



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





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 of which are filled with a light teal color. The background is a teal-to-blue gradient.

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

A decorative graphic at the bottom of the slide, similar to the one at the top, but rendered in white and light blue lines and dots against a dark blue background.

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



A decorative graphic at the top of the slide consisting of a cluster of white-outlined hexagons of various sizes, some of which are filled with a light teal color. The background is a solid teal color.

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”





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



STEP 3

Feature Extraction



STEP 4

Classificatori

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 e capire in quali punti il modello pone maggiormente la sua attenzione



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

...

Abbiamo calcolato una ROC
curve per rappresentare la
relazione tra il FAR e il FRR
al variare di una soglia di
decisione

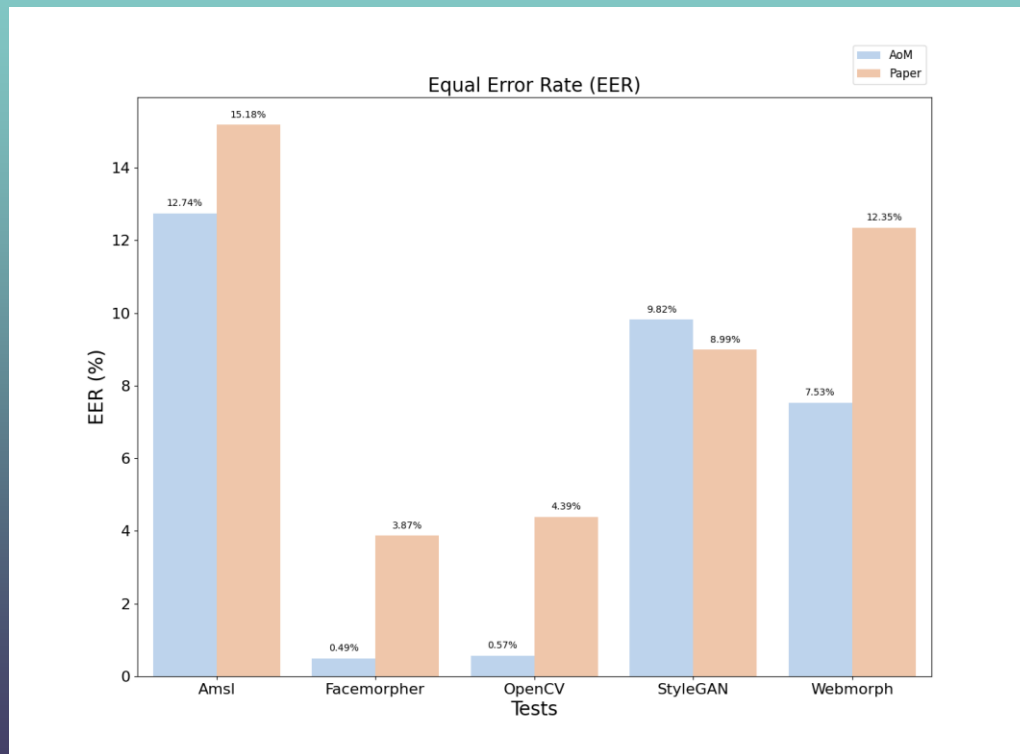
A decorative graphic on the left side of the slide. It features a grid of hexagons in various shades of teal and blue. Some hexagons are solid, while others are outlined. Small teal dots are placed at the vertices of the hexagonal grid, and thin white lines connect some of these dots, creating a network-like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

04

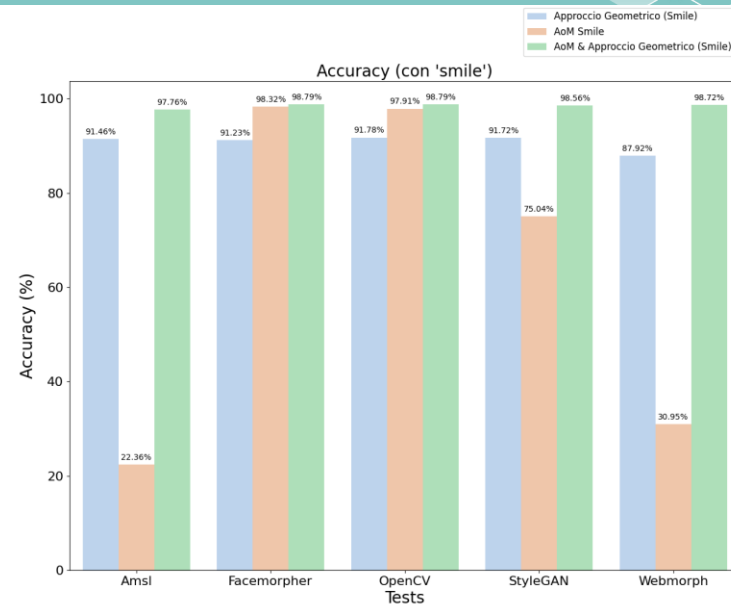
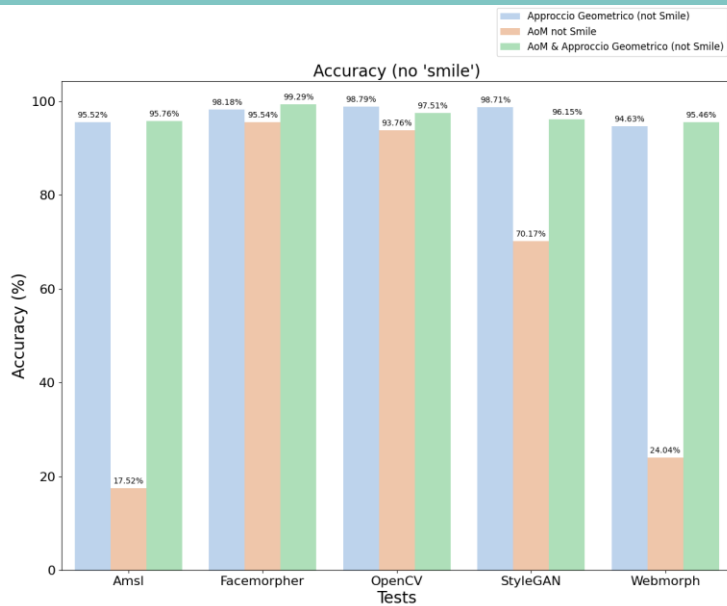
ANALISI DEI RISULTATI

Grafici e Conclusioni

AoM vs PAPER



ACCURACY



MATRICI DI CONFUSIONE – AoM



Not Smile						
Confusion Matrix	DecisionTreeClassifier()		RandomForestClassifier()		GaussianNB()	
AMSL	96	6	100	2	102	0
	1973	202	2102	73	1878	297
FaceMorpher	96	6	100	2	102	0
	97	1125	59	1163	59	1163
OpenCV	96	6	100	2	102	0
	163	1066	124	1105	83	1146
StyleGAN	96	6	100	2	102	0
	478	744	527	695	395	827
WebMorph	96	6	102	0	102	0
	1099	122	1193	28	1005	216

Smile						
Confusion Matrix	DecisionTreeClassifier()		RandomForestClassifier()		GaussianNB()	
AMSL	195	9	204	0	204	0
	1968	207	2107	68	1847	328
FaceMorpher	195	9	204	0	204	0
	77	1145	45	1177	24	1198
OpenCV	195	9	204	0	204	0
	129	1100	100	1129	30	1199
StyleGAN	195	9	198	6	204	0
	481	741	532	690	356	866
WebMorph	195	9	204	0	204	0
	1097	124	1194	27	984	237

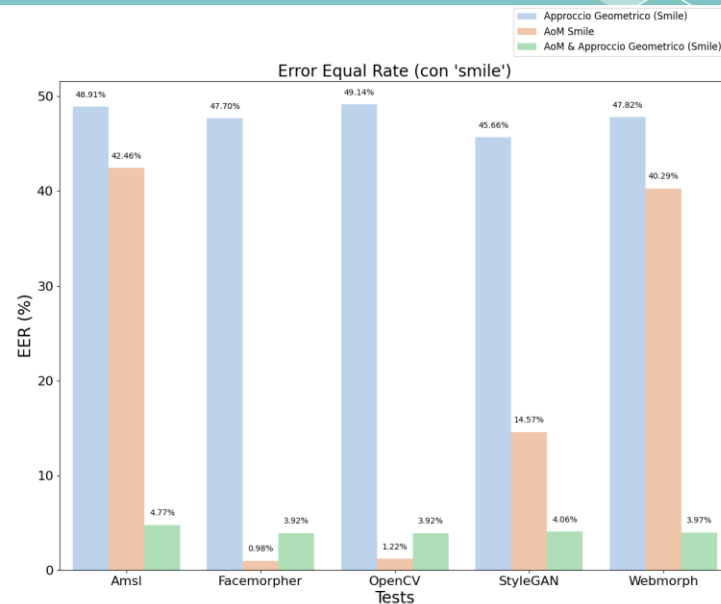
MATRICI DI CONFUSIONE – AoM & AP



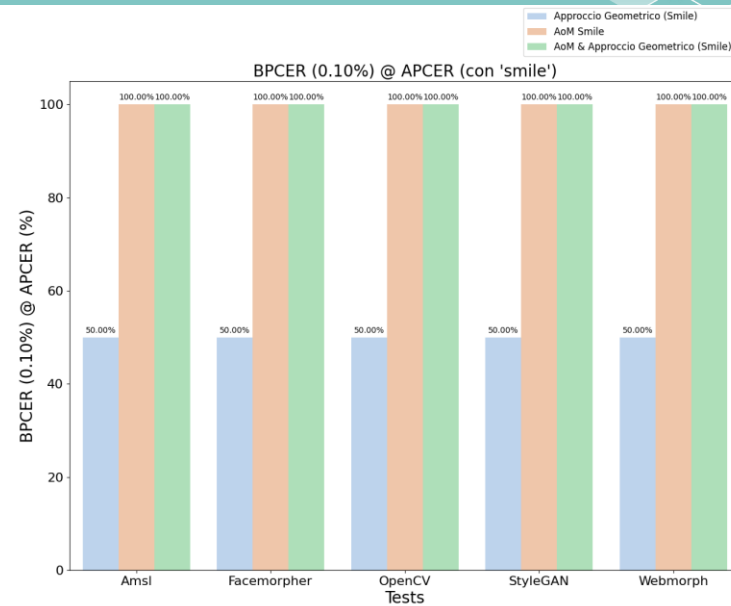
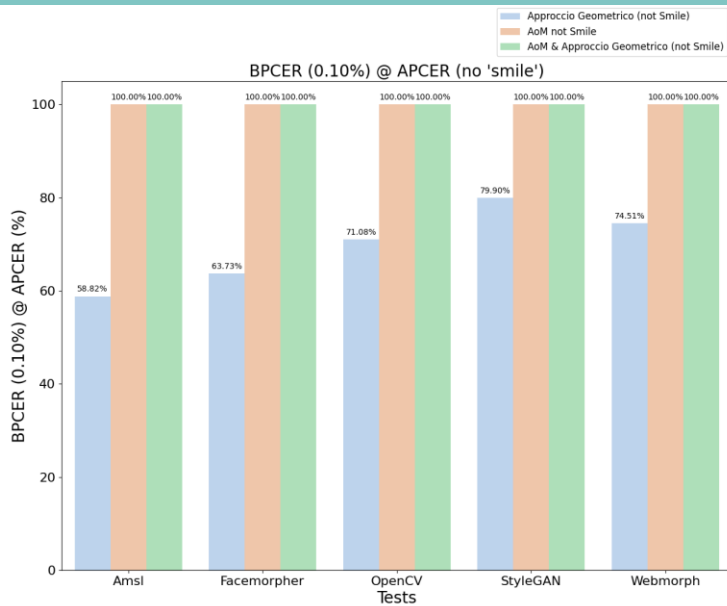
Not Smile						
Confusion Matrix	DecisionTreeClassifier()		RandomForestClassifier()		GaussianNB()	
AMSL	94	8	96	6	99	3
	892	138	925	105	45	985
FaceMorpher	98	4	102	0	99	3
	25	1005	8	1022	14	1200
OpenCV	98	4	102	0	99	3
	84	946	41	989	30	1191
StyleGAN	94	8	96	6	99	3
	420	802	400	822	48	1174
WebMorph	94	8	96	6	99	3
	1062	159	1135	86	57	1164

Smile						
Confusion Matrix	DecisionTreeClassifier()		RandomForestClassifier()		GaussianNB()	
AMSL	199	5	190	14	188	16
	1829	244	1886	187	35	2038
FaceMorpher	199	5	190	14	188	16
	42	1078	29	1091	0	1120
OpenCV	199	5	190	14	188	16
	92	1027	1042	1077	0	1119
StyleGAN	186	18	190	14	188	16
	379	741	363	757	3	1117
WebMorph	186	18	190	14	188	16
	989	130	1041	78	1	1118

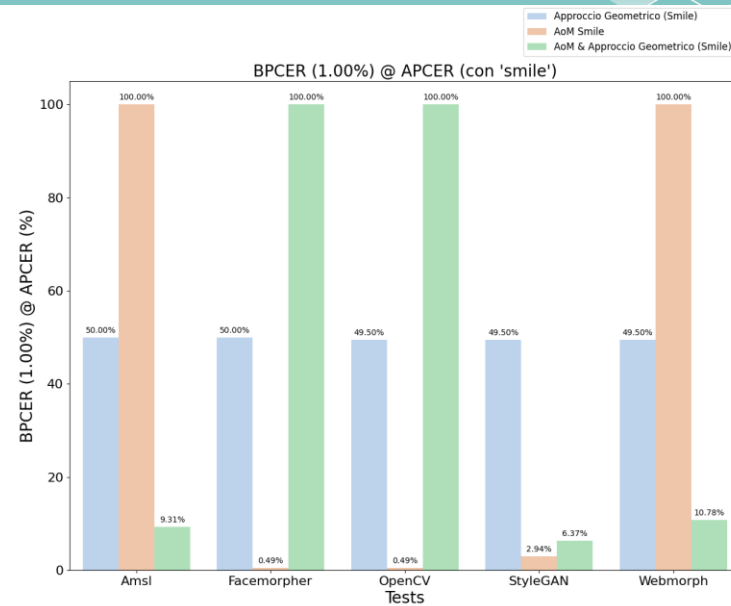
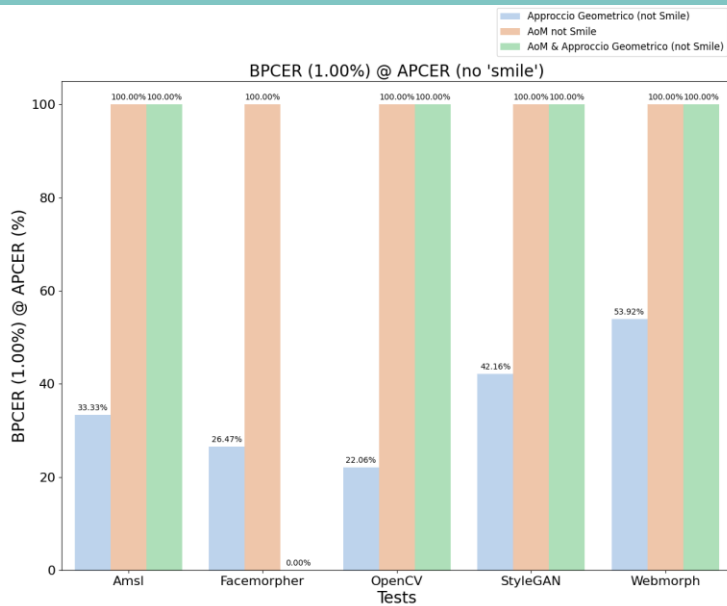
EQUAL ERROR RATE (EER)



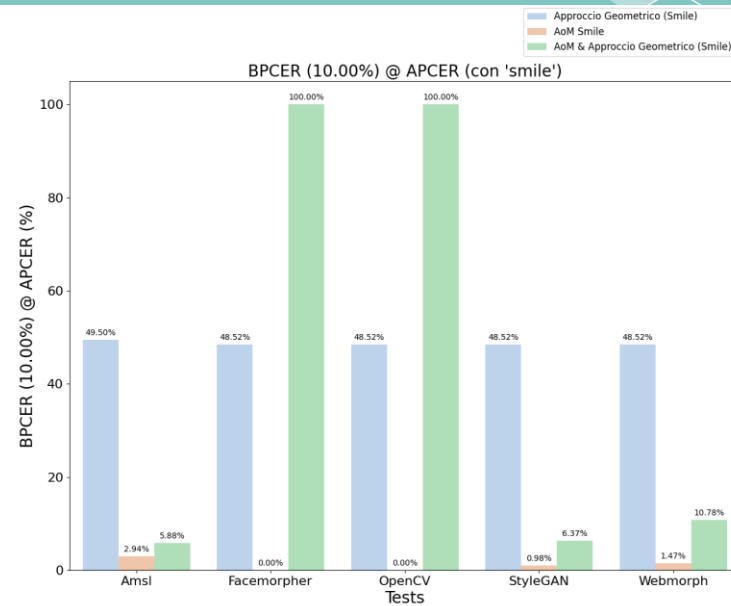
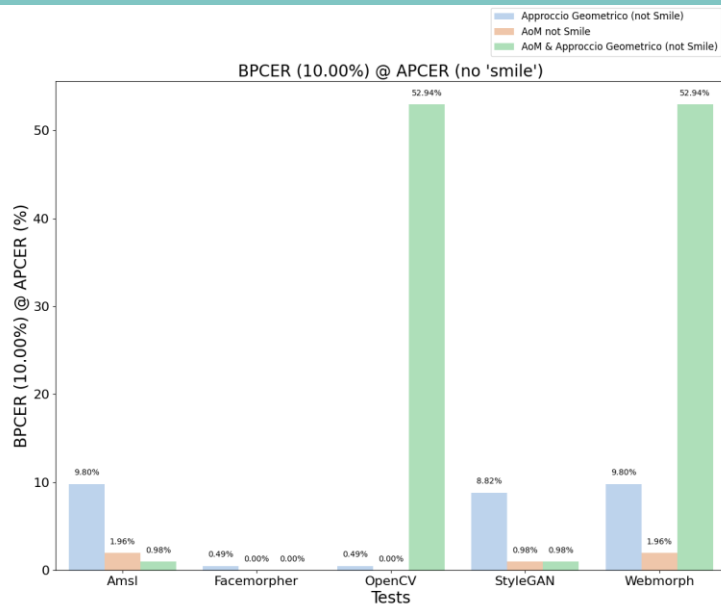
BPCER (0.10 %) @ APCER =



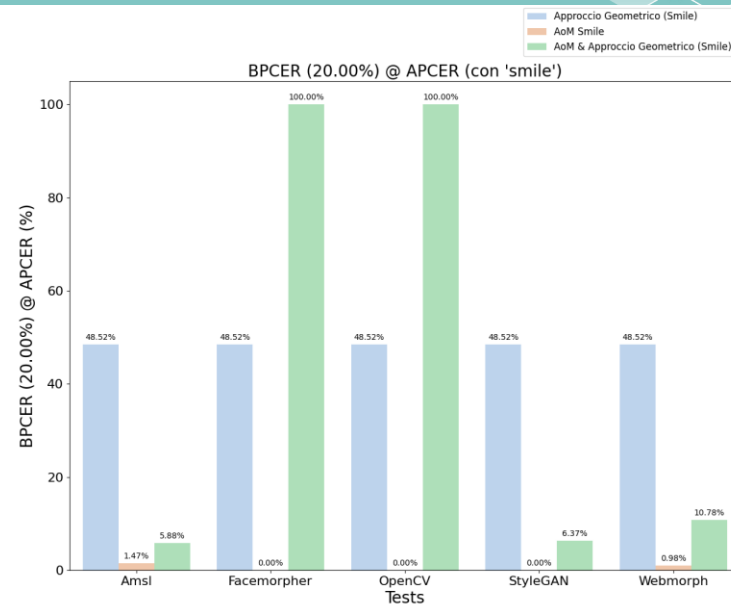
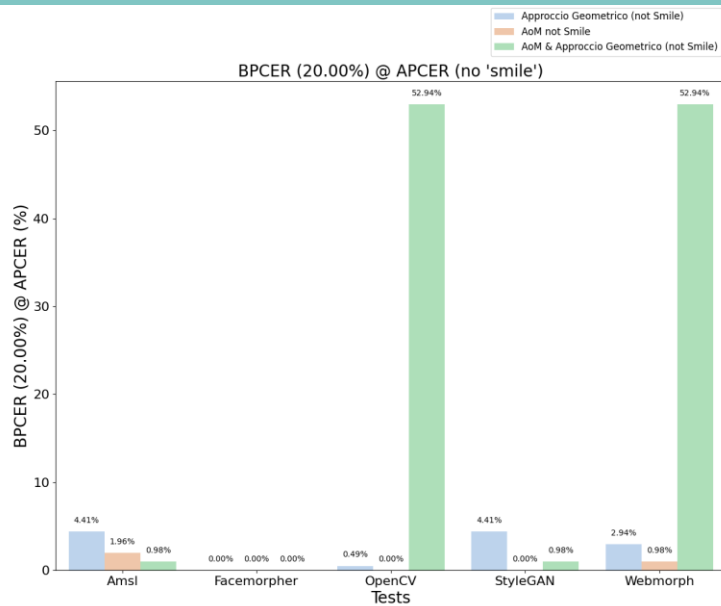
BPCER (1.00 %) @ APCER =



BPCER (10.00 %) @ 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.

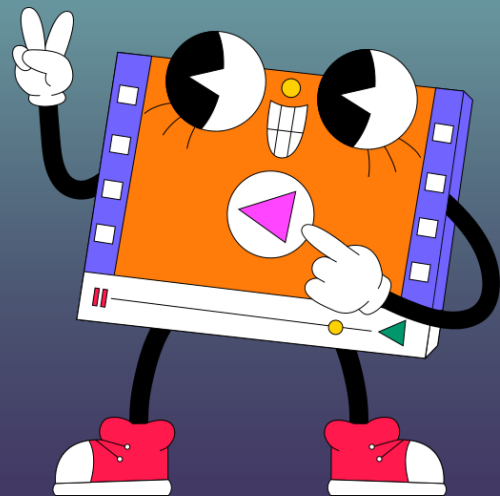


Approccio geometrico migliorato nel riconoscimento dei sorrisi.



Sviluppo futuro

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



GRAZIE!

Alessandro Aquino
Alberto Montefusco
Simone Tartaglia

