Riconoscimento di volti morphed: un approccio basato su Deep Learning

Visione artificiale e riconoscimento

Relatore:

Prof. Matteo Ferrara

Co-relatore:

Dott. Guido Borghi

Presentata da:

Emanuele Pancisi

Università di Bologna – Campus di Cesena, Italia

Biometric System Laboratory
DISI - University of Bologna

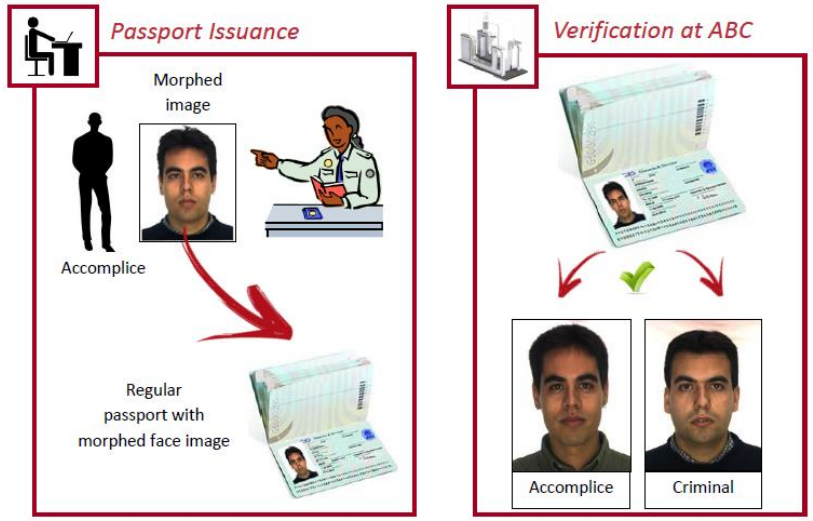
Face Morphing e Face Morphing Attacks

- **Face Morphing**
  Trasformazione fluida e **graduale** tra i **volti** di **due soggetti** diversi

- **Problema**
  I sistemi di **riconoscimento facciale** associano il volto **morphed** ad **entrambi** i **soggetti**
  - **Caso applicativo**: **ABC** gate negli **aeroporti**

- **Face Morphing Attack**[1]
  1. **Richiesta del passaporto** da parte del **complice** fornendo una foto morphed
  2. **Utilizzo del passaporto** regolare per la verifica dell'identità realizzata da **entrambi** i soggetti

complice morphed criminale



I due passi di un Face Morphing Attack

1. *Ferrara, Matteo, et. al "The magic passport." IEEE IJCB 2014*

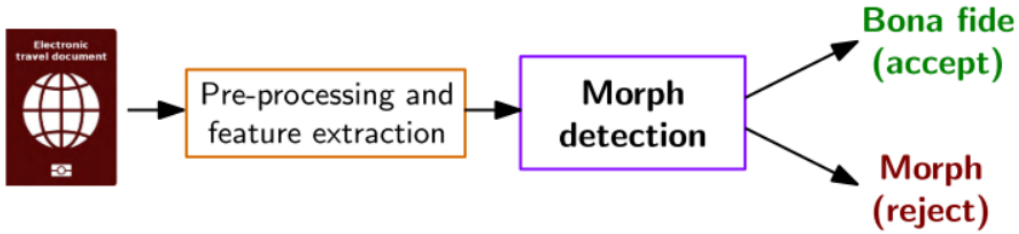
Morphing Attack Detection (MAD)

- Necessari algoritmi di **Morphing Attack Detection (MAD)**

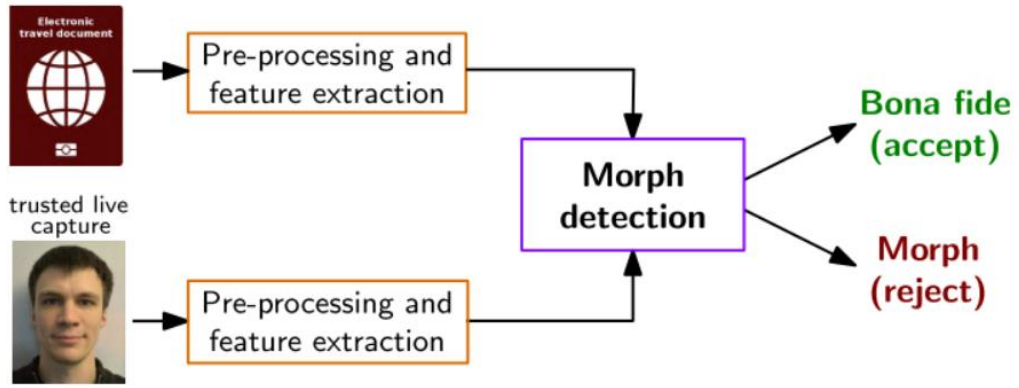
- **Due scenari** in base al numero di immagini in input:

  - **Single-images (S-MAD):** lavorano sull'immagine del **passaporto** elettronico (eMRTD)

  - **Differential-images (D-MAD):** lavorano sull'immagine del **passaporto** e una **foto scattata** sul momento
    - Due ulteriori scenari in base a chi si presenta:
      - **Criminale**
      - **Complice**



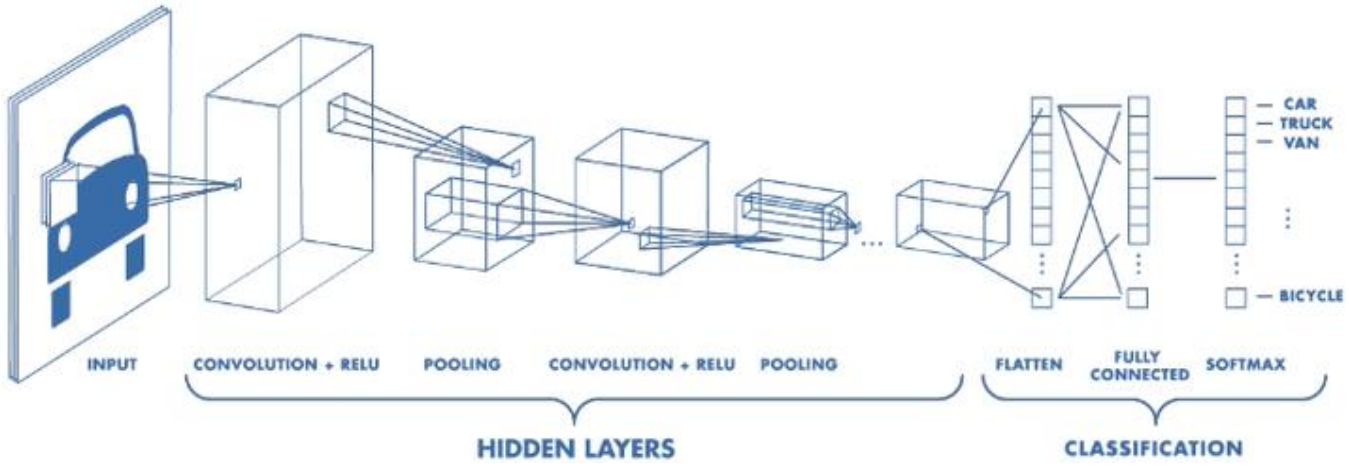
Single-image Morphing Attack Detection (S-MAD)



Differential Morphing Attack Detection (S-MAD)

Obiettivi

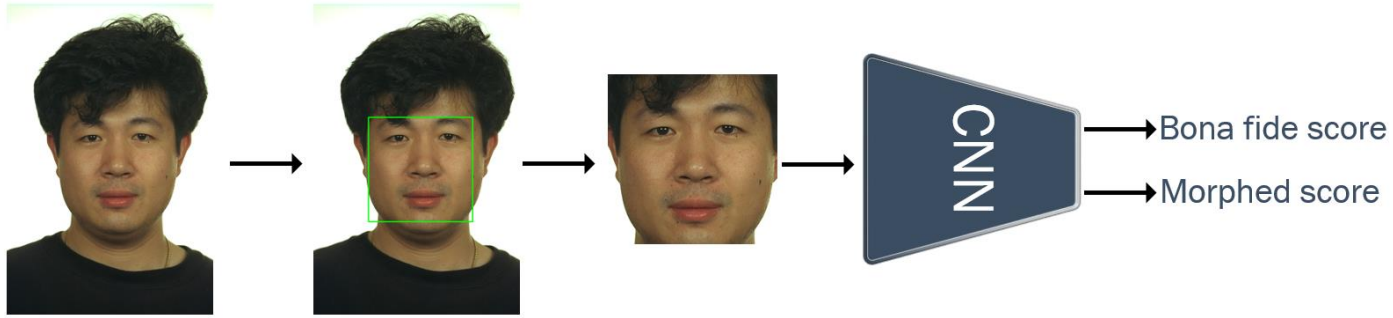
- Affrontare il **problema** del **face morphing** proponendo metodi basati su **Deep Learning**
  - Apprendimento supervisionato con Convolutional Neural Networks (**CNN**)



- Affrontare sia lo scenario a **singola immagine** che quello a **differenziale**
  - **Due metodi** per scenario **singola immagine** basati su **analisi qualitativa** (**ricerca di artefatti** legati al morphing)
  - **Due metodi** per scenario **differenziale** basati su **analisi qualitativa** e **analisi d'identità**

S-MAD basato su immagine intera

- **Idea**: utilizzare una rete neurale (**CNN**) per ricercare la **presenza di artefatti** all'interno del **volto**
- **Input**:
  - **Crop** del **volto** estratto tramite *dlib*[1]
- **Output**:
  - **Due score** nel range **[0, 1]** che rappresentano la **probabilità** che **l'immagine** sia **morphed** e **bona fide**
- **Addestramento**:
  - Pesi inizializzati **casualmente** (from scratch)
  - **Fine-tuning** di reti **preaddestrate** su diversi dataset (*Imagenet* [2] o *VGGFace2*[3] e *MS1M*[4])

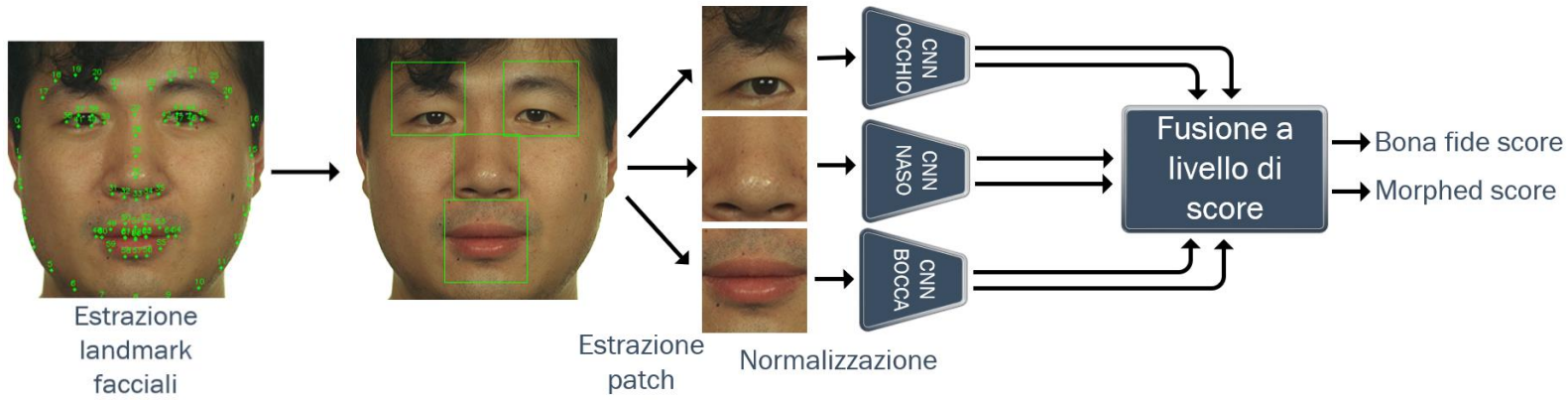


1. http://dlib.net/
2. *Jia, Deng, et al. "Imagenet: A large-scale hierarchical image database." IEEE CVPR 2009*
3. *Qiong, Cao, et al. "Vggface2: A dataset for recognising faces across pose and age." IEEE FG 2018*
4. *Yandong, Guo, et al. "Ms-celeb-1m: A dataset and benchmark for large-scale face recognition." Springer ECCV 2016*

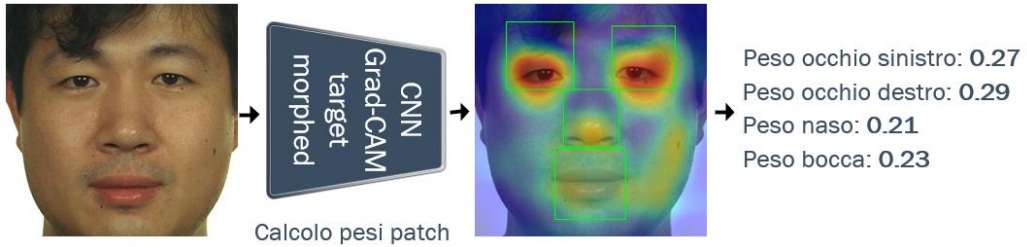
S-MAD basato su fusione a livello di score di singole patch

- **Idea**: utilizzare più reti neurali (**CNN**) per ricercare la **presenza di artefatti** all'interno di **parti del volto** e fondere i risultati ottenuti

- **Input**:
  - **Crop** di **occhi**, **naso** e **bocca** estratti in base ai landmark facciali di *dlib*



- **Output:**
  - **Fusione** attraverso media di **score**:
    - **Media semplice**
    - **Media pesata** in base alle **attivazioni** del **gradiente (Grad-CAM)**[1]



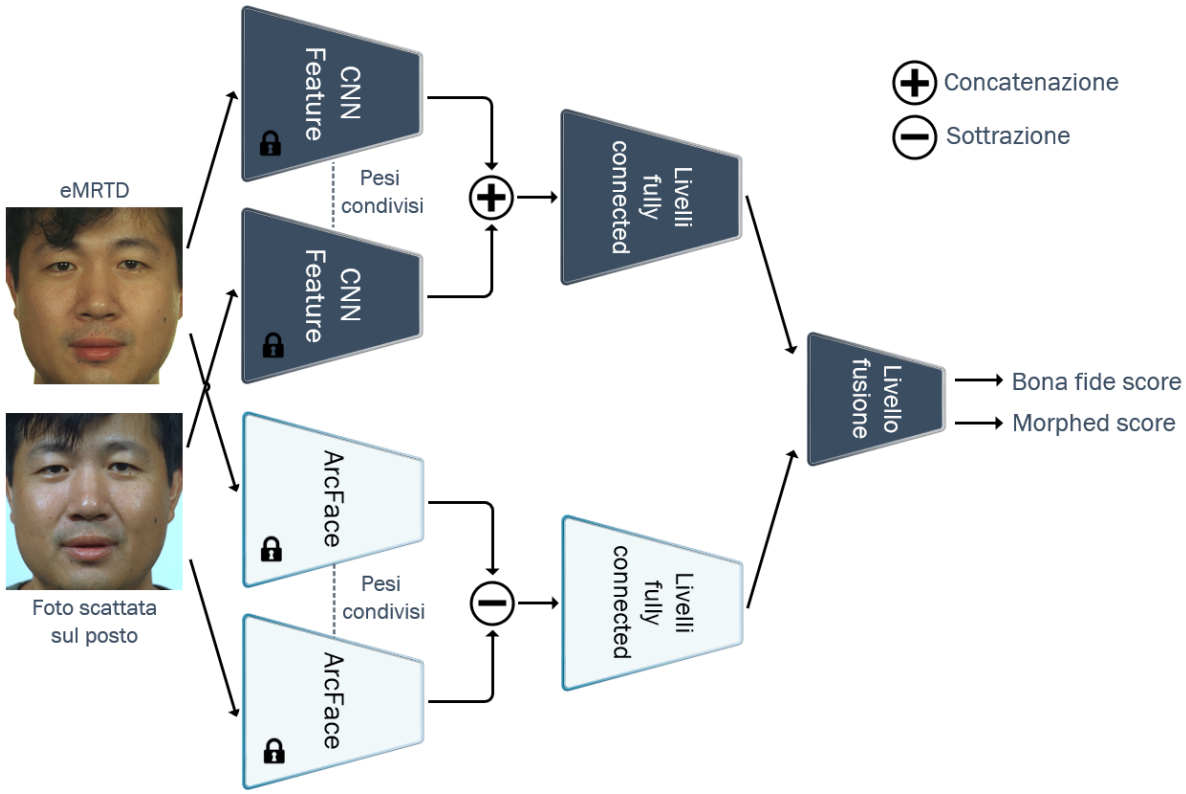
1. *Selvaraju, Ramprasaath R, et. al "Grad-cam: Visual explanations from deep networks via gradient-based localization." IEEE ICCV 2017*

D-MAD basato su rete Siamese

- **Idea**: utilizzare un'architettura di **rete Siamese** per unire **l'analisi qualitativa** e quella **d'identità**

- Due blocchi:
  1. **Analisi qualitativa** e ricerca di artefatti
  2. **Analisi d'identità** (rete stato dell'arte ***ArcFace*** [1])

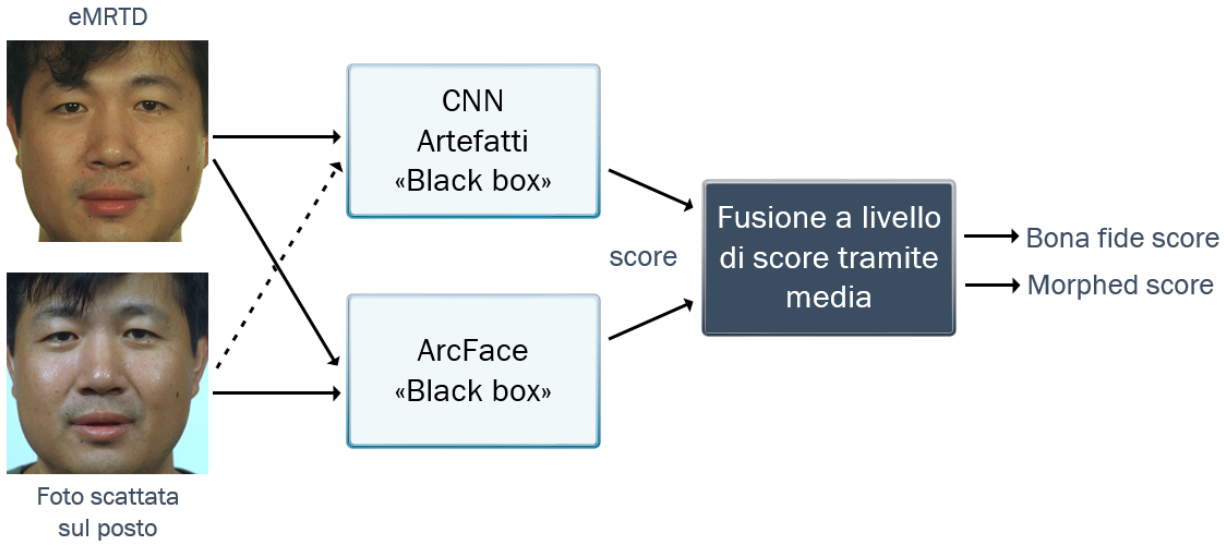
- **Addestramento**:
  - **Riutilizzo reti fine-tuned** per riconoscimento morphing
  - L'aggiornamento dei **pesi** delle **«backbone»** di entrambi i sottosistemi è **bloccato**
  - **Addestramento** livelli **fully connected** in **due fasi**:
    - 10 epoche per **blocco analisi d'identità**
    - 2 epoche per **blocco analisi qualitativa**



1. *Scherhag, Ulrich, et al. "Deep Face Representations for Differential Morphing Attack Detection." IEEE TIFS 2020*

D-MAD basato su fusione di score

- **Idea**: realizzare la **fusione a livello di score** di un sistema per **l'analisi qualitativa** e uno per quella **d'identità**
- **Input**:
  - **Crop** del **volto** dell'immagine del **passaporto** per il sistema di **analisi qualitativa**
  - **Crop** del **volto** dell'immagine del **passaporto** e della **foto scattata sul posto** per il sistema di **analisi d'identità**
- **Output**: **Fusione** attraverso **media semplice** degli **score** dei **due sistemi** utilizzati singolarmente



- Sistemi utilizzati come «**black box**»
- Possono essere utilizzati direttamente **entrambi** i **metodi** presentati nel caso a **singola immagine**

Training, validation e test

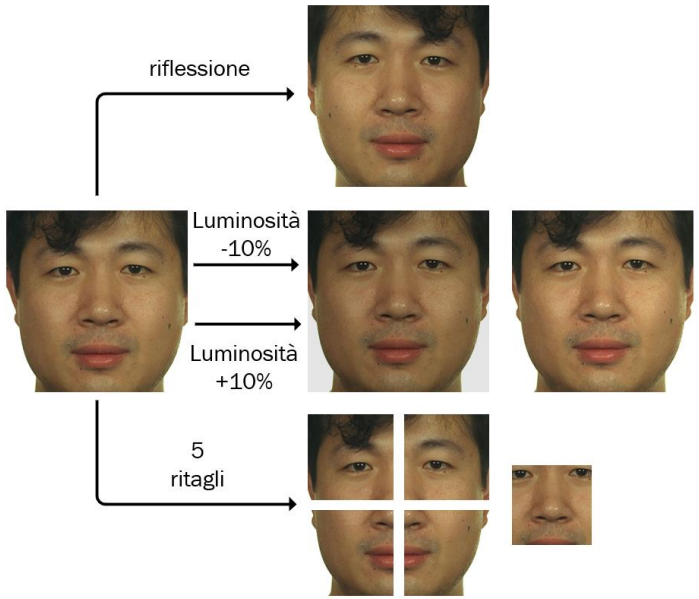
- **Tre dataset** disponibili:
  - **PMDB**: immagini morphed **generate automaticamente**
  - **MorphDB**: immagini morphed **ritoccate manualmente**
  - **LondonDB**: immagini morphed **compresse** con **JPEG**

- Valutazione **cross-dataset**

- Suddivisione dataset
  - **Training** set: **80%** dei soggetti di **PMDB**
  - **Validation** set: **20%** dei soggetti di **PMDB**
  - **Test** set: **MorphDB, LondonDB**

- Applicazione **data augmentation** online per **ridurre overfitting**
  1. **Riflessione orizzontale**
  2. **Ritaglio** casuale
  3. **Cambio** di **luminosità** casuale

PMDB MorphDB LondonDB



Metriche

- **Metriche** per la valutazione di algoritmi di MAD**:**
  - **Attack Presentation Classification Error Rate (APCER):** proporzione **attacchi morphed classificati** come **bona fide**

$$APCER = \frac{M}{N_m}$$

M= numero di immagini morphed classificate come bonafide
N_m = numero totale di immagini morphed

  - **Bona Fide Presentation Classification Error Rate (BPCER):** proporzione **immagini bona fide classificate** come **morphed**

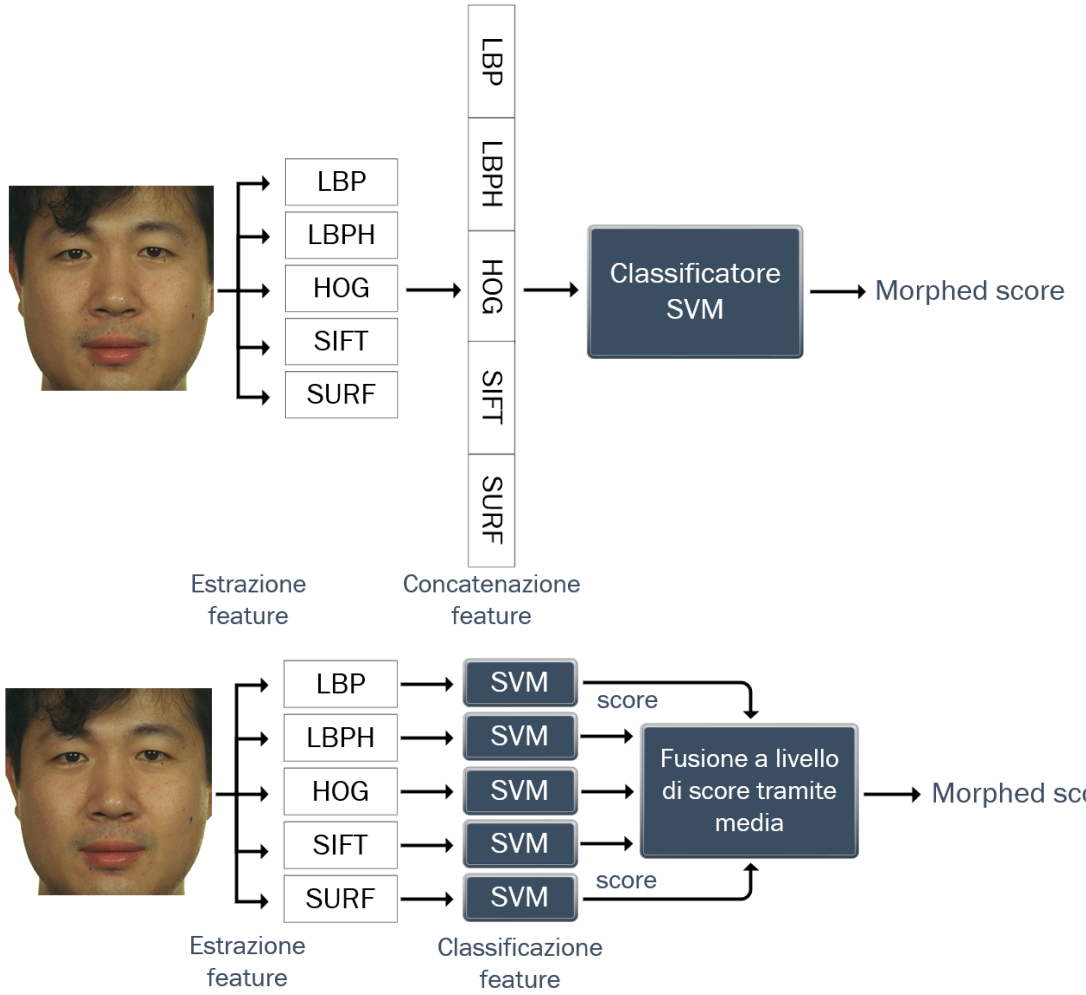
$$BPCER = \frac{N}{N_b}$$

N= numero di immagini bona fide classificate come morphed
N_b = numero totale di immagini bonafide

  - **Equal Error Rate (EER):** tasso di **errore** nel **punto** in cui **APCER=BPCER**

Comparazione con lo stato dell'arte MAD

- **S-MAD**
  - **Re-implementazione** tecniche di MAD basate su **descrittori (feature) manuali**[1]
  - Feature estratte:
    - **LBP, LBPH, HOG, SIFT** e **SURF**
  - **Combinazione** delle **feature**:
    - **Concatenazione feature** e successiva classificazione
    - **Fusione** degli **score** delle singole feature



- **D-MAD**
  - Rete stato dell'arte ***ArcFace***[2] per l'estrazione di **feature d'identità**

1. *Scherhag, Ulrich, et al. "Towards detection of morphed face images in electronic travel documents." IEEE DAS 2018*
2. *Scherhag, Ulrich, et al. "Deep Face Representations for Differential Morphing Attack Detection." IEEE TIFS 2020*

Risultati S-MAD

Architettura ***Se-ResNet50*** **preaddestrata** su dataset di volti (*VGGFace2* e *MS1M*)

Test set	Metodo	EER	$BPCER_{100}$	$BPCER_{1000}$
MorphDB	**LBP+SIFT+SURF**	**10.75%**	73.00%	75.50%
	Volto intero	**0.75%**	0.50%	7.00%
	Fusione media	**0.25%**	0.50%	0.50%
	Fusione Grad-CAM	0.75%	0.50%	2.00%
LondonDB	**LBPH+SIFT+SURF**	**19.69%**	75.00%	89.71%
	Volto intero	**2.44%**	6.37%	44.12%
	Fusione media	**2.92%**	10.78%	54.41%
	Fusione Grad-CAM	3.42%	11.28%	48.04%

Risultati D-MAD

Test set	Coppia	Rete	EER	$BPCER_{100}$	$BPCER_{1000}$
MorphDB	Criminale	**ArcFace**	**0.64%**	0.53%	2.91%
		Fusione media	0.52%	0.00%	1.85%
		Siamese	**0.00%**	0.00%	0.00%
	Complice	**ArcFace**	**12.33%**	92.86%	99.47%
		Fusione media	2.51%	5.03%	7.01%
		Siamese	**1.42%**	1.85%	4.50%
	Entrambi	**ArcFace**	**8.20%**	72.88%	99.47%
		Fusione media	1.85%	2.51%	7.01%
		Siamese	**1.06%**	1.32%	4.50%
LondonDB	Criminale	**ArcFace**	**0.46%**	0.00%	1.96%
		Fusione media	0.09%	0.00%	7.84%
		Siamese	**0.14%**	0.00%	5.88%
	Complice	**ArcFace**	**1.95%**	2.94%	7.84%
		Fusione media	0.25%	0.00%	22.55%
		Siamese	**0.09%**	0.00%	1.96%
	Entrambi	**ArcFace**	**1.10%**	1.96%	5.88%
		Fusione media	0.17%	0.00%	16.67%
		Siamese	**0.12%**	0.00%	5.88%

Risultati su immagini Print&Scan

- Lo **scenario più realistico** è quello delle immagini **Print&Scan**
- La **stampa** e **riacquisizione rimuove informazioni** relative al morphing e ne **aggiunge** di **non correlate**
- **Risultati inferiori** ma **buoni** considerando che **non viene fatto fine-tuning** su questo tipo di immagini

digitale

Print&Scan

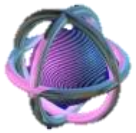
Tipo immagine	EER	$BPCER_{100}$	$BPCER_{1000}$
Digitale	**0.75%**	0.50%	7.00%
Print&Scan	**11.25%**	33.00%	51.50%

S-MAD su MorphDB

Coppia	Tipo immagine	EER	$BPCER_{100}$	$BPCER_{1000}$
Criminale	Digitale	0.00%	0.00%	0.00%
	Print&Scan	3.55%	7.14%	18.65%
Complice	Digitale	1.42%	1.85%	4.50%
	Print&Scan	10.23%	34.52%	38.76%
Entrambi	**Digitale**	**1.06%**	1.32%	4.50%
	Print&Scan	**7.14%**	23.41%	38.76%

D-MAD su MorphDB

Conclusioni e sviluppi futuri



- Conclusioni:
  - I metodi proposti sono stati testati in modalità **cross-dataset** su **due dataset** di **test molto differenti**
  - I **risultati** sono **migliori rispetto** a quelli ottenuti con **tecniche** presenti nello **stato dell'arte**
  - La **problematica** più evidente è la **scarsa quantità** di **dati** su cui è stato effettuato **l'addestramento** e la conseguente **difficoltà** a **generalizzare** su **sorgenti** dati molto **diverse**

- Sviluppi futuri:
  - **Test su altri dataset** per verificare le prestazioni
  - **Sottomissione** nei **benchmark ufficiali** (**SOTAMD**[1] e FRVT-MORPH[2])
  - **Studio** più **approfondito** dello scenario **Print&Scan**

1. *https://biolab.csr.unibo.it/fvcongoing/UI/Form/IJCB2020MAD.aspx*
2. *https://pages.nist.gov/frvt/html/frvt_morph.html*

Riconoscimento di volti morphed: un approccio basato su Deep Learning

Grazie per l'attenzione

Relatore:

Prof. Matteo Ferrara

Co-relatore:

Dott. Guido Borghi

Presentata da:

Emanuele Pancisi

Università di Bologna – Campus di Cesena, Italia

Biometric System Laboratory
DISI - University of Bologna