Re-identification of anonymised MRI head images with publicly available software: investigation of the current risk to patient privacy

Katharina Steeg,[a,*] Evelyn Bohrer,[a] Stefan Benjamin Schäfer,[a] Viet Duc Vu,[a] Jan Scherberich,[a] Anton George Windfelder,[a,b,c] and Gabriele Anja Krombach[a,c]

[a]Department of Diagnostic and Interventional Radiology, University Hospital Giessen, Justus-Liebig-University Giessen, Klinikstraße 33, 35392, Giessen, Germany
[b]Department of Bioresources, Fraunhofer Institute for Molecular Biology and Applied Ecology IME, Giessen, Germany

eClinicalMedicine 2024;78: 102930
Published Online 20 November 2024
https://doi.org/10.1016/j.eclinm.2024.102930

Summary

Background Facial recognition software (FRS) has historically been perceived as lacking the capability to identify individuals from cross-sectional medical images. Utilising such data for identification purposes was considered infeasible due to the substantial computational power and specialised technical expertise it would require. However, recent advancements in accessible artificial intelligence-based (AI-based) software and open-source tools have made these applications widely available and easy to use, raising new privacy concerns.

Methods This proof-of-concept was designed as a cross-sectional study and included participants with a verified online presence. Standard magnetic resonance imaging (MRI) head scans were performed on these participants, from which three-dimensional rendering (3DR) images were created using free and publicly available software. These images were used for face searches by free and publicly available FRS. Different head orientations and hairstyles were applied to the 3DR images to assess whether non-facial features influenced the FRS results. All results were obtained between the 10th of February 2024 and the 1st of March 2024.

Findings Face searches of 3DR images in a database containing over 800 million images from the World Wide Web (WWW) yielded correct matches for 50% of the participants in less than 10 min. The user-friendly software required minimal computational knowledge or resources, making this process broadly accessible. Modifying elements such as hairstyles or the orientation of the 3DR to better resemble actual photographs of the participants improved FRS matches.

Interpretation Current existing FRS can swiftly and accurately identify individuals from MRI head scans. This poses a significant privacy risk for participants in enrolled clinical trials and highlights the urgent need for improved data protection measures and increased sensitivity to ensure participant confidentiality.

Funding There was no funding source for this study.

Keywords: Face recognition; De-facing; Re-identification; Anonymization; Patient privacy

Introduction

In radiology, digital image processing and the associated three-dimensional rendering (3DR), including 3D surface rendering and 3D volume rendering improve the visualisation of patient-specific anatomical structures and pathologies, enabling personalised medicine, and have become a standard tool for diagnosis and treatment.[1,2] Contrary, this has also led to concerns regarding the potential abuse of cross-sectional images, derived from examinations such as computed tomography (CT) and magnetic resonance imaging (MRI), to serve as templates for 3D facial reconstructions to obtain private medical information using artificial intelligence-based (AI-based) facial recognition software (FRS).[3–5] These concerns have been disregarded because abusing such data for identification requires significant computational

*Corresponding author.
E-mail address: Katharina.Steeg@radiol.med.uni-giessen.de (K. Steeg).
[c]These authors jointly supervised this work.

Research in context

Evidence before this study

A Web of Science and PubMed search from inception until February 2024 with keywords for ("facial recognition software") AND ("anonymization" OR "privacy") AND ("medical images") led to 13 articles. Of these, five studies expressed and explored concerns that three-dimensional renderings (3DR) of medical cross-sectional head images could be exploited for re-identification of research participants through artificial intelligence-based (AI-based) facial recognition software (FRS). These studies utilised local or freely available databases, and FRS, which did not comprise more than 100,000 images accessed from the World Wide Web (WWW), were not ready to use and required initial setup and, therefore, did not resemble a real-world scenario. Consequently, the concerns were dismissed due to the high computational knowledge and resources required for such identifications. The remaining eight studies focused on evaluating and improving de-facing algorithms, which aim to obscure or remove facial parts of cross-sectional image data to prevent complete 3DR and subsequent identification. A Google search for "face recognition search engine" in March 2024 yielded PimEyes and FaceCheck.ID within the top 10 FRS, highlighting their easy accessibility.

Added value of this study

Against previous assumptions, this study demonstrated that free and publicly available FRS provides a ready-to-use website interface and can identify, e.g., research participants based on medical cross-sectional head reconstructions without extensive computational knowledge or resources. Four participants were sufficient to demonstrate that current FRS are easy to use and that identification is possible in less than 10 min. The FRS used in this study searches a pool of over 800 million images, simulating a real-world scenario where a vast database could be used to identify individuals. This study also showed that altering 3DRs with random hairstyles or aligning them in different orientations to match original photographs of the participants increases the likelihood of identification. These findings imply that a higher number of publicly available photos of a person on the internet increases the risk of unwanted identification.

Implications of all the available evidence

This study aims to strengthen awareness about the risk of re-identification by 3DR of medical images that also include medical information. Currently, there are no mandatory, standardised regulations for de-facing cross-sectional head image data. This proof-of-concept study demonstrated that participants could be identified easily, highlighting the need for mandatory, standardised de-facing protocols to maintain anonymity while still encouraging data sharing for research purposes. It underscores the urgent need for comprehensive data anonymisation and protection regulations globally, raising awareness about the critical balance between data sharing and participant privacy.

resources and advanced technical skills.[6–8] However, recent advancements in the accessibility of AI-based software and open-source tools have made 3DR software and FRS available to anyone with a suitable dataset, thereby raising novel privacy concerns.[3]

FRS is a subset of computer vision techniques that first detects and then identifies faces in uploaded photographs.[9] During detection, an AI-based algorithm localises a face in an uploaded image for subsequent identification. Upon identification, the FRS usually extracts so-called facial features, which are typically unchangeable and easily recognisable points, such as the tip of the nose or pupil distance, to infer the person's biometrics.[9,10] While some software extracts facial features, other FRS may not rely on predefined landmarks. Subsequently, the biometric data serve as the input for often proprietary algorithms for facial recognition. These algorithms facilitate the matching of the input image against a database of faces, a process known as "1:N matching". This database can vary in size, quality, and source—sometimes, it needs to be defined by the user itself. In the final step, the FRS outputs a list of several images ranked according to their likelihood of depicting the same individual as the input image. An FRS is only as good as the dataset it was trained on. Depending on the training dataset's diversity, the FRS can ignore non-facial features, such as hairstyle or facial hair, at the input image to find the best matches.[11,12]

FRS was already considered in the General Data Protection Regulation (GDPR) that has been in force in the European Union (EU) since 2018 and has been transposed into national law in the associated countries.[13] According to Art. 9 Para. 1 GDPR, facial identification via biometric data, which are classified as sensitive inferences, may only be carried out with the consent of the person concerned.[13] However, despite this regulation, many online FRS are still publicly available in the EU.

In research, data often need to be transferred between sites and different medical disciplines, e.g., in clinical multicenter trials or projects like the Radiological Cooperative Network to COVID-19 pandemic (RACOON).[14] For blinded studies and data protection reasons, these data must be de-identified before transmission. The increasing risk of identifying faces by 3DR images can require additional protection measures in the future.

This proof-of-concept study aimed to ascertain the feasibility of a publicly available FRS, representing state-of-the-art technology, in identifying individuals based on their 3DRs from a vast and regularly updated database

accumulating images from the World Wide Web (WWW). This contrasts with earlier research that used smaller and sometimes self-generated databases, which were found to not adequately represent real-world scenarios.[8] To simulate a real-world scenario, the study assessed whether an individual without specialised knowledge in medical or computational domains could successfully perform a re-identification. To accomplish this, 3DR images were derived from MRI head scans and subsequently used for identification via a freely accessible online FRS.

Methods

In line with EU and German data protection rules, the study enrolled only participants who fully understood the implications of their consent and participation. The descriptive approach of this cross-sectional proof-of-concept assesses the feasibility of using a state-of-the-art FRS to identify individuals based on 3DRs from a vast, evolving database of WWW images. Only participants who self-reported using social media and for whom a Google search of their name yielded photographs were enrolled. The same workflow was performed for each participant who consented to participate in this study. Each participant received a T1-weighted sagittal scan of the head at a 1.5 T MRI Scanner (MAGNETOM Avanto, Siemens Healthineers, Erlangen, Germany) with a voxel resolution of 1.0 mm. This imaging sequence was based on a head examination used in a clinical routine and was not specifically designed for face reconstruction. Previous tests have demonstrated that sufficient image quality had to be guaranteed to achieve high quality at 3DR. Therefore, images in 1.0 mm segments with no spacing were acquired.

An individual with a background in biomedical sciences, though not specialised in diagnostic radiology or image computing, was assigned the task of visualising MRI images in 3D and subsequently performing facial recognition using freely available software. Digital Imaging and Communications in Medicine (DICOM) data of each MRI was loaded into 3D Slicer 5.6.1, a free software designed for the analysis and visualisation of medical images and for the processing of 3D data.[15] For 3DR, several presets within the 3D Slicer were tested, including those designed for MRI and soft tissue visualisation (Supplementary Figure S1). However, the MRI presets did not result in visually identifiable reconstructions. Due to that, the standard "uCT-Bone 8bit" preset was chosen for its ability to produce visually detailed and human-like representations in terms of contrast, colour, surface smoothness, and lightning. Visual artifacts that were not part of the facial structures were minimised by adjusting the shift setting within the 3D Slicer software. To test the impact of different head orientations (frontal, side view, half side view, and top view) on the hit rate of the FRS, screenshots of different raw head alignments were processed and saved as portable network graphics (PNG) files. Orientation 1 refers to the frontal view of the face, where all facial features are aligned symmetrically, making it, in theory, the most effective orientation for FRS. Because hairstyle can affect the accuracy of an FRS, hair was added to the 3DR in Orientation 1 (Fig. 1) in PowerPoint.[11] To

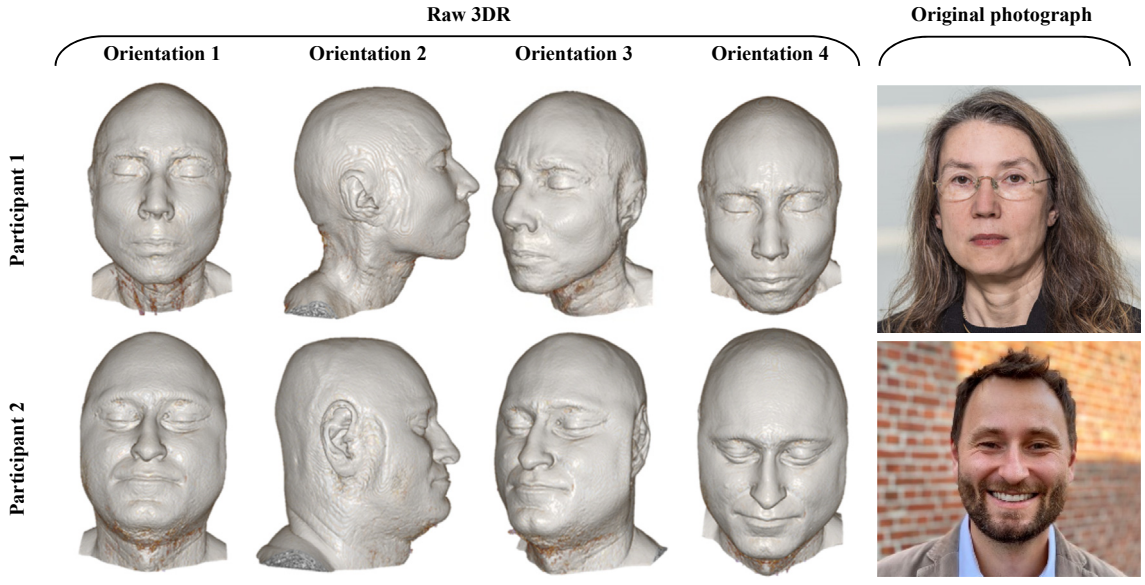

Fig. 1: **Examples of three-dimensional rendering (3DR) images for a female (top row) and male (bottom row) participant with varying head orientations alongside their original photograph on the right side**. Participants 1 and 2 provided explicit consent for the publication of their face images.

circumvent any potential bias due to the colour of the added hairstyles, the investigation encompassed both coloured images and those converted to black and white. Hairstyles for processing were obtained from Freepik.[16]

Facial recognition testing was performed using the free, publicly available identification software FaceCheck.ID, which attempts to match an input face to images of the respective individual from the WWW. FaceCheck.ID was selected because it is easy to use and searches a database with over 800 million entries, making it a likely choice for a malicious actor. Additionally, it allows unlimited searches without payment. The provider of FaceCheck.ID states that input images are deleted within 24 h and are not added to the training data of the FRS. However, FaceCheck.ID's algorithm is a proprietary AI for facial recognition and the specific methods used by this FRS are not disclosed. FaceCheck.ID updates its algorithm and database regularly, influencing the results. All results were obtained between the 10th of February 2024 and the 1st of March 2024.

To validate a sufficient online presence and FaceCheck.ID's ability to identify the participants, a photograph of each participant (hereinafter referred to as the original photograph) was employed as a positive control.

When uploading an image and the FRS verifies a face, it performs a face search; otherwise, the search is canceled. For each face search, FaceCheck.ID provides a ranked list of potential matches. The same match could be listed repeatedly when accessed from different websites. A correct match was considered a successful identification when it was placed within the top five total matches. Placements of the correct matches were indicated relative to the total number of matches. MRI images of successfully identified participants were subsequently de-faced using *mri_deface*, one frequently used de-facing algorithm, to test whether de-facing can prevent identification.[17] After defacing, new 3DR were created as described before and used as input for FaceCheck.ID.

The time required for a search was evaluated by measuring the duration from data upload to create a 3DR until the appearance of displayed matches in FaceCheck.ID.

Participants consent

Written informed consent was obtained from all participants before enrolment. Participants 1 and 2 provided explicit consent for the publication of their face images.

Ethics statement

An ethical approval was not required as this study was no medical research.

Role of the funding source

There was no funding source for this study.

Results

Three male and one female team member with self-reported online presence, all of European descent, between the ages of 35 and 55, were confirmed eligible for this study.

Due to the specific conditions of MRI scans, the appearance of the 3DR differed from that of original photographs. In contrast to upright photographs, where participants are typically facing the camera and smile, in these scans, participants lied supine with relaxed facial expressions and wore ear protection (Fig. 1). This resulted in non-smiling faces with closed eyes, and due to the ear protection in MRI, the 3DR appeared dented around the ears. Since hair is not detected in MRI scans, the raw 3DR images were also devoid of hair.

Each participant's original photograph attained at least one correct match (Table 1). For Participants 1–3,

	Participant 1		Participant 2		Participant 3		Participant 4	
	No. of matches	Placement of correct match	No. of matches	Placement of correct match	No. of matches	Placement of correct match	No. of matches	Placement of correct match
Original photograph	48	1 (100%), 2 (99%)	77	1 (100%), 2 (99%), 3 (97%), 4 (96%)	73	1 (100%), 2 (99%)	48	1 (100%)
Hairless photograph	41	1 (100%), 2 (99%)	69	1 (100%), 2 (99%), 3 (97%), 4 (96%)	86	1 (100%), 2 (99%)	49	1 (100%)
Raw 3DVR Orientation 1	68	– –	74	1, (100%), 3, (97%), 12, (85%), 60 (20%)	71	– –	71	4 (96%)

Original photographs and hairless photographs were used as positive controls. Placement of the correct match relative to the total number of matches is indicated in brackets.

Table 1: **The three-dimensional rendering (3DR) in orientation 1 led to identifications for participants 2 and 4.**

further correct photographs were detected. Due to the absence of hair in 3DR images, searches were also conducted using hairless photographs (Table 1). These yielded the same number and placement of correct matches as the search with the original photograph. The placement of correct matches relative to the total number of matches per search does not directly represent the accuracy of the search; however, it provides valuable context by indicating the rank of the correct match within the overall set of results.

Subsequently, MRI-derived 3DRs were used as input images. With the frontal 3DR, the FRS was feasible to find correct matches for Participants 2 and 4 (Table 1). All four available correct matches of Participant 2 were found, positioned at 1st, 3rd, 12th, and 60th place out of 74 total matches. Even though Participant 2 exhibited a smile, subjectively altering its facial appearance compared to the frontal 3DR, the original photograph was still identified. The correct match of Participant 4 was found in 4th place out of 71 total matches. However, using only the frontal 3DR did not yield correct matches for Participants 1 and 3 (Table 1 bottom row).

Subsequent de-facing with *mri_deface* prevented the re-identification of the two participants previously identified (Supplementary Figure S2). Inferences of biometric data can be affected by changes in head orientation in photographs. Different head orientations demonstrated that correct matches were ranked higher when the reconstructed head's orientation closely resembled the original photograph. For instance, Participant 4's correct match was elevated from 4th to 2nd place when the head orientation was aligned closer to the original photograph (Table 2). Correspondingly, one correct match for Participant 2 dropped from first place when the 3DR was aligned frontally to 17th place when the 3DR was rotated to the right or 4th place when oriented facing downwards. No orientation of the 3DR led to correct matches of Participants 1 or 3.

Additionally, hairstyles can affect the biometrics in photographs by obscuring significant landmarks such as the forehead or jawbones. Therefore, FaceCheck.ID was tested to recognise participants with different hairstyles with coloured images and images converted to black and white (Fig. 2). The results remained consistent among both options, suggesting that hair colour did not significantly affect the matching process.

Adding the hairstyle from the original photograph to the 3DR yielded the same number of identifications for each participant as the original photographs (Table 3). However, for Participant 2, the addition of original hair changed the placement of the third and fourth correct matches, moving from 12th to 4th and from 60th to 6th, respectively. The correct match for Participant 4 remained in 4th place, regardless of the presence of Original hair.

For Participant 2, Hairstyle 1 (Fig. 2), which covers only a small part of the forehead, resulted in a higher number of total matches. Accordingly, the number of correct matches also increased (the same photograph was listed several times). However, these matches were not ranked higher than those obtained from the frontal 3DR.

On the other hand, for Participant 4, Hairstyle 1 moved the correct match from 4th to the 1st place compared to the frontal 3DR results. Other hairstyles for Participant 4 resulted in varying placements of the correct match but were always ranked lower than the match achieved by the frontal 3DR.

So far, the frontal 3DR of Participant 3 only led to correct matches when processed with Original hair. After adding Hairstyle 2, the correct match was ranked at placement 26. No correct match was obtained for Participant 1 with Hairstyles 1–6. Finally, it was observed that even with different hairstyles for each participant, one celebrity was frequently suggested as a match with different photographs. For Participant 1, it was Lady Gaga; for Participant 2, it varied depending on the haircut; for Participant 3, it was Richard Tice; and for Participant 4, it was Boris Becker.

The time required to create a 3DR and then perform a face search was evaluated. After initial software installation and setup, the workflow took no more than 10 min per image. This included 1 min for the data upload, 2 min to create and save the 3DR, and between one and 7 min for the face search, depending on the capacity of FaceCheck.ID.

	Participant 1			Participant 2			Participant 3			Participant 4		
	No. of matches	Placement of correct match		No. of matches	Placement of correct match		No. of matches	Placement of correct match		No. of matches	Placement of correct match	
Raw 3DR Orientation 2	65	–	–	56	–	–	82	–	–	64	–	–
Raw 3DR Orientation 3	74	–	–	81	17 56	(80%), (32%),	81	–	–	77	2	(98%)
Raw 3DR Orientation 4	76	–	–	80	4 5 22	(96%), (95%), (74%)	71	–	–	58	16	(72%)

Placement of the correct match relative to the total number of matches is indicated in brackets.

Table 2: **Aligning the 3DR in different head orientations changed the number and placement of correct matches.**

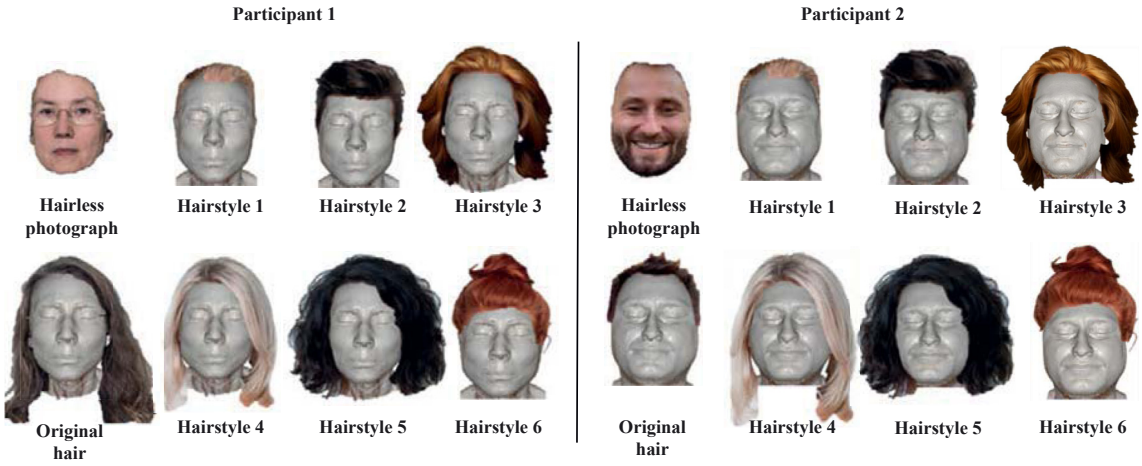

***Fig. 2:* Examples of 3DR processed with different hairstyles for participants 1 and 2**. Images of hairstyles were obtained from Freepik.

FaceCheck.ID successfully identified 50% of the participants using MRI-derived 3DRs, with the first correct match ranked among the top five total matches. Different head orientations and hairstyles impacted match rankings, with closer alignment to the Original photograph generally improving the placement of correct matches. However, obscuring the participants 3DRs by de-facing prevented re-identification. The total time for generating a 3DR and performing a face search did not exceed 10 min per participant.

Discussion

After a short introduction, a person without domain expertise was able to create 3DR images and conduct a facial search on the internet within minutes. MRI images of four participants and freely available software were already sufficient to prove that it is possible to identify research participants in photographs from the WWW. The results showed that the biometric features of the 3DR were detailed enough for identification. Additionally, this study confirmed the hypothesis that

	Participant 1		Participant 2		Participant 3		Participant 4	
	No. of matches	Placement of correct match	No. of matches	Placement of correct match	No. of matches	Placement of correct match	No. of matches	Placement of correct match
Raw 3DR Original hair	90	1 (100%)	71	1 (100%), 3 (97%), 4 (96%), 6 (93%)	80	4 (96%)	79	4 (96%)
Raw 3DR Hairstyle 1	73	– –	165	2 (99%), 3 (99%), 51 (69%), 82 (50%), 88 (47%), 90 (45%), 136 (18%), 160 (3%)	79	– –	62	1 (100%)
Raw 3DR Hairstyle 2	74	– –	76	37 (51%), 43 (43%)	72	26 (65%)	77	31 (58%)
Raw 3DR Hairstyle 3	53	– –	64	14, 37 (80%), (44%)	65	– –	76	9 (89%)
Raw 3DR Hairstyle 4	92	– –	58	44 (25%)	71	– –	78	10 (88%)
Raw 3DR Hairstyle 5	71	– –	57	– –	44	– –	86	12 (87%)
Raw 3DR Hairstyle 6	65	– –	73	– –	75	– –	79	7 (92%)

3DR in frontal orientation was used for processing. Placement of the correct match relative to the total number of matches is indicated in brackets.

***Table 3:* Different hairstyles led to a change in the number and placement of correct matches.**

publicly available FRS, according to the current state-of-the-art, can identify individuals based on reconstructions of their MRI head scans with little effort from large and regularly updated databases including images from the WWW.

Previous studies have shown the feasibility of using MRI head images to reconstruct a research participant's face and subsequently using FRS to match these reconstructions to photos of the actual person in a user-defined local database.[4,5,18,19] In 2012, Mazura et al. identified individuals based on reconstructed CT-head scans from a pool of 29 photographs imported by the authors. Although the Google Picasa 3.6 FRS used in this study was only successful in 27.5% of searches, it highlighted the potential risk of reconstructed medical data for unwanted identification.[18] Seven years later, Schwarz et al. trained the Microsoft Azure FRS on participant-specific internal features of MRI reconstructions.[5] Subsequently, the FRS matched an individual's photographs to the correct photograph in 96–98% of 182 participants.[20] These previous studies have shown the feasibility of utilising 3DR of MRI data for the identification of an individual from a user-defined local and not regularly updated database. In contrast, FaceCheck.ID is updated regularly and thereby continuously grows in size and diversity. Consequently, it offers to match input images against a vast database comprising over 800 million faces, including data from social media platforms, blogs, and videos. Due to that, this study further demonstrated that state-of-the-art FRS are easy and fast to use and enable identification of 3DR images even from significantly larger databases, including photographs from the WWW.

Due to concerns regarding radiation exposure inherent in CT and positronic-emissions-tomography-CT (PET-CT) scans, this study used MRI scans exclusively. However, previous studies have already shown the feasibility of conducting face searches using CT and PET-CT data.[18,19,21] The quality of 3DR, crucial for identifying facial features and biometric data points, is influenced by various factors, including scan parameters such as MRI sequence, CT tube current, and reconstructed slice thickness.[21]

Methodological constraints intrinsic to MRI scans led to notable discrepancies between 3DRs and original photographs. These included closed eyes, a relaxed mouth and receded cheeks resulting from the supine positioning, and dented areas around the ears caused by ear protection. While FRS theoretically partially disregards facial expressions, eye closure, or head orientation because biometrics are as distinct as fingerprints, previous studies have shown that changes in certain facial attributes can impede accuracy.[10,11,22] Consequently, shifts in facial features induced during MRI scans can alter the participant's appearance on 3DR and may also affect matching accuracy. This is why passport photographs require a frontal view, neutral facial expressions and opened eyes—because these are the conditions biometrics are best represented.[11]

Although non-facial features, such as head pose, hairstyle and colour, or facial hair, may not be decisive factors, they have been shown to impact face recognition accuracy in various studies.[11,23,24] The algorithm's ability to accurately identify individuals despite variations in facial and non-facial features is largely dependent on the diversity and composition of the training dataset. Previous research has indicated that FRS have lower accuracy for females which may be based on the smaller representation of female images in some datasets.[24] This aligns with the results for Participant 1, a female who was not detected using the hairless 3DR as input, potentially due to biases in the training dataset of FaceCheck.ID. A later study suggested that the gender accuracy gap may due to imbalanced test data, such as variations in hairstyles and facial hair, rather than deficiencies in the training data itself.[12] Consequently, this study examined whether variations in head orientations and hairstyles affected the performance of FaceCheck.ID.

Due to its low water content, hair is difficult to detect in standard clinical MRI scans.[25] Consequently, the 3DRs in this study were hairless. Altering the hairstyle and head orientation to better match the original photograph led to more accurate matches. This was particularly true for Participant 3, which was not recognised using the 3DR, but when Hairstyle 1 or 2 was added, the original photograph appeared as a match. Besides, the fact that the results changed only marginally with the pictures converted to black and white indicates that not the hair colour but something else about the hairstyles (shape, structure, parts of the face that were now covered) was essential to match photographs of the correct individual. This was also shown by Boutet et al., who examined the impact of facial hair on FRS, comparing the *GEO* approach, which relies on geometrical features, with the *Deepface* approach, based on deep learning of facial features.[23] With hair present on the input images, *GEO* outperformed *Deepface*, as the geometrical features remain identifiable despite the hair. However, once facial hair and hairstyle was removed and the input images more closely resembled the hairless MRI reconstructions, *Deepface* performed better. This study underscores that FRS accuracy is highly dependent on the training data and underlying architecture. While it was not possible to determine how FaceCheck.ID processed hair due to its proprietary nature, the improved match rankings when the 3DR more closely resembled those of original photographs suggest that it may utilise an algorithm more akin to *Deepface* than *GEO*.

Regardless, randomly adding hairstyles to 3DR is more likely to result in misidentification rather than accurate identification, as correct matches may not consistently be ranked first. For instance, it was

observed that for each participant, one celebrity was frequently suggested as a match with different photographs. In this study, it was known that the participants were not any of the celebrities, but a motivated individual would not know which of the proposed image mismatches were. Mismatches can result in misidentification, which can be just as problematic for the person concerned as correct identification.

Several cases have been reported where misinterpretation of FRS matches has resulted in the arrest of innocent citizens. In 2019, a man was arrested at an airport and accused of a serious theft that had occurred three years earlier after an FRS matched him as the suspected perpetrator. Subsequent investigation revealed that the misidentification was not due to the FRS's suggestions but rather to a misinterpretation of the matches it had provided.[26] In another recent case, a man was wrongly jailed for six days based on the results of an FRS.[27]

Conversely, FRS has proven its potential with the arrest of a German ex-terrorist of the "Rote Armee Fraktion" in February 2024. Despite the ex-terrorist being detained by the police not as a result of FRS identification, it was later revealed that journalists had already tracked this person in November 2023 using the publicly available FRS "PimEyes" and photographs that were 30 years old.[28] Given the controversy surrounding using PimEyes by authorities in the EU and the United States (US), this study focused on FaceCheck.ID.

However, these cases demonstrate the power and responsibility for decisions based on FRS data. At best, a correct identification may lead to a wanted criminal; at worst, a misidentification may result in discrimination and a violation of someone's dignity.[29] This highlights the urgent need to sensitise and train users to interpret the results of FRS and other AI-driven tools. This is also essential to guarantee data protection regulations and the steady development of data protection protocols to match the current state of technical feasibility.

Currently, non-facial features or feature shifts may still present a challenge for FRS, but like AI, the field is developing rapidly.[30] Furthermore, in addition to the ongoing advancement of technologies, the growing amount of available image material also represents a potential challenge to data protection. For example, in the US, traffic and pedestrian cameras, street surveillance systems, body-worn cameras, or dash-cams used by law enforcement agencies are capturing an increasing amount of images of individuals without requesting explicit permission.[31] The accumulation of image data exponentially increases the number of references for comparison by FRS, suggesting that individuals with more images online are more likely to be identified. This was supported by Participant 2, who had the most photographs available and was identified most frequently and accurately. In contrast, participants with only one photograph were identified less often or not at all. Future studies with larger cohorts will be needed to verify this hypothesis.

As the number of identifications increases, so does the risk of misidentifications, exacerbating the potential for false accusations and unjust violations of individual rights and dignity.[29] MRI-based identification can reveal personal and medical information that may be abused for identity theft, insurance deceit, or even exclusion from insurance services, falsely applying for medication and related offenses.[5,32]

Protecting patient data is crucial, and de-facing algorithms are one approach to prevent face reconstruction from cross-sectional head images. However, these algorithms face the challenge of obscuring or removing facial voxels without compromising important data for diagnosis.[33] In this context, previous studies found that even after de-facing, up to 38% of participants could still be identified by FRS.[4] Later, Jwa et al. highlighted that identification accuracies would be lower in real-world scenarios due to a significantly larger pool of potential matches. Based on simulations of a database with 800,000 entries, they estimated only a 0.6% re-identification likelihood after de-facing.[4,5,8] This current study addressed this gap using FaceCheck.ID, which searches a database of over 800 million entries–1000 times larger than the simulation database—and identified 50% of the participants. After de-facing with *mri_deface*, both participants were no longer recognisable, despite the eye region being left intact.[17] Although this could theoretically allow identification, FaceCheck.ID could not identify the participants based on these residual features, suggesting that standardised de-facing regulations are a promising solution. While these findings imply a higher risk of identification in a real-world scenario as previously assumed, we acknowledge that our results are more qualitative and call for further comprehensive analysis, including the evaluation of the remaining risk after different de-facing algorithms.

Triggered by the advent of the Coronavirus disease 2019 (COVID-19) pandemic, the FRS research focused on AI-driven biometric identification algorithms that can identify individuals with half of their face covered or obscured, e.g., by masks.[3,30] These developments also affect the effectiveness of de-facing algorithms, which have not undergone such fast progress. To address this issue, Schwarz et al. recently presented a new version of their de-facing algorithm, *mri_reface* 0.3, which reduced identification to less than 8%.[20] Besides, there is currently no standardised regulation for de-facing cross-sectional head image data. So even if the ideal algorithm would exist, de-facing of MRI, CT, or PET-CT data is not yet mandatory, and execution of this process varies between institutions.

This was partly taken into account by a new draft law adopted by the EU Parliament on 9th December 2023, which is due to come into force in 2026.[34] It sets out much stricter rules for the use and public accessibility of AI

applications. The law assesses existing and future applications according to risk and provides further procedural options depending on their classification.[34] For example, AI applications that can identify people based on biometrics will be classified as high-risk and restricted for the public in the EU in the future.[34] Unlike the EU, many non-EU countries do not regulate software that uses biometric data. Due to this, potentially critical software may continue to be placed online and be accessible from the EU.

To comply with EU and German data protection guidelines, the study was limited to a small number of team members who fully understood the implications of their consent and participation. Consequently, to minimise online data exchange, FaceCheck.ID was selected from other free available FRS as the provider states that searches are not stored for longer than 24 h, and input data are not used to further train the FRS algorithm. 3D Slicer was selected from among free available 3DR software for its ability to quickly create visually appealing reconstructions. The small sample size, comprising four participants, introduced limitations to the generalisability of the findings. While the qualitative insights provided are valuable for understanding the potential risks of FRS, the limited number of participants restricts the ability to draw broad, quantitative conclusions regarding the risk for everyone. Nevertheless, the study effectively demonstrated that FRS can identify individuals from MRI-based 3DR within minutes and with no considerable effort. This study was designed as a proof-of-concept to promptly highlight the existing challenges and deficiencies in the implemented security measures that might impact participants in research studies. Future research has the potential to expand upon these findings on a larger and more diverse cohort to validate and further explore the implications for privacy risks and identification in real-world scenarios. However, conducting further research in concordance with the already existing data protection guidelines might be challenging in the future.

The study demonstrated that no high level of expertise is required to create 3DRs from MRIs and search for them with an FRS. Nowadays, FRS can be used on standard laptops and provides a user-friendly interface and can be used without considerable effort. Creating a 3DR based on cross-sectional image data and subsequent identification of an individual does not necessitate coding skills, high-end hardware, or domain knowledge. To mitigate this risk, it is crucial to establish data anonymisation and protection regulations under evolving technical capabilities and to raise awareness about which data should be shared.

Contributors

Writing the first draft of the manuscript: Katharina Steeg.

Supervision of the project: Evelyn Bohrer, Anton George Windfelder, Gabriele Anja Krombach.

Data collection, data analysis, and data interpretation: Katharina Steeg, Evelyn Bohrer.

Accessed and verified the data: Katharina Steeg, Evelyn Bohrer writing–review & editing: Katharina Steeg, Evelyn Bohrer, Viet Duc Vu, Stefan Benjamin Schäfer, Anton George Windfelder, Jan Scherberich, Gabriele Anja Krombach.

Providing data or critical feedback on data sources: Katharina Steeg, Viet Duc Vu, Stefan Benjamin Schäfer, Anton George Windfelder, Jan Scherberich, Gabriele Anja Krombach.

Data sharing statement

Data is available from the lead contact Prof. Dr. Gabriele Anja Krombach (Gabriele.Krombach@uniklinikum-giessen.de).

Declaration of interests

Viet Duc Vu's position is funded by the Radiological Cooperative Network to COVID-19 pandemic (RACOON) "NUM 2.0" (FKZ: 01KX2121).

All other authors declare no competing interests.

Acknowledgements

The authors want to acknowledge the help of Beate Stefan. The authors acknowledge the support of the Radiological Cooperative Network to COVID-19 pandemic (RACOON) "NUM 2.0" (FKZ: 01KX2121).

Appendix A. Supplementary data

Supplementary data related to this article can be found at https://doi.org/10.1016/j.eclinm.2024.102930.

References

1 Duran AH, Duran MN, Masood I, Maciolek LM, Hussain H. The additional diagnostic value of the three-dimensional volume rendering imaging in routine radiology practice. *Cureus*. 2019;11:e5579.
2 Haleem A, Javaid M, Suman R, Singh RP. 3D printing applications for radiology: an overview. *Indian J Radiol Imaging*. 2021;31:10–17.
3 European Parliament. *Directorate general for parliamentary research services. Regulating facial recognition in the EU: in depth analysis*. LU: Publications Office; 2021. https://data.europa.eu/doi/10.2861/140928. Accessed April 29, 2024.
4 Schwarz CG, Kremers WK, Wiste HJ, et al. Changing the face of neuroimaging research: comparing a new MRI de-facing technique with popular alternatives. *Neuroimage*. 2021;231:117845.
5 Schwarz CG, Kremers WK, Therneau TM, et al. Identification of anonymous MRI research participants with face-recognition software. *N Engl J Med*. 2019;381:1684–1686.
6 *Why concern about facial recognition from brain scans is overblown*. Spectrum|Autism Research News; 2020. https://www.spectrumnews.org/opinion/viewpoint/why-concern-about-facial-recognition-from-brain-scans-is-overblown/. Accessed March 13, 2024.
7 Kolata G. *You got a brain scan at the hospital. Someday a computer may use it to identify you*. The New York Times; 2019. https://www.nytimes.com/2019/10/23/health/brain-scans-personal-identity.html. Accessed March 13, 2024.
8 Jwa AS, Koyejo O, Poldrack RA. Demystifying the likelihood of reidentification in neuroimaging data: a technical and regulatory analysis. *Imaging Neurosci*. 2024;2:1–18.
9 Dirin A, Suomala J, Alamäki A. *AI-Based facial recognition in emotional detection*. 2019.
10 Face detection, attributes, and input data - face - Azure AI services| Microsoft learn. https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/concept-face-detection. Accessed December 18, 2023.
11 Grother P, Ngan M, Hanaoka K. *Face recognition vendor test (FRVT) part 2: identification*. Gaithersburg, MD: National Institute of Standards and Technology; 2019.
12 Bhatta A, Albiero V, Bowyer KW, King MC. The gender gap in face recognition accuracy is a hairy problem. In: *2023 IEEE/CVF winter conference on applications of computer vision workshops (WACVW)*. Waikoloa, HI, USA: IEEE; 2023:1–10.
13 Vollmer N. *Article 9 EU general data protection regulation (EU-GDPR)*; 2023. https://www.privacy-regulation.eu/en/article-9-processing-of-special-categories-of-personal-data-GDPR.htm. Accessed December 19, 2023.

14 Racoon – radiological cooperative network. https://racoon.network/. Accessed March 21, 2024.
15 Fedorov A, Beichel R, Kalpathy-Cramer J, et al. 3D slicer as an image computing platform for the quantitative imaging network. *Magn Reson Imaging*. 2012;30:1323–1341.
16 Freepik|Erstelle großartige designs, noch schneller. Freepik. https://de.freepik.com. Accessed March 16, 2024.
17 Bischoff-Grethe A, Ozyurt IB, Busa E, et al. A technique for the deidentification of structural brain MR images. *Hum Brain Mapp*. 2007;28:892–903.
18 Mazura JC, Juluru K, Chen JJ, Morgan TA, John M, Siegel EL. Facial recognition software success rates for the identification of 3D surface reconstructed facial images: implications for patient privacy and security. *J Digit Imaging*. 2012;25:347–351.
19 Schwarz CG, Kremers WK, Lowe VJ, et al. Face recognition from research brain PET: an unexpected PET problem. *Neuroimage*. 2022;258:119357.
20 Schwarz CG, Kremers WK, Arani A, et al. A face-off of MRI research sequences by their need for de-facing. *Neuroimage*. 2023;276:120199.
21 Uchida T, Kin T, Sato K, et al. Reproducibility of facial information in three-dimensional reconstructed head images: an exploratory study. *Curr Med Imaging*. 2023;19:1387–1393.
22 Alrubaish HA, Zagrouba R. The effects of facial expressions on face biometric system's reliability. *Information*. 2020;11:485.
23 Boutet A, Frindel C, Maouche M. Towards an evolution in the characterization of the risk of re-identification of medical images. In: *2023 IEEE international conference on big data (BigData)*. Sorrento, Italy: IEEE; 2023:5454–5459.
24 Albiero V, Zhang K, Bowyer KW. How does gender balance in training data affect face recognition accuracy?. In: *2020 IEEE international joint conference on biometrics (IJCB)*. 2020:1–10.
25 Soga S, Koyama T, Mikoshi A, et al. MR imaging of hair and scalp for the evaluation of androgenetic alopecia. *Magn Reson Med Sci*. 2020;20:160–165.
26 *Un hombre estuvo seis días preso por un error policial*. infobae; 2019. https://www.infobae.com/sociedad/policiales/2019/08/02/un-hombre-estuvo-seis-dias-preso-por-un-error-del-sistema-de-reconocimiento-facial/. Accessed March 20, 2024.
27 Simerman J. *JPSO used facial recognition technology to arrest a man. The tech was wrong*. NOLA.com; 2023. https://www.nola.com/news/crime_police/jpso-used-facial-recognition-to-arrest-a-man-it-was-wrong/article_0818361a-8886-11ed-8119-93b98ecccc8d.html. Accessed April 17, 2024.
28 Solomon E, Schuetze CF. *How Germany's most wanted criminal hid in plain sight*. The New York Times; 2024. https://www.nytimes.com/2024/03/01/world/europe/daniela-klette-red-army-faction.html. Accessed April 29, 2024.
29 Raposo VL. When facial recognition does not 'recognise': erroneous identifications and resulting liabilities. *AI Soc*. 2023;39:1857–1869. https://doi.org/10.1007/s00146-023-01634-z.
30 Andrejevic M, O'Neill C, Smith G, Selwyn N, Gu X. Granular biopolitics: facial recognition, pandemics and the securitization of circulation. *New Media Soc*. 2024;26:1204–1226.
31 Bromberg DE, Charbonneau É, Smith A. Public support for facial recognition via police body-worn cameras: findings from a list experiment. *Govern Inf Q*. 2020;37:101415.
32 Pool J, Akhlaghpour S, Fatehi F, Burton-Jones A. A systematic analysis of failures in protecting personal health data: a scoping review. *Int J Inf Manag*. 2024;74:102719.
33 Gao C, Landman BA, Prince JL, Carass A. Reproducibility evaluation of the effects of MRI defacing on brain segmentation. *J Med Imaging*. 2023;10:064001.
34 Council of the European Union. *Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*; 2024. https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf. Accessed March 19, 2024.