HOMOMORPHIC ENCRYPTION FOR DEPENDABLE CLOUD IMAGE FILTERING USING COLUMN PERMUTATION OF PIXEL MATRICES

*Dimitra Georgiou (1) *, Melitine Bardi (2), Alireza Mirataei (3), Oleksandr Markovskyi (3)*

(1) Department of Mathematics and Engineering Sciences, Hellenic Army Academy, Vari; (2) Department of Computer Science and Biomedical Informatics, University of Thessaly, Lamia; (3) National Technical University of Ukraine "Igor Sikorsky" Kyiv Polytechnic Institute Kyiv,
(1, 2) Greece, (3) Ukraine

* Corresponding Author, e-mail: dimitrageorgiou@ssl-unipi.gr

Abstract: Cloud-based image filtering provides substantial computational benefits but exposes sensitive image data to security risks when processing is per-formed on remote systems outside the user's control. This paper proposes a homomorphic encryption method for secure arithmetic mean image filtering based on column permutation of pixel matrices. The approach encrypts im-ages by permuting their columns before cloud transmission, delegates the computationally intensive filtering stage to remote systems, and reconstructs the filtered images locally using the inverse permutation. Experimental evaluation shows that the proposed method accelerates image filtering by one to two orders of magnitude, approaching the performance of the fastest additive masking techniques while requiring minimal user-side computation. Furthermore, it provides significantly stronger resistance to statistical reconstruction attacks, making it an efficient and secure solution for dependable cloud-based image filtering.

Key words: homomorphic encryption; cloud image filtering; column permutation; secure image processing; image streams.

1. INTRODUCTION

Advances in information technology stimulate the dynamic expansion of the class of applied tasks, including computer analysis of image streams. A strong impetus for development in this direction was given by the appearance on the market of cheap hardware components of computer vision systems [1]. Accordingly, real-time systems are intensively developed for which the speed of digital image processing is a crucial component of effectiveness.

The need for significant computing resources is inherent in all tasks of computer image processing since they consist of millions of points and further improving their quality results to increase the number of points. Besides, image processing algorithms are continually becoming more complicated. Thus, the trends in the use of computer image analysis in modern information technology require a significant increase in the amount of computing resources, the growth rate of which is significantly ahead of the progress of processor power [2].

The most promising way to accelerate computer image processing is to attract to solve applied problems, almost unlimited computing resources provided by modern cloud technologies. These technologies make it possible to integrate robust computer systems on a global scale and provide access to them to a wide range of users. Also, it is cloud technology that determines the economic efficiency of supercomputers, ensuring their almost full load with the tasks of users from around the world [3].

Today, the biggest obstacle to the widespread exploitation of the benefits of cloud computing for image processing is their vulnerability to unauthorized access. Practically it is a question of processing of images of the user on computer systems which are not under their control, remotely and potentially open to unauthorized access. Existing means of encrypting information allow ensuring the secrecy of images only during their transmission over the Internet, but not in the process of their direct processing on remote computer systems [4]. For most applied tasks of computer image analysis, it is essential to only allow limited access to them by outsiders. Thus, the scientific task of protecting images in the process of their remote processing, including filtering on computer systems not controlled by users, is relevant for the current stage of information technology development.

The main contribution of this paper is a lightweight method for secure remote arithmetic-mean image filtering based on column permutation. The computationally dominant partial-filtering stage is performed remotely, while inverse permutation and final filtering are performed locally. Its novelty lies in adapting column-level permutation to arithmetic-mean filtering, reducing user-side computational overhead while increasing resistance to unauthorized reconstruction.

2. ANALYSIS OF THE PROBLEM OF IMAGE PROTECTION IN THE PROCESS OF REMOTE PROCESSING

This section analyses the problem of secure remote image filtering using established arithmetic-mean filtering formulations and computational models reported in the literature. The equations presented in this section are based on previously published image-processing approaches, as indicated by the corresponding references, and are not claimed as original contributions of this work. They provide the analytical basis for identifying the computational and security requirements addressed by the proposed method in Section 4.

One of the most common types of image processing is arithmetic which means filtering. It allows improving the quality of images by removing pulse noise that occurs during the formation and transmission of images [1]. The essence of this type of processing is to scan the image with a square aperture of odd size with the replacement

of the central element of the current aperture by the value of the arithmetic mean of its points. The image is given matrix P with k rows and h columns of intensity values p_{ij}, $0 < i \le k$, $0 < j \le h$,

$$P = \begin{pmatrix} p_{11} & p_{12} \cdots p_{1h} \\ p_{21} & p_{22} \cdots p_{2h} \\ & .... \\ p_{k1} & p_{k2} \cdots p_{kh} \end{pmatrix}$$

Following the conventional arithmetic-mean filtering formulation presented in [1], each element q_{ij} of the filtered image Q is calculated as follows:

$$\begin{aligned} &\forall i \in \{\frac{a+1}{2}, \frac{a+1}{2}+1, \ldots, k-\frac{a-1}{2}\}, \\ &j \in \{\frac{a+1}{2}, \frac{a+1}{2}+1, \ldots, h-\frac{a-1}{2}\}: \\ &q_{ij} = \frac{1}{a^2} \sum_{x=i-\frac{a-1}{2}}^{i+\frac{a-1}{2}} \sum_{y=j-\frac{a-1}{2}}^{j+\frac{a-1}{2}} p_{xy}. \end{aligned} \tag{1}$$

A direct implementation requires approximately a^2 additions and one division per processed pixel; therefore, its cost increases rapidly with image size and aperture width. The sliding-aperture formulation reduces repeated work by updating adjacent sums and provides the computational basis used in the proposed remote-processing scheme. Based on the conventional filtering procedure described in [1], its computational time can be expressed as:

$$T_0 = k \cdot h \cdot (a^2 \cdot t_a + t_d) \tag{2}$$

where t_a is the execution time of the addition operation, and td is the execution time of the division operation.

For the more efficient arithmetic-mean filtering algorithm based on updating the aperture sums [1], the corresponding processing time T_1 is expressed as:

$$T_1 = k \cdot h \cdot (2 \cdot a \cdot t_a + t_d) \tag{3}$$

For most applications, the problem of filtering images is solved, not for one image, but for a stream of images. Therefore, when using a single processor, the image filtering rate coincides with the values of T_0 or T_1.

As mentioned above, increasing the rate of image stream filtering can be achieved by involving remote computer systems in cloud technology. Since such systems consist of many processors that can perform parallel filtering of several images, the processing rate of their flow is practically determined by the speed of the network communication channel with the cloud [5].

The organization of secure filtering of an image stream with the involvement of remote computer systems, introduces overhead calculations related to the encryption of images before their transfer to the cloud, and the subsequent decryption of the result.

Accordingly, two criteria are considered for evaluating secure remote image processing methods [6–8]: filtering acceleration and resistance to unauthorized image reconstruction. Following the evaluation approach reported in [6–8], the filtering-acceleration coefficient β is adopted in this work as a baseline performance metric and is expressed as follows:

$$\beta = \frac{T}{T_{ed}} \tag{4}$$

The level of image protection is estimated by the computational effort required for unauthorized reconstruction of the original image. Based on these formulations, the authors adopt filtering acceleration and reconstruction resistance as the evaluation criteria used to analyse existing approaches in Section 3 and evaluate the proposed method in Section 5.

3. ANALYSIS OF EXISTING SCHEMES OF REMOTE IMAGE FILTERING

This section analyses previously published secure remote image-filtering schemes according to the computational-efficiency and image-protection criteria defined in Section 2. The methods discussed below originate from the cited literature. The authors' contribution in this section consists in the comparative analysis and in identifying the limitations that motivate the proposed method.

Existing secure remote-filtering schemes mainly use additive masking or spatial permutation. In additive masking, a random mask is combined with the source image before transmission, the cloud filters the protected matrix, and the user removes the filtered mask from the returned result [9–13]. These approaches preserve the linearity required by arithmetic-mean filtering, but they add local preprocessing and postprocessing. Their protection can also weaken when mask statistics or repeated structures reveal information about the underlying image.

More elaborate masking increases resistance to statistical reconstruction by grouping images or selecting mask values through secret parameters [12, 13]. The improvement comes at the cost of additional arithmetic, key management, and local processing. Consequently, the acceleration obtained from cloud resources decreases as the protection mechanism becomes more complex. This trade-off is particularly important for continuous image streams, where the user-side workload must remain substantially smaller than the delegated filtering workload.

Spatial permutation offers a lighter alternative because it changes image organization without changing pixel values. Prior work permuted matrix rows before cloud filtering [14]. However, row permutation does not align naturally with the horizontal sliding operations used by efficient mean-filter implementations and may retain structural dependencies that facilitate reconstruction. The present work instead permutes columns and adapts the remote and local stages so that filtering remains correct after inverse permutation.

Recent studies confirm that privacy-preserving cloud image processing remains an active research area. Homomorphic and fully homomorphic encryption is increasingly used for secure image processing [16–20], while alternative privacy-preserving

techniques seek to balance security and computational efficiency [20, 21]. However, computational complexity, communication overhead, and scalability remain significant challenges, motivating lightweight approaches for secure remote image processing.

In contrast to computationally intensive homomorphic-encryption approaches, the design objective of the proposed method is to provide a lightweight mechanism for secure remote filtering of image streams. The method combines three properties: low-cost user-side protection, compatibility with efficient cloud filtering, and a permutation search space large enough to make exhaustive recovery impractical for realistic image widths. The proposed method uses paired direct and inverse column-permutation tables as secret permutation parameters and delegates the computationally dominant partial-filtering stage to the remote system.

The above analysis identifies a gap between lightweight permutation-based protection and computationally intensive cryptographic approaches. Masking methods introduce additional user-side arithmetic, while homomorphic-encryption approaches may impose considerable computational and communication overhead. Moreover, row-permutation approaches do not directly exploit the structure of efficient arithmetic-mean filtering. The proposed method addresses this gap through column-level permutation combined with distributed partial filtering, reducing user-side computational overhead while increasing resistance to unauthorized reconstruction. Its novelty lies in providing a lightweight construction specifically adapted to secure remote arithmetic-mean image filtering, rather than replacing general-purpose homomorphic-encryption frameworks.

Its main contribution is therefore the use of column-level permutation specifically adapted to arithmetic-mean filtering, enabling most of the filtering workload to be outsourced while keeping the user-side processing overhead low.

4. METHOD OF PROTECTED ARITHMETIC MEAN FILTERING OF IMAGES BASED ON MIXING

Based on the analysis presented in Sections 2 and 3, this section introduces the original secure remote image-filtering method proposed by the authors.

The original image $P$is transformed into the mixed image $G$by column permutation and partially filtered remotely. The resulting matrix $R$is returned to the user, who restores the column order and completes the final filtering phase to obtain Q, as shown in Fig 1.

The proposed method performs image mixing by permuting the columns of the original image matrix P, where:

$$P: P = \{\vartheta_1, \vartheta_2, ..., \vartheta_h\},\ \forall j \notin \{1,2,..., h\} : \vartheta_j = \{p_{1,j},\ p_{2\,j}, ..., p_{kj}\}$$

The column permutation is specified by a direct permutation table T_D, selected by the user, and its corresponding inverse permutation table T_R. Both tables contain $h$entries, where $h$is the number of columns in the image.

As part of the proposed method, the authors define the direct permutation mapping TD as follows:

$$w = TD(v)$$

Correspondingly, the authors define the inverse permutation mapping TR, which, during reverse shuffling, returns the original position v of the column located at position w in the transformed image, as follows:

$$v = TR(TD(v))$$

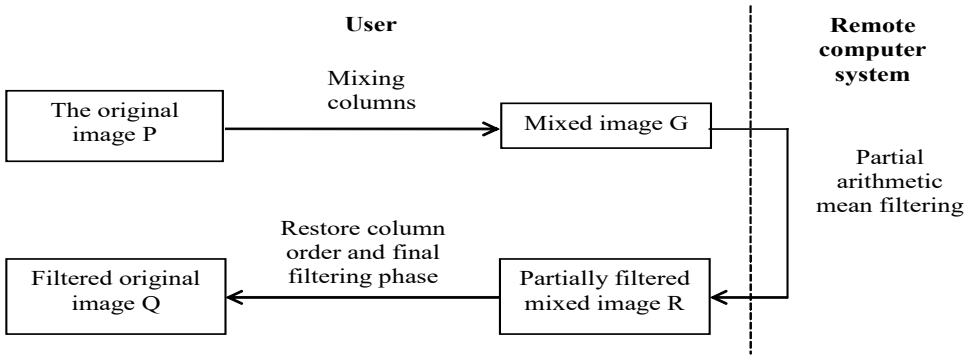


Figure 1. The structure of the execution of the protected arithmetic mean filtering of images in the proposed method

The user pre-generates random T_D *and* T_R table pairs that serve as permutation keys. The proposed secure arithmetic-mean filtering method involving remote computing resources consists of the following steps:

Step (1): Selection of the permutation tables

The user selects a pair of TD and TR tables for direct and reverse image layout.

Step (2): Column permutation of the original image.

The user rearranges the columns $\vartheta_1, \vartheta_2, ..., \vartheta_h$ of the original image matrix (P) according to the direct permutation table TD.

$$G = \begin{pmatrix} g_{11}\ g_{12} \cdots g_{1h} \\ g_{21}\ g_{22} \cdots g_{2h} \\ \cdots \\ g_{k1}\ g_{k2} \cdots g_{kh} \end{pmatrix}$$

As part of the proposed method, the authors formulate the generation of the permuted matrix G as follows:

$$\forall i \in \{1, 2, ..., k\}, j \in \{1, 2, ..., h\} : g_{ij} = p_{i,TD(j)}$$

Step (3): Transmission of the mixed image

The mixed image matrix (G) is transmitted by the user to the remote computer system for processing.

Step (4): Partial arithmetic-mean filtering on the remote system

The remote system performs partial arithmetic-mean filtering of matrix G, producing matrix R. For the proposed method, the authors formulate the partial-filtering operation and the resulting elements of matrix R as follows:

$$R = \begin{pmatrix} r_{11}\ r_{12} \ldots r_{1h} \\ r_{21}\ r_{22} \ldots r_{2h} \\ \ldots. \\ r_{k1}\ r_{k2} \ldots r_{kh} \end{pmatrix}$$

$$\forall i \in \{\frac{a+1}{2}, \frac{a+1}{2}+1, ..., k-\frac{a+1}{2}\},$$

$$j \in \{1, 2, ..., h\} : r_{ij} = \frac{1}{a^2} \sum_{x=i-\frac{a-1}{2}}^{i+\frac{a-1}{2}} g_{i,j}.$$

To ensure the required filtering accuracy, the elements of the matrix R are calculated in floating-point format.

Step (5): Return of the partially filtered image

The matrix R, obtained as a result of partial arithmetic-mean filtering on the remote computer system, is returned to the user.

Step (6): Reconstruction and completion of the filtering process

Using the received matrix R, the user reconstructs the filtered image Q by applying the inverse column permutation defined by TR and completing the final filtering phase.

$$Q = \begin{pmatrix} q_{11}\ q_{12} \ldots q_{1h} \\ q_{21}\ q_{22} \ldots q_{2h} \\ \ldots. \\ q_{k1}\ q_{k2} \ldots q_{kh} \end{pmatrix}$$

Boundary pixels, which remain unchanged during arithmetic-mean filtering, are copied directly from the original image P. As part of the proposed reconstruction procedure, the authors formulate the computation of the elements of matrix Q from matrix R as follows:

$$\forall i \in \{\frac{a+1}{2}, \frac{a+3}{2}, ..., k-\frac{a-1}{2}\},$$

$$j = \left\{\frac{a-1}{2}, \frac{a+3}{2}, ..., h-\frac{a-1}{2}\right\} : q_{i,j} = \sum_{l=j-\frac{a-1}{2}}^{j+\frac{a-1}{2}} r_{i,TR(l)}. \quad (5)$$

To reduce the computational cost of the proposed reconstruction procedure, the authors derive Equation (6) for the elements of the first non-boundary column: i.e. [(a + 1) / 2]th column:

$$\forall i \in \{\frac{a+1}{2}, \frac{a+3}{2}, ..., k-\frac{a-1}{2}\},$$

$$j = \frac{a+1}{2} : q_{i,j} = \sum_{l=j-\frac{a-1}{2}}^{j+\frac{a-1}{2}} r_{i,TR(l)}. \quad (6)$$

For the remaining columns of the matrix Q, the authors derive the following recursive formulation, requiring one addition and one subtraction operation:

$$\forall i \in \{\frac{a+3}{2}, \frac{a+5}{2}, ..., k-\frac{a-1}{2}\},$$
$$j \in \{\frac{a+1}{2}, ..., h-\frac{a-1}{2}\}: \quad (7)$$
$$q_{i,j} = q_{i,j-1} - r_{i,TR(j-\frac{a+1}{2})} + r_{i,TR(j+\frac{a-1}{2})}$$

The proposed method is illustrated by an example of a remote arithmetic filtering of the image P in the overview part of the article.

$$P = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1 & 1 & 2 & 5 & 9 \\ 1 & 5 & 1 & 3 & 1 & 7 \\ 1 & 1 & 2 & 3 & 1 & 8 \\ 1 & 2 & 3 & 4 & 3 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}$$

When executing the protected image filtering P according to the developed method, the user randomly preliminarily generates a table TD of permutations of the columns of the image matrix. As an example, table TD is considered as presented in (Table 1). Accordingly, the TR back-mixing table has the form shown in (Table 2).

Table 1. Table of direct mixing of td columns

Image column number	
The original R	Mixed G
1	3
2	6
3	5
4	1
5	4
6	2

Table 2. Table tr back mixing columns

Image column number	
Mixed	The original
1	4
2	6
3	1
4	5
5	3
6	2

Using table TD, the user forms a mixed image G, the matrix of which has the following form:

$$G = \begin{pmatrix} 2 & 6 & 1 & 4 & 1 & 1 \\ 2 & 9 & 1 & 5 & 1 & 1 \\ 3 & 7 & 1 & 1 & 1 & 5 \\ 3 & 8 & 1 & 1 & 2 & 1 \\ 4 & 8 & 1 & 3 & 3 & 2 \\ 4 & 9 & 2 & 5 & 3 & 2 \end{pmatrix}$$

This matrix is sent by the user to the cloud. On a remote computer system, partial arithmetic means filtering of the mixed image G is performed with the formation of a matrix R:

$$R = \begin{pmatrix} 2 & 6 & 1 & 4 & 1 & 1 \\ 0{,}78 & 2{,}44 & 0{,}33 & 1{,}11 & 0{,}33 & 0{,}78 \\ 0{,}89 & 2{,}67 & 0{,}33 & 0{,}78 & 0{,}44 & 0{,}78 \\ 1{,}11 & 2{,}56 & 0{,}33 & 0{,}56 & 0{,}67 & 0{,}89 \\ 1{,}22 & 2{,}78 & 0{,}44 & 1 & 0{,}89 & 0{,}56 \\ 4 & 9 & 2 & 5 & 3 & 2 \end{pmatrix}$$

The image, returns to the user who copies the extreme points of the original image P into the image matrix Q. The values of the elements in the second column, from the second to the fifth row of matrix Q, are calculated according to Equation (6), while all remaining elements are calculated recursively according to Equation (7). As a result, the user receives the following matrix Q:

$$Q = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1{,}44 & 1{,}89 & 2{,}22 & 4{,}33 & 9 \\ 1 & 1{,}56 & 2{,}11 & 2{,}11 & 4{,}33 & 7 \\ 1 & 1{,}89 & 2{,}67 & 2{,}33 & 4{,}22 & 8 \\ 1 & 1{,}89 & 2{,}67 & 3{,}11 & 5 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}$$

After rounding the values of the elements, the user receives the matrix Q of the original filtered image:

$$Q = \begin{pmatrix} 1 & 1 & 1 & 2 & 4 & 6 \\ 1 & 1 & 2 & 2 & 4 & 9 \\ 1 & 2 & 2 & 2 & 4 & 7 \\ 1 & 2 & 3 & 2 & 4 & 8 \\ 1 & 2 & 3 & 3 & 4 & 8 \\ 2 & 2 & 3 & 4 & 5 & 9 \end{pmatrix}$$

It is evident that the resulting matrix Q is identical to the matrix of direct arithmetic means filtering.

5. EVALUATION OF EFFECTIVENESS

Based on the computational model and evaluation criteria defined in Section 2, the following expressions are derived by the authors specifically for the proposed method.

In the proposed method, image encryption requires only column rearrangement and therefore introduces negligible computational overhead. During the final filtering phase, the user performs one addition and one subtraction for all matrix elements except those of the first non-boundary column. The additional operations required for this column affect less than $1/h$of the elements, i.e., less than 0.1% for modern images. Thus, the

average user-side processing time per image point can be approximated as $2t_a$, and the total processing time $T$is:

$$T = k \cdot h \cdot 2 \cdot t_a$$

Hence, the coefficient β of filtering acceleration due to the involvement of remote computer systems in the calculations for the proposed method is:

$$\beta = \frac{T_0}{T} = \frac{k \cdot h \cdot (a^2 \cdot t_a + t_d)}{k \cdot h \cdot 2 \cdot t_a} = \frac{a^2}{2} + \frac{t_d}{2 \cdot t_a}$$

The obtained value practically coincides with the performance reported for the fastest additive-masking variant [9].

However, in comparison with this variant of secure filtering on remote computer systems, the proposed solution provides a significantly higher level of protection against unauthorized attempts to restore the image by statistical analysis.

For an image with h columns, the proposed method provides $h!$ possible column permutations. Using the standard Stirling approximation:

$$\eta = (\frac{h}{e})^h \cdot \sqrt{2 \cdot \pi \cdot h}$$

For $h = 1024$, the resulting search space makes exhaustive reconstruction computationally impractical. For contour images, targeted reconstruction may reduce the search space by 2–3 orders of magnitude. To strengthen protection, $n$images can be jointly permuted, increasing the number of possible permutations to $(nh)!$without increasing the protection or final-filtering time.

6. CONCLUSION

This study developed a secure remote arithmetic-mean filtering method for cloud-based image streams. Column permutation protects the source image before transmission, partial filtering is performed remotely, and the user reconstructs the final result with the inverse permutation. The approach keeps local preprocessing inexpensive and avoids transmitting the original spatial arrangement.

Analytical evaluation shows a one-to-two-order acceleration, close to the fastest additive-masking approaches, while offering a substantially larger reconstruction search space. The method is suitable for dependable cloud image analysis where efficiency and confidentiality are both required. Future work will evaluate larger and more diverse image streams, quantify reconstruction resistance empirically, and extend the construction to additional linear filters and distributed edge–cloud settings.

REFERENCES

[1] Russ, J.C., Neal, F.B. *The Image Processing Handbook*, 7th ed. CRC Press, 2016.

[2] Sathish, V., Sangeetha, T.A. Cloud-based image processing with data priority distribution. *Journal of Computer Applications*, vol. 6, no. 1, 2013, pp. 6–8

[3] Boroujerdi, M.M., Nazem, S. Cloud computing: Changing cogitation about computing. *World Academy of Science, Engineering and Technology, International Journal of Computer and Information Engineering*, vol. 3, no. 10, 2009.

[4] Wang, P., Wang, J., Chen, Y., Ni, G. Rapid processing of remote sensing images based on cloud computing. *Future Generation Computer Systems*, vol. 29, no. 8, 2013, pp. 1963–1968.

[5] Ahmed, M., Hossain, M.A. Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications*, vol. 6, no. 1, 2014, pp. 25–36.

[6] Bardis, N.G. Secure modular arithmetic for IoT and cloud applications. In: *Green IT Engineering*. Springer, 2017, pp. 43–64.

[7] Markovskyi, O.P., et al. Secure modular exponentiation in cloud systems. *Proceedings of the Congress on Information Technology, Computational and Experimental Physics (CITCEP 2015), Krakow, Poland, 18–20 December 2015*

[8] Stavroulakis, P., Kolisnyk, M., Kharchenko, V., Doukas, N., Markovskyi, O.P., Bardis, N.G. Reliability, fault tolerance and other critical components for survivability in information warfare. In: *E-Business and Telecommunications*, Springer, 2019, pp. 346–370.

[9] Bansal, Upma et al. A new methodology for SP noise removal in digital image processing. *IEEE Annual Symposium on Foundations of Computer Science* (2015)

[10] Pareek, N.K., et al. Image encryption using a chaotic logistic map. *Image and Vision Computing*, vol. 24, no. 9, 2006, pp. 926–934.

[11] Qin, Z., et al. Privacy-preserving image processing in the cloud. *IEEE Cloud Computing*, vol. 5, no. 2, 2018, pp. 48–57.

[12] Elashry, I.F., et al. Homomorphic image encryption. *Journal of Electronic Imaging*, vol. 18, no. 3, 2009, pp. 2–14.

[13] Doukas, N. Low colour-depth image encryption scheme for use in COTS smartphones. *WSEAS Transactions on Systems*, vol. 11, no. 9, 2012, pp. 527–538.

[14] Mirataei, A., Rusanova, O., Tribynska, K., Markovskyi, O. Organization of protected filtering of images in clouds. *Information, Computing and Intelligent Systems*, no. 3, 2022. DOI: 10.20535/2708-4930.3.2022.269132.

[15] Jia, H., Cai, D., Yang, J., et al. Efficient and privacy-preserving image classification using homomorphic encryption and chunk-based convolutional neural network. *Journal of Cloud Computing*, vol. 12, 2023, Article 175.

[16] Liu, Q., Zhou, F., Chen, H. Secure medical data on cloud storage via DNA homomorphic encryption technique. *Physical Communication*, vol. 64, 2024, Article 102295.

[17] Bai, Y., Zhao, H., Shi, X., Chen, L. Towards practical and privacy-preserving CNN inference service for cloud-based medical imaging analysis: A homomorphic encryption-based approach. *Computer Methods and Programs in Biomedicine*, vol. 261, 2025, Article 108599. DOI: 10.1016/j.cmpb.2025.108599

[18] Saeed, K., Adak, M.F. Secured cloud-based image data processing of self-driving vehicles using full homomorphic encryption. *Kuwait Journal of Science*, vol. 52, no. 4, 2025, Article 100449. DOI: 10.1016/j.kjs.2025.100449

[19] Hamza, R. A quantum-resistant FHE framework for privacy-preserving image processing in the cloud. *Algorithms*, vol. 18, no. 8, 2025, Article 480. DOI: 10.3390/a18080480.

[20] Luo, Y., Chen, Y., Dou, H., Tan, C., Zhou, H. Enhancing privacy management protection through secure and efficient processing of image information based on the fine-grained thumbnail-preserving encryption. *Information Processing & Management, vol. 61, no. 5, 2024,* Article 103789. DOI: 10.1016/j.ipm.2024.103789

[21] Li, M., Cui, Q., Wang, X., Zhang, Y., Xiang, Y. FTPE-BC: Fast thumbnail-preserving image encryption using block-churning. *Expert Systems with Applications*, vol. 255, 2024, Article 124574. DOI: 10.1016/j.eswa.2024.124574

Information about the authors:

Dimitra Georgiou – is an Adjunct Lecturer at the Department of Mathematics and Engineering Sciences, Hellenic Military Academy, Vari, Greece. Her research interests include cybersecurity, cloud computing security, privacy-preserving technologies and critical infrastructure protection. She has authored numerous scientific publications and actively participates in European and international research projects in information security and digital resilience.

Melitine Bardi– Student at University of Thessaly

Alireza Mirataei, National Technical University of Ukraine “Igor Sikorsky” Kyiv Polytechnic Institute Kyiv, Ukraine. She is a security analyst and researcher specializing in computer engineering, cloud computing security, and homomorphic encryption.

Oleksandr Markovskyi –is a researcher and assistant professor in the Department of Computer Engineering at the National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”. His work focuses on cryptography, computer security and error-control coding

Manuscript received on 13 August 2026