IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

Master Face Attacks on Face Recognition Systems

Mr. Pradeep Nayak[1], Darshan S[2], Yashvardhan SG[3], Sudeep K[4], Finny Paul[5]
Assistant Professor, Department of Information Science and Engineering[1]
Students, Department of Information Science and Engineering[2,3,4,5]
Alvas's Institute of Engineering and Technology, Mijar, Moodbidre, Karnataka, India

Abstract: *Due to its simplicity, face authentication is currently more frequently used than authentication using a personal identification number or an unlock pattern, especially on mobile devices. This has made it a seductive target for attackers who use a demonstration assault. Traditional presentation attacks employ the victim's face or victim footage. The existence of master faces—faces that match numerous enrolled templates in face recognition systems—has been demonstrated in earlier research, and their presence increases the effectiveness of presentation attacks. In this article, we present the results of a thorough investigation of latent variable evolution (LVE), a technique frequently employed to produce master faces. To determine the characteristics of master faces, an LVE algorithm was used in a variety of settings and with many databases and/or face recognition systems.*

Keywords: Master face, wolf attack, face recognition system, latent variable evolution

I. INTRODUCTION

Strong passwords, which can be challenging to remember, should be used, and they should be updated frequently to maintain security. Passwords are less handy than personal identification numbers and unlock patterns, yet the user is still needed to keep them in mind, and passersby might be able to sneak a glimpse at them. Biometric authentication, which makes use of a distinctive biometric feature, is an even more practical technique.
Fig. depicts the phases of master biometrics research. The following is a summary of our contributions:

We are the first to create master faces that can match many faces with various identities, building on our earlier work [4]. We extend our prior work by examining the impact of employing multiple databases (DBs) and/or several FR systems for the latent variable evolution (LVE) algorithm used to construct master faces. This capability makes FR systems susceptible to a master face attack. Attack performance was improved overall by some DB/FR system combinations, but not by others due to to disputes within components. Understanding the circumstances in which strong master faces can be formed and properly assessing the dangers require knowledge of the successful combinations.

- By adding more scenarios, employing an additional facial database, and an additional FR system trained with the angular margin loss [8] for the defender side, we broaden the scope of our earlier work. In order to gain

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

greater understanding of master faces, we also present visualisation in the face embedding (identity) space. These insights are priceless since they can be used to increase the FR systems' robustness.

- We analysed master face attacks by carrying out presentation attacks using printed photographs and the equivalent digital images in order to show the real threat that master faces offer to disputes within components. Understanding the circumstances in which strong master faces can be formed and properly assessing the dangers require knowledge of the successful combinations.
- By adding more scenarios, employing an additional facial database, and an additional FR system trained with the angular margin loss [8] for the defender side, we broaden the scope of our earlier work. In order to gain greater understanding of master faces, we also present visualisation in the face embedding (identity) space. These insights are priceless since they can be used to increase the FR systems' robustness.
- We analysed master face attacks by carrying out presentation attacks using printed photographs and the equivalent digital images in order to show the real threat that master faces offer**.**

II. RELATED WORK

2.1 Facial Image Generation

The face is a frequent target in deep learning research, which is a key area of study. Variational autoencoders (VAEs) and generative adversarial networks are the two main methods for creating images.(GANs) . They could initially only produce little, poor-quality images. GANs were challenging to train, while VAEs frequently produced hazy images. The training problem was handled by later GAN advancements (WGAN)and WGAN Gradient Penalty (WGAN-GP)), which allowed GANs to be utilised to create master prints .High-resolution images can be produced using VAEs and GANs] in their most recent iterations. Karras et alprogressive .'s GAN was successful in producing images with a resolution of 1024 1024 pixels by gradually adding more layers during training to produce larger images .Later research improved the disentanglement network termed StyleGAN by fusing the concepts of progressive training and style transfer. StyleGAN employs a mapping network to convert a latent vector into intermediate style vectors that are used to synthesise images, in contrast to typical GANs that use a latent vector directly to generate images. The facial characteristics can be altered by manipulating these intermediary style vectors. The best techniques for creating master faces are Style GAN and its following version, which have the strengths of powerful disentanglement and high-quality facial image production.

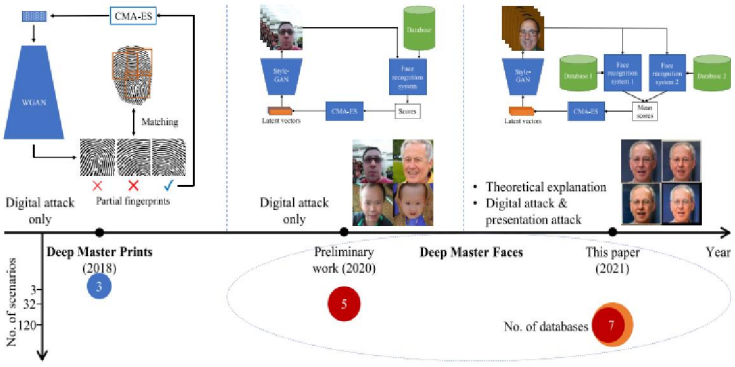
2.2 Face Recognition

Large databases have been made available, such as the CASIA-WebFace database [19] and the MS-Celeb database , and recent developments in convolutional neural networks (CNNs) have greatly enhanced FR system performance and made it possible for them to function well in diverse domains . A network design that performed well in the ImageNet Challenge is used by the majority of cutting-edge FR systems, including the VGG (Visual Geometry Group) network architecture and the inception network architecture. The VGG-Face network was developed by Parkhi et al. using training data from a large-scale database they created themselves. Ten times fewer parameters than the VGG-Face network are proposed by Wu et al. in their lightweight CNN . De Freitas Pereira et al. built heterogeneous FR networks using the inception design , and Schroff et al. created the FaceNet network . FaceNet was re-implemented by Sandberg as an open-source platform . DeepFace is a system developed by Taigman et al. that uses explicit 3D face modelling to enhance the facial alignment stage and a CNN to extract face representation . Contrary to other approaches that employ discriminative classifiers, Tran et algenerative .'s classifier, dubbed DR-GAN, learns a disentangled representation .The embedding distribution optimization is the main emphasis of more recent methods. To increase the FR model's ability to discriminate between different inputs and to stabilise the training process, Deng et al. suggested employing the additive angular margin loss (ArcFace) rather than the more widely utilised cosine distance loss . In their UniformFace FR system, Duan et al. advocated adopting a uniform loss to train equally distributed representations since they believed that the distribution of the features is crucial .

The biometric (FR) system's intended policy by the (facial) capturing subsystem. 1 A photo attack is a presentation attack in which the attacker shows the FR system sensor a picture of the victim. This image can be printed on paper or viewed on a screen device (such as a laptop, tablet, or smartphone) . Another presentation assault is a replay attack,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

which plays the victim's video instead of presenting a picture . An FR system can incorporate a presentation attack detector to reduce presentation attacks .



Building on some of the innovations mentioned above, we carried out rigorous experiments with four modern (and conceptually dissimilar) state-of-the-art master faces to explore the security danger posed by master faces.

2.3 Wolf Attack and Master Biometric Attack

In a biometric recognition system, a "wolf sample" is an input sample that could be mistakenly recognised as a match with several user templates (also known as "enrolled subjects") . Both biometric and non-biometric wolf samples are acceptable. a wolf specimen is employed in an attack by wolves on a biometric identification system. In Fig. 3, a hypothetical wolf assault is depicted. Attacks on fingerprint recognition systems were the original purpose of wolves .
The highest likelihood of a successful attack with a single wolf sample, or wolf attack probability (WAP), serves as a theoretical measure of success . A strategy for preventing wolf attacks on biometric identification systems was put out by Inuma et al. : build a secure matching algorithm that determines the entropy of the probability distribution of each input value.

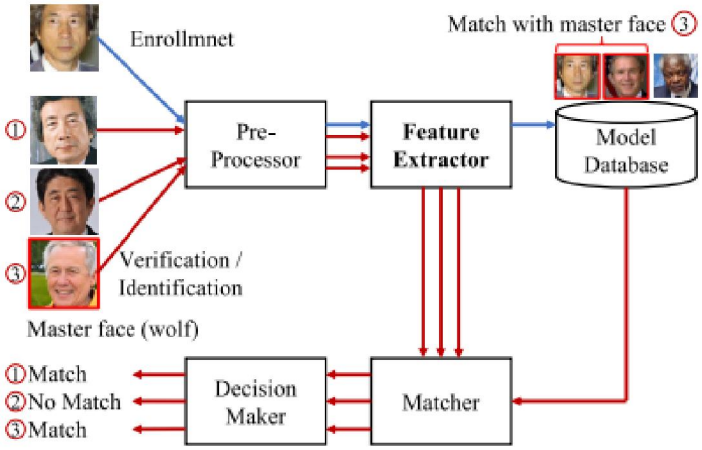


Fig. 3. Operation of typical FR system. There are two phases: enrollment (blue path) and verification/identification (red path). The master face (face 3) was falsely matched with the two faces of two enrolled subjects. Best viewed in color.

They are produced by GANs utilising the LVE method to increase the erroneous matching rates (and thus, increase WAPs). A master face attack targets fingerprint recognition (FR) systems, which need better resolution photos, while FR systems use small sensors with limited resolution [4]. When using the LVE method to build master faces in this work, we utilised several FR systems and databases. We also used master faces to replicate presentation attacks to determine the true harm they posed.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

2.4 Latent Variable Evolution

Since they do not require any assumptions about the underlying fitness landscape, evolution algorithms are frequently employed in artificial intelligence applications to approximate complicated, multimodal, and non-differentiable functions. Designed for non-linear and non-convex problems, the covariance matrix adaptation evolution strategy (CMA-ES) is a potent method functions . Bontrager et al. used CMA-ES with a pretrained GAN to perform interactive evolutionary computation to improve the quality of generated samples . This strategy was used in subsequent work on the LVE algorithm to maximize the WAP of generated partial fingerprint images . In our previous work , we modified the LVE algorithm scoring method so that it could work smoothly with high-resolution facial images generated by StyleGAN . Given n random initial vectors Z = {z1, z2,..., zn}, a generation model G, a scoring function F, and m enrolled templates T = {t1,t2,...,tm}, the LVE algorithm runs in a loop in which n samples are first generated by G using Z. Each sample is then matched with m templates in T to obtain a mean score s. An evolution algorithm (e.g., CMA-ES) takes the set of the mean scores s to evolve n new latent vectors Z for the next loop.We have now added one more database and/or FR system to the LVE algorithm to better approximate the target FR system and database so that the generated master faces have better generalizability.

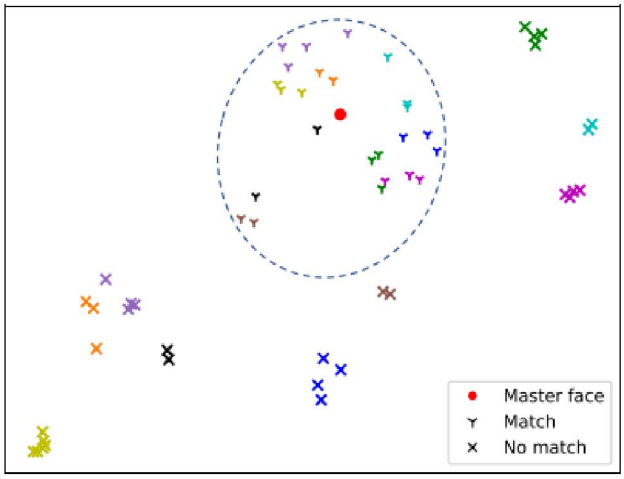


Fig. 4. UMAP visualization of identity space containing embeddings of a master face and of "match" and "no-match" faces of 18 enrolled subjects. For each cluster (match or no match), symbols with the same color correspond to the same subject. Best viewed in color.

III. DEEP MASTER FACES

3.1 Existence of Master Faces

We briefly describe the existence of master faces before going into the suggested master face generating algorithm. Pre-processing the input, extracting its features, comparing them to those of the enrolled subject(s) in the model database, and making a conclusion are the four phases of a typical FR system (or biometric identification system in general) (Fig. 3). A mapping function is played by the feature extractor. It links the identification domain to the facial image domain. When training the feature extractor, the goal is to make the mapping function as efficient as possible such that the mappings of faces with the same identity are adjacent to one another in the identity space and vice versa. The solution is just an approximation because this is an optimization problem. Furthermore, the mapping is not guaranteed to be accurate. Master faces may exist as a result of dense regions in the identity (embedding) space employed by FR systems, which is not spread uniformly. When we create an identifier for a location in a congested area, it can be mistakenly matched in the identity space, multiple close-by faces. After numerous evolutions, the LVE algorithm seeks to locate such a place in a dense region of the identification space. We use uniform manifold approximation and projection (UMAP) to depict the identity space and one of the master faces created in this study in Fig. 4 to intuitively and empirically demonstrate this. This point (red dot) is surrounded by several embeddings and contains the master face produced by our algorithm (explained in the following section).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

3.2 Latent Variable Evolution With Multiple Databases and/or Face Recognition Systems

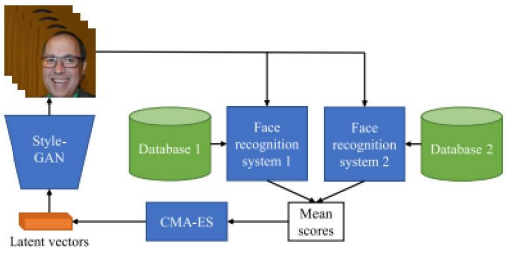


Fig. 6. Overview of extended LVE algorithm. Latent vectors are fed into StyleGAN [17] to generate facial images. One or more surrogate FR system(s) then calculates mean score for each image on the basis of the subjects in one or more database(s). For example, for the *combination 3* setting described in Table III, **database 1** is LFW - Fold 1, **database 2** is mobile biometry (MOBIO), **FR system 1** is Inception-ResNet-v2 network (trained on MS-Celeb database), and **FR system 2** is DR-GAN network. The CMA-ES [35] algorithm uses these scores to generate new latent vectors.

We extended our previous work by using one more database and/or FR system to generate master faces, which requires support from the LVE algorithm. The extended LVE algorithm is formalised in Algorithm 1 and is depicted in Fig. 6. M latent vectors, z1,..., zm, are first initialised at random first. They are then used as input into a style-trained GAN network to produce faces, m. The similarity between all subject faces in databases E(1) j and E(2) j is determined by two face matching functions, FaceMatching(1) (,), and FaceMatching(2) (,) (corresponding to two FR systems). The outcomes of FaceMatching(1) (,) and FaceMatching(2) (,) yield two m dimension mean score vectors, s(1) and s(2). The best local master face Fb is chosen among the m produced faces using the mean s of these two vectors. Finally, s is used to feed fresh latent vectors (z1,..., zm) into the CMA-ES algorithm.

Algorithm 2 Database Refining

$\mathcal{M} = \{M_1, \ldots, M_n\}$ ▷ Previous master faces
procedure REFINE_DATABASE($\mathcal{M}$, E)
  $\mathbf{E}' = \{\}$ ▷ Initialize refined database
  for face E_i in data **E** **do**
    keep ← true
    for face M_j in $\mathcal{M}$ **do**
      if isMatch(E_i, M_j) **is true then**
        keep ← false
    if keep **is true then**
      $\mathbf{E}' \leftarrow \mathbf{E}' \cup \{E_i\}$
  return $\mathbf{E}'$

Algorithm 1 Latent Variable Evolution

$m \leftarrow 22$ ▷ Population
procedure RUNLVE(m, n)
  $\mathcal{F} = \{\}$ ▷ Master face set
  $\mathcal{S} = \{\}$ ▷ and corresponding score set
  $\mathcal{Z} = \{\mathbf{z_1} \leftarrow rand(), \ldots, \mathbf{z_m} \leftarrow rand()\}$ ▷ Initialize
  for n iterations **do** ▷ Run LVE algorithm n times
    $F \leftarrow StyleGAN(\mathcal{Z})$ ▷ Generate m faces F
    $\mathbf{s^{(1)}} \leftarrow 0, \mathbf{s^{(2)}} \leftarrow 0$ ▷ Initialize scores $\mathbf{s^{(1)}}, \mathbf{s^{(2)}} \in \mathbb{R}^m$
    for face F_i in faces **F** **do**
      for face $E_j^{(1)}$ in data $\mathbf{E^{(1)}}$ **do**
        $s_i^{(1)} \leftarrow s_i^{(1)} + FaceMatching^{(1)}(F_i, E_j^{(1)})$
      $s_i^{(1)} \leftarrow \frac{s_i^{(1)}}{|\mathbf{E^{(1)}}|}$ ▷ Mean scores of 1st system
      for face $E_j^{(2)}$ in data $\mathbf{E^{(2)}}$ **do**
        $s_i^{(2)} \leftarrow s_i^{(2)} + FaceMatching^{(2)}(F_i, E_j^{(2)})$
      $s_i^{(2)} \leftarrow \frac{s_i^{(2)}}{|\mathbf{E^{(2)}}|}$ ▷ Mean scores of 2nd system
      $s_i = \frac{s_i^{(1)} + s_i^{(2)}}{2}$ ▷ Mean scores of both systems
    $F_b, s_b \leftarrow GetBestFace(\mathbf{F}, \mathbf{s})$
    $\mathcal{F} \leftarrow \mathcal{F} \cup \{F_b\}$ ▷ Append best master face
    $\mathcal{S} \leftarrow \mathcal{S} \cup \{s_b\}$ ▷ and its corresponding score
    $\mathcal{Z} \leftarrow$ CMA_ES(**s**)
  return $\mathcal{F}, \mathcal{S}$
$F_b, s_b \leftarrow GetBestFace(\mathcal{F}, \mathcal{S})$ ▷ Final (best) master face

Out of the n best master faces F obtained in the n iterations, the overall (global) best master face is selected.When creating a new master face, all faces that match the As seen in Algorithm 2, it is necessary to eliminate any previously generated master face(s) from the training database(s). As a result, the new master face won't cover the old master face (s). displays an illustration of a second master face alongside the first master face, the real wolf face, and their associated FMRs. The second master face's FMR is lower than the first one's, and any succeeding master face often follows suit.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

IV. GENERATING MASTER FACES

We created a number of LVE algorithm settings and a number of attack scenarios that cover white-box, gray-box, and black-box attacks in order to assess the dangers and threats posed by a master face attack. While only one of the target FR system's architecture or its training database is known for gray-box attacks, both are known for white-box attacks. There is no information available regarding the target FR system for black-box assaults.

Attackers can increase the likelihood that their attack is a white-box or gray-box attack by using multiple FR systems for the LVE algorithm. To more accurately approximation the distribution of the model database of the target FR system, they can employ more than one database for the LVE technique.

This section is set up as follows:

4.1 Experiment Materials

A. Face Recognition Systems

We used five mainstream publicly available high-performance FR systems in our experiments:

One trained on the CASIA-WebFace database and one trained on the MS-Celeb database by de Freitas Pereira et al. are Inception-ResNet-v2 based FR systems.

Sandberg implemented and trained an open-source version of FaceNet on the MS-Celeb database.

TABLE I
DETAILS OF DATABASES USED IN OUR EXPERIMENTS

Database	Year	No. of images	Resolution
Flickr-Faces-HQ [17]	2019	70,000	1024 × 1024
CASIA-WebFace [19]	2014	494,414	256 × 256
MS-Celeb [20]	2016	10,490,534	Up to 300 × 300
Multi-PIE [37]	2009	755,370	3072 × 2048
LFW [39]	2007	13,233	Various
MOBIO [40]	2012	30,326	Various
IJB-A [41]	2015	5,712	Various

The CASIA-WebFace database and the Multi-PIE database were used to train the DR-GAN.

The MS-Celeb database was used to train ArcFace .

The two Inception-ResNet-v2 based FR systems, DR-GAN, and all of the FR systems were utilised to generate master faces and assess master face attacks.

2 The Bob toolkit was used to pretrain all FR systems .

Table I displays specifics on the databases used. The databases utilised to train StyleGAN, the FR systems, and the LVE method do not contain any topics that are similar. This indicates that the LVE method can still function effectively even if some of its components use competing databases.

In order to generate master faces and estimate the age and gender distributions of the databases used for training the FR and StyleGAN systems, we employed the InsightFace library4. We used annotated gender data from the MOBIO database. We disregarded the Multi-PIE database because it just adds to the database used to train the DR-GAN FR system. Figs. 7 and 8 display the estimated distributions, respectively. Particularly in the CASIA-WebFace, MS-Celeb, and MOBIO databases, the ages are primarily between 21 and 40. With a higher percentage of people between the ages of 41 and 60, the LFW - Fold 1 database is more evenly distributed. Except for the MOBIO database, which has none, all databases contain a small number of child faces.

MOBIO databases are the most unbalanced, with less than 25% female faces. This may cause bias in the FR systems as well as affect the properties of the generated master faces, as explained in the following section.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

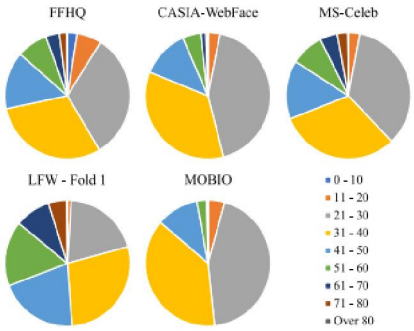


Fig. 7. Estimated age distribution of five databases used for training StyleGAN, FR systems, and generation of master faces. Best viewed in color.

B. Latent Variable Evolution Configurations

With the current computation and temporal resources, it is not possible to evaluate all conceivable combinations due to the large number of FR systems and databases. So, in order to provide the broadest feasible coverage, we chose a subset. We created eight parameters (Table II) for the LVE method utilising three FR systems, two databases (LFW - Fold 1 and MOBIO), and two versions of Inception-ResNet-v2 (one trained on the CASIA-WebFace database and one trained on the MS-Celeb database). One FR system and one database are used in five settings (single 1 to single 5) while more than one FR system and/or database are utilised in three settings (combination 1, combination 2, and combination 3).

Each combination setting, which merged two single settings, was chosen for having adequate case coverage.Table III highlights the primary variations between the three combination settings. The databases used to train the FR systems were comparable, and just one database was used with the LVE algorithm in the combination 1 setting.

TABLE III
COMPARISON OF THREE COMBINATION SETTINGS FOR LVE ALGORITHM. FOR FR SYSTEMS, WE COMPARED THEIR ARCHITECTURES AND TRAINING DATABASES

Setting	Database 1 vs. Database 2	FR System 1 vs. FR System 2	
		Architectures	Training DBs
Combination 1	Same	Different	Similar
Combination 2	Different	Same	Different
Combination 3	Different	Different	Different

C. Master Face Analysis

On the evaluation set of the LFW-Fold 1 database , the master face created using the combination 1 setting and the faces it matched using the Inception-ResNet-v2 based FR system are presented in Fig. 10. Matching the master face those of people of both sexes, of different racial backgrounds (White, Black, and Asian), and of different ages (from infants to seniors). Numerous times, the lighting and facial angles were different from those of the master face. Both of the subjects' eyes are covered by spectacles (eyeglasses or sunglasses). About 10 to 50 identities can be matched by a typical master face. The uneven LFW database (as seen in Figs. 7 and 8) causes a disproportionate percentage of the matched faces to be male. Additionally, the majority of the matched faces are those of seniors because the master face belongs to the elder cluster (explained below).To construct the density maps, we utilised a kernel density estimation method to the reduced spaces after running the uniform manifold approximation and projection (UMAP) dimension reduction algorithm on the embedding spaces of three FR systems. We achieved it while taking into account both gender and age. To estimate the embedding space density, we employed the ArcFace FR system, two InceptionResNet-v2 based FR systems (CASIA-WebFace version and MS-Celeb version), and InceptionResNet-v2. The ArcFace FR system was exclusively employed on the defender side, while the two Inception-ResNet-v2 FR systems were used on both the attacking and defender sides. In Fig. 11, the estimated densities are displayed. Along with the placements of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

the intermediate master faces, we additionally provided.The chosen dense area may belong to a younger, middle-aged, or older cluster depending on its age. Since just one age group included in the training data for the FR systems,These methods might not be able to correctly distinguish between young and old faces given a few samples of both types of faces. The production of elder male master faces may occur as a result of the CASIA version of the Inception-ResNet-v2 based FR system's low performance on older male faces. It's interesting to note that the centroid of the ArcFace FR system, which is exclusively employed on the defender side, coincides with the master face created using the combination 1 setting. Even if we utilise the angle margin loss in training for this scenario, dense areas still occur.

D. False Matching Rate Analysis

The performance of attacks employing master faces was then assessed. The higher the FMR, the more enrolled subjects there are that closely resemble the created master face. Therefore, we contrasted the FMRs of two tests:

- Normal test: One side of the test pairings contained either a real face or an imposter face created with no effort in accordance with the database's test guidelines.
- Master face test: All of the participants' faces were paired with the master face in this test.
- These findings suggest two guidelines for designing LVE algorithm settings:
- Running the LVE method on many databases is problematic since the algorithm can favour the databases with the easiest data sets.
- Utilizing additional FR systems is acceptable. The architectures they use and the databases they were educated on can be the same or different.
- Combo settings in Table IV in conjunction with the Fig. 13 FMR curves.
- Master face attacks can affect any FR system.
- Compared to other systems, some are simpler to trick.
- The attack capabilities of the master faces were generated for the master face utilising the appropriate single settings with the combination 1 setting (single 1 and single 2). In this instance, there was no disagreement.
- Their master faces lacked some of the attack capabilities of the master faces formed with the comparable single settings when using the conflicting combination 2 and combination 3 settings. The combination 2 setting, where six attacks that were successful in the single settings failed, is a glaring example of this.

Target DB	Target FR System	*Single 1*		*Single 2*		*Single 3*		*Single 4*		*Single 5*		*Comb. 1*		*Comb. 2*		*Comb. 3*	
LFW - Fold 1	Inception-ResNet-v2	*2.3*	*3.3*	2.3	3.3	2.3	3.3	2.3	3.3	2.3	3.3	*2.3*	*3.3*	2.3	3.3	2.3	3.3
	(CASIA-WebFace)	***29.9***	***34.7***	**15.4**	**19.7**	2.4	2.3	0.4	0.4	0.8	0.2	***26.6***	***29.7***	***23.4***	***27.3***	**5.1**	4.4
	Inception-ResNet-v2	0.5	0.3	0.5	0.3	*0.5*	*0.3*	*0.5*	*0.3*	0.5	0.3	0.5	0.3	*0.5*	*0.3*	*0.5*	*0.3*
	(MS-Celeb)	0.1	0.8	1.0	1.1	***7.3***	***5.7***	***10.0***	***8.1***	1.1	0.6	1.2	1.7	*2.0*	*2.3*	*2.3*	*0.8*
	FaceNet (Inception-v1)	0.7	0.3	0.7	0.3	0.7	0.3	0.7	0.3	0.7	0.3	0.7	0.3	0.7	0.3	0.7	0.3
	(MS-Celeb)	0.0	1.1	0.3	1.1	0.4	0.8	0.5	1.5	0.4	0.2	1.3	0.6	0.8	1.3	1.2	0.6
	DR-GAN	3.3	3.7	*3.3*	*3.7*	3.3	3.7	3.3	3.7	*3.3*	*3.7*	*3.3*	*3.7*	3.3	3.7	*3.3*	*3.7*
	(CASIA-WebFace)	**6.2**	**8.1**	***30.1***	***33.3***	1.1	0.8	2.0	0.8	*4.3*	*3.6*	***27.3***	***27.8***	3.5	2.8	***6.0***	***5.5***
	ArcFace	14.3	12.3	14.3	12.3	14.3	12.3	14.3	12.3	14.3	12.3	14.3	12.3	14.3	12.3	14.3	12.3
	(MS-Celeb)	11.6	13.6	**21.3**	**26.3**	2.4	2.5	4.9	2.5	9.7	7.6	**22.1**	**23.5**	14.3	15.3	13.6	14.6
MOBIO	Inception-ResNet-v2	*1.9*	*2.1*	1.9	2.1	1.9	2.1	1.9	2.1	1.9	2.1	*1.9*	*2.1*	*1.9*	*2.1*	1.9	2.1
	(CASIA-WebFace)	*2.4*	*0.0*	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	*2.4*	*0.0*	*0.0*	*0.0*	**4.8**	**5.2**
	Inception-ResNet-v2	1.0	0.4	1.0	0.4	*1.0*	*0.4*	*1.0*	*0.4*	1.0	0.4	1.0	0.4	*1.0*	*0.4*	*1.0*	*0.4*
	(MS-Celeb)	0.0	0.0	0.0	0.0	*0.0*	*0.0*	*0.0*	*0.0*	0.0	0.0	0.0	0.0	*0.0*	*0.0*	*0.0*	*0.0*
	FaceNet (Inception-v1)	0.8	0.5	0.8	0.5	0.8	0.5	0.8	0.5	0.8	0.5	0.8	0.5	0.8	0.5	0.8	0.5
	(MS-Celeb)	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.7	0.0	0.0	0.0	0.0	0.0	0.0
	DR-GAN	2.3	1.3	*2.3*	*1.3*	2.3	1.3	2.3	1.3	*2.3*	*1.3*	*2.3*	*1.3*	2.3	1.3	*2.3*	*1.3*
	(CASIA-WebFace)	0.0	0.0	*0.0*	*0.0*	0.0	0.0	0.0	0.0	*2.4*	***12.1***	*0.0*	*0.0*	0.0	0.0	***4.8***	***6.9***
	ArcFace	8.2	7.8	8.2	7.8	8.2	7.8	8.2	7.8	8.2	7.8	8.2	7.8	8.2	7.8	8.2	7.8
	(MS-Celeb)	0.0	0.0	2.4	1.7	0.0	0.0	0.0	0.0	0.0	0.0	4.8	1.7	0.0	0.0	4.8	3.4
IJB-A	Inception-ResNet-v2	*10.1*		10.1		10.1		10.1		10.1		*10.1*		*10.1*		10.1	
	(CASIA-WebFace)	***37.5***		**15.2**		**13.4**		9.8		2.7		***20.5***		***25.0***		2.7	
	Inception-ResNet-v2	3.1		3.1		*3.1*		*3.1*		3.1		3.1		*3.1*		*3.1*	
	(MS-Celeb)	0.0		1.8		***20.5***		***22.3***		0.0		1.8		*0.9*		*0.0*	
	FaceNet (Inception-v1)	5.7		5.7		5.7		5.7		5.7		5.7		5.7		5.7	
	(MS-Celeb)	4.5		2.7		**9.8**		**8.0**		1.8		6.2		4.5		4.5	
	DR-GAN	10.8		*10.8*		10.8		10.8		*10.8*		*10.8*		10.8		*10.8*	
	(CASIA-WebFace)	4.5		***16.1***		7.1		**14.3**		*5.4*		***17.9***		5.4		*1.8*	
	ArcFace	10.7		10.7		10.7		10.7		10.7		10.7		10.7		10.7	
	(MS-Celeb)	0.0		3.6		0.9		0.9		2.7		0.9		0.9		0.9	

Conflict still took place in this situation, but it was not as bad as it was in combination 2.

The insights mentioned here offer insightful tips for efficiently building the LVE algorithm. Conflicts can be safely avoided when running the LVE algorithm by using only one database.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

Using many databases and FR systems may result in unpredictable successful assaults when a single setup fails, notwithstanding the severe side effects owing to conflicts.

V. PRESENTATION ATTACKS

Finally, we assessed the threat and risk of presentation attacks on FR systems utilising master faces. We selected two master face candidates: one produced using the combination 1 setting and another using the single 2 setting. We selected two attack scenarios from the IJB-A database where the two master faces were mistakenly accepted by the Inception-ResNet-v2 based FR system (CASIA-WebFace version) and the DR-GAN FR system as candidates for digital attacks.

5.1 Experiment Design

To simulate simple presentation attacks like the one shown in Fig. 14, we needed to prepare PAIs and cameras. For the PAIs of each of the two selected master faces, we used three kinds of materials:

- Color photos printed on plain A4 paper.
- Color photos printed on 127 mm × 178 mm photo paper.
- Color photos displayed on the screen of an Apple 13-inch MacBook Pro 2017. For the cameras, we used two types:
- The rear camera in an iPhone XR.
- A Canon EOS 60D DSLR camera with a Canon EF 40mm F2.8 STM lens.

We took pictures of the PAIs with these cameras in a typical room setting in order to keep things simple. The cameras' positioning was altered such that they were roughly parallel to
they could capture as much of the exhibited PAIs as possible without losing any contents by adhering to the surface of the PAIs. This syndrome resembles presentation attacks in the real world.

5.2 Results

Table VI includes the FMRs for attacks using PAI master faces, attacks using digital master faces, and attacks using the usual dev set of the IJB-A database.

19 out of the 24 attacks were successful, proving that PAI master faces can be useful in actual attacks. Eight instances involved FMRs that were higher than those of assaults made with computerised master faces. This is explained by the fact that, as a result of camera processing, the distribution of PAI master faces is more resemblant to the distribution of faces in the facial databases (which include faces also captured with a camera). The lower rate in the other situations is attributable to the PAI materials' arte facts rather than the camera processing having a larger impact. Seven of the eight PAI attacks conducted on computer screens were successful, compared to all of the PAI attacks conducted on plain paper. The attacks that used photo paper—which readily reflects light—performed the poorest. Those who used images captured by an iPhone camera outperformed those who used images captured by a Canon camera.This is explained by the fact that, as a result of camera processing, the distribution of PAI master faces is more resemblant to the distribution of faces in the facial databases (which include faces also captured with a camera). Artifacts from the other cases are thought to be the cause of the reduced rate.

PAI materials are more important than how the camera is processed. Seven of the eight PAI attacks conducted on computer screens were successful, compared to all of the PAI attacks conducted on plain paper. The attacks that used photo paper—which readily reflects light—performed the poorest. Those who used images captured by an iPhone camera outperformed those who used images captured by a Canon camera.

VI. DEFENSE AGAINST MASTER FACE ATTACKS

What fundamental flaw in the current FR architecture gives rise to master faces? We postulated that it originates from embedding space distributions where the retrieved features are not evenly distributed. As a result, clusters develop, including multi-identity clusters as well as ones based on age and gender. The training data and the objective function design are two potential causes of this issue. The training data was uneven in terms of age and gender, as can be seen in Figs. 7 and 8. This might change how the FR systems distribute the embeddings so that faces in the majority group are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 3, Issue 1, January 2023
Impact Factor: 7.301

discriminated against more effectively than those in the minority group. For instance, the face embeddings from 30 to 60 years old.

When it comes to objective function design, the major goal is to keep same-identity embeddings close together while keeping different-identity embeddings apart.

This is made better by the inclusion of the angular margin loss whereas the embeddings are forced to have a uniform distribution by the uniform loss. These upgrades mostly concentrate on identity, despite the fact that they lessen the chance of master face attacks.

The attack is successful in some instances because gender, age, and race are also significant factors. This shows that there is room for improvement in the design of the objective functions used to train the FR systems.

VII. CONCLUSION

We have one more shown that master face attacks constitute a serious security danger if the FR systems are not well safeguarded, particularly in our presentation attack experiment. Our thorough analysis of the LIVE algorithm's effectiveness in a variety of circumstances, including single and combination settings, has revealed various characteristics of master faces as well as the LVE algorithm itself. While some of the combination settings led to intra-component disputes, others had intriguingly favourable outcomes. To increase the robustness of FR systems, it is essential to understand the existence of master faces and their characteristics. Master face attacks could be mitigated by combining the employment of a FR system with a well-designed goal function trained on a sizable balanced database and a false picture detector. since master face attacks continue to improve, these attacks cannot be taken lightly. Future work will focus on designing a better method to generate master faces and one to detect master face attacks.

ACKNOWLEDGMENT

The authors would like to thank Dr. Tiago de Freitas Pereira and Dr. Amir Mohammadi of the Biometrics Security and Privacy (BSP) group at the Idiap Research Institute for providing the pretrained face recognition systems and for their support with the Bob toolkit.

REFERENCES

[1]. "The Goode Intelligence Biometric Survey 2021." Goode Intelligence. Apr. 2021. [Online]. Available:https://www.goodeintelligence.com/ report/the-goode-intelligence-biometric-survey-2021/

[2]. S. Bhattacharjee, A. Mohammadi, A. Anjos, and S. Marcel, "Recent advances in face presentation attack detection," in Handbook of Biometric Anti-Spoofing. Cham, Switzerland: Springer, 2019, pp. 207–228.

[3]. P. Bontrager, W. Lin, J. Togelius, and S. Risi, "Deep interactive evolution," in Proc. Int. Conf. Comput. Intell. Music Sound Art Des., 2018, pp. 267–282.

[4]. H. H. Nguyen, J. Yamagishi, I. Echizen, and S. Marcel, "Generating master faces for use in performing wolf attacks on face recognition systems," in Proc. IJCB, 2020, pp. 1–10.

[5]. U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face recognition systems under morphing attacks: A survey," IEEE Access, vol. 7, pp. 23012–23026, 2019.

[6]. P. Bontrager, A. Roy, J. Togelius, N. Memon, and A. Ross, "DeepMasterPrints: Generating MasterPrints for dictionary attacks via latent variable evolution," in Proc. BTAS, 2018, pp. 1–9.

[7]. M. Une, A. Otsuka, and H. Imai, "Wolf attack probability: A new security measure in biometric authentication systems," in Proc. ICB, 2007, pp. 396–406.

[8]. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in Proc. CVPR, 2019, pp. 4690–4699.

[9]. D. P. Kingma and M. Welling, "Auto-encoding variational bayes," in Proc. ICLR, 2014.

[10]. I. Goodfellow et al., "Generative adversarial nets," in Proc. NIPS, 2014, pp. 2672–2680.