serta keterbatasannya. Jika menyangkut penelitian dengan makhluk hidup, maka dibutuhkan adanya *ethical clearance*, di bagian ini hal itu akan dibahas. Demikian juga tentang keterbatasan ataupun masalah yang akan timbul.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Pembahasan Hasil 1 (Ubah Judul Sesuai dengan Hal yang Hendak dibahas)

Poin pertama adalah membahas tujuan penelitian pertama. Dapat ditambahkan beberapa sub bab jika diperlukan.

4.2 Pembahasan Hasil 2 (Ubah Judul Sesuai dengan Hal yang Hendak dibahas)

Poin kedua adalah membahas tujuan penelitian kedua. Dapat ditambahkan beberapa sub bab jika diperlukan. Dapat juga diteruskan ke Sub Bab Pembahasan hasil 3 dan seterusnya, jika ada tiga atau lebih tujuan penelitian.

4.3 Perbandingan Hasil Penelitian dengan Hasil Terdahulu

Pembahasan penutup dapat menjelaskan mengenai kelebihan hasil pengembangan / penelitian dan kekurangan dibandingkan dengan skripsi atau penelitian terdahulu atau perbandingan terhadap produk lain yang ada di pasaran. Penulis dapat menggunakan tabel untuk membandingkan secara gamblang dan menjelaskannya.

BAB V
TAMBAHAN (OPSIONAL)

Anda boleh menambahkan Bab jika diperlukan. Jumlah Bab tidak harus sesuai dengan *template*.

BAB VI
KESIMPULAN DAN SARAN

6.1 Kesimpulan

Kesimpulan dapat diawali dengan apa yang dilakukan dengan tugas akhir ini lalu dilanjutkan dengan poin-poin yang menjawab tujuan penelitian, apakah tujuan sudah tercapai atau belum, tentunya berdasarkan data ataupun hasil dari Bab pembahasan sebelumnya. Dalam beberapa hal, kesimpulan dapat juga berisi tentang temuan/*findings* yang Anda dapatkan setelah melakukan pengamatan dan atau analisis terhadap hasil penelitian.

6.2 Saran

Saran berisi hal-hal yang bisa dilanjutkan dari penelitian atau skripsi ini, yang belum dilakukan karena batasan permasalahan. Saran bukan berisi saran kepada sistem atau pengguna, tetapi saran diberikan kepada aspek penelitian yang dapat dikembangkan dan ditambahkan di penelitian atau skripsi selanjutnya.

DAFTAR PUSTAKA

[1] E. Khermaza, I. Tkachenko, and J. Picard, "Can copy detection patterns be copied? evaluating the performance of attacks and highlighting the role of the detector," in *2021 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2021, pp. 1–6.

[2] J. Picard, P. Landry, and M. Bolay, "Counterfeit detection with qr codes," in *Proceedings of the 21st ACM Symposium on Document Engineering*, 2021, pp. 1–4.

[3] BASCAP and INTA, *The Economic Impacts of Counterfeiting and Piracy*. Business Action to Stop Counterfeiting and Piracy (BASCAP), 2016.

[4] C. W. Hill, "Digital piracy: Causes, consequences, and strategic responses," *Asia Pacific Journal of Management*, vol. 24, pp. 9–25, 2007.

[5] B. Depoorter, "Intellectual property infringements & 3d printing: Decentralized piracy," *Hastings LJ*, vol. 65, p. 1483, 2013.

[6] R. L. Van Renesse, *Optical document security*. Artech House Publishers, 1998.

[7] C. W. Wong and M. Wu, "Counterfeit detection based on unclonable feature of paper using mobile camera," *IEEE Transactions on Information Forensics and Security*, vol. 12, 2017.

[8] R. Schraml, L. Debiasi, and A. Uhl, "Real or fake: Mobile device drug packaging authentication," in *Proceedings of the 6th ACM workshop on information hiding and multimedia security*, 2018, pp. 121–126.

[9] J. Picard, "Digital authentication with copy-detection patterns," in *Optical Security and Counterfeit Deterrence Techniques V*, vol. 5310. SPIE, 2004, pp. 176–183.

[10] A. T. Phan Ho, B. A. Mai Hoang, W. Sawaya, and P. Bas, "Document authentication using graphical codes: Reliable performance analysis and channel optimization," *EURASIP Journal on Information Security*, vol. 2014, pp. 1–17, 2014.

[11] J. Picard, "On the security of copy detectable images," in *NIP & Digital Fabrication Conference*, vol. 2008, no. 2. Society for Imaging Science and Technology, 2008, pp. 796–798.

[12] A. E. Dirik and B. Haas, "Copy detection pattern-based document protection for variable media," *IET Image Processing*, vol. 6, no. 8, pp. 1102–1113, 2012.

[13] D. ADC, "Qr code essentials," 2011.

[14] J. Picard, C. Vielhauer, and N. Thorwirth, "Towards fraud-proof id documents using multiple data hiding technologies and biometrics," in *Security, Steganography, and Watermarking of Multimedia Contents VI*, vol. 5306. SPIE, 2004, pp. 416–427.

[15] C. Harwood, "Optical document security," *Kybernetes*, vol. 27, no. 5, pp. 586–588, 1998.

[16] J. Sivic and A. Zisserman, "Video google: A text retrieval approach to object matching in videos," in *Computer Vision, IEEE International Conference on*, vol. 3. IEEE Computer Society, 2003, pp. 1470–1470.

[17] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C.-Y. Fu, and A. C. Berg, "Ssd: Single shot multibox detector," in *Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11–14, 2016, Proceedings, Part I 14*. Springer, 2016, pp. 21–37.

[18] H. Schütze, C. D. Manning, and P. Raghavan, *Introduction to information retrieval*. Cambridge University Press Cambridge, 2008, vol. 39.

[19] M. P. Deisenroth, A. A. Faisal, and C. S. Ong, *Mathematics for machine learning*. Cambridge University Press, 2020.

[20] S. Al-Anazi, H. Almahmoud, and I. Al-Turaiki, "Finding similar documents using different clustering techniques," vol. 82, 2016.

[21] P. H. Sneath, R. R. Sokal *et al.*, *Numerical taxonomy. The principles and practice of numerical classification.*, 1973.

[22] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.

[23] E. Alpaydin, "Introduction to machine learning ethem alpaydin." *Introduction to Machine Learning, Third Edition*, 2014.

[24] K. P. Murphy, *Machine learning: a probabilistic perspective*. MIT press, 2012.

Catatan: Daftar pustaka adalah apa yang dirujuk atau disitasi, bukan apa yang telah dibaca, jika tidak ada dalam sitasi maka tidak perlu dituliskan dalam daftar pustaka.

LAMPIRAN

L.1 Isi Lampiran

Lampiran bersifat opsional bergantung hasil kesepakatan dengan pembimbing dapat berupa:

1. Bukti pelaksanaan Kuesioner seperti pertanyaan kuesioner, resume jawaban responden, dan dokumentasi kuesioner.
2. Spesifikasi Aplikasi atau Sistem yang dikembangkan meliputi spesifikasi teknis aplikasi, tautan unduh aplikasi, manual penggunaan aplikasi, hingga screenshot aplikasi.
3. Cuplikan kode yang sekiranya penting dan ditambahkan.
4. Tabel yang terlalu panjang yang masih diperlukan tetapi tidak memungkinkan untuk ditayangkan di bagian utama skripsi.
5. Gambar-gambar pendukung yang tidak terlalu penting untuk ditampilkan di bagian utama. Akan tetapi, mendukung argumentasi/pengamatan/analisis.
6. Penurunan rumus-rumus atau pembuktian suatu teorema yang terlalu panjang dan terlalu teknis sehingga Anda berasumsi bahwa pembaca biasa tidak akan menelaah lebih lanjut. Hal ini digunakan untuk memberikan kesempatan bagi pembaca tingkat lanjut untuk melihat proses penurunan rumus-rumus ini.

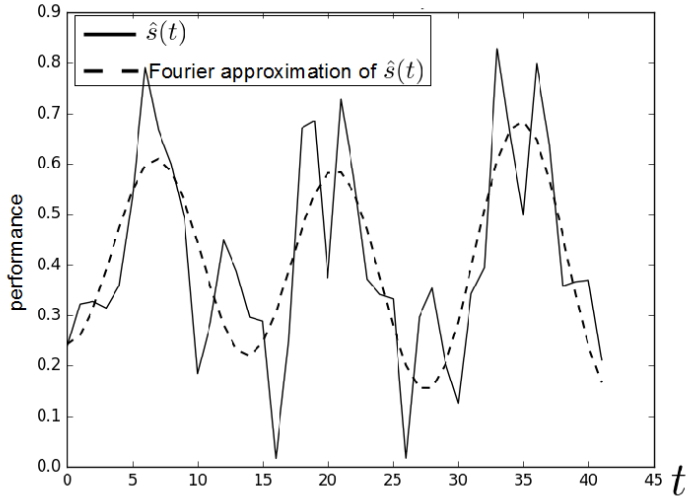
LAMPIRAN

L.2 Panduan Latex

L.2.1 Syntax Dasar

L.2.1.1 Penggunaan Sitasi

L.2.1.2 Penulisan Gambar



Gambar 1. Contoh gambar.

L.2.1.3 Penulisan Tabel

Tabel 1. Tabel ini

ID	Tinggi Badan (cm)	Berat Badan (kg)
A23	173	62
A25	185	78
A10	162	70

Contoh penulisan tabel bisa dilihat pada Tabel 1.

L.2.1.4 Penulisan formula

Contoh penulisan formula

$$L_{\psi_z} = \{t_i \mid v_z(t_i) \leq \psi_z\} \tag{1}$$

Contoh penulisan secara *inline*: $PV = nRT$. Untuk kasus-kasus tertentu, kita membutuhkan perintah "mathit" dalam penulisan formula untuk menghindari adanya jeda saat penulisan formula.

Contoh formula **tanpa** menggunakan "mathit": $PVA = RTD$

Contoh formula **dengan** menggunakan "mathit": $PVA = RTD$

L.2.1.5 Contoh list

Berikut contoh penggunaan list

1. First item
2. Second item
3. Third item

L.2.2 Blok Beda Halaman

L.2.2.1 Membuat algoritma terpisah

Untuk membuat algoritma terpisah seperti pada contoh berikut, kita dapat memanfaatkan perintah *algstore* dan *algrestore* yang terdapat pada paket *algcompatible*. Pada dasarnya, kita membuat dua blok algoritma dimana blok pertama kita simpan menggunakan *algstore* dan kemudian di-restore menggunakan *algrestore* pada algoritma kedua. Perintah tersebut dimaksudkan agar terdapat kesinamungan antara kedua blok yang sejatinya adalah satu blok.

Algorithm 1 Contoh algorima

```
1: procedure CREATESET(v)
2:     Create new set containing v
3: end procedure
```

Pada blok algoritma kedua, tidak perlu ditambahkan caption dan label, karena sudah menjadi satu bagian dalam blok pertama. Pembagian algoritma menjadi dua bagian ini berguna jika kita ingin menjelaskan bagian-bagian dari sebuah algoritma, maupun untuk memisah algoritma panjang dalam beberapa halaman.

```
4: procedure CONCATSET(v)
5:     Create new set containing v
6: end procedure
```

L.2.2.2 Membuat tabel terpisah

Untuk membuat tabel panjang yang melebihi satu halaman, kita dapat mengganti kombinasi *table* + *tabular* menjadi *longtable* dengan contoh sebagai berikut.

Tabel 2. Contoh tabel panjang

header 1	header 2
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar
foo	bar

L.2.2.3 Menulis formula terpisah halaman

Terkadang kita butuh untuk menuliskan rangkaian formula dalam jumlah besar sehingga melewati batas satu halaman. Solusi yang digunakan bisa saja dengan memindahkan satu blok formula tersebut pada halaman yang baru atau memisah rangkaian formula menjadi dua bagian untuk masing-masing halaman. Cara yang pertama mungkin akan menghasilkan alur yang berbeda karena ruang kosong pada halaman pertama akan diisi oleh teks selanjutnya. Sehingga di sini kita dapat memanfaatkan *align* yang sudah diatur dengan mode *allowdisplaybreaks*. Penggunakan *align* ini memungkinkan satu rangkaian formula terpisah berbeda halaman.

Contoh sederhana dapat digambarkan sebagai berikut.

$$\begin{aligned} x &= y^2 \\ x &= y^3 \\ a + b &= c \\ x &= y - 2 \\ a + b &= d + e \\ x^2 + 3 &= y \\ a(x) &= 2x \end{aligned} \tag{2}$$

$$
\begin{aligned}
b_i &= 5x \\
10x^2 &= 9x \\
2x^2 + 3x + 2 &= 0 \\
5x - 2 &= 0 \\
d &= \log x \\
y &= \sin x
\end{aligned}
$$

LAMPIRAN

L.3 Format Penulisan Referensi

Penulisan referensi mengikuti aturan standar yang sudah ditentukan. Untuk internasionalisasi DTETI, maka penulisan referensi akan mengikuti standar yang ditetapkan oleh IEEE (*International Electronics and Electrical Engineers*). Aturan penulisan ini bisa diunduh di http://www.ieee.org/documents/ieeecitationref.pdf. Gunakan Mendeley sebagai *reference manager* dan *export* data ke format Bibtex untuk digunakan di Latex.

Berikut ini adalah sampel penulisan dalam format IEEE:

L.3.1 Book

Basic Format:

[1] J. K. Author, "Title of chapter in the book," in Title of His Published Book, xth ed. City of Publisher, Country: Abbrev. of Publisher, year, ch. x, sec. x, pp. xxx–xxx.

Examples:

[1] B. Klaus and P. Horn, Robot Vision. Cambridge, MA: MIT Press, 1986.

[2] L. Stein, "Random patterns," in Computers and You, J. S. Brake, Ed. New York: Wiley, 1994, pp. 55-70.

[3] R. L. Myer, "Parametric oscillators and nonlinear materials," in Nonlinear Optics, vol. 4, P. G. Harper and B. S. Wherret, Eds. San Francisco, CA: Academic, 1977, pp. 47-160.

[4] M. Abramowitz and I. A. Stegun, Eds., Handbook of Mathematical Functions (Applied Mathematics Series 55). Washington, DC: NBS, 1964, pp. 32-33.

[5] E. F. Moore, "Gedanken-experiments on sequential machines," in Automata Studies (Ann. of Mathematical Studies, no. 1), C. E. Shannon and J. McCarthy, Eds. Princeton, NJ: Princeton Univ. Press, 1965, pp. 129-153.

[6] Westinghouse Electric Corporation (Staff of Technology and Science, Aerospace Div.), Integrated Electronic Systems. Englewood Cliffs, NJ: Prentice-Hall, 1970.

[7] M. Gorkii, "Optimal design," Dokl. Akad. Nauk SSSR, vol. 12, pp. 111-122, 1961 (Transl.: in L. Pontryagin, Ed., The Mathematical Theory of Optimal Processes. New York: Interscience, 1962, ch. 2, sec. 3, pp. 127-135).

[8] G. O. Young, "Synthetic structure of industrial plastics," in Plastics, vol. 3,

Polymers of Hexadromicon, J. Peters, Ed., 2nd ed. New York: McGraw-Hill, 1964, pp. 15-64.

L.3.2 Handbook

Basic Format:

[1] Name of Manual/Handbook, x ed., Abbrev. Name of Co., City of Co., Abbrev. State, year, pp. xx-xx.

Examples:

[1] Transmission Systems for Communications, 3rd ed., Western Electric Co., Winston Salem, NC, 1985, pp. 44-60.

[2] Motorola Semiconductor Data Manual, Motorola Semiconductor Products Inc., Phoenix, AZ, 1989.

[3] RCA Receiving Tube Manual, Radio Corp. of America, Electronic Components and Devices, Harrison, NJ, Tech. Ser. RC-23, 1992.

Conference/Prosiding

Basic Format:

[1] J. K. Author, "Title of paper," in Unabbreviated Name of Conf., City of Conf., Abbrev. State (if given), year, pp.xxx-xxx.

Examples:

[1] J. K. Author [two authors: J. K. Author and A. N. Writer] [three or more authors: J. K. Author et al.], "Title of Article," in [Title of Conf. Record as], [copyright year] © [IEEE or applicable copyright holder of the Conference Record]. doi: [DOI number]

Sumber Online/Internet

Basic Format:

[1] J. K. Author. (year, month day). Title (edition) [Type of medium]. Available: http://www.(URL)

Examples:

[1] J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com

Skripsi, Tesis dan Disertasi

Basic Format:

[1] J. K. Author, "Title of thesis," M.S. thesis, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.

[2] J. K. Author, “Title of dissertation,” Ph.D. dissertation, Abbrev. Dept., Abbrev. Univ., City of Univ., Abbrev. State, year.

Examples:

[1] J. O. Williams, “Narrow-band analyzer,” Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993. [2] N. Kawasaki, “Parametric study of thermal and chemical nonequilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993

LAMPIRAN

L.4 Contoh Source Code

L.4.1 Sample algorithm

Algorithm 2 Kruskal's Algorithm

```
1:  procedure MAKESET(v)
2:      Create new set containing v
3:  end procedure
4:
5:  function FINDSET(v)
6:      return a set containing v
7:  end function
8:
9:  procedure UNION(u,v)
10:     Unites the set that contain u and v into a new set
11: end procedure
12:
13: function KRUSKAL(V, E, w)
14:     A ← {}
15:     for each vertex v in V do
16:         MakeSet(v)
17:     end for
18:     Arrange E in increasing costs, ordered by w
19:     for each (u,v) taken from the sorted list do
20:         if FindSet(u) ≠ FindSet(v) then
21:             A ← A ∪ {(u, v)}
22:             Union(u, v)
23:         end if
24:     end for
25:     return A
26: end function
```

L.4.2 Sample Python code

```
import numpy as np

def incmatrix(genl1,genl2):
  m = len(genl1)
  n = len(genl2)
  M = None #to become the incidence matrix
  VT = np.zeros((n*m,1), int)  #dummy variable

  #compute the bitwise xor matrix
  M1 = bitxormatrix(genl1)
  M2 = np.triu(bitxormatrix(genl2),1)

  for i in range(m-1):
    for j in range(i+1, m):
      [r,c] = np.where(M2 == M1[i,j])
      for k in range(len(r)):
        VT[(i)*n + r[k]] = 1;
        VT[(i)*n + c[k]] = 1;
        VT[(j)*n + r[k]] = 1;
        VT[(j)*n + c[k]] = 1;

  if M is None:
    M = np.copy(VT)
  else:
    M = np.concatenate((M, VT), 1)

  VT = np.zeros((n*m,1), int)

  return M
```

L.4.3 Sample Matlab code

```
function X = BitXorMatrix(A,B)
%function to compute the sum without charge of two vectors

  %convert elements into usigned integers
  A = uint8(A);
  B = uint8(B);

  m1 = length(A);
  m2 = length(B);
  X = uint8(zeros(m1, m2));
  for n1=1:m1
    for n2=1:m2
      X(n1, n2) = bitxor(A(n1), B(n2));
    end
  end
```