Masked Face Recognition for Secure Authentication

Aqeel Anwar¹, Arijit Raychowdhury²
Department of Electrical and Computer Engineering
Georgia Institute of Technology, Atlanta, GA, USA
aqeel.anwar@gatech.edu, arijit.raychowdhury@ece.gatech.edu²

Abstract—With the recent world-wide COVID-19 pandemic, using face masks have become an important part of our lives. People are encouraged to cover their faces when in public area to avoid the spread of infection. The use of these face masks has raised a serious question on the accuracy of the facial recognition system used for tracking school/office attendance and to unlock phones. Many organizations use facial recognition as a means of authentication and have already developed the necessary datasets in-house to be able to deploy such a system. Unfortunately, masked faces make it difficult to be detected and recognized, thereby threatening to make the in-house datasets invalid and making such facial recognition systems inoperable. This paper addresses a methodology to use the current facial datasets by augmenting it with tools that enable masked faces to be recognized with low false-positive rates and high overall accuracy, without requiring the user dataset to be recreated by taking new pictures for authentication. We present an open-source tool, MaskTheFace to mask faces effectively creating a large dataset of masked faces. The dataset generated with this tool is then used towards training an effective facial recognition system with target accuracy for masked faces. We report an increase of $38\%$ in the true positive rate for the Facenet system. We also test the accuracy of re-trained system on a custom real-world dataset MFR2 and report similar accuracy.

I. INTRODUCTION

The world is currently under the onslaught of COVID-19. COVID-19 is an infectious disease caused by severe acute respiratory syndrome (SARS-CoV-2) [1]. People can become infected by coming into close social contact with the infected person through respiratory droplets during coughing, sneezing and/or talking. Moreover, the virus can also be spread by touching a surface or object that has the virus on it, and then by touching your mouth, nose, or eyes. For now, we can protect ourselves by avoiding getting exposed to the virus. According to CDC the best way to avoid spreading or being infected with the disease is to practice social distancing and wearing face covering when in public areas [2]. The two main prevention approaches are avoiding unnecessary contact and wearing face mask. Implementing these guidelines, seriously impacts the current security systems based on facial recognition that has already been put by several corporations and government organizations in place. Fingerprint or password-based security system, which involves contacting finger with sensor hence is not a good way to prevent the spread of disease making it unsafe. Face recognition-based security system however avoids unnecessary contact making it much safer than the former one. But such systems assume the that a picture of the entire face can be taken to perform recognition effectively. Widespread use of face masks thus renders the existing facial recognition systems in-efficient and they can make the entire infrastructure around facial recognition inoperable. Modern deep learning based face recognition systems have proven superior accuracy [3]–[7]. The accuracy of these systems depends on the nature of the available training images. Most of these systems assume access to un-occluded faces for recognition. This condition is fair when you can make sure that the system has access to the complete un-occluded face of the person being recognized. The system trained on such images learns to pay attention to important face features such as the eyes, nose, lips, face edges etc. But when these systems are presented a faced mask, the system fails to identify the person rendering the system unusable. We address this security problem with an effort to make the face recognition-based system reliable when presented with masked faces. The most important problem is the unavailability of the data for the system to be trained with.

Our contributions are as follows
- Open-source tool MaskTheFace to generate masked face dataset from face dataset with extended feature support
- Masked Faces in Real World for Face Recognition (MFR2) - A small dataset of aligned masked faces in real world
- Using MaskTheFace to retrain existing facial recognition system to improve accuracy

Due to lack of the masked face dataset, we propose using simulated masked face to train a deep network for face recognition through our open-source masking tool MaskTheFace. MaskTheFace is computer vision-based script to mask faces in images. It uses a dlib [8] based face landmarks detector to identify the face tilt and six key features of the face necessary for applying mask. Based on the face tilt, corresponding mask template is selected from the library of mask. The template mask is then transformed based on the six key features to fit perfectly on the face. The complete block diagram can be seen in Fig. [8](a). MaskTheFace provides about 100 different mask variations to select from. It is difficult to collect mask dataset under various conditions. MaskTheFace can be used to convert any existing face dataset to masked-face dataset. It identifies all the faces within an image, and applies the user selected masks to them taking into account various limitations such as face angle, mask fit, lighting conditions etc. A single image, or entire directory of images can be used
as input to code.

Following are the features of the proposed system:

- **Support for multiple mask types**: MaskTheFace provides support for 5 different mask types. Moreover, new custom face masks can be easily added by the user.
- **Support for mask variations**: MaskTheFace provides 24 existing patterns that can be applied to mask types above to create more variations of the existing mask types. Moreover, users can easily add custom patterns and colors following the guidelines provided.
- **Support for both single and multi-face images**: MaskTheFace can apply masks to all the faces in the images without any restriction of one face per image.
- **Wide face angle coverage**: Each face mask has multiple templates based on angle hence covering a wide range of face tilts.
- **Bulk masking on dataset**: Face datasets can be easily converted to masked face datasets by providing the folder path

There are many useful face datasets available such as CelebA [9], CASIA webfaces [10], Labeled faces in the wild (LFW) [11] and VGGFace2 [12], to name a few, for the application of face detection/recognition. MaskTheFace can be used to convert these existing datasets into masked-face dataset which can then be used to train an efficient deep network for the underlying application.

## II. Experimentation

In this paper, we point out the significant degradation in performance when a state-of-the-art face recognition system is presented masked images for recognition and then propose a solution that regains the degraded performance. This section covers the details on the selected face recognition system, training data and the performance metrics used to evaluate the trained network.

### A. Face recognition system:

We select the state-of-the-art deep network-based face recognition system Facenet [13]. Facenet creates unified embeddings of the faces and then compares the faces in the embedding space to carry out decision making. The complete block diagram for Facenet based face recognition system can be seen in Fig. 1 (b). During the training phase, multiple image pairs are provided to the network. The network maps these image pairs to embedding vectors and calculates triplet loss [14]. The triplets consist of two image pairs of same and different identities. Triplet loss aims to separate the pair of same identity (positive pair) from the pair of different identities (negative pair) by a distance margin.

\[
\|f(x_i^a) - f(x_i^p)\|^2 + \alpha < \|f(x_i^a) - f(x_i^n)\|^2 \quad (1)
\]

where \(f(\cdot)\) is the underlying deep network to be trained, \(x_i^a, x_i^p, x_i^n\) are the embedding of the anchor, corresponding positive and negative image. \(\alpha\) is an L2 distance margin that is imposed between positive and negative pairs and \(T\) is the set of all possible triplets under consideration. Online triplet mining method is used to generate the triplets on the go to minimize the triplet loss.

### B. Training data:

For the purpose of training facenet, we select VGGFace2 [12] which is a large-scale face dataset that contains about 3 million images of 9131 identities, with an average of \(\sim 362\) images per identity varying in pose, age, ethnicity and illumination. From VGGFace2 we create a subset, VGGFace2-mini, by randomly sampling 42 images per identity. This dataset contains the un-masked images of the identities. From VGGFace2-mini, we further generate VGGFace2-mini-SM dataset by applying randomly selected masks (surgical-green, surgical-blue, N95, cloth) to each image nearly doubling the dataset size. Table II summarizes these datasets.

For comparison purpose, we train two different Facenet networks, one with VGGFace2-mini (no-mask network) and the other with VGGFace2-mini-SM (mask network). Comparing the performance of two networks trained on datasets of different sizes is normally and un-fair comparison since the network trained on the larger dataset had access to more information hence having a tendency to make better decision.


| Dataset                  | Type       | # Identities | # Images    | Avg. images/identity | # Testing pair |
|-------------------------|------------|--------------|-------------|----------------------|----------------|
| VGGFace2-mini           | Simulated  | 8,631        | 362,502     | 42                   | -              |
| VGGFace2-mini-SM1       | Simulated  | 8,631        | 697,084     | 80.77                | -              |
| LFW-SM (combined)       | Simulated  | 5,749        | 64,973      | 11.3                 | 29,235         |
| MFR2                    | Real-world | 53           | 269         | 5                    | 848            |

**TABLE I:** Summary of the four datasets used for training and inference. The first two datasets are used for training, while the last two are used for testing the trained network.

In our case, the extra images in VGGFace2-mini-SM are generated from the original images and they won’t add any extra information for training no-mask network, hence the comparison is fair enough. We use Inception-resnet v1 \[^{[15]}\] as the deep network \( f(\cdot) \) to map images to their embedding. An embedding size of 512 was selected. Each of the two networks were trained from scratch.

C. **Performance Metrics:**

To analyze the performance of the trained networks, we use the following metrics as used in \[^{[13]}\]

- **Max Accuracy (%)**: The maximum accuracy of the network in terms of identifying the test input image pairs as -ve or +ve.
- **ACC @ FAR=0.1% (%)**: The accuracy of the network in terms of identifying the test input image pairs as -ve or +ve at the selected threshold for which the false acceptance rate is 0.1%.
- **TPR @ FAR=0.1% (%)**: The true positive rate (%age of the time that the +ve input image pairs were identified +ve) of the network at the selected threshold for which the false acceptance rate is 0.1%.

To summarize

\[
\text{MaxAccuracy} = \frac{TP + TN}{TP + TN + FP + FN}
\]

\[
\text{ACC@FAR}0.1\% = \frac{TP + TN}{TP + TN + FP + FN} \quad \text{s.t.} \quad \frac{TP + FP}{TP + FN} = 0.001
\]

\[
\text{TPR@FAR}0.1\% = \frac{TP}{TP + FN} \quad \text{s.t.} \quad \frac{TP + FP}{TP + FN} = 0.001
\]

where TP, TN, FP and FN are True positives, true negatives, false positives and false negatives respectively.

III. **Results**

In this section we compare the performance of the trained no-mask and mask networks on the following test datasets based on performance metrics mentioned in the previous section.

A. **LFW-SM - Dataset with simulated masks**

Labelled Faces in the Wild (LFW) dataset \[^{[11]}\] is a standard benchmark dataset used to evaluate the performance of face recognition systems. It contains 5,749 identities with a total of 13,233 images. As mentioned previously, the goal of masked face recognition is to accurately recognize identities both with and without the masks on. For this purpose, we use the following variations of the LFW dataset to draw effective comparisons.

- **LFW**: Original unmasked LFW dataset.
- **LFW-SM-SG**: LFW dataset with the surgical-green simulated mask applied.
- **LFW-SM-SB**: LFW dataset with the surgical-blue simulated mask applied.
- **LFW-SM-N95**: LFW dataset with the N95 simulated mask applied.
- **LFW-SM-Cloth**: LFW dataset with the cloth simulated mask applied.
- **LFW-SM-Mixed**: LFW dataset with one randomly selected mask applied to each image.

LFW-SM dataset only contains images with the simulated mask applied on them. The purpose of these variations is to provide a detailed performance analysis.

The facenet network takes input a pair of images (template-image, unknown-image) comparing the identity of the person in unknown image to the template image. This comparison is carried out in the embedded space based on the distance between the two. The selection of the L2 distance threshold is carried out on 9 splits of the underlying test dataset and the 10th split is used to report the performance metrics, similar to leave-one-out cross validation approach. The images in the test pairs are selected across the datasets to evaluate the robustness of the network.

The L2 distance threshold is found by averaging out the optimum threshold for the 9 out of 10 splits and then is kept constant across all the variations of image pairs. The selected optimal threshold is 2.5 for maximum accuracy and 1.67 for FAR=0.1%. The mask network is trained on a combination of masked and un-masked faces. The L2 distance threshold is therefore calculated on the LFW original unmasked dataset. This L2 distance threshold is found by averaging out the optimum threshold for the 9 out of 10 splits and then is kept constant across all the variations of image pairs. The selected optimal threshold is 2.5 for maximum accuracy and 1.67 for FAR=0.1%. The mask network is trained on a combination of masked and un-masked faces. The L2 distance threshold is therefore calculated on the LFW-SM-mixed dataset. Similar to the no-mask network, the L2 distance threshold is found by averaging out the optimum threshold for the 9 out of 10 splits.
and then is kept constant across all the variations of image pairs. The selected optimal threshold is 2.62 for maximum accuracy and 2.01 for FAR=0.1%. Fig. 2 (b) reports the performance metrics when the network was evaluated on LFW-SM dataset.

**B. MFR2 - Dataset with real masks**

In the previous section we showed the network performance on the LFW Dataset with simulated masks applied through MaskTheFace tool. In this section we study the performance of the system trained on simulated masks but tested on the real-world masked faces. To the best of our knowledge there is no diverse enough, pre-processed, ready-to-use real-world aligned masked face dataset of identities. [17] has, by far, the largest face recognition dataset with 24,771 images. But the dataset faces are not consistent or aligned making it a little harder to be used. Moreover, the masks on the face makes it really hard to find and align faces for the purpose of face recognition. Also, the dataset lacks unmasked faces of the identities and is not diverse enough in terms of ethnicity. Therefore, we decided to create a rather smaller but pre-processed dataset of real-world masked faces consisting of celebrities and politicians. This dataset is not a replacement of the Wuhan dataset, but simply an approach for us to show the effectiveness of the simulated masks dataset on the real-world masked images. Masked faces in real world for face recognition (MFR2) is a small dataset with 53 identities of celebrities and politicians with a total of 269 images that...
are collected from the internet. Each identity has on average of 5 images. The dataset contains both masked and unmasked faces of the identities. The dataset is processed in terms of face alignment and image dimensions. Each image has a dimension of (160 × 160 × 3). Images from the MFR2 dataset and the distribution of different mask types can be seen in Fig. 3. In the future we plan on expanding this dataset to contain more identities and images. For the purpose of network performance evaluation, we consider a total of 848 image pairs from MFR2 (424 positive pairs, and 424 negative pairs). The pairs are evaluated through the network trained on VGGFace2-SM dataset. The overcome the gap between the simulated mask images and real-world mask images, the distance threshold is re-calculated for MFR2 using data splits as was done for LFW-SM. The performance of the network when evaluated on MFR2 is plotted in Fig. 4. We compare the performance of no-mask network and mask network. Since this dataset is smaller in size than the LFW dataset, a FAR of 0.1% means all the 894 pairs being predicted correct (1/894 = 0.0012 > 0.001). We relax this constraint to 0.22% (2/894 = 0.0022) giving the network room for 2 wrong predictions.

IV. DISCUSSION

A. LFW-SM Dataset

Fig. 2 (b) reports the detailed performance metrics of the two networks mentioned above on the LFW-SM dataset. Each performance metric is plotted as heat-map for visual comparison for 25 different possible image pairs. On the horizontal axis are the template images, while on the vertical axis we have unknown image of the test pairs. The darker the cell color, the better the performance metric. Fig. 2 (b) left reports the pair-wise maximum accuracy of the no-mask (top) and mask (bottom) network. It can be seen that the accuracy is best (∼97%) for the pairs when both the template and unknown image belongs to the un-masked dataset, while for all the other combinations the accuracy varies between 86 to 93%. This might not seem a significant drop in the accuracy, but when things are kept in perspective, we realize that this performance metric might not be the best one for comparison. The accuracy is the average accuracy of the binary decision whether the pairs belonged to same identity or not. A better metric is to maintain the false acceptance rate to below a certain threshold (0.1%) [13]. False acceptance rate (FAR) is the ratio of image pairs of different identities which was predicted same identity by the network over all the negative pairs. We want this metric to be as small as possible (ideally zero). An acceptable value of 0.1% was selected for the FAR and the corresponding L2 distance threshold was calculated. The image pairs were then evaluated for their accuracy and true positive rate (TPR) at this threshold.

Fig. 2 (b) center reports the accuracy at @FAR=0.1%. It can be seen that the accuracy dropped to 76 to 85% when masked faces were presented to the network. The worst accuracy is for the combination where the template image is no-mask and the unknown image is N95 masked.
image. Furthermore, if we look at the TPR@FAR=0.1% in Fig. 2 (b) right, we see that the no-mask trained network drops the TPR from ~ 86% to ~ 30% in the worst case scenario. This significant drop in the TPR makes the no-mask trained network highly vulnerable to prediction errors rendering the face recognition system inefficient. Fig. 2 (b) also plot the results for the mask network (on the right). It can be seen that the network trained on the MaskTheFace generated dataset performs almost equally well for all the cross-dataset pair-wise combination. In fact, in some cases it slightly outperforms the no-mask trained network. The reason for this slight improvement could be the masked images which act as regularizers avoiding the network to overfit to VGGface2-mini and hence performing slightly better on the unseen test dataset. Fig. 4 (a) compares the average performs of the no-mask and mask networks across all the combinations for the considered performance metrics. It can be seen that the mask network significantly outperforms the no-mask network across all the three performance metrics.

C. Clustering MFR2 dataset

Facenet created embedding of the images can be used to cluster faces into identities. We tried to cluster the MFR2 dataset into clusters based on the embedding created by the no-mask and mask network. Fig. 5 (a) shows the MRF2 dataset clustered into groups based on the no-mask network. We only show 24 out of 53 clusters for better view. It can be seen that the no-mask network has some tendency of grouping images of same identities into one cluster (and hence a good accuracy from previous section). But there can be seen a few discrepancies in the clustering such as images mapped to wrong identities, same identities mapped to different clusters, different identities mapped to same cluster and different identities mapped into one cluster based on mask nature and hence a reduced accuracy and tpr @FAR=0.2%. Fig. 5 (b) shows the clustering of MRF2 dataset based on the embedding created by the mask network. We only see single type of discrepancy (image mapped to wrong identity) and that too for only a few clusters, while all the other images are mapped into correct clusters.

V. METHODS

A. Dataset generation using MaskTheFace

Faces dataset were converted into masked face dataset using MaskTheFace. For each image in the dataset, a mask was selected from cloth, surgical-green, surgical-blue and N95 uniformly at random. Moreover, the original un-masked image was made a part of the dataset alongside with masked images. This was done to make sure that the network trained, performs equally well on both the masked and un-masked images.

B. Training Details

The VGGFace2 dataset was aligned and cropped using MTCNN [18] to get a tight bound on the faces in the images. This gets rid of the redundant background in the
image putting more focus on the face. The training of the facenet system was carried out on a GTX1080 workstation for 100 epochs. An equally spaced three-step learning rate with values 0.05, 0.005 and 0.0005 was used. Training each network took $\sim 42$ hours.

VI. CONCLUSION

In this paper we addressed the issue of recognizing masked faces through existing face recognition systems with reliable accuracy. We present an open-source tool, MaskTheFace which can be used to mask faces. This results in the creation of a large dataset of masked faces. The dataset generated with this tool can then used towards training an effective facial recognition system with target accuracy for masked faces. Using MaskTheFace, we report an increase of $\sim 38\%$ in the true positive rate for the existing Facenet system for both masked and un-masked faces. The accuracy of re-trained system was also tested on a custom real-world dataset MFR2 and reported similar accuracy, hence being able to extend out to real life masked faces.

VII. CODE AVAILABILITY

MaskTheFace tool and the MFR2 dataset is available for use to other researchers at the following link [https://github.com/aqeelanwar/MaskTheFace](https://github.com/aqeelanwar/MaskTheFace).

VIII. ACKNOWLEDGEMENTS

This work was supported in part by C-BRIC, one of six centers in JUMP, a Semiconductor Research Corporation
REFERENCES

[1] C. I. Paules, H. D. Marston, and A. S. Fauci, “Coronavirus infections—more than just the common cold,” Jama, vol. 323, no. 8, pp. 707–708, 2020.

[2] “How to protect yourself & others from coronavirus disease.” https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html, 2020.

[3] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “Arcface: Additive angular margin loss for deep face recognition,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2019, pp. 4690–4699.

[4] W. Liu, Y. Wen, Z. Yu, and M. Yang, “Large-margin softmax loss for convolutional neural networks,” in ICML, vol. 2, no. 3, 2016, p. 7.

[5] W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, and L. Song, “Sphereface: Deep hypersphere embedding for face recognition,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 212–220.

[6] B. Liu, W. Deng, Y. Zhong, M. Wang, J. Hu, X. Tao, and Y. Huang, “Fair loss: margin-aware reinforcement learning for deep face recognition,” in Proceedings of the IEEE international conference on computer vision, 2019, pp. 10052–10061.

[7] A. Tuan Tran, T. Hassner, I. Masi, and G. Medioni, “Regressing robust and discriminative 3d morphable models with a very deep neural network,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 5163–5172.

[8] [http://dlib.net/].

[9] Z. Liu, P. Luo, X. Wang, and X. Tang, “Deep learning face attributes in the wild,” in Proceedings of International Conference on Computer Vision (ICCV), December 2015.

[10] D. Yi, Z. Lei, S. Liao, and S. Z. Li, “Learning face representation from scratch,” arXiv preprint arXiv:1411.7923, 2014.

[11] G. B. Huang, M. Mattar, T. Berg, and E. Learned-Miller, “Labeled faces in the wild: A database for studying face recognition in unconstrained environments,” 2008.

[12] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, “Vggface2: A dataset for recognising faces across pose and age,” in International Conference on Automatic Face and Gesture Recognition, 2018.

[13] F. Schroff, D. Kalenichenko, and J. Philbin, “Facenet: A unified embedding for face recognition and clustering,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 815–823.

[14] K. Q. Weinberger and L. K. Saul, “Distance metric learning for large margin nearest neighbor classification.” Journal of Machine Learning Research, vol. 10, no. 2, 2009.

[15] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, “Inception-v4, inception-resnet and the impact of residual connections on learning,” in Thirty-first AAAI conference on artificial intelligence, 2017.

[16] G. B. Huang and E. Learned-Miller, “Labeled faces in the wild: Updates and new reporting procedures,” Dept. Comput. Sci., Univ. Massachusetts Amherst, Amherst, MA, USA, Tech. Rep, pp. 14–003, 2014.

[17] Z. Wang, G. Wang, B. Huang, Z. Xiong, Q. Hong, H. Wu, P. Yi, K. Jiang, N. Wang, Y. Pei et al., “Masked face recognition dataset and application,” arXiv preprint arXiv:2003.09093, 2020.

[18] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multitask cascaded convolutional networks,” IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499–1503, 2016.