# **BAB I PENDAHULUAN**

## **Pendahuluan**

Pada bab ini akan dibahas berkenaan dengan garis besar pokok-pokok pikirandalam penelitian ini. Pokok pikiran yang akan dibahas antara lain latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan manfaat penelitian. Pokok-pokok pikiran yang diuraikan akan dijadikan acuan dalam kajian penelitian ini.

## **Latar Belakang Masalah**

Perkembangan terbaru ***Deep Neural Networks (DNN)*** telah secara signifikan meningkatkan realisme wajah yang disintesis AI, dengan contoh yang paling menonjol adalah ***DeepFakes****.* Teknologi ***DeepFake*** dapat mensintesis wajah subjek target dari wajah subjek lain, sambil mempertahankan atribut wajah yang sama. Dengan portal media sosial yang meningkat pesat (Facebook, Instagram, dll), wajah-wajah palsu realistis ini menyebar dengan cepat melalui Internet, menyebabkan dampak negatif yang luas bagi masyarakat.

Dalam beberapa tahun terakhir, berita palsu telah menjadi isu yang merupakan ancaman bagi wacana publik, masyarakat manusia, dan demokrasi (Borges et al., 2019; Qayyum et al., 2019). Berita palsu mengacu pada konten gaya berita fiktif yang dibuat untuk menipu publik (Aldwairi & Alwahedi, 2018; Jang &Kim, 2018). Informasi palsu menyebar dengan cepat melalui media sosial, di mana hal itu dapat berdampak pada jutaan pengguna (Figueira & Oliveira, 2017). Saat ini, satu dari lima pengguna internet mendapatkan berita mereka melalui YouTube, kedua setelah Facebook (Anderson, 2018). Peningkatan popularitas video ini menyoroti perlunya alat untuk mengkonfirmasi keaslian konten media dan berita, karena teknologi baru memungkinkan manipulasi video yang meyakinkan (Anderson, 2018). Mengingat kemudahan dalam memperoleh dan menyebarkan informasi yang salah melalui platform media sosial, semakin sulit untuk mengetahui apa yang harus dipercaya, yang menghasilkan konsekuensi berbahaya bagi pengambilan keputusan berdasarkan informasi, antara lain (Borges et al., 2018; Britt et al., 2019). Memang, hari ini kita hidup dalam apa yang oleh beberapa orang disebut era "*post-truth*", yang ditandai dengan disinformasi digital dan perang informasi yang dipimpin oleh aktor jahat yang menjalankan kampanye informasi palsu untuk memanipulasi opini publik (Anderson, 2018; Qayyum et al., 2019; Zannettou et al.,2019).

Kemajuan teknologi baru-baru ini telah membuatnya mudah untuk menciptakan apa yang sekarang disebut "deepfakes", video hiper-realistis menggunakan face swap yang meninggalkan sedikit jejak manipulasi (Chawla, 2019). Deepfakes adalah produk dari aplikasi kecerdasan buatan (AI) hasil penggabungan dari proses, menggabungkan, mengganti, dan melapiskan gambar dan penjepit video untuk membuat video palsu yang tampak otentik (Maras &Alexandrou, 2018). Teknologi Deepfake dapat menghasilkan, misalnya, video lucu, pornografi, atau politik seseorang yang mengatakan apa pun, tanpa persetujuan orang yang gambar dan suaranya terlibat (Hari, 2018; Fletcher, 2018). Faktor deepfakes yang mengubah permainan adalah ruang lingkup, skala, dan kecanggihan teknologi yang terlibat, karena hampir semua orang dengan komputer dapat membuat video palsu yang praktis tidak dapat dibedakan dari media otentik (Fletcher, 2018). Sementara contoh awal deepfakes berfokus pada pemimpin politik, aktris, komedian, dan penghibur yang wajah mereka berkelok-kelok ke dalam video porno (Hasan & Salah, 2019), deepfakes di masa depan kemungkinan akan semakin banyak digunakan untuk balas dendam porno, intimidasi, bukti video palsu di pengadilan, sabotase politik, propaganda teroris, pemerasan, manipulasi pasar, dan berita palsu (Maras &Alexandrou, 2019).

Baru-baru ini, sintesis wajah berbasis **Deep Neural Network (DNN)** telah menarik perhatian yang meningkat. Menggunakan data pribadi (misalnya, gambar selfie atau video) yang dipanen dari portal jejaring sosial (misalnya, YouTube, Facebook, dan Instagram), ada banyak alat perangkat lunak opensource yang dapat digunakan untuk membuat ***DeepFakes*** seperti *FakeApp, DFaker github, Faceswap-GAN github, Faceswap github, DeepFaceLab,* yang merupakan wajah sintesis dari realisme tingkat tinggi. Ketika ***DeepFakes*** menantang kepercayaan media online, dalam beberapa tahun terakhir, banyak metode telah dikembangkan untuk mengendalikan potensi dampak negatif mereka. Sebagian besar upaya telah dikhususkan untuk membangun detektor DeepFake seperti *Exposing AI generated fake face videos by detecting eye blinking* (Y. Li, M.-C. Chang, and S. Lyu WIFS, 2018). Namun, mengingat penyebaran video DeepFake yang cepat dan luas di media sosial, bahkan detektor DeepFake terbaik mungkin tidak tepat waktu untuk membatasi kerusakan begitu mereka muncul secara online. Ini dapat dilengkapi dengan metode yang bertujuan untuk memecah atau memperlambat proses generasi DeepFakes seperti *Hiding faces in plain sight* (Y. Li, X. Yang, B. Wu, and S. Lyu 2019). yang berfokus pada mengganggu deteksi wajah atau model sintesis itu sendiri.

## **Rumusan Masalah**

Berdasarkan permasalahan pada latar belakang yang telah diuraikan maka rumusan masalah dari penelitian ini adalah

1. Bagaimana cara memproteksi citra gambar dengan metode CMUA-Watermark?
2. Bagaimana pengaruh DNN pada aplikasi Deepfake terhadap citra yang telah diproteksi dengan metode CMUA- Watermark ?

## **Tujuan Masalah**

Tujuan dari penelitian ini adalah:

1. Membangun perangkat lunak yang dapat memproteksi citra gambar menggunakan metode CMUA-Watermark.
2. Mengetahui tingkat akurasi penggunaan metode CMUA-Watermark dalam memproteksi citra dari deepfakes.

## **Manfaat Penelitian**

Manfaat yang diperoleh dari penelitian ini adalah:

1. Sistem yang dibuat dapat membantu pengguna untuk memproteksi citra gambar menggunakan metode CMUA-Watermark.
2. Hasil penelitian dapat dijadikan sebagai rujukan untuk penelitian terkait di masa mendatang.

## **Batasan Masalah**

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Dataset yang digunakan merupakan dataset yang dipakai dalam penelitian milik Deep Learning Face Attributes in the Wild (2015).
2. Data uji yang digunakan merupakan dataset foto mahasiswa jurusan Teknik Informatika Universitas Sriwijaya Angkatan 2018.
3. Ekstensi citra yang didukung oleh perangkat lunak adalah .jpg.

## **Sistematika Penulisan**

Sistematika penulisan tugas akhir mengikuti standar penulisan tugas akhir Fakultas Ilmu Komputer Universitas Sriwijaya yaitu sebagai berikut:

**BAB I. PENDAHULUAN**

Pada bab ini akan membahas landasan dari penelitian, seperti latar belakang, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah serta sistematika penulisan.

**BAB II. KAJIAN LITERATUR**

Pada bab ini membahas literatur pada penelitian, seperti pengertian Hotel, Klasifikasi Teks, Seleksi Fitur, Seleksi fitur Information gain dan algoritma Support Vector Machine, dan penelitian yang relevan.

**BAB III. METODOLOGI PENELITIAN**

Pada Bab ini menjelaskan pelaksanaan alur penelitian. yakni pengumpulan data dan perancangan pembangunan perangkat lunak. Serta tahapan dijelaskan secara detail berdasarkan kerangka yang dibuat.

**BAB IV. PENGEMBANGAN PERANGKAT LUNAK**

Pada Bab ini membahas analisa dan rancangan pengembangan perangkat lunak. Dimulai dengan kebutuhan analisis, perancangan dan konstruksi, serta diakhiri dengan melakukan pengujian yang bertujuan untuk memastikan pengembangan sistem sesuai rancangan dan kebutuhan yang telah dibuat.

**BAB V. HASIL DAN ANALISA PENELITIAN**

Pada bab ini menjelaskan hasil pengujian sesuai perancangan. Tabel hasil evaluasi pengujian dan analisis serta grafik akan menjadi patokan dari kesimpulan yang akan diambil dalam penelitian.

**BAB VI. KESIMPULAN DAN SARAN**

Pada Bab ini membahas mengenai kesimpulan dari semua uraian pada bab sebelumnya serta saran yang diuraikan dari hasil penelitian.

## **Kesimpulan**

Pada Bab ini telah menjelaskan dasar dan patokan pada penelitian , seperti latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah dan sistematika penulisan.

# **BAB II KAJIAN LITERATUR**

## **Pendahuluan**

pada bab ini akan dijelaskan mengenai dasar-dasar teori digunakan pada penelitian ini. Serta penjelasan hasil dari penelitian - penelitian terkait pengenai *Facial landmark extractors*, *Deepfakes*, serta *Adversarial Perturbations.*

## **Landasaran Teori**

### **2.2.1 Citra**

### **2.2.2 Deepfake**

### **2.2.3** **CMUAI-Watermark**

### **2.2.4 RUP**

## **Penelitian Lain yang Relevan**

## **Kesimpulan**