UDC 004.052.42

ORGANIZATION OF PROTECTED FILTERING OF IMAGES IN CLOUDS

A. Mirataei, O. Rusanova, K.Tribynska, O. Markovskyi

The article proposes an approach to using cloud technologies to accelerate the filtering of image streams while ensuring their protection during processing on remote computer systems. Homomorphic encryption of images during their remote filtering is proposed to be carried out by shuffling rows of pixel matrices. This provides a high level of protection against attempts to illegally restore images on computer systems that filter them. The developed approach makes it possible to speed up the performance of this important image processing operation by 1-2 orders of magnitude.

***Key words**: Arithmetic mean filtration, images processing, homomorphic encryption, secure clouds computing.*

Introduction

One of the defining features of the current stage of information technology development is the rapid process of qualitative improvement of the interface between computer systems and the outside world. Image processing, analysis and recognition is a key element of computer perception of objects in the outside world. Solving these problems includes a number of stages, one of which is improving the quality of the image and updating it, that is, removing elements from it that do not carry useful information for solving a specific problem of image analysis. The main tool of the image updating process is its filtering. In addition to performing the task of updating, image filtering ensures an increase in their quality by removing the interference that occurred during image reception and transmission [1].

In practice, two types of filtering are used: median and arithmetic mean. Both types of filtering involve scanning the image with an aperture of a certain size and are characterized by significant resource consumption, proportional to the product of the number of pixels in the image by the square of the aperture size. On the other hand, image filtering procedures allow simultaneous processing of several of their fragments. This determines the feasibility of using multiprocessor computer systems for image filtering [2].

For most practical applications of image analysis, it must be performed in real-time on terminal low-power microcontrollers. This dictates the need to involve remote powerful computer systems using the capabilities of modern cloud technologies to perform resource-intensive analysis and image recognition operations [3]. Currently, the vast majority of terminal microcontrollers are equipped with built-in radio modems, which makes it possible to connect them to the Internet. A significant obstacle to the use of cloud technologies for the radical acceleration of image processing is that, for a significant part of practical applications, the condition of confidentiality must be fulfilled, which excludes the possibility of access to the images by third parties who can potentially use this information to disrupt the operation of computer health monitoring systems objects of the real world. Based on this, the task of protecting images in the process of their processing and, in particular, filtering, on remote computer systems arises. In practical terms, we are talking about homomorphic encryption of images. which makes it impossible to illegally reconstruct them on remote computer systems performing filtering.

Thus, the scientific task of ensuring the protection of images in the process of their filtering on uncontrolled remote multiprocessor computing systems is relevant and practically important for the current stage of development of computer technologies.

Problem statement and review of methods for its solution

The need for significant computing resources is characteristic of all image processing, analysis, and recognition tasks. This is due to the fact that modern images consist of millions of dots, and the continuous process of improving their quality results in an increase in the number of dots. In addition, modern image processing algorithms are constantly becoming more complex. Thus, trends in the use of computer image analysis in modern conditions dictate the need for a significant increase in the

amount of computing resources, the growth rates of which significantly outpace the progress of increasing the speed of processors [1]. With this in mind, the most effective way to speed up computer image processing is to use cloud technologies that provide access to practically unlimited computing resources [4].

The main obstacle to the implementation of this possibility is that for the vast majority of practical applications it is unacceptable to transfer images to potentially accessible remote computer systems. Therefore, for the possibility of remote processing and analysis of images, it is necessary to carry out their homomorphic encryption, which allows processing with the possibility of decrypting the obtained results. For estimate of effectiveness of such type encryption is used followed criterias [5]:

Acceleration of the implementation of filtering due to the use of cloud systems, which is estimated by the coefficient γ. The value of this coefficient is determined by the ratio of the time T_0 of filtering the image on the terminal device to the time T_{cd} of its performing homomorphic encryption of the image and decryption of the obtained results:

$$\gamma = \frac{T_0}{T_{ed}} . \tag{1}$$

The level of security of images when using homomorphic encryption, which is estimated by the amount of resources needed to carry out illegal image restoration on a remote computer system.

In the last decade, results were obtained [6,7], which show the fundamental possibility of creating homomorphic ciphers invariant to processing procedures. However, the computational complexity of the samples of such ciphers created so far makes their practical use impractical.

Therefore, in practice, specialized homomorphic ciphers adapted to certain data processing procedures are used. For the tasks of secure filtering of images on remote computer systems, a number of specialized homomorphic ciphers have also been proposed to date [8,9]. The vast majority of them are based on additive masking of image pixels. The essence of additive masking is that when masking an image, which is given by the matrix $B=\|b_{i,j}\|$, $i\in\{1,2,\ldots n\}, j\in\{1,2,\ldots,m\}$, an image is created-mask, which is given by the matrix $V==\|v_{i,j}\|$. When performing median filtering with an aperture of odd size h, its central element $b_{i+(h+1)/2,j+(h+1)/2}$ is replaced by the median h^2 of the aperture pixels. It is obvious that the additive masking should be performed in such a way that the order between the values of the aperture pixels is not violated, that is, the code of each pixel of the mask $v_{i,j}$ should depend on the corresponding code of the original image. This significantly reduces the effectiveness of additive masking due to the fact that significant computing resources are spent on homomorphic encryption and decryption. With arithmetic mean filtering, the central element $b_{i+(h+1)/2,j+(h+1)/2}$ of the aperture is replaced by the arithmetic mean of its pixels:

$$\forall i = 1,2,..,n,\ j = 1,2,..,m : b_{i,j} = \frac{1}{h^2} \cdot \sum_{l=1}^{h} \sum_{q=1}^{h} b_{i+l,j+q} . \tag{2}$$

The operation of additive encryption consists in adding to each pixel of the original image the corresponding pixel of the mask: $u_{i,j} = b_{i,j} + v_{i,j}$. On the remote computer system, filtering of the masked image U is performed, during which a new value $u_{i,j}$ is formed in the form:

$$u_{i,j} = \frac{1}{h^2} \cdot \sum_{l=1}^{h} \sum_{q=1}^{h} u_{i+l,j+q} = \frac{1}{h^2} \cdot \sum_{l=1}^{h} \sum_{q=1}^{h} b_{i+l,j+q} + \frac{1}{h^2} \cdot \sum_{l=1}^{h} \sum_{q=1}^{h} v_{i+l,j+q} . \tag{3}$$

It follows from formula (3) that the result of remote filtering is the sum of the result of filtering the original image B and the mask V. Accordingly, homomorphic encryption consists in subtracting from each pixel of the resulting image U the code of the pixel of the same name as the result of mask filtering.

The main disadvantage of homomorphic ciphers based on additive masking is that it requires an additional mask image filtering procedure. In paper [10], it is proposed to randomly select one of the previously filtered images as a mask. For a wide range of practical applications, the stream of processed images is sufficiently correlated, which significantly reduces the level of security of images during their remote processing. Therefore, a significant drawback of the additive masking method

using a permanent mask or one of the previously filtered images is that it does not provide a high level of security. Accordingly, the disadvantage of the known method of homomorphic encryption of images during their remote filtering is an insufficiently high level of security.

Purpose and objectives of research

The purpose of the work is to increase the efficiency of secure image processing in the clouds, in particular, their arithmetic mean filtering on remote computer systems by increasing the level of security.

The main tasks of the research in accordance with the set goal are as follows.

1. Analysis of computational operations of arithmetic mean filtering, identification of homomorphic ciphers invariant to the filtering procedure, and selection of the most effective of them for further development.

2. Development of a method of homomorphic encryption of images based on string permutations to increase the level of security during remote arithmetic mean filtering.

3. Theoretical and experimental evaluation of homomorphic encryption efficiency indicators based on changing the order of lines during arithmetic mean filtering on remote computer systems.

The object of research is the processes of homomorphic encryption of images for their protected arithmetic mean filtering in clouds.

Method of homomorphic encryption of image upon arithmetic mean filtration

The conducted analysis of the possibilities of increasing the efficiency of protected filtering of images in the clouds allows us to conclude that the most promising way to achieve the goal is to use mixing. This procedure, traditional for cryptography, does not require significant computing resources and can be performed directly during image transmission. In favor of such a conclusion, the fact that the significant amount of information contained in modern images makes shuffling a sufficiently effective means of protection against attempts to reconstruct images using technologies of directed enumeration or statistical analysis. Based on this, the basis of the proposed method of homomorphic encryption of images during their arithmetic mean filtering is their mixing.

Within the framework of the developed method, the original image B is transformed into an encrypted image U by rearranging its lines in a certain order. At the same time, the order of permutation of the rows of the image matrix B is used as a key for its homomorphic encryption. After homomorphic encryption, the image U is sent to a remote computer system where it is partially filtered. The image R obtained as a result of such filtering is returned to the terminal microcontroller, which performs homomorphic decoding of R by restoring the order of lines, and also performs the final filtering phase.

The order of shuffling the rows of matrix B is chosen arbitrarily and fixed in the form of a table Q of direct permutation. From the table Q, the table G of the reverse permutation is formed, so that the condition $a=G(Q(a))$ is fulfilled. Table G is used for homomorphic decryption of remote processing results.

The proposed method of homomorphic encryption of images for their protected arithmetic mean filtering on remote computer systems involves the periodic operation of generating tables of forward Q and reverse G permutation of matrix rows of image pixels.

The process of remote secure processing of the image specified by the matrix B, according to the proposed method, consists of the following sequence of actions:

1. According to table Q, the rows of the matrix B are permuted, in the result matrix U of the encrypted image is formed:

$$U = \begin{pmatrix} u_{11}\ u_{12} \ldots u_{1m} \\ u_{21}\ u_{22} \ldots u_{2m} \\ \ldots \\ u_{n1}\ u_{n2} \ldots u_{nm} \end{pmatrix}.$$

2. The U matrix of the shuffled image obtained as a result of the homomorphic encryption described above is sent to a remote computer system.

3 On a remote computer system, a partial arithmetic average filtering of the elements of the matrix U is performed. The result of this operation is formed in the form of a matrix C:

$$C = \begin{pmatrix} c_{11}\ c_{12}\ldots c_{1m} \\ c_{21}\ c_{22}\ldots c_{2m} \\ \ldots. \\ c_{n1}\ c_{n2}\ldots c_{nm} \end{pmatrix}.$$

The procedure of partial arithmetic mean filtering provided by the developed method consists in replacing each element $u_{i,j}$ of the matrix U divided by h^2 by the sum of h elements of the fragment of the i-th row of the matrix, such that its central element belongs to the j-th column of the matrix:

$$\forall i \in \{(h+1)/2,..,n-(h-1)/2\},\ j \in \{(h+1)/2,...,m-(h-1)/2\} : c_{i,j} = \frac{1}{h^2} \cdot \sum_{l=j-h/2}^{j+h/2} u_{i,l} \ . \quad (4)$$

4. Formed as a result of partial arithmetic mean filtering on remote computer systems, matrix C is returned to the computer platform that performs image processing and analysis.

5. Over the received matrix C, the reverse permutation of rows is performed using table G; as a result, the matrix F is formed.

6. On the matrix F, the operation of the final stage of filtering is performed, which consists in the fact that each element $f_{i,j}$ of the matrix F is replaced by the sum of h elements of the fragment formed by the j-th column, and the central element of this fragment is the element belonging to the i-th row matrices F :

$$\forall i \in \{(h+1)/2,..,n-(h-1)/2\},\ j \in \{(h+1)/2,...,m-(h-1)/2\} : f_{i,j} = \sum_{l=i-h/2}^{i+h/2} f_{l,j} \ . \quad (5)$$

The image F formed by the described procedure is a filtered original image B with an aperture equal to h.

Evaluation of the developed method effectiveness

Evaluation of the effectiveness of the developed and proposed method of protected remote arithmetic mean filtering can be carried out according to the criteria specified in the review section.

Acceleration of the implementation of filtering due to the use of cloud systems is estimated by the coefficient γ. To determine it, it is necessary to determine the spent time T_0 filtering the image on the terminal device, as well as the time T_{cd} for it to perform homomorphic encryption of the image and decrypt the results received from the cloud. When performing filtering on the terminal microcontroller of the image processing system, h^2 addition operations and one division operation must be performed for each of the $n \cdot m$ image points. Considering that the execution time of the division command is about 50 times longer than the addition operation [11], the numerical value of T_0 can be estimated by the expression: $T_0 \approx n \cdot m \cdot (h^2 + 50) \cdot t_a$, where t_a is the execution time of the addition command on the terminal microcontroller.

The time T_{cd} for the execution of encryption, decryption and the final filtering stage by the terminal microcontroller is determined by calculating the following. The proposed method for homomorphic encryption of images before their transmission to the cloud does not involve special calculations, as it is reduced to permuting the rows of the pixel matrix. Technologically, the process of permuting the rows of the matrix is reduced to changing the order of transferring image points to the network and, accordingly, does not require additional time. That is, the process of homomorphic image encryption in reality can be combined with the process of data transmission from the terminal microcontroller to a remote computer system.

Similarly, the process of homomorphic decoding of a partially filtered image, which is carried out by reverse shuffling of the image pixel matrix rows using table *G*, can be combined with the process of transferring a partially filtered image from a remote computer system to a terminal microcontroller. This means that in the proposed method of their protected arithmetic average filtering of images in the cloud, the decryption process also does not require additional time resources of the terminal microcontroller. This property of permutation ciphers combined with the remote nature of image processing, which requires cycles of transmission over the Internet, is the main factor in the increased efficiency of homomorphic encryption compared to other known methods of specialized homomorphic encryption in terms of image processing acceleration.

Thus, the time T_{cd} when using the proposed method is determined by the time required to perform the final stage of filtering, which, in accordance with formula (5), consists in adding h numbers from the matrix F for each pixel of the specified matrix. Realistically, when scanning the matrix of images, it is more expedient not to recalculate the sum, but to perform only two operations: to subtract the value of the element that goes beyond the boundaries of the fragment during scanning and to add the value of the element that entered the boundaries of the fragment. That is, the process of processing each point of the image in the process of the final stage of its filtering requires only two arithmetic operations. In other words, the numerical value of time T_{ed} is determined by the product $T_{ed} = n \cdot m \cdot 2 \cdot t_a$. Accordingly, the value of the coefficient γ of accelerating the implementation of filtering due to the use of cloud systems is calculated as:

$$\gamma = \frac{T_0}{T_{ed}} = \frac{m \cdot n \cdot t_a \cdot (h^2 + 50)}{m \cdot n \cdot 2 \cdot t_a} = \frac{1}{2} \cdot (h^2 + 50). \quad (6)$$

For example, with a value of h=15 typical for practical applications, calculated according to formula (6), the value of the coefficient γ of accelerating the implementation of filtering due to the use of cloud technologies is 137.5. According to experimental research, the value of the coefficient γ is slightly smaller and is about 130. The obtained value of the coefficient γ practically coincides with the estimation of acceleration of filtering for the fastest known variants of homomorphic encryption of images by the method of additive masking.

When applying the proposed method of secure image filtering on remote computer systems, the time required to process each point of the image consists of the time of performing h operations of arithmetic addition, as well as the time of performing the operation of division by the square of the aperture size h^2 of the received sum using one division command . In other words, the specific weight υ of operations performed on the terminal microcontroller during the implementation of the final stage in the total volume of arithmetic mean filtering operations is determined by the following expression:

$$\upsilon = \frac{T_{ed}}{T_T} = \frac{n \cdot m \cdot 2 \cdot h \cdot t_a}{n \cdot m \cdot t_a \cdot (h + 50)} = \frac{2}{h + 50}, \quad (7)$$

where T_T is the processing time on the terminal microcontroller of one point during partial arithmetic mean filtering of the image. At the value h=15 typical for real applications, the value of the specific weight υ of operations performed on the terminal microcontroller is υ = 0.0307 or 3.07%, calculated by formula (7). For additive masking of images with their protected processing in the cloud, this indicator is 4.5%.

The analysis of formula (7) indicates that in the proposed method of homomorphic encryption of images, only about 3% of the volume of calculations related to filtering is carried out on the terminal microcontroller, and, accordingly, 97% of the volume of calculations is implemented on remote computer systems. Thus, the conducted analysis proved that compared to other known methods of homomorphic encryption of images with their remote arithmetic mean filtering, the proposed method based on permutations of rows of the image matrix has better time indicators compared to the known method of additive masking. This effect is achieved due to the fact that the proposed method is based on permutation operations, which can be combined in practice with data transfer processes from the terminal microcontroller to cloud systems and back.

However, the main advantage of the proposed method of protecting images from their illegal reconstruction during filtering on remote computer systems is a significantly higher level of security.

Known methods of homomorphic encryption of images for their protected arithmetic mean filtering, in particular, methods based on additive masking, actually have to use the same mask for image processing, for which arithmetic mean filtering needs to be performed on the user's computing platform. The use of one mask for homomorphic encryption of several images makes it possible to detect this by means of spectral analysis. Accordingly, the party carrying out the attack has the opportunity to restore the masking image and, accordingly, decipher the real image in the process of its processing on a remote computer system not controlled by the user.

The level of security of an image can be estimated by the amount of resources required by the party aiming to restore the original image. When using the developed method of homomorphic encryption of images for their protected arithmetic mean filtering, the number d of possible permutations of rows of the pixel matrix is $n!$. For real images, the number of n rows of the pixel matrix is 1024, respectively, the number of d options for permuting the columns of such an image is $d=1024! = 6.421 \cdot 10^{2639}$. It is clear that the analysis of such a large number of options makes it practically impossible to restore the original image by selecting the reverse permutation, since the selection of such a significant number of options is far beyond the scope of technical implementation with modern computer means. The implementation of such a large number of options is impossible even in the near term of 20-40 years, even if the capabilities of quantum computers are used.

For certain classes of contour images, the volume of the considered search can be significantly reduced due to directional image reconstruction. This technology involves selecting rows in such a way that two adjacent ones are minimally different from each other. The conducted experimental studies showed that for real contour images, the volume of the search can be reduced by 2-3 orders of magnitude in this way. But it is quite clear that reducing the sorting order by 0.02% does not significantly affect the technical implementation of such sorting by modern computer means.Even with the application of the described technology, the selection of such a significant number of options is far beyond the scope of modern technical implementation capabilities. When processing images of these classes using the developed method, it is recommended to organize simultaneous filtering of a group of k images. At the same time, n rows of k images can be rearranged according to the proposed technology within the group. The number of images within one group does not affect the time taken to encrypt the image before sending it to the network and the final filtering phase. However, the number of permutation options increases to $(n \cdot k)!$, which very effectively increases the level of security of images. for example, even with $k=2$, the number of row sorting options is $1.67 \cdot 10^{5894}$.

Conclusion

As a result of research aimed at increasing the level of security of images when filtering them on remote computer systems, a new method of homomorphic encryption was theoretically substantiated, developed and researched.

The proposed method of homomorphic encryption of images to protect against their illegal reconstruction during arithmetic mean filtering on remote computer systems differs in that the main element of protection is the shuffling of image pixel matrix rows. The shuffling order can change randomly and serves as a secret key for homomorphic encryption of images. Within the framework of the developed method, procedures for partial arithmetic mean filtering, which is carried out on remote systems, as well as procedures for the final stage of filtering are defined, which is carried out on a terminal platform that performs processing and analysis of a real image. The developed method of protected filtering based on shuffling the rows of the pixel matrix allows, due to the use of remote computing power, to speed up this operation by 1-2 orders of magnitude, which practically coincides with the similar indicator of the fastest-acting variant of image protection based on additive masking.

The main advantage of the developed method is a much higher level of protection against attempts, using statistical analysis, to gain illegal access to images during their processing on remote computer systems not controlled by the user.

The proposed method can be used to speed up the processing and analysis of images by terminal devices of computer systems for remote monitoring of the state of real-world objects and their management.

References

1. Russ J.C. The Image Processing Handbook. 7- Edition / J.C. Russ, F. Brent Neal // CRC Press.- 2016.- 1053 p.
2. Markovskyi O.P. Protected implementation of image filtration on GRID systems / O.P. Markovskyi, A.M. Bilashevska, M.O. Nevdashenko // Visnik of National Technical University of Ukraine "KPI" Informatics, Control and Computer Engineering.- 2014.- Vol. 61,- PP.105-109.
3. Sathish V. Cloud-based Image Processing With Data Priority Distribution Mechanism / Sathish V.A. , Sangeetha T.A. // Journal of Computer Applications.- Vol.6, №1.- 2013.- P. 6-8.
4. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – 2012. – №3. – P. 169-180.
5. Markovskyi O.P. The method of accelerated secure image filtering on remote computer systems / O.P. Markovskyi, I.O.Gymenuk, Alireza Mirataei, J.I. Turoshanko, M.O. Voloshuk // Telecommunication and information technology.- 2019,- Vol.65.-no.4.- PP.99-110.
6. Van Dijk M. Fully homomorphic encryption over the integers./ M. Van Dijk, C. Gentry, S. Halevi // In Annual International Conference on the Theory and Applications of Cryptographic Techniques.- Springer, -2010,- pp. 24–43.
7. Gentry C. Implementing gentry's fully-homomorphic encryption scheme / C.Gentry, S.Halevi // In Annual international conference on the theory and applications of cryptographic techniques.- Springer, - 2011,- pp. 129– 148.
8. Markovskyi O.P. The method of accelerated secure image filtering on remote computer systems / O.P. Markovskyi, I.O.Gymenuk, Alireza Mirataei, J.I. Turoshanko, M.O. Voloshuk // Telecommunication and information technology.- 2019,- Vol.65.-no.4.- PP.99-110.
9. Monjur Ahmed. Cloud Computing and Security Issues in the Cloud / Monjur Ahmed, Mohammad Ashraf Hossain // International Journal of Network Security & Its Applications (IJNSA).- Vol.6, №1.- 2014.- pp.25-36.
10. Humenuk I.O. Method removed Arithmetic mean filtration of images / I.O. Humenuk, O.H. Slusarenko // Almanac of sciense .- 2019.- № 11 (32).- P.40-43.
11. Subero A. Programming PIC Microcontrollers wit XC8. – 2018.- Apress Berkeley,CA.- 434 P. DOI.ORG/10.1007/978-1-4842-3273-6.