UNIVERSITÄT AUGSBURG
Universitätsbibliothek

OPEN ACCESS
OPUS AUGSBURG

# Towards privacy-preserving medical image processing using homomorphic encryption [Abstract]

**Michael Schlottke-Lakemper, Max Grübmeyer, Arseniy Kholod, Thomas Wendler**

**Angaben zur Veröffentlichung / Publication details:**

Schlottke-Lakemper, Michael, Max Grübmeyer, Arseniy Kholod, and Thomas Wendler. 2026. "Towards privacy-preserving medical image processing using homomorphic encryption [Abstract]." *Biomedical Engineering / Biomedizinische Technik* 71 (s1). https://doi.org/10.1515/bmt-2026-1001.

**Nutzungsbedingungen / Terms of use:**

**CC BY 4.0**

*Dieses Dokument wird unter folgenden Bedingungen zur Verfügung gestellt: / This document is made available under these conditions:*
***CC-BY 4.0: Creative Commons: Namensnennung***
*Weitere Informationen finden Sie unter: / For more information see:*
*https://creativecommons.org/licenses/by/4.0/deed.de*

# Towards privacy-preserving medical image processing using homomorphic encryption

Michael Schlottke-Lakemper[12,*], Max Grübmeyer[12], Arseniy Kholod[12], Thomas Wendler[23456,†]

[1] High-Performance Scientific Computing, Institute of Mathematics, University of Augsburg, Germany
[2] Centre for Advanced Analytics and Predictive Sciences, University of Augsburg, Germany
[3] Department of Diagnostic and Interventional Radiology and Neuroradiology, University Hospital Augsburg, Germany
[4] Digital Medicine, University Hospital Augsburg, Germany
[5] Computer-Aided Medical Procedures, Technical University Munich, Germany
[6] Bavarian Center for Cancer Research (BZKF) Augsburg, Germany

[*] michael.schlottke-lakemper@uni-a.de, [†] thomas.wendler@med.uni-augsburg.de

## Introduction

The use of cloud-based services for medical image processing is limited by strict data protection requirements (e.g., HIPAA, GDPR). This is particularly critical for volumetric data such as 3D head CT scans, where anatomical structures can enable reconstruction of facial geometry and thus potential re-identification, even when metadata are removed. Fully homomorphic encryption (FHE) offers a promising approach by enabling computations directly on encrypted data.

## Methods

We present a framework for processing multidimensional medical imaging data using the Cheon–Kim–Kim–Song (CKKS) scheme. A common characteristic of FHE is that it natively supports only one-dimensional vector operations, which complicates the implementation of algorithms for inherently multidimensional data such as 2D/3D CT or multi-parametric MRI. To address this, we introduce a simple, high-level multidimensional array abstraction built on top of ciphertext vectors, together with corresponding shift operations, enabling the direct formulation of stencil- and convolution-based algorithms.

## Results

As a demonstrator, we implement Laplacian of Gaussian (LoG) filtering for 2D and 3D head CT data using different kernel sizes. The results show that the encrypted computations reproduce the unencrypted "plaintext" results with high numerical accuracy, while remaining straightforward to implement using the proposed abstraction. However, the computational cost remains significant: while plaintext implementations run in seconds, encrypted 3D computations can require more than an hour for large kernels on a single CPU core. We further analyze performance characteristics and discuss optimization strategies.

## Conclusion

We demonstrate the feasibility of using FHE for privacy-preserving medical image processing on realistic 3D data, and that multidimensional array abstractions remove a key barrier for implementing such algorithms. At the same time, the results highlight current challenges in performance and indicate the limitations in handling more complex, non-linear operations, which remain important topics for future work.

Open Access. © 2026 The Author(s), published by De Gruyter. This work is licensed under the Creative Commons Attribution 4.0 International License.