



Attack on Morphing

Un moderno classificatore per la detection di attacchi di morphing

Prof.:

Michele Nappi

Dott.ssa:

Lucia Cascone

Anno Accademico
2022/2023

Presentazione di:

Alessandro Aquino,
Alberto Montefusco,
Simone Tartaglia

CONTENUTI

01

INTRODUZIONE

Problema: Morph Attacks

02

WORKFLOW

Detection di MA

03

IMPLEMENTAZIONE

Feature Extraction e
Classificazione

04

ANALISI DEI RISULTATI

Grafici e Conclusioni



A decorative graphic on the left side of the slide. It features a grid of hexagons in various shades of teal and blue. Some hexagons are solid, while others are outlined. Small teal dots are placed at the vertices of the hexagonal grid.

01

INTRODUZIONE

Sistemi di riconoscimento facciale e Morph Attacks

A decorative graphic at the top of the slide consisting of a cluster of white-outlined hexagons of various sizes, some overlapping, set against a teal background.

INTRODUZIONE

L'utilizzo di sistemi di riconoscimento facciale volti alla tutela della sicurezza sta prendendo sempre più piede

Tuttavia, questo implica anche una maggior esposizione ad attacchi da parte di utenti malintenzionati



TIPOLOGIE DI ATTACCHI

FALSIFICAZIONE

Utilizzo di dati biometrici falsi per ingannare il sistema.

ALTERAZIONE

Modifica di dati biometrici già acquisiti.

SPOOFING

Creazione di imitazioni dei tratti biometrici.



CASO DI STUDIO: MORPH ATTACKS

Un Morph Attack (MA) è un tipo di attacco che consente di associare un unico volto a più persone

Molteplici persone potrebbero identificarsi utilizzando lo stesso documento!



ESEMPIO DI MORPH ATTACK





SOLUZIONE: MORPH ATTACK DETECTOR

Un Morph Attack Detector (MAD) è un sistema in grado di rilevare automaticamente attacchi di Morphing

Sfruttando il ML, un MAD può distinguere automaticamente immagini reali da immagini “morphed”



STATO DELL'ARTE

Privacy-friendly Synthetic Data for the Development of Face Morphing Attack Detectors

Approccio geometrico


(Ossia, l'approccio basato sulla geometria dei volti)





OBIETTIVI

Combinazione migliore tra:

- **Paper vs AoM**
 - **Approccio Geometrico vs AoM**
 - **Approccio Geometrico vs AoM
vs Approccio Geometrico & AoM**
- 

A decorative graphic on the left side of the slide. It features a grid of hexagons in various shades of teal and blue. Some hexagons are solid, while others are outlined with thin white lines. Small teal dots are placed at the vertices of the hexagonal grid.

02

WORKFLOW

Sviluppo e utilizzo di Attack on Morphing

WORKFLOW



STEP 1

DataSet: train,
validation, test



STEP 2

Training e Testing
della MixNet-S



Train	
Bonafide	Attack
25000	15000

Validation				
Attack				
facemorpher	stylegan	amsi	opencv	webmorph
45	45	75	45	45

Test						
Attack					Bonafide	
facemorpher	stylegan	amsi	opencv	webmorph	smile	no smile
1222	1222	2175	1229	1221	205	103

A decorative graphic on the left side of the slide. It features a grid of hexagons in various shades of teal and blue. Some hexagons are solid, while others are outlined. Small teal dots are placed at the vertices of the hexagonal grid.

03

IMPLEMENTAZIONE

MixNet-s, Feature Extraction e Classificazione



MODELLO MIXNET-S

Unisce molteplici kernel, ognuno di dimensioni differenti, in un'unica operazione convoluzionale, così da ottenere facilmente diversi tipi di pattern dalle immagini ricevute in input





FEATURE EXTRACTION

Estrarre le caratteristiche più rilevanti con lo scopo di effettuare un'analisi dettagliata; prendendo le features del penultimo layer e salvarle all'interno di un file csv



PRE-PROCESSING:

PCA



CODE

```
pca = PCA(n_components='mle', copy=True)
pca_values = pca.fit_transform(x)
```

Permette di individuare le caratteristiche più informative dei dati e scartare quelle che contribuiscono meno alla varianza complessiva

Questo permette di ottenere una rappresentazione ridotta dei dati che preservano la maggior parte delle informazioni importanti

CLASSIFICATORI



DECISION TREE

```
model = DecisionTree()  
model.fit(pca_values , y)
```



GAUSSIANNB

```
model = GaussianNB()  
model.fit(pca_values , y)
```



RANDOM FOREST

```
model = RandomForest()  
model.fit(pca_values , y)
```



VISUALIZZAZIONE DELLE METRICHE

BPCR

Tasso di errore di
classificazione delle
presentazioni bonafide

...

Indica la percentuale di casi
in cui il sistema riconosce
erroneamente una
presentazione bonafide
come un attacco



VISUALIZZAZIONE DELLE METRICHE

APCER

Tasso di errore di
classificazione delle
presentazioni attacco

...

Indica la percentuale di casi
in cui il sistema riconosce
erroneamente una
presentazione di attacco
come bonafide



VISUALIZZAZIONE DELLE METRICHE

BPCER (%) APCER =

Calcolo dell'APCER in
relazione ad una soglia
fissata del BPCER

...

1. BPCER = 0.10 %
2. BPCER = 1.00 %
3. BPCER = 10.00 %
4. BPCER = 20.00 %




VISUALIZZAZIONE DELLE METRICHE

EER

Punto di equilibrio in cui il
tasso di FAR e il FRR sono
uguali

...

L'obiettivo è stato di
minimizzare il più possibile
l'EER

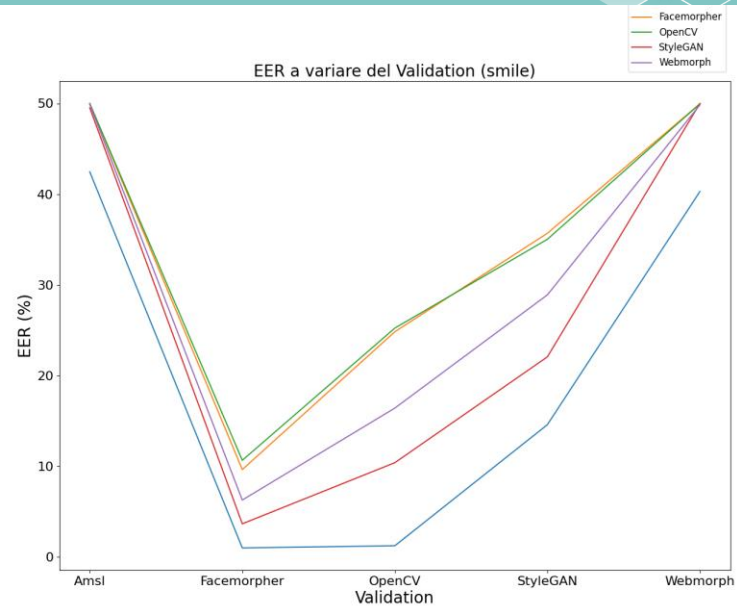
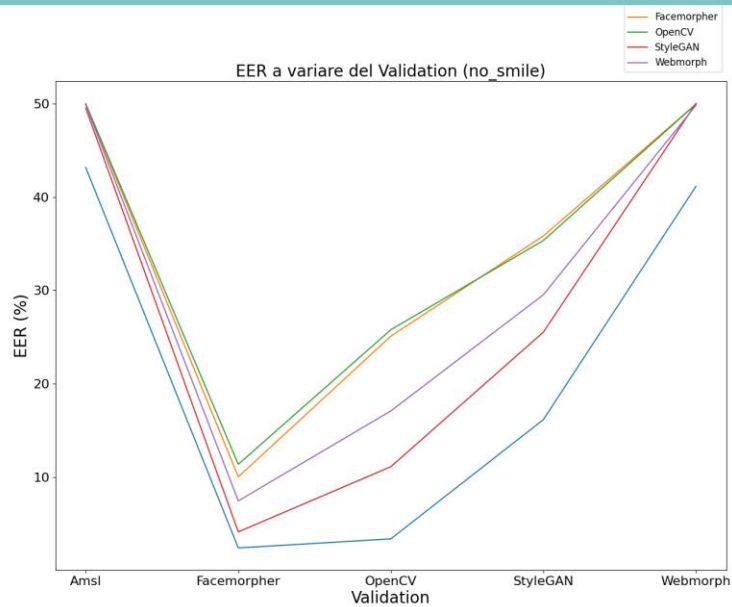
A decorative graphic on the left side of the slide. It features a grid of hexagons in various shades of teal and blue. Some hexagons are solid, while others are outlined. Small teal dots are placed at the vertices of the hexagonal grid, connected by thin white lines.

04

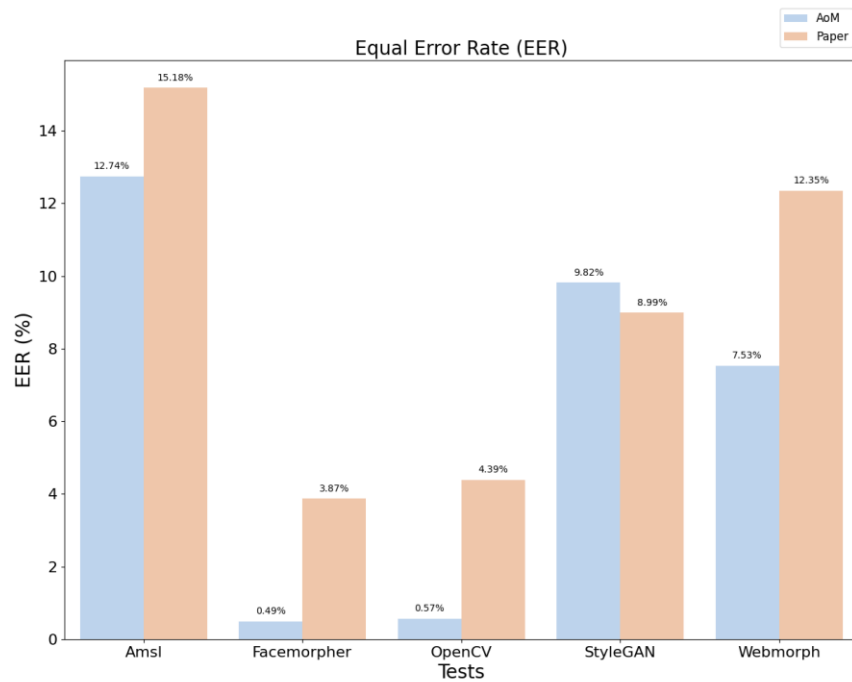
ANALISI DEI RISULTATI

Grafici e Conclusioni

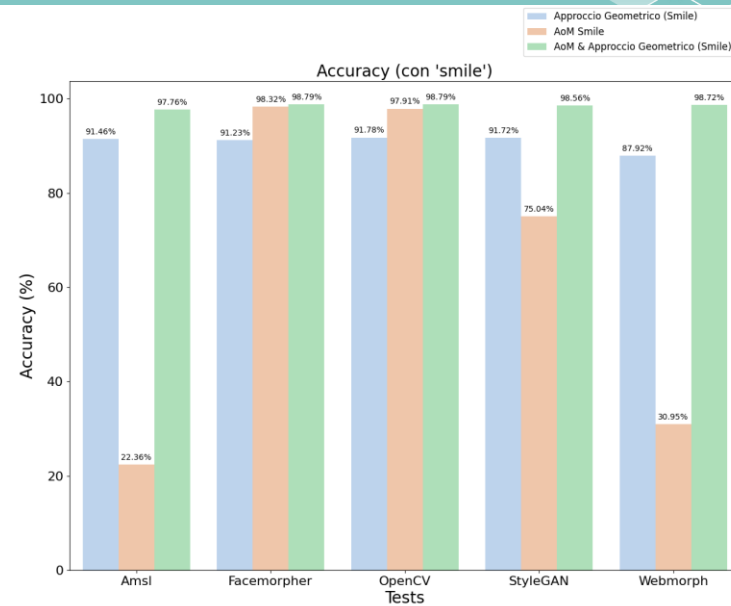
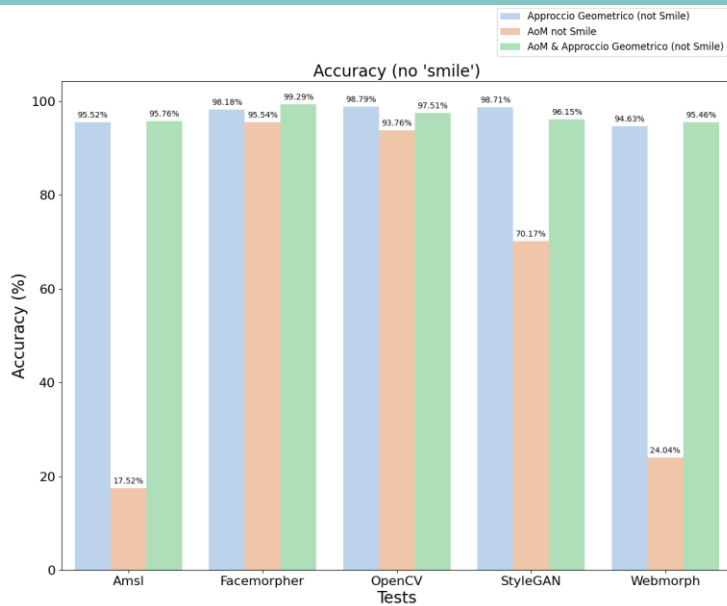
VALIDATION TEST



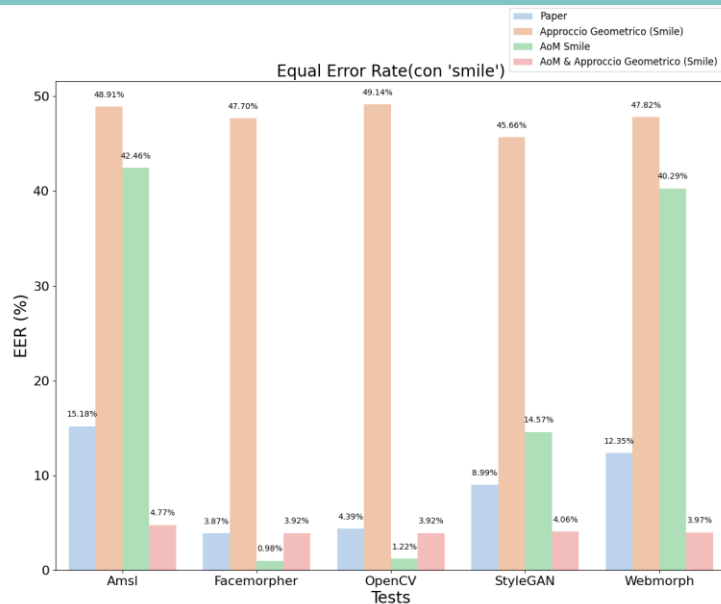
AoM vs PAPER



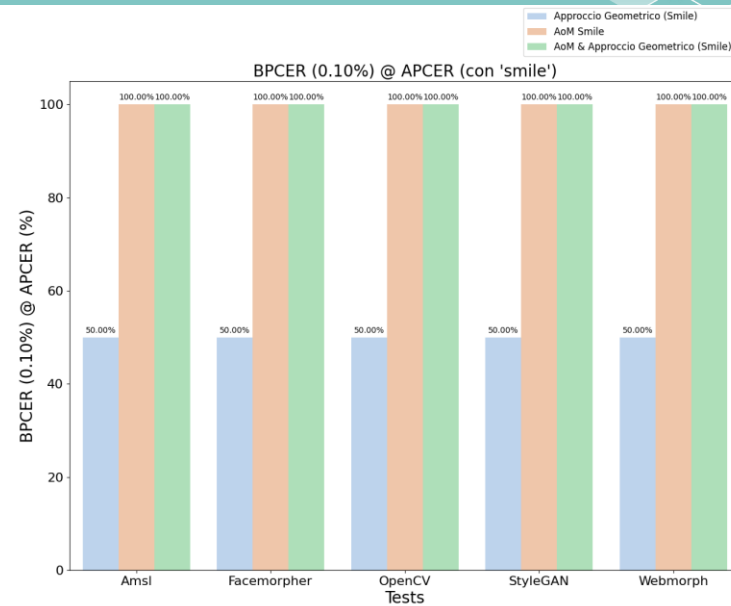
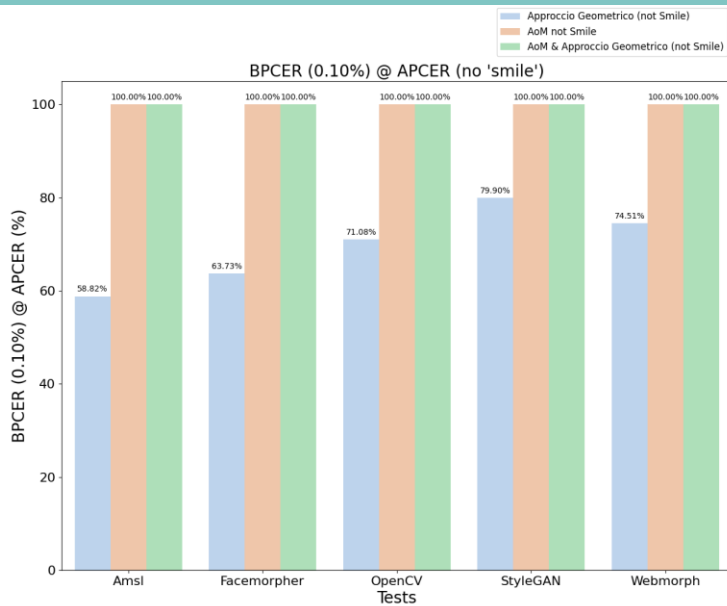
ACCURACY



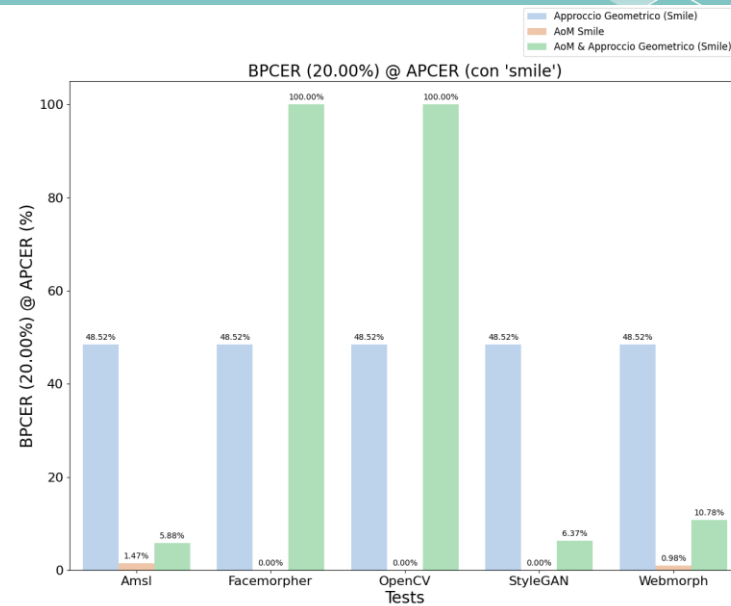
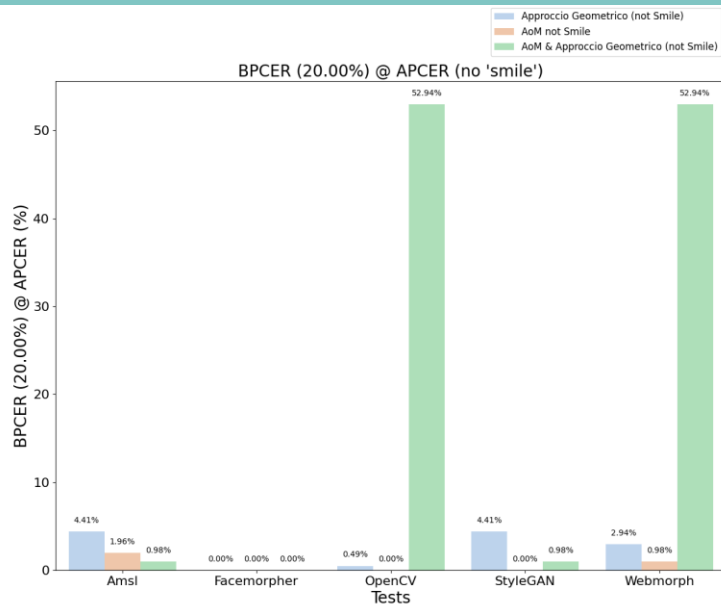
EQUAL ERROR RATE (EER)



BPCER (0.10 %) @ APCER =



BPCER (20.00 %) @ APCER =





05

Conclusioni e Implementazioni Future

Conclusioni



Il pre-processing ha migliorato la classificazione



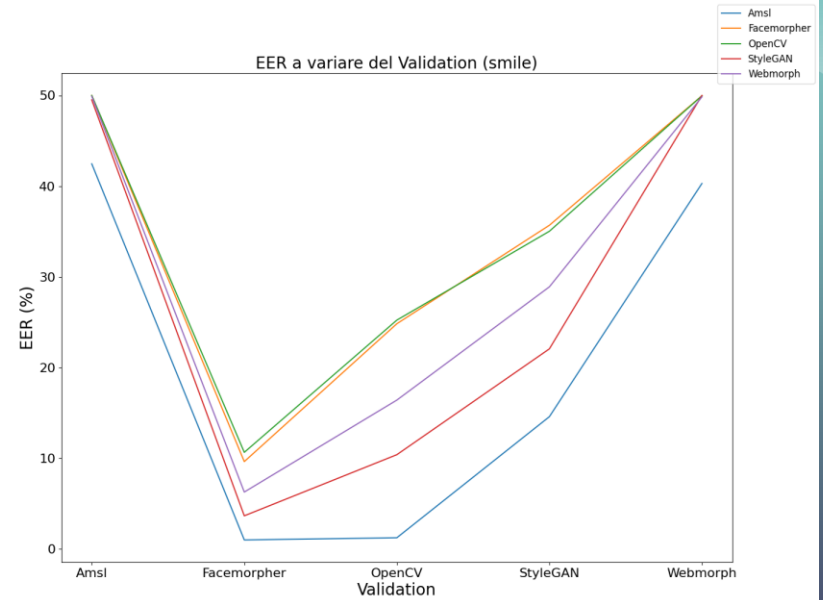
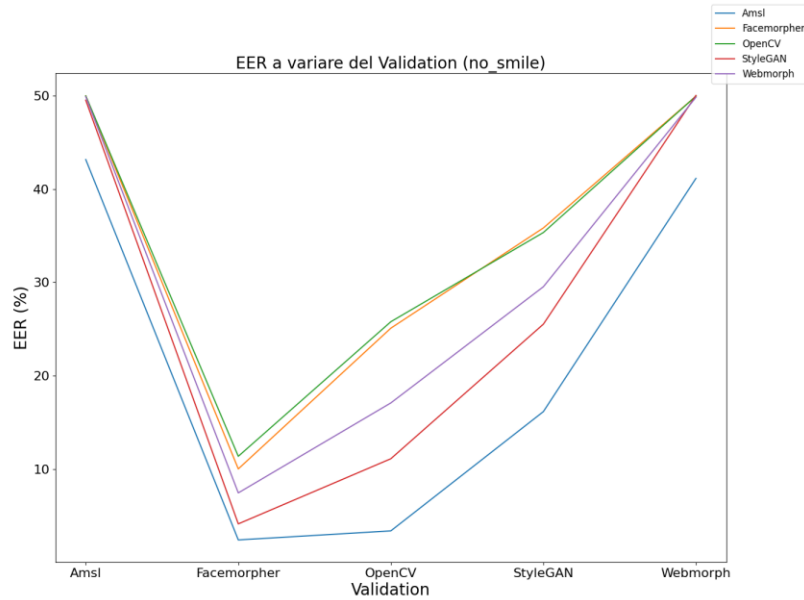
Il merge in media ha portato dei miglioramenti al nostro AoM.



Approccio geometrico migliorato nel riconoscimento dei sorrisi.

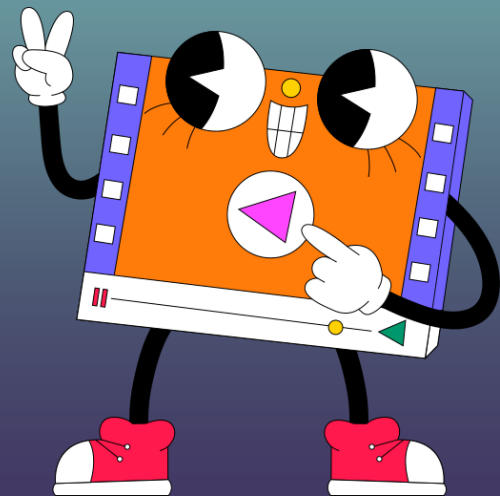


Sviluppi futuri



Sviluppo futuro

Utilizzare un dataset contenente video per considerare ulteriori caratteristiche dovute al movimento



GRAZIE!

Alessandro Aquino
Alberto Montefusco
Simone Tartaglia

