1st Open Day and Workshop
14th July 2022

INSTITUTO DE SISTEMAS E ROBÓTICA
UNIVERSIDADE DE COIMBRA

Robustness of deep learning based face recognition under morphing attacks

Iurii Medvedev

Face Morphing

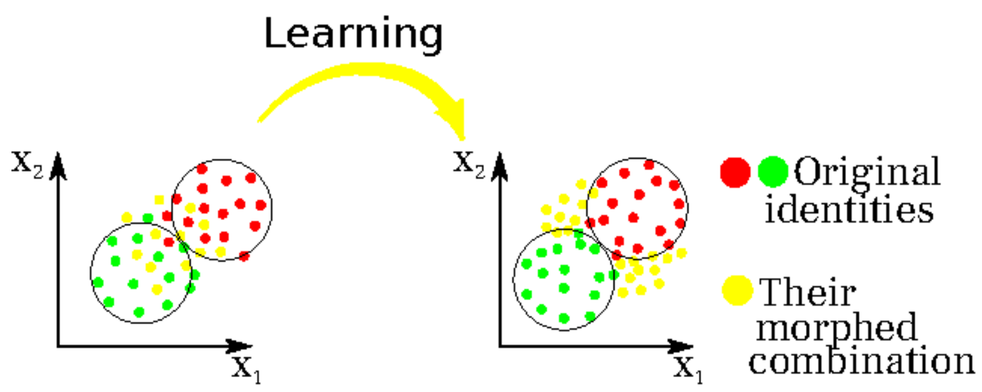
- Image morphing techniques are used to combine information from two (or more) images into one image.

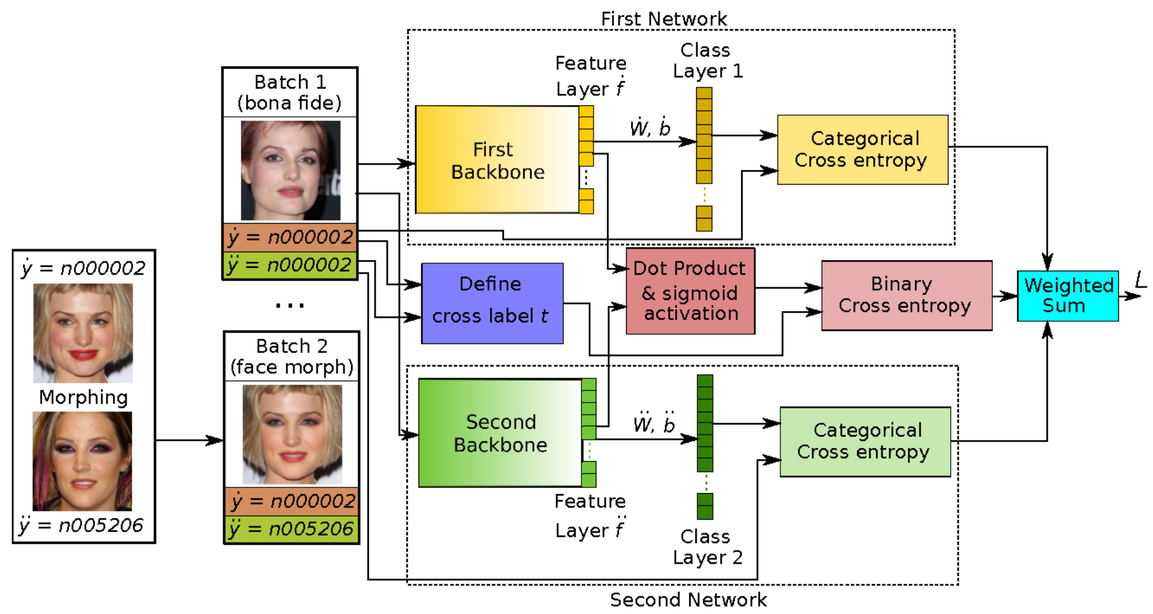
- Face Morphing oppose significant risks for document security.
- Two scenarios of morphing detection are usually considered :
  - No-reference (enrollment scenario)
  - Differential (border control scenario).

Methodology

-We propose to investigate several strategies for no-reference morphing detection and improving resistance of face recognition to face morphing.

- Our approaches imply following deep learning based face recognition and designing sophisticated sample mining techniques with use of morphed face images for better control of deep feature distribution.





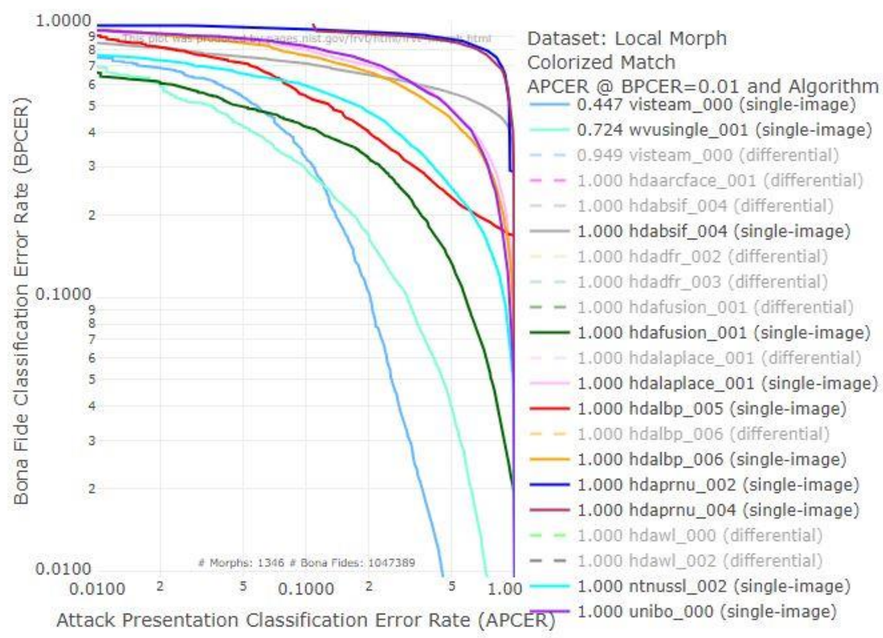
$$L_1 = -\frac{1}{N}\sum_i^N \log\left(\frac{e^{\dot{W}_{\dot{y}_i}^T \dot{f}_i + \dot{b}_{\dot{y}_i}}}{\sum_j^C e^{\dot{f}_{\dot{y}_j}}}\right) \qquad L_2 = -\frac{1}{N}\sum_i^N \log\left(\frac{e^{\ddot{W}_{\ddot{y}_i}^T \ddot{f}_i + \ddot{b}_{\ddot{y}_i}}}{\sum_j^C e^{\ddot{f}_{\ddot{y}_j}}}\right)$$

$$L_3 = -\frac{1}{N}\sum_i^N t \log\frac{1}{1+e^{-D}} + (1-t)\log\left(1-\frac{1}{1+e^{-D}}\right)$$

$$t = abs(sgn(\dot{y}_i - \ddot{y}_i)) \qquad D = \dot{f}\cdot\ddot{f}$$

$$L = \alpha_1 L_1 + \alpha_2 L_2 + \beta L_3$$

NIST FRVT MORPH benchmark results



Conclusion and current achievements:

-SOTA performance in several benchmarks of NIST FRVT MORPH.

-The project have received the direct Nvidia Hardware support.

-First publication is pending for reviews.

Further work:

- Refine no-reference morphing detection for the new NIST report.
- Expand the method to differential morphing detection.

For questions please videocall via WhatsApp
+351 911132127