공학석사 학위논문

빅데이터 구축을 위한 딥러닝 알고리즘 응용 의료 영상 비식별화 소프트웨어 개발

Development of medical image de-identification software applying deep learning algorithm for big data platform

울 산 대 학 교 대 학 원

의 과 학 과

정 연 욱

빅데이터 구축을 위한 딥러닝 알고리즘 응용 의료 영상 비식별화 소프트웨어 개발

지 도 교 수 김 영 학

이 논문을 공학석사 학위 논문으로 제출함

2021년 2월

울 산 대 학 교 대 학 원

의 과 학 과

정 연 욱

정연욱의 공학석사 학위 논문을 인준함

심사위원 심 우 현 인

심사위원 이 현 나 인

심사위원 김 영 학 인

울 산 대 학 교 대 학 원

2021년 2월

Abstract

High-resolution medical images that include facial regions can be used to recognize the subject's face when reconstructing 3-dimensional (3D)-rendered images from 2-dimensional (2D) sequential images, which might constitute a risk of infringement of personal information when sharing data. According to the Health Insurance Portability and Accountability Act (HIPAA) privacy rules, full-face photographic images and any comparable image are direct identifiers and considered as protected health information. Moreover, the General Data Protection Regulation (GDPR) categorizes facial images as biometric data and stipulates that special restrictions should be placed on the processing of biometric data.

This study aimed to develop software that can remove the header information of Digital Imaging and Communications in Medicine (DICOM) format files and facial features (eyes, nose, and ears) at the 2D sliced-image level to anonymize personal information in medical images.

A total of 240 cranial magnetic resonance (MR) images were used to train the deep learning model (144, 48, and 48 for the training, validation, and test sets, respectively, from the Alzheimer's Disease Neuroimaging Initiative [ADNI] database). To overcome the small sample size problem, we used a data augmentation technique to create 576 images per epoch. We used attention-gated U-net for the basic structure of our deep learning model. To validate the performance of the software, we adapted an external test set comprising 100 cranial MR images from the Open Access Series of Imaging Studies (OASIS) database.

The facial features (eyes, nose, and ears) were successfully detected and anonymized in both test sets (48 from ADNI and 100 from OASIS). Each result was manually validated in both the 2D image plane and the 3D rendered images. Furthermore, the ADNI test set was verified using Microsoft Azure's face recognition artificial intelligence service. By adding a user interface, we developed and distributed (via GitHub) software named "Deface program" for medical images as an open-source project.

In summary, I developed deep learning-based software for the anonymization of MR images that distorts the eyes, nose, ears and mouth to prevent facial identification of the subject in reconstructed 3D images. It could be used to share medical big data for secondary research while making both data providers and recipients compliant with the relevant privacy regulations.

This study was summited in the Journal of Medical Internet Research, and contains advanced content.

Contents

Abbreviations

2D: two-dimensional

3D: three-dimensional

ADNI: Alzheimer's Disease Neuroimaging Initiative

AI: Artificial Intelligence

DICOM: Digital Imaging and Communications in Medicine

FOV: field of view

GDPR: General Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

MPRAGE: Magnetization Prepared RApid Gradient Echo

MR: magnetic resonance

MRI: magnetic resonance imaging

NIFTI: Neuroimaging Informatics Technology Initiative

OASIS: Open Access Series of Imaging Studies

List of figures

List of tables

Introduction

It is becoming important to handle and share big data in the healthcare field, and accordingly, there is a big trend to share and protect individual patient data for secondary research [1-3]. To utilize big data, data anonymization is necessary so as not to violate laws for personal privacy such as those stipulated by the Health Insurance Portability and Accountability Act (HIPAA) in the United States and General Data Protection Regulation (GDPR) in Europe (Table 1) [4,5]. There is a trade-off between data usability and privacy protection. Nevertheless, sufficient administrative and technical measures for previously collected information in accordance with personal information protection regulations are necessary when using the information secondarily without consent.

High-resolution magnetic resonance (MR) images of the head risk exposing a subject's face, which can be regarded at the level of photography by facial reconstruction [6]. According to HIPAA's privacy rules, full-face photographic images and any comparable images are considered to be protected health information (Table 1). Budin et al [7] tested human observer recognition of 3-dimensional (3D)-rendered MR images and reported that the likelihood of correctly matching a 3D-rendered face image with a portrait of that person is higher than random guessing. Additionally, anyone can reproduce the 3D facial image from head MR images through 3D volume rendering using freeware. Therefore, it is necessary to anonymize medical images that include the face.

Facial image anonymization is not fully conducted in public medical image repositories, while some public databases even provide the original images. For example, the Alzheimer's Disease Neuroimaging Initiative (ADNI) [8] and Open Access Series of Imaging Studies (OASIS) [9] usually anonymize only metadata, while the original MR images are shared in a nonanonymized form. Anonymizing only the metadata from the medical image is not sufficient to prevent identification from the remaining medical images after removing the metadata, and existing anonymizing software is rarely used to prevent the possibility of recognition due to concerns over the deterioration of the brain image quality [10].

Previous approaches to anonymizing faces in medical images usually remove the entire facial

region using a voxel classifier and mask the brain to preserve the brain image using a skull stripping technique or a convex hull [11,12]. However, since using a voxel classifier and skull stripping can be affected by variation in the characteristics of the MR images, they can produce unexpected results from heterogeneous MR image data [13]. In addition, the solution of cutting off the face has the limitation of information loss concerning the eye orbits, nasal cavity, and other underlying structures [6]. In another technique, the Human Connectome Project (HCP) HCP [14], a public repository of MRI images, conducted distorting by modifying a certain thickness of the facial surface [13]. In this study, the Deface program distorted the ears in addition to the face surface, with options to blur the eyes, the nose, ears, and mouth separately, as may be required when conducting secondary research. The images with eyes, nose, ears, and mouth anonymized were verified by applying a face recognition tool. Furthermore, while previous studies have applied algorithms to process single MRI datasets, our Deface program was tested on 2 different MRI datasets to improve compatibility.

The aim of this study was to develop software that can selectively distort the major facial features (eyes, nose, ears, and mouth) which are the main factors for identifying a face, and make a robust anonymization algorithm that can be used on various MR images. In addition, image pixels other than the major facial features are preserved as original, so that there is no obstacle to secondary research.

Materials and Methods

Defacing Process Overview

Figure 1 schematically illustrates our Deface program development process (Figure1A) and an application example (Figure1B). We created a deep-learning model that learns the labels of the eyes, nose, ears, and mouth. The training set consisted of 3D cranial MR images and manually marked regions corresponding to each MR image. We implemented data augmentation to increase the diversity of the training data. The deep learning model was developed based on a 3D CNN. The trained model called a "facial feature detector" can detect the eyes, nose, ears, and mouth in a 3D MR image. After the regions of the facial features have been obtained from a nonanonymous 3D MR image through the facial feature detector, the regions are anonymized according to each characteristic.

Image Acquisition

The Neuroimaging Informatics Technology Initiative (NIFTI) and Digital Imaging and Communications in Medicine (DICOM) formats of MR imaging (MRI) files were collected from the ADNI database (MPRAGE scans; voxel size: 1.0 x 1.0 x 1.2 mm; inplane resolution: 1.0 x 1.0 mm2; interslice spacing: 1.2 mm; field of view [FOV]: 240 x 256 x 160 mm). A total of 240 NIFTI format files were used in the creation of the deep-learning model: 144, 48, and 48 for the training, validation, and test sets, respectively.

Other NIFTI format MRI files were collected from the OASIS-3 database for use as the external test set. The 100 MR images differed in orientation, resolution, and intensity from those in the ADNI data (MPRAGE scans; voxel size: 1.0 x 1.0 x 1.0 mm; FOV: 176 x 256 x 256 mm).

Labeling

In general, supervised learning requires pairs consisting of the input object and the desired output value. In this study, the input object is a 3D cranial MR image and the output values are regions containing the eyes, nose, ears and mouth (the facial features). We manually drew labels that were the same as the desired output values in all of the ADNI and 20 OASIS-3 images using the AFNI program [15]. In Figure 1A, the manually drawn labels show the eyes (red) and nose (green), which

are marked as spherical shapes at the corresponding positions, and the ears (blue), which are marked as the auricle regions. The mouth (not shown in the figure) was marked by covering the surface with a certain thickness, and it did not overlap with the mark on the nose. Each center point of the eyes and nose area was labeled in the form of a sphere. Since ears have different sizes and shapes for each person, only the auricle of the ear was segmented and labeled.

Data Augmentation

Three image augmentations were performed per 1 image in the training set. The augmented images were randomly transformed and then used for model training. As a result, 576 images per epoch were trained. Data augmentation was performed by filtering Gaussian noise, rotating from -15° to +15° around each axis in the image, randomly flipping each axis, randomly transposing between the axes, shifting each axis from 0 to 0.10, shearing each axis from 0 to 0.20, and resizing the image from 0.90 to 1.10 times the original size. After executing 1 image augmentation per original image, the validation set was validated for a total of 96 images per epoch.

The Deep Learning Algorithm

The deep learning model was trained with the manually labeled data. We created a deep learning model that can generate labels similar to manually drawn labels on the regions of the eyes, nose, and ears from cranial MR image input. The basic structure of our deep-learning model is attention-gated U-net [16]. The detailed structure of our model can be found in Figure 2.

Metric and Loss Function

In machine learning, the "loss" or "error" variable is set to achieve the goals through the training of the model. In addition, the "metric" variable indicates how much we have achieved the goals through the model training. A machine learning model has metrics to indicate the achievement rate and is trained to reduce loss.

In this study, the metric to determine whether the model can make labels similar to the manually drawn labels is the Dice coefficient, which is double the area of overlap divided by the total number of pixels or voxels in both images: it returns 1 if the predicted regions of the model exactly match the correct answers from the labels and 0 if the regions do not overlap. When the region of the

label is Y and the region predicted by the trained model is X, the Dice coefficient can be represented by

$$\frac{2|X \cap Y|}{|X|+|Y|} .$$

This can also be expressed as

$$\frac{2TP}{2TP+FP+FN} ,$$

where TP is the number of true positives, FP is the number of false positives, and FN is the number of false negatives.

The loss function in our model was (1 – the Dice coefficient + 0.1 × categorical cross-entropy). Categorical cross-entropy is the loss function mainly used in multiclass classification, and it induces our model to learn to distinguish whether a specific pixel is from the eye, nose, ear, or another area. This model computes the loss function between the correct answer labels and the predictive labels and is trained in the direction of loss reduction (toward zero).

The model calculated Dice coefficients for 96 images in the validation set for each epoch. After 5 epochs at the highest metric score, learning was stopped when there was no further improvement.

Image Processing

Here, we describe the process of image anonymization based on the output of the facial feature detector. The deep learning model was trained by identifying eyes, nose, ears, and mouth (6 regions), after which the program proceeded with the image anonymization process.

Identification of the eyes, nose, ears and mouth was automatically conducted on different images according to each feature by the deep learning algorithm. The detection region for the eyes is a spherical area covering the eyeball and the skin around the eye. The process of anonymizing the surface of the eye consists of 2 steps. First, based on the detection regions for the eyes, 2 boxes

capable of covering the periocular area (the skin around the eyes) are formed. Second, the contour of the face surface was obtained within the range of the boxes, and a range of ±2 voxels along each axis from that surface was modified to the same intensity value. The nose was processed by removing the image and setting the intensity of the voxels to 0 in the area where the binding box for the detected region was doubled to each side. The detection region for the ears is the protruding part called the auricle. For the anonymization of the ears, random values were assigned to each voxel of the detection regions of the ears, and those values were generated in the noise range of the air in the MR image. The marked area of the mouth surface is converted into pixels of constant brightness. If the user wants to preserve the nose image, the de-identification of the mouth takes place outside the scope of the nose.

In the case of the medical images in DICOM format, it is necessary to anonymize the personal information in the header, and so we carried this out on the 20 DICOM file headers using the Deface program (the DICOM headers are listed in Table 2). The list was selected based on the HIPAA safe harbor provision [17].

Results

In the 20th epoch, the average Dice coefficient of the validation set was the highest at 0.857. In the 25th epoch, the training of the model was stopped because the Dice score of the validation set did not improve. The average Dice score of 576 images trained over 20 epochs was 0.832 The average Dice scores using the test sets comprising 48 ADNI and 20 OASIS-3 images were 0.866 and 0.819, respectively. The Deface program was applied to the ADNI data, but anonymization was performed on the OASIS-3 data without any additional manipulation.

Figure 1B shows the process of distorting a sample nonanonymized cranial MR image. Three axial views of the cross-sectional MR image were obtained from a representative image in the ADNI test set. The first is the nonanonymized cranial MR image, the second is an MR image with the detection regions as output for the facial feature detector, and the third is the final anonymized image based on the detection regions. The image was distorted according to the characteristics of each facial feature. The 3D box space containing the entire volume of the nose was removed. The eyes and the mouth were covered with similar brightness intensity on the surface. For the ears, the detection regions were replaced by space with noise.

We applied the Deface program to 48 ADNI subjects and 100 OASIS-3 subjects as the test sets, and then confirmed the accuracy of distorting the facial features in the 3D reconstructions of the face (Figure 3 shows the 3D volume-rendered images). Since face reconstruction is in violation of the OASIS data use terms, OASIS data were not included in the figure. A sample image was selected from the ADNI test sets, and we compared the before and after anonymization. As shown in Figure 3, the facial features clearly identifiable in the 3D images beforehand are distorted after processing: The auricle and nose have disappeared, and the eyes and the mouth appear blurry.

The Deface program was used to validate the de-identification performance by Microsoft Azure's facial recognition AI service (Face detection_01 model) [18]. We found that all 48 reconstructed face images from the ADNI test set were de-identified. Although 46 unmodified images were recognized as faces and location information of face landmarks was derived, the faces in all 48 defaced images were not recognized. The other 2 unmodified images failed the face recognition

process because they were noisy or parts of the face were cropped. The result of the face detection service for 1 representative image of the ADNI test set can be found in Figure 4.

We have produced software that can be used conveniently in client environment based on this Deface program. Figure 5 shows a screen shot of user interface of the Deface software. DICOM and NIFTY format can be selected from the file type, and the program loads the corresponding format files under the target folder path. A prefix to identify newly created defaced files can be attached. Users can run the program by selecting the right part of the eyes, nose, mouth and ears from the check box. The processing time depended on computer's specifications. Since it is based on deep learning computation, the better the GPU performance, the faster the computation. When testing with the RTX 2080ti, it takes 2 seconds per person and about 30 seconds for the CPU. The demo version of this program can be easily experienced through web browser, and the web address runs on the internal network of Asan medical center.

Discussion

In this study, we developed a program that can recognize the eyes, nose, ears, and mouth in MR images by applying artificial intelligence, after which they were blurred. We implemented the facial feature detector based on the 3D U-net deep-learning model to automatically detect the eyes, nose, ears, and mouth. The reason for the development of this anonymization program is that 3D facial reconstruction of high-resolution MRI can show an individual's similarity to a facial photograph [6,7], which contravenes the rules for protecting personal information required by regulating bodies such as HIPAA. Anonymization is required for the sharing of medical image data so as not to infringe on the personal information rules. However, distorting images is disadvantageous for secondary research due to the loss of information, but too little distorting leads to the possibility of recognition [10]. We attempted to anonymize the face while minimizing the loss of information by modifying only the surface of the eyes, nose, and ears in cranial MR images. In addition, in the case of the DICOM format, a function to remove text including personal information that can be obtained from the header was added. We released the source code to GitHub [19].

Figure 1A shows the process of developing the facial feature detector. The cranial MR images and manually marked facial features (eyes, nose, ears and mouth) were used as the training set. We drew different labels for each facial feature for the manually drawn labels. Although the eyes and nose can be specified in a range of only the central location information, the shape of the ear varies relatively widely among people. Furthermore, because the ears are adjacent to the brain, images of the brain can be obscured during the image distortion. Therefore, only the segmented regions of the auricle were used as labels so that the program did not select regions other than the ear.

Although the training data for the deep learning model comprised 144 images from ADNI, we introduced data augmentation to achieve robust performance in other MRI standards (Figure 1A). The training set was augmented via various techniques so that the facial feature detector could show robust performance even with unknown data. We evaluated OASIS-3 data in which the adjustment, orientation, FOV, resolution, and intensity histograms were completely different from the ADNI data in the training set. We confirmed that the facial features were distorted in 100 OASIS-3 images by the MRI viewer. Labels were manually drawn on 20 OASIS-3 images, and our facial feature detector worked well with an average Dice coefficient of 0.819. This has the potential to

assist in the construction of anonymous big data with different MRI standards collected from multiple institutions. In addition, we confirmed by training 24 CT images from Asan Medical Center that the same anonymization operation is possible if the face of the CT image is high enough to be recognized.

We applied different processes to blur each facial feature location. The eyes are close to the frontal lobe, so they were distorted only along the surface. The intensity of the pixels was converted to a value similar to the surface of the skin to make it appear on the surface when 3D rendering. Since the nose is usually the most protuberant part of the face, the area that covers the entire range of the nose was deleted to make it impossible to infer the original shape of the nose. The 3D box space containing the entire volume of the nose was removed to prevent recognition via the nose shape. This 3D box is used as an area where images are preserved when users want to preserve the nose. The ears were only segmented by the facial feature detector, so only the corresponding regions were distorted to preserve the brain image. If regions such as the shape of the ears are simply removed, the shape of the ears may be revealed by the noise from air in the MR image. We reduced the possibility of recognition by replacing the ear regions with generated random values within the air noise range of the input MR image. Finally, the surface of the mouth was covered with pixels of similar brightness to the skin.

3D facial reconstruction of high-resolution MRI can be generated by a freeware MRI viewer [20]. Moreover, the faces of patients in MR images from publicly available data can be revealed (Figure 3). As the OASIS-3 images are smoother than the ADNI images, they can be reconstructed with a clearer face image in the case of high-resolution MRI. However, we showed that the face could be distorted in the 3D rendered image after applying our Deface program. Since the image was preserved except for the user-designated facial features, researchers can obtain the necessary information from MRI images without revealing the patient's identity. Furthermore, while previous studies have applied algorithms to process single MRI datasets, our Deface program was tested on two different MRI datasets to improve compatibility.

In summary, Patients' faces can be reconstructed from high-resolution cranial MR images at the photograph level; so, there is a risk of infringing the personal information rules prescribed by HIPAA and GDPR when sharing data. Hence, we suggested a method to perceive the facial features in MR

images via deep learning technology to specifically blur certain facial features. Users can create anonymization regions that blur the desired parts of the patient's face (eyes, nose, ears or mouth), which helps provide data for secondary research without violating relevant personal information regulations.

Regulation	Details
HIPAA Privacy Rule [21]	According to the "Safe Harbor Privacy Rule 164.514(b)(2)", 18 specific identifiers are removed from the records or photographs. The information is then deemed "deidentified" and no longer considered identifiable. Deidentified health information created after this method is no longer protected by the Privacy Rule. Eighteen identifiers to be removed for deidentification. 1. Name 2. All geographic subdivisions smaller than a state 3. All elements of data (except year) for dates directly related to the individual (date of birth, date of admission, date of discharge, date of death). Also, all ages over 89 years or elements of dates indicative of such age. 4. Telephone numbers 5. Fax numbers 6. Email addresses 7. Social security numbers 8. Medical record numbers 9. Health plan beneficiary numbers 10. Account numbers 11. Certificate/license numbers 12. Vehicle identification or serial numbers including license plate numbers 13. Device identification or serial numbers 14. Web Universal Resource Locators (URLs) 15. Internet Protocol (IP) addresses 16. Biometric identifiers including finger and voice prints 17. Full-face photographs and any comparable images 18. Any other unique identifying number, characteristic or code
GDPR [22]	The GDPR makes critical differences between personal data, pseudonymized data, and anonymized data. Facial images are categorized as biometric data under the GDPR and need to be protected. Nevertheless, the further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is to

	be carried out when the controller has assessed the feasibility to fulfil th ose purposes by processing data which do not permit or no longer per mit the identification of data subjects, provided that appropriate safegua rds exist (such as, for instance, pseudonymisation of the data), according to the Article 89. Otherwise, the GDPR Recital 26 stipulates that anony mous data is no longer applied to the GRPR.

Table 1. Information Protection Regulations

The table shows the information protection regulations defined by HIPAA and GDPR.

Tag	Attribute
(0008, 0012)	Instance Creation Date
(0008, 0013)	Instance Creation Time
(0008, 0020)	Study Date
(0008, 0030)	Study Time
(0008, 0021)	Series Date
(0008, 0031)	Series Time
(0008, 0022)	Acquisition Date
(0008, 0032)	Acquisition Time
(0008, 0023)	Content Date
(0008, 0033)	Content Time
(0008, 0080)	Institution Name
(0008, 0081)	Institution Address
(0008, 0090)	Referring Physician's Name
(0008, 1050)	Performing Physician's Name Attribute
(0008, 1070)	Operators' Name
(0010, 0010)	Patient's Name
(0010, 0020)	Patient ID
(0010, 0030)	Patient's Birth Date
(0010, 0040)	Patient's Sex
(0010, 1010)	Patient's Age

Table 2. DICOM header with personal information

The DICOM standard includes header information, some of which may reveal personal information. In this study, the Deface program anonymized the DICOM image by deleting the 20 headers information.

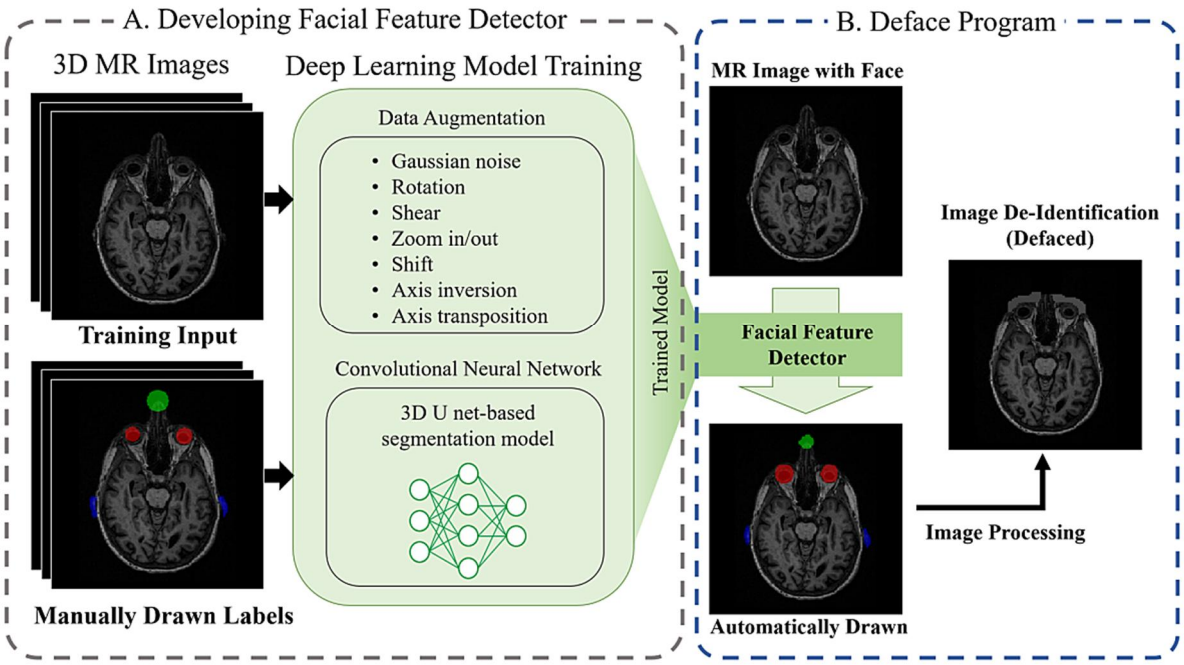

Figure 1. Overview of development process and application example of deface program

(A) The process of developing the facial feature detector. 3D cranial MR images and manually marked facial features (the eyes, nose, ears, and mouth) were used as the training set. The deep-learning model was trained to automatically draw labels on the facial features in MR images. The trained deep-learning model (the facial feature detector) can detect the eyes, nose, and ears in 3D cranial MR images. (B) The process of distorting the facial features in nonanonymized cranial MR images. When the regions of the eyes, nose, and ears are specified by the facial feature detector, the program anonymizes the image by distorting the detected regions.

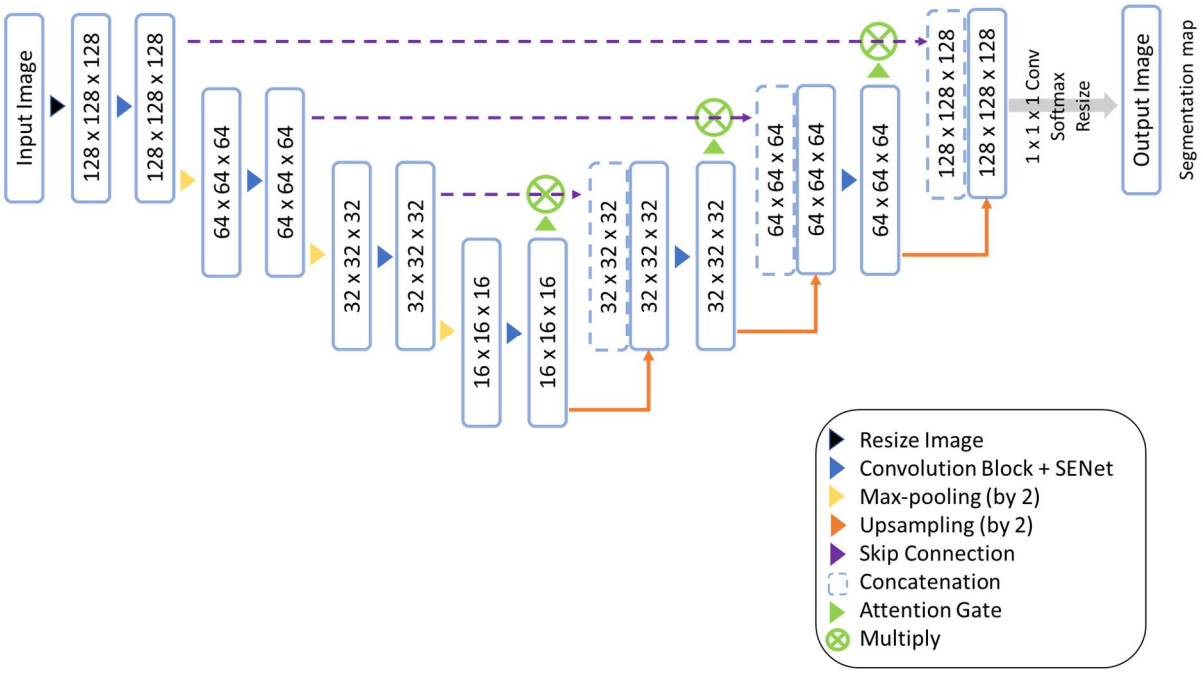

Figure 2. The Deep learning model structure

Figure 2 shows the structure of deep learning model for facial feature detector in this study. It is based on U-net structure with attention gate, and input image is resized because the memory capacity occupied by the 3-dimensional Magnetic Resonance image is large. The Python code for this model structure has released on GitHub [19].

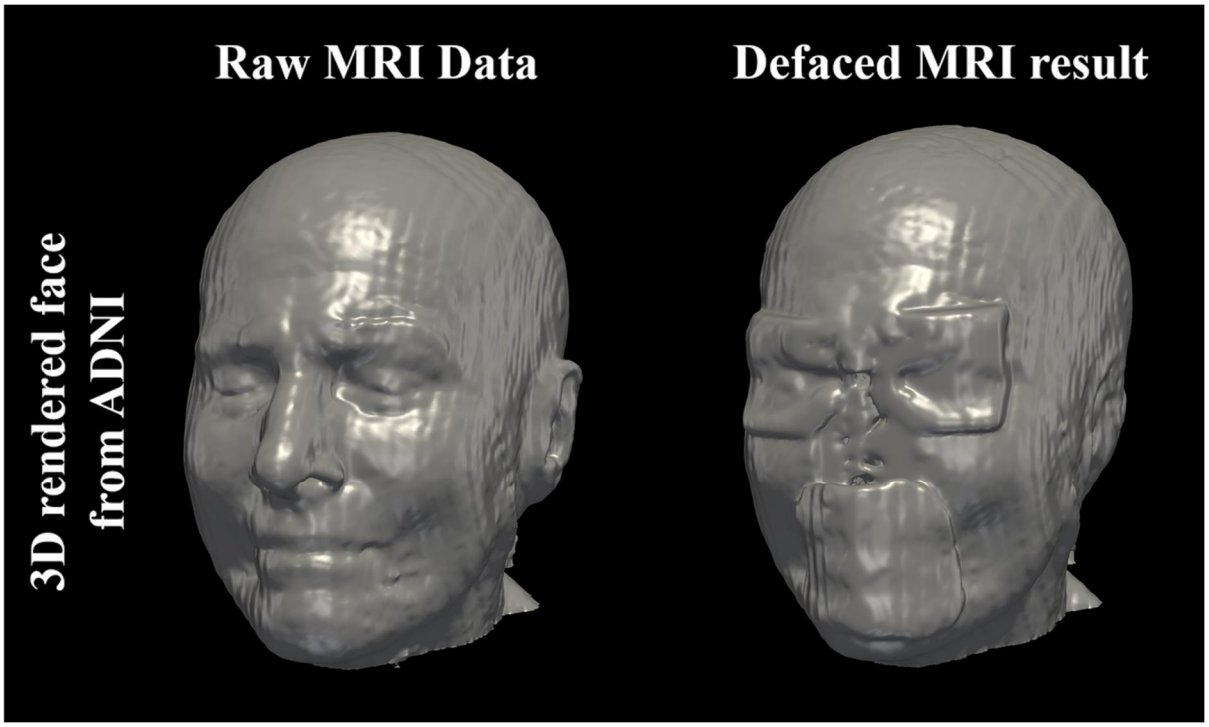

Figure 3. The 3D volume rendering of MR images

Left and right: the rendered MR images of the unmodified and defaced images from the ADNI test set, respectively.

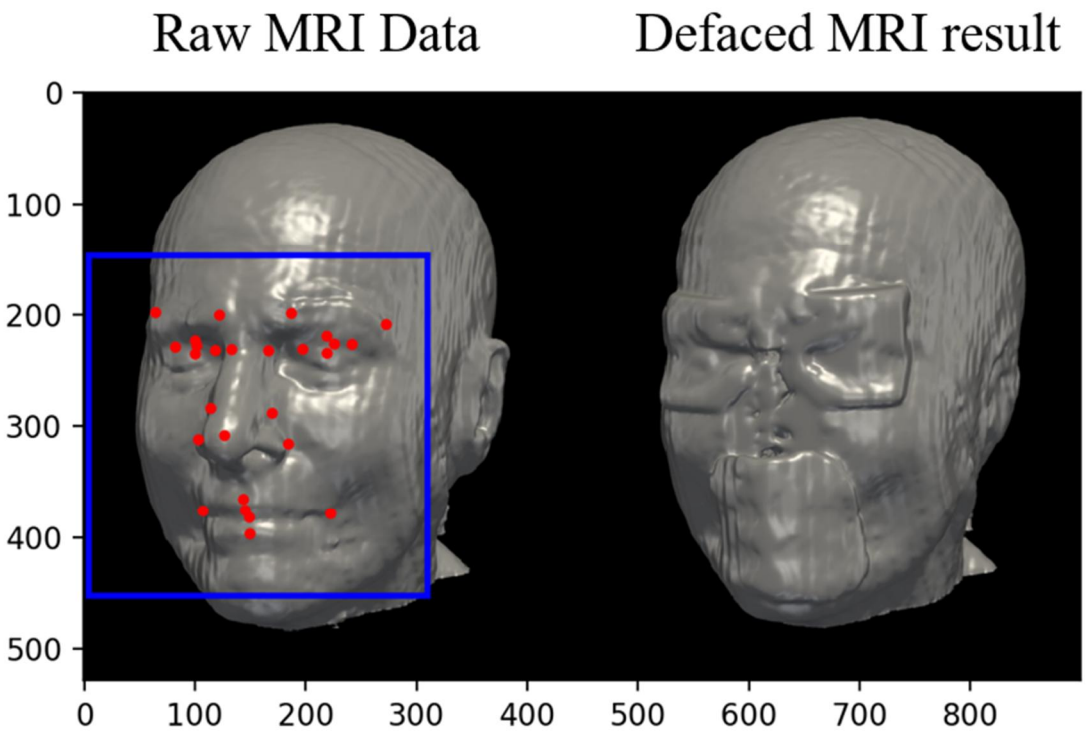

Figure 4. Face recognition test

This is the result of applying the 3D rendered MR images of the unmodified and defaced images in the ADNI test set to the Microsoft Azure's face recognition AI service. In the unmodified image, the face was recognized and the coordinates of the main facial features were derived, but the defaced image was not.

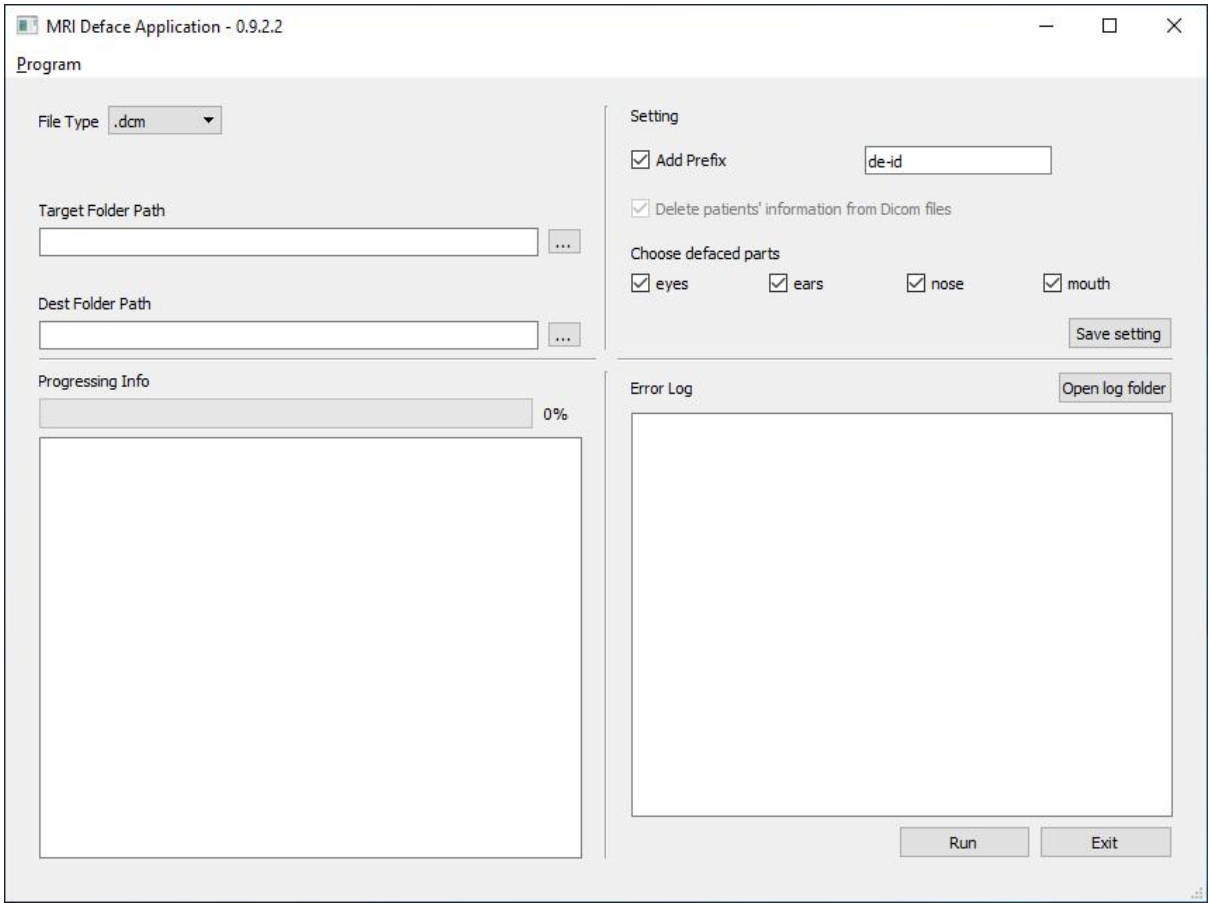

Figure 5. User interface of deface software

This is the user interface screen of deface software. DICOM and NIFTY format can be selected from the file type, and the program loads the corresponding format files under the target folder path. A prefix to identify newly created defaced files can be attached. Users can run the program by selecting the right part of the eyes, nose, mouth and ears from the check box.

References

1. Raghupathi W, Raghupathi V. Big data analytics in healthcare: promise and potential. Health Inf Sci Syst. 2014;2(1):3. PMID: 25825667 doi: 10.1186/2047-2501-2-3

2. Vallance P, Chalmers I. Secure use of individual patient data from clinical trials. Lancet. 2013 Sep 28;382(9898):1073-4. PMID: 24075034 doi: 10.1016/S0140-6736(13)62001-2

3. El Emam K, Rodgers S, Malin B. Anonymising and sharing individual patient data. BMJ. 2015 Mar 20;350:h1139. PMID: 25794882 doi: 10.1136/bmj.h1139

4. Chevrier R, Foufi V, Gaudet-Blavignac C, Robert A, Lovis C. Use and understanding of anonymization and de-identification in the biomedical literature: scoping review. J Med Internet Res. 2019 May 31;21(5):e13484. PMID: 31152528 doi: 10.2196/13484

5. Kayaalp M. Patient privacy in the era of big data. Balkan Med J. 2018 Jan 20;35(1):8-17. PMID: 28903886 doi: 10.4274/balkanmedj.2017.0966

6. Prior FW, Brunsden B, Hildebolt C, Nolan TS, Pringle M, Vaishnavi SN, et al. Facial recognition from volume-rendered magnetic resonance imaging data. IEEE Trans Inf Technol Biomed. 2009 Jan;13(1):5-9. PMID: 19129018 doi: 10.1109/TITB.2008.2003335

7. Budin F, Zeng D, Ghosh A, Bullitt E. Preventing facial recognition when rendering MR images of the head in three dimensions. Med Image Anal. 2008 Jun;12(3):229-39. PMID: 18069044 doi: 10.1016/j.media.2007.10.008

8. ADNI. Alzheimer's disease neuroimaging initiative [cited 2019 June 5]; Available from: http://adni.loni.usc.edu

9. OASIS. Open access series of imaging studies. [cited 2019 Aug 20]; Available from: https://www.oasis-brains.org/.

10. Schwarz CG, Kremers WK, Therneau TM, Sharp RR, Gunter JL, Vemuri P, et al. Identification of anonymous MRI research participants with face-recognition software. N Engl J Med. 2019 Oct 24;381(17):1684-6. PMID: 31644852 doi: 10.1056/NEJMc1908881

11. Schimke N, Kuehler M, Hale J. Preserving privacy in structural neuroimages. In: Li Y, editor. Data and Applications Security and Privacy XXV. Berlin, Heidelberg: Springer Berlin Heidelberg; 2011. p. 301-8.

12. Bischoff-Grethe A, Ozyurt IB, Busa E, Quinn BT, Fennema-Notestine C, Clark CP, et al. A technique for the deidentification of structural brain MR images. Hum Brain Mapp. 2007

Sep;28(9):892-903. PMID: 17295313 doi: 10.1002/hbm.20312

13. Milchenko M, Marcus D. Obscuring surface anatomy in volumetric imaging data. Neuroinform. 2013 Jan;11(1):65-75. PMID: 22968671 doi: 10.1007/s12021-012-9160-3

14. Van Essen DC, Smith SM, Barch DM, Behrens TE, Yacoub E, Ugurbil K, et al. The WU-Minn Human Connectome Project: an overview. NeuroImage. 2013 Oct 15;80:62-79. PMID: 23684880 doi: 10.1016/j.neuroimage.2013.05.041

15. Cox RW. AFNI: software for analysis and visualization of functional magnetic resonance neuroimages. Comput Biomed Res. 1996 Jun;29(3):162-73. PMID: 8812068 doi: 10.1006/cbmr.1996.0014

16. Schlemper J, Oktay O, Schaap M, Heinrich M, Kainz B, Glocker B, et al. Attention gated networks: Learning to leverage salient regions in medical images. Med Image Anal. 2019 Apr;53:197-207. PMID: 30802813 doi: 10.1016/j.media.2019.01.012

17. e-CFR. Electronic code of federal regulations. [cited 2020 May 7]; Available from: https://www.ecfr.gov/cgi-bin/text-idx?SID=20e0360351a51dd55ee6e80cc9aae47c&node=se45.1.164_1514&rgn=div8.

18. Microsoft Azure. Facial recognition AI service [cited 2020 Aug 27]; Available from: https://azure.microsoft.com/en-us/services/cognitive-services/face/#demo

19. Jeong Y. De-facer: de-identifier reconstructable facial information in Medical image (CT, MRI). [cited 2020 June 26]; Available from: https://github.com/yeonuk-Jeong/Defacer.

20. Debus C, Floca R, Ingrisch M, Kompan I, Maier-Hein K, Abdollahi A, et al. MITK-ModelFit: a generic open-source framework for model fits and their exploration in medical imaging - design, implementation and application on the example of DCE-MRI. BMC Bioinformatics. 2019 Jan 16;20(1):31. PMID: 30651067 doi: 10.1186/s12859-018-2588-1

21. The HIPAA Privacy Rule. US Department of Health and Human Services website. [cited 2020 Sep 1]; Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

22. The General Data Protection Regulation (GDPR). The European Parliament and of the Council. [cited 2020 Sep 1]; Available from: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

23. Jeong YU, Yoo S, Kim YH, Shim WH. De-Identification of Facial Features in Magnetic Resonance Images: Software Development Using Deep Learning Technology. J Med Internet Res. 2020 Nov.; PMID: 33208302 doi: 10.2196/22739

국문요약

헬스케어 분야에서 빅데이터가 갈수록 주목받고 응용 연구가 다양해짐에 따라, 동의 없는 2차적 정보 이용은 개인 정보 보호 규정에 다른 충분한 관리와 기술적 조치가 필요하다. 의료 데이터 중 두경부를 촬영하는 고해상도 의료영상은 2차원의 연속적 이미지를 3 차원 재구성하여 환자나 피험자의 안면을 사진에 준하는 수준으로 재현할 수 있어서 개인정보 유출의 위험을 내포하고 있다. 개인정보 보호를 위한 법률 중 미국의 HIPAA는 얼굴 전체의 사진을 보호해야할 개인정보로 규정하고 있고, 유럽의 GDPR은 안면의 이미지를 생체 인증 데이터로 분류하고 특별한 제한을 두도록 규정한다.

특히 두경부 MRI에서 안면 노출은 개개인을 식별 가능한 수준이다. 고해상도 T1 두경부 MRI 이미지를 이용해 피험자의 안면을 사진 수준으로 재구성 가능하다는 보고와, 이것을 피험자의 인물사진과 일치시키는 실험을 하여 유의미하게 개개인을 구분해낼 수 있다는 발표가 있었다. 연속적인 2차원 MRI영상을 이용해 3차원 얼굴을 재구성하는 것은 무료 소프트웨어로 누구나 가능하기 때문에, 2차적 연구를 위한 빅데이터를 구축할 때에는 법적, 기술적 조치가 필요하다. 그럼에도 불구하고 현재 공개된 데이터베이스들에서 안면이 드러난 원본 MRI 영상이 공유되고 있다. 예를 들어, ADNI와 OASIS에서는 두경부 영상에서 안면의 이미지에 비식별화 조치를 별도로 하지 않은 영상을 얻을 수 있다.

의료 영상에서 안면을 비식별화 하려는 작업들이 발표된 적 있으나 대부분 뇌의 앞부분 데이터 전체를 삭제하여 얼굴을 없애거나, 안면 전체에 두껍게 이미지 처리를 흐리게 하였다. 본 연구에서는 의료 영상의 2차적 활용도를 더욱 높이기 위해서 안면의 주요 식별부위인 눈, 코, 입, 귀를 따로 비식별화 할 수 있는 기능을 두었다. 예를 들어, 인후두를 연구하고 싶은 연구자는 이전의 안면 전체를 삭제한 데이터를 활용할 수 없으나 본 연구의 프로그램을 활용하여 눈과 귀만 비식별화 한다면 익명화 된 데이터를 공유 받아 연구가 가능해지는 장점이 있다.

본 연구에서는 고해상도 의료영상인 T1 MRI에서 안면의 주요 식별부위인 눈, 코, 입, 귀를 따로 비식별화 처리할 수 있는 소프트웨어를 개발하고, 다양한 MRI 영상에서 검증하였다. 또한 CT 데이터를 추가로 학습하여 CT 영상에서도 동일한 작업이 수행될 수 있음을 확인하였다. 이러한 비식별화 작업은 의료 빅데이터의 구축에서 개인정보를 보호하고 개인정보보호 관련법에 저촉되지 않게 함이며, 데이터의 변형을 최소화하여 다양한 2차적 연구에 도움을 줄 수 있다.

이 연구는 journal of Medical Internet Research에 발표하였으며 이후 발전된 내용을 포함하고 있다.