**Face Pasting Attack**

Niklas Bunzel  
Fraunhofer SIT / ATHENE  
Darmstadt, Germany  
bunzel@sit.fraunhofer.de

Lukas Graner  
Fraunhofer SIT / ATHENE  
Darmstadt, Germany  
graner@sit.fraunhofer.de

**ABSTRACT**

Cujo AI and Adversa AI hosted the MLSec face recognition challenge. The goal was to attack a black box face recognition model with targeted attacks. The model returned the confidence of the target class and a stealthiness score. For an attack to be considered successful the target class has to have the highest confidence among all classes and the stealthiness has to be at least 0.5. In our approach we paste the face of a target into a source image. By utilizing position, scaling, rotation and transparency attributes we reached 3rd place. Our approach took approximately 200 queries per attack for the final highest score and about \( \sim 7.7 \) queries minimum for a successful attack. The code is available at https://github.com/bunni90/FacePastingAttack.

**KEYWORDS**

Adversarial Attack, Face Recognition, Challenge, Black Box

**1 INTRODUCTION**

The Machine Learning Security Evasion Competition takes place at the DEFCON AI Village since 2019 with tasks like attacking ML based malware detection or antiphishing systems or defending against attacks. In this years competition there are two tasks evading an anti phishing system and evading a face recognition system. In this paper we focus on the task of evading the face recognition system. Face recognition is being used in production systems more and more, for example in video identification\(^1\) or to unlock and pay with your smartphone. But neural networks are prone to adversarial attacks and a variety of diverse attacks exist. In this challenge a black box face recognition system, which is secured against adversarial attacks is to be attacked by impersonation. This challenge and the attacks implemented therefore closely reflect a real world attack scenario.

**2 RELATED WORK**

The first adversarial attack L-BFGS [11] was published in 2014, since then a lot of research was conducted in this field. Madry et. al implemented the PGD [8] attack which is still considered as one of the strongest white box attacks. For black box attacks two main approaches have emerged: transfer-based attacks [9] and query-based attacks [2]. Brown et. al developed the adversarial patch [1], where the adversarial perturbation size and shape are constrained. The adversarial patch can be placed into an image to force a specific classification.

\(^{1}\)https://www.webid-telecom.de/de/#webidai

**3 BACKGROUND**

The challenge. The MLSec face recognition challenge 2022, held from August 12 to September 23, is part of the DEFCON AI Village and is organized by Adversa AI, Cujo AI and Robust Intelligence. The goal is to attack a given face recognition system, by slightly altering given face images in order to be misclassified. Since access to the model is provided solely through API calls without any further information given about it, such as architecture or training data, the model is effectively a black box. After passing an (altered) image, two scores are returned by the API: 1. confidence \( \in [0; 1] \), which represents the target class probability score of the image calculated by the model, and 2. stealthiness \( \in [0; 1] \), which is a similarity score (presumably based on SSIM) to the unaltered source images.

For the challenge 10 source images are given \( I_0, ..., I_9 \), depicting the faces of 10 persons which represent the set of classes \( C_0, ..., C_9 \). The goal is for each source image \( I_t \) to construct 9 alterations \( I_t^1 \) (where \( t \neq s \)), that will be classified as a different class \( C_t \) by the face recognition system. This results in 90 attacks in total, comprising all unequal pairs of source and target classes.

Although contestants compete for the highest confidence only, an attack is only considered successful, when the probability score of the target class (i.e. confidence) is the highest among all classes and stealthiness is at least 0.5.

**4 FACE PASTING ATTACK**

Our attack approach is fairly straightforward. Given a source image \( I_t \) and target class \( C_t \), we paste the face region of \( I_t \) into \( I_t \) yielding our altered image \( I_t' \). We found this strategy to be very effective in increasing the confidence score, which is to be expected, since the altered image literally comprises the face of another person. Nevertheless, in order to achieve a stealthiness of at least 0.5 and
thus a successful attack, the pasting needs to be carefully adjusted. For this we considered the following parameters:

- **Position**: The x and y coordinates of the position in the source image, where to place (the center of) the target face.
- **Scaling**: The x and y scaling (between 60% and 180%) of the pasted target face.
- **Rotation**: The rotation of the pasted target face (between $-40^\circ$ and $40^\circ$, where 0 represents no rotation).
- **Transparency**: In order to mask out non-face regions of the target image, we implemented two approaches, one using manually created masks and one utilizing the face segmentation model BiseNet [12] to calculate and extracts a mask automatically.

  - **Manual masking**: Since there is a limited set of only 10 target face images, we manually constructed continuous valued alpha masks $M_0, \ldots, M_9$ (see Figure 1) in a simple graphics editor. We highlighted face regions that we believe to be relevant for a face recognition system. Furthermore, for a single attack, a mask $M_i$ is additionally parameterized by a bias $b$ (between 0 and 1) and slope $w$ (between 5 and 40) resulting in the eventually used mask $M_i^* = \text{sigmoid}((M_i - b) \cdot w)$, where pixel values of 0 and 1 represent full transparency and full opaqueness of the respective target image pixel, respectively. This allows gradual tuning of the contour and intensity of relevant regions from the target face that will be inserted into the source image.

  - **BiseNet masking**: As an alternative to manual masking, we utilized BiseNet to automatically select the masks. The resulting mask is binary and the transparency is implemented by a gaussian blur of the white pixels with a parameter $\sigma$ (between 0 and 20). A $\sigma$ near 0 is affecting the edge, by increasing the $\sigma$ we increase the affected pixels.

We use Bayesian Optimization with Gaussian Processes in order to approximate the optimal parameter settings for each one of the 90 attacks. Hereby, the objective to be maximized is:

\[
\text{confidence} + \min(0.5, \text{stealthiness})
\]

We, therefore, consider **stealthiness** as irrelevant unless it is lower than 0.5 and thus focus on maximizing **confidence** while ensuring the attack is successful.

We performed a straightforward ablation study in regards to the parameters and found, that the **position** is by far the most relevant parameter for both **confidence** and **stealthiness**. Placing the face over the source face region, effectively erasing most information of the source class, significantly increases the **confidence**3. However, in some cases this also has a negative impact on **stealthiness**, rendering many of attacks as unsuccessful. We found that by favoring positions at the edges of the face or overall source image (allowing about 50% of the target face to be cropped), this problem can easily be overcome, achieving **stealthiness** scores near 1.0, while still maintaining high **confidence**. We suspect, that the underlying (SSIM) similarity calculation was improperly calibrated and only considered regions near the source face. For the **scaling** and its considered value range we were not able to find a correlation to the **confidence**. However a larger scaling lowered the stealthiness, which is to be expected, since the source image is obstructed more. In regards to the **rotation**, we found that a greater angle was slightly disadvantageous for the **confidence**. Queries of near zero rotation and greater angles near $\pm40^\circ$ achieved on average a confidence of 0.95 and 0.88, respectively. The effects of position and rotation on **confidence** is further visualized in Figure 2.



3| Although, we found, that even when placing the target face over the source face, achieving the maximum **confidence** of 1.0 is challenging (for example for $s = 8$ and $t = 2$)
5 EVALUATION

We evaluated our manual and automatic approaches with different parameters for the Bayesian Optimization such as the total number of queries and number of initial queries before utilizing Gaussian Processes. For the other parameters we set the ranges as we considered reasonable (as described in 4).

We settled with 200 queries in total, comprising 50 initial queries per attack, which results in a confidence of 89.995315 and stealthiness of 58.232452 for the manual mask approach and a confidence of 89.992083 and stealthiness of 54.825226 for the automatic BiseNet mask approach. Note, that the overall scores are summed over all attacks. However, we can sacrifice confidence in order to significantly improve stealthiness as shown in Figure 3. In regards to the manual approach, for example, we are able to achieve a stealthiness gain of about 20 while the confidence is only reduced by about 0.03. In respect to minimum queries for a successful attack, on average 7.689 and 9.467 queries are needed for the manual and automatic approach, respectively. By selecting the best results of both approaches, we arrived at our final submission of 89.996278 confidence and 61.19255 stealthiness.

6 CONCLUSION & FUTURE WORK

The MLSec face recognition competition by Adversarial AI and CUJO AI challenged the participants to attack a face recognition black box system in a setting similar to the real world. Our straightforward attack approach parses target faces into source images and achieves near perfect results in confidence and stealthiness with 200 queries per attack, which is quite remarkable considering the simplicity. However, the calculation of the stealthiness does not seem to be optimal, since we are able to achieve very high stealthiness for images that are clearly different from the source. This observation shows that every aspect of such systems needs to be carefully designed to ensure an overall robust system. Future work may comprise more complete evaluation of the parameters for the face pasting and providing insights into the workings of a face recognition model. This competition was designed to reflect a real world scenario, with a black box system, returning the target confidence score. We should consider other face recognition systems, which return, for example, only the label of the top class.

ACKNOWLEDGEMENT

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

REFERENCES

[1] Tom B. Brown, Dandelion Mané, Aurko Roy, Martin Abadi, and Justin Gilmer. 2017. Adversarial Patch. https://doi.org/10.48550/ARXIV.1712.09665
[2] Pin-Yu Chen, Huan Zhang, Yash Sharma, Jinfeng Yi, and Cho-Jui Hsieh. 2017. ZOO: Zeroth Order Optimization Based Black-box Attacks to Deep Neural Networks without Training Substitute Models. In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, AISec@CCS 2017, Dallas, TX, USA, November 3, 2017. Bhavani Thuraisingham, Battista Biggio, David Mandell Freeman, Brad Miller, and Arunesh Sinha (Eds.). ACM, 15–26. https://doi.org/10.1145/3128572.3149448
[3] Ying Guo, Xiongxin Wei, Guoqin Wang, and Bo Zhang. 2021. Meaningful Adversarial Stickers for Face Recognition in Physical World. https://doi.org/10.48550/ARXIV.2104.06729
[4] Ameya Joshi, Amitangshu Mukherjee, Soumik Sarkar, and Chinmay Hegde. 2019. Semantic Adversarial Attacks: Parametric Transformations That Fool Deep Classifiers. In 2019 IEEE/CVF International Conference on Computer Vision, ICCV 2019, Seoul, Korea (South), October 27 - November 2, 2019. IEEE, 4772–4782. https://doi.org/10.1109/ICCV.2019.00487
[5] Tero Karras, Miika Aittala, Janne Hellsten, Samuli Laine, Jaakko Lehtinen, and Timo Aila. 2020. Training Generative Adversarial Networks with Limited Data. https://doi.org/10.48550/ARXIV.2006.06676
[6] Edgar Kaziakhmedov, Klim Kireev, Grigorii Melnikov, Mikhail Pautov, and Aleksandr Petiushko. 2019. Real-world Attack on MTCCN Face Detection System. In 2019 International Multi-Conference on Engineering, Computer and Information Sciences (SIBIRCON). IEEE. https://doi.org/10.1109/sibircon.858566.2019.8958122
[7] Stepan Komkov and Aleksandr Petiushko. 2021. AdrHat: Real-world Adversarial Attack on ArcFace ID System. In 2020 25th International Conference on Pattern Recognition (ICPR). 819–826. https://doi.org/10.1109/ICPR48806.2021.9412236
[8] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. 2018. Towards Deep Learning Models Resistant to Adversarial Attacks. In 6th International Conference on Learning Representations, ICLR 2018, Vancouver, BC, Canada, April 30 - May 3, 2018, Conference Track Proceedings. OpenReview.net. https://openreview.net/forum?id=rJzIBfZAb
[9] Nicolas Papernot, Patrick D. McDaniel, Ian J. Goodfellow, Somesh Jha, Z. Berkay Celik, and Ananthram Swami. 2017. Practical Black-box Attacks against Machine Learning. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017. Ramesh Karri, Ozgur Sinanoglu, Ahmad-Reza Sadeghi, and Xun Yi (Eds.). ACM, 506–519. https://doi.org/10.1145/3052973.3053009
[10] Mahmood Sharifi, Sruji Bhagavatula, Lojo Bauer, and Michael K. Reiter. 2019. A general framework for adversarial examples with objectives. ACM Transactions on Privacy and Security (2019).
[11] Christian Szegedy, Wojciech Zaremba, Ilya Sutskever, Joan Bruna, Dumitru Erhan, Ian J. Goodfellow, and Rob Fergus. 2014. Intriguing properties of neural networks. In 2nd International Conference on Learning Representations, ICLR 2014, Banff, AB, Canada, April 14–16, 2014, Conference Track Proceedings, Yoshua Bengio and Yann LeCun (Eds.). http://arxiv.org/abs/1312.6199
[12] Changqian Yu, Jingbo Wang, Chao Peng, Changxin Gao, Gang Yu, and Nong Sang. 2018. BiSeNet: Bilateral Segmentation Network for Real-time Semantic Recognition (ICPR). 819–826. https://doi.org/10.1109/ICCV.2019.00487
[13] Kaipeng Zhang, Zhanpeng Zhang, Zhifeng Li, and Yu Qiao. 2016. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. IEEE Signal Processing Letters 23, 10 (oct 2016), 1499–1503. https://doi.org/10.1109/LSP.2016.2603342
[14] Yaoyao Zhong and Weihong Deng. 2021. Towards Transferable Adversarial Attack Against Deep Face Recognition. IEEE Transactions on Information Forensics and Security 16 (2021), 1452–1466. https://doi.org/10.1109/TIFS.2020.3036801
APPENDIX

Face Morphing Attack. We also considered a face morphing attack by interpolating the source and target face in StyleGAN [5] latent space. However, our initial tests were not promising since the stealthiness did not exceed over 0.5. For example the background, which is left after the face alignment is also interpolated, resulting in many changed pixels and therefore a reduced SSIM and stealthiness, as shown in Figure 4.

PGD transfer attack. To evaluate our pasting approach against different attack methods we implemented a PGD transfer attack, where the perturbation is constrained by the SSIM score of the image, such that we reach a stealthiness of nearly exact 0.5. We utilized an InceptionResNetV1 pretrained on VGGFace2 as a surrogate. As the given images are too big for the model and also tend to have a lot of background, we used MTCNN [13] to detect, crop and scale the face to 160x160 pixels for the model. After the PGD attack we mapped the perturbation back to the original image. But this approach does not lead to a successful attack, with the confidence values reported from the black box system have a mean of 0.0037 and a maximum of 0.22.  

https://github.com/timesler/facenet-pytorch

Figure 4: Example of a face morphing attack, for source image $I_0$ and target image $I_1$. 