BAB 1 PENDAHULUAN

1.1 Latar Belakang

Deepfake adalah sebuah bentuk kecerdasan buatan yang digunakan untuk memanipulasi gambar atau video dalam sebuah peristiwa. Manipulasi yang dilakukan oleh *deepfake* adalah dengan menggabungkan anggota tubuh seseorang dengan wajah seorang yang lain maupun sebaliknya. *Deepfake* menggunakan teknologi kecerdasan buatan yang dikenal dengan *Generative Adversarial Network (GAN)*[1]. Namun *deepfake* sendiri tidak digunakan dengan baik oleh para penggunanya. Hampir 96% video *deepfake* yang beredar di internet mengandung muatan negatif. Muatan negative ini pun bermacam-macam bentuknya, politik adu domba, *hoax* yang seolah-olah disebarkan oleh figur ternama, bahkan sampai ke ranah pornografi[2]. Sehingga secara tidak langsung banyak pihak yang dirugikan oleh hal tersebut. Selain itu, perkembangan *deepfake* yang semakin merajalela juga dipengaruhi oleh kehadiran perangkat lunak yang semakin banyak. Baik yang digunakan oleh professional bahkan yang dapat masyarakat pada umunya gunakan, seperti *FaceApp, faceSwap,* dll. Namun kehadiran perangkat pembuatnya tidak seimbang dengan perangkat lunakn untuk mendeteksi video *deepfake* itu sendiri[3]. Oleh karena itu, perkembangan dari teknologi *deepfake* ini sendiri perlu diseimbangkan, agar tidak dianggap menjadi teknologi yang negatif.

Dari banyaknya dampak negatif yang disebabkan oleh *deepfake* itu sendiri, terutama video-video yang banyak tersebar merupakan video dengan wajah atau badan dari orang yang tidak diketahui tentunya banyak pihak yang akan merasa terfitnah oleh video yang mungkin bahkan mereka tidak pernah berpikir untuk membuatnya. Dampak yang akan ditinggalkan ke korban sendiri tentunya akan berdampak luas terhadap kehidupan pribadinya, selain dari merasa tidak nyaman di depan umum, korban juga dapat semakin tertekan apabila tidak dapat membuktikan video *deepfake* tersebut bukanlah dirinya[4].

Berdasarkan permasalahan tersebut, sudah ada beberapa solusi terkait dengan latar belakang yang sama untuk menemukan cara pendeteksian video *deepfake* tersebut dengan metode yang dapat digunakan masyarakat umum. *Kaggle.com* sebuah *website* dataset paling komplit di dunia, mengadakan sebuah lomba yang berlangsung selama 2 tahun yaitu *Kaggle Deepfake Detection Challenge* untuk menemukan teknologi paling efektif dalam mendeteksi manipulasi dalam video deepfake[5]. Selain itu riset yang dilakukan oleh *Springer Nature Singapore* juga menghasilkan metode *machine learning* dengan menggunakan *Key Frame Extraction* pada video yang diperoleh dari sosial media[6]. Tak hanya itu, Konkuk *University* di Korea juga menciptakan sebuah metode yaitu, *DeepVision.* Pendeteksian video *deepfake*

dengan melihat pola kedipan mata pada subjek video. Karena salah satu kelemahan dari video *deepfake* itu sendiri adalah pola kedipan mata yang biasanya berubah dan tidak seperti seharusnya. Sehingga pola tersebut akan disesuaikan dengan pola kedipan mata yang seharusnya berdasarkan faktor umur dan jenis kelamin[7].

Dari solusi yang sudah ada, nyatanya masih belum terlalu membantu masyarakat umum untuk melakukan pembuktian *deepfake* karena kebanyakan masih berupa pemodelan *machine learning* yang tentu hanya orang-oreang tertentu yang dapat menggunakannya. Sehingga masyarakat umum tetap kesulitan dalam mendeteksi video *deepfake* itu sendiri. Oleh karena itu, dengan membangun sebuah aplikasi *website* yang dapat diakses semua kalangan masyarakat dapat sangat membantu korban untuk membuktikan bahwa subjek dalam video bukanlah diri korban.

Salah satu solusi yang dapat mengatasi masalah tersebut adalah pembangun aplikasi *website* dengan penggunaan *machine learning* agar dapat mengetahui, membedakan dan memberi kesimpulan dari video yang ingin dibuktikan oleh masyarakat umum. Karena penggunaan *website* yang mudah, bisa dilakukan di berbagai perangkat tanpa melakukan unduhan apapun. Sehingga dapat mudah digunakan baik untuk pengguna pada umunya yang hanya melakukan pendeteksian satu atau dua kali maupun pengguna yang memiliki perhatian khusus pada bidang video *deepfake* yang akan melakukan pendeteksian berulang.

Maka dari itu, hasil akhir dari penelitian ini adalah rekayasa perangkat lunak berupa aplikasi web yang dapat digunakan masyarakat pada umunya untuk melakukan pendeteksian video *deepfake*. Penelitian ini sendiri akan menggunakan metode *Convolutional Neural Network* dan *Long Short Term Memory.* Untuk melakukan pemisahan dan klasifikasi dari video yang akan dilatih.

Aplikasi web ini sendiri diharapkan dapat membantu para korban video *deepfake* baik dari kalangan manapun untuk membuktikan bahwa subjek pada video tersebut bukan merupakan dirinya. serta dapat digunakan oleh pengguna umum sebagai pemeriksa keaslian sebuah video.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang sudah diuraikan, maka dapat ditetapkan rumusan masalah yang diinginkan sebagai berikut:

1. Bagaimana membangun sistem aplikasi web dengan implementasi *DEEP LEARNING* agar dapat membedakan sebuah video merupakan video asli atau *deepfake?*

2. Bagaimana membangun aplikasi web yang sederhana, cepat dan mudah digunakan oleh berbagai kalangan masyarakat umum?
3. Bagaimana performa akurasi yang dihasilkan oleh metode *Long Short Term Memory* dalam pendeteksian wajah dalam sebuah video?

1.3 Tujuan Penelitian

Merancang dan mengembangkan sebuah aplikasi web yang sederhana dan mudah digunakan oleh semua kalangan untuk melakukan pendeteksian video *deepfake* dengan waktu yang singkat sehingga dapat membantu masyarakat serta figur publik yang merasa dirugikan oleh kehadiran video *deepfake* untuk membuktikan bahwa subjek dalam video tersebut bukanlah dirinya.

1.4 Batasan Masalah

Hal – hal yang menjadi batasan dari penelitian yang dilakukan adalah sebagai berikut:

1. Penelitian ini menghasilkan aplikasi web yang hanya digunakan untuk pengunggahan video yang akan dideteksi.
2. Penelitian ini menggunakan algoritma *machine learning* yang telah dikembangkan pada referensi yang digunakan.
3. Penelitian ini hanya melakukan deteksi pada bagian wajah dengan subjek tunggal, tanpa bagian tubuh yang lain serta terdapat dua atau lebih subjek pada video.
4. Penelitian ini hanya digunakan untuk pendeteksian, tidak untuk menjamin korban di dalam ranah hukum.

1.5 Hasil dan Manfaat

Hasil akhir dari penelitian ini adalah sebuah aplikasi *website* yang dapat digunana oleh siapa saja untuk melakukan pendeteksian video *deepfake* apakah video tersebut asli atau palsu.

Dengan harapan dapat memberikan manfaat bagi para penggunanya yang merasa menjadi korban untuk membuktikan bahwa mereka bukanlah pihak yang berada dalam video *deepfake* tersebut serta dapat membantu para pengguna umum untuk memeriksa keaslian sebuah video.

1.6 Metodologi Penelitian

1. Tempat dan Waktu Penelitian

Penelitian ini dilakukan di Institut Teknologi Harapan Bangsa yang beralamat di Jl. Dipatiukur No. 80. Dago, Kecamatan Coblong, Kota Bandung, Jawa Barat. Penelitian ini dilaksanakan dengan jangka waktu dari Desember 2021 – Juni 2022.

2. Subjek Penelitian

Pada penelitian ini yang akan menjadi subjek adalah video-video yang dianggap video asli oleh para penggunanya. Video tersebut akan difokuskan pada bagian wajah sebagai *parameter* pemeriksaan video asli atau palsu.

3. Alat dan model yang digunakan

3.1 Perangkat keras

Laptop dengan spesifikasi sebagai berikut:

a. 64 bit *Windows* 10
b. 12 GB *Random Access Memory (RAM)*
c. 1 TB *Hard Drive*

3.2 Perangkat lunak

a. Google Collab

   Perangkat lunak yang desediakan oleh Google untuk melakukan komputasi *machine learning* secara daring dan menggunakan *cloud computing*

b. Google Cloud

   Sebagai alat menyimpan *dataset* yang akan digunakan dalam penelitian

c. Python
d. Javascript
e. Django

4. Teknik pengumpulan data

Data-data yang digunakan pada penelitian ini, peneliti dapatkan dari dua sumber yaitu:

a. *Kaggle Deepfake Detection Challenge Dataset*
b. *FaceForencics++ Dataset*

Data yang didapatkan gratis dan bebas dari *copyright* sehingga dapat digunakan untuk penelitian dengan aman.

5. Rancangan Penelitian

a. Membagi *dataset*

Dari *dataset* yang sudah disebutkan di poin sebelumnya, *dataset* tersebut akan dibagi menjadi 80 : 20. Dimana 80% *dataset* menjadi *data training* dan 20% nya menjadi *data testing*

b. Membangun model *pre-processing*
   Melakukan pembangunan model awal *machine learning* untuk memecah *frame* video dan mengambil wajah subjek video sebagai *feature* yang akan di proses
c. Membangun pemodelan *Machine Learning*
   Membangun model inti *machine learning* menggunakan *Convolutional Neural Network* untuk mengambil *feature* yang dibutuhkan serte pmeberian *label* dan juga *Long Short Term Memory* untuk mengklasifikasi video tersebut
d. Melakukan *testing* model
   Model *machine learning* yang sudah jadi lalu dites menggunakan *data testing* untuk menilai persentase akurasi model
e. Membangun aplikasi web
   Memulai pembangunan *website* dengan menggunakan HTML dan Bootstrap serta Javascript
f. Memasukan model *machine learning* ke dalam aplikasi web
   Model *machine learning* yang sudah jadi akan dimasukan ke *backend website* sehingga aplikasi web dapat melakukan pendeteksian video *deepfake*

1.7 Sistematika Penulisan

Untuk mempermudah melihat dan mengetahui pembahasan yang ada pada tugas akhir ini secara menyeluruh, maka perlu dikemukakan sistematika yang merupakan kerangka dan pedoman penulisan tugas akhir. Adapun sistematika penulisannya adalah sebagai berikut :

BAB I Pendahuluan

Bab ini berisi latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, hasil dan manfaat, metodologi penelitian, sistematika penulisan.

BAB 2 Kajian Referensi

Bab ini berisi identifikasi masalah, pemangku kepentingan, sistem eksisting dan sistem yang diusulkan.

BAB 3 Perancangan dan Implementasi

Bab ini akan berisi perancangan cara kerja sistem yang dibangun, perancangan dan implementasi antarmuka dan implementasi sistem.

BAB 4 Pengujian dan Analisis