UDC 004.383.3, 004.056

ALIREZA MIRATAEI,
HANA KHALIL,
MARKOVSKYI O.

PROTECTED DISCRETE FOURIER TRANSFORM IMPLEMENTATION ON REMOTE COMPUTER SYSTEMS

Annotation: Effective method of the discrete Fourier transform acceleration with the use of cloud computing is theoretically substantiated and developed. The reigning feature of the suggested method is homomorphic encryption of the input signals, which provides efficient protection during the remote calculation. It has been shown theoretically and experimentally that the proposed method allows one to 1-2 orders of magnitude to speed up the processing of signals while maintaining their confidentiality. The proposed method can be applied for effective signal stream processing in clouds.

Keywords: discrete Fourier transform, cloud computer systems, remote signal processing, homomorphic encryption.

1. Introduction

The cloud technologies development radically changed the organization of computer information processing. In response to cloud systems, a wide range of users obtain access to powerful computing systems. The emergence of such opportunity allows solving qualitatively new classes of tasks, multiply speeds up solution of a wide range of tasks with high computational complexity. Wide variety of applied tasks related to the interface implementation between computer systems and the outside world is used digital signal processing methods, including the discrete Fourier transform. Most of these tasks are performed in real time, that sets strict conditions for the fast discrete Fourier transform implementation. One of the most innovative lines of attack on the problem is using the cloud technologies capabilities [1]. Remote multiprocessor computer systems open wide possibilities for parallelization of the discrete Fourier transform, respectively accelerating their computing implementation.

For the vast majority of real-life signal processing systems, it is important to maintain confidentiality of the signals and their processing results. This factor significantly restricts the cloud technologies using for remote signal processing. These determinates the necessity for development of the homomorphic signals encryption methods in their remote processing in clouds [2].

Thus, the scientific task of developing the method for realization of the discrete protected Fourier transform on remote computer systems is relevant for the modern stage in the evolution of information technology.

2. Problem statement and review of methods for its solution

Digital signal processing is one of the most important tasks of modern computer technologies. Actually, the digital signal processing implements the interface between the real world and the computer systems [3]. For most practical uses, the problem of signal processing needs to be carried out in real time. This dictates hard conditions for the time-consuming implementation of computing that implement digital signal processing and, in particular, the discrete Fourier transform. For this purpose, specialized chips are developed and serially produced, which in favor of parallelization of computing at the hardware level solve the problem of Fourier transform accelerating [4]. Wide range of related hardware tools are developed by well-known firms like Texas Instruments INC, Motorola, Intel and Analog Devices. In particular, Texas Instruments INC produces series of fast Fourier transform processors that characteristically differ in speed performance and functional peripherals.

Fourier transform is one of the most used transforms for function decomposition. This transform allows to get the signals of different origin (images, voice signals, radio signals etc.) organized as a set of real numbers. It allows to compare, analyze, and read the signals.

Any kind of signals, that are specified by the set of measurements from identical periods of time, could be written as a sum of sinusoids. Sinusoidal functions have such characteristics: amplitudes (A1, A2, …), frequencies (ω, 2·ω, 3·ω, 4·ω …) and phases (φ1, φ2, φ3…).

As for input array (x0, x1, … xn-1) for Discrete Fourier Transform (DFT) we use calculated signal data through fixed time periods. Array from n complex elements (y0, y1, … yn-1) is output data of DFT, its components have amplitudes and phases of sinusoids, their sum recreates initially set input signal. If we take gi as real yi component, qi as imaginary yi component, Ai as spectral amplitude and φi as phase transport of yi then will be used next formulas [3]:

$$\forall i \in \{0,1,...,n-1\} : d_i = \frac{1}{n} \cdot \sum_{j=0}^{n-1} x_j \cdot \cos\frac{2 \cdot \pi \cdot i \cdot j}{n}, \quad q_i = \frac{1}{n} \cdot \sum x_j \cdot \sin\frac{2 \cdot \pi \cdot i \cdot j}{n} \quad (1)$$

Using the obtained values (from formulas (1)) of the real and imaginary components of the sinusoidal signal with the frequency i·ω we can calculate the amplitude of this signal, as well as its phase shift using the formulas [3]:

$$\forall i \in \{0,1,...,n-1\} : A_i = \sqrt{q_i^2 + g_i^2}, \quad \varphi_i = arctg(\frac{g_i}{q_i})^2 \quad (2)$$

For most practical applications of signal processing, the calculation according to the formula (2) is not performed [5], therefore the Fourier transform time is determined by the calculations described by the formula (10. It is obvious that the number of floating-point multiplication and floating-point additions for the implementation of the formula (1) is equal n2. This means that as the number of n increases, the number of floating-point multiplication and addition operations increases rapidly. Consequently, it is necessary to organize a remote calculation of formulas (1) on multiprocessing computing systems to reduce the execution time of the DFT. From the structure of the formulas (1) it is obvious that they can be calculated simultaneously on n processors.

Cosines and sinuses do not depend on the values x0, x1, ... xn-1 and they can be considered as constant numbers, the values of which depend only on indexes. Therefore, the components of formulas (1) can be calculated and organized in advance as a set of coefficients, which, in consequent researches, can be considered as permanent. The calculation of coefficients can be carried out in accordance with the following formulas [4]:

$$\forall i, j \in \{0,1,...,n-1\} : \quad a_{ij} = \frac{1}{n} \cdot \cos\frac{2 \cdot \pi \cdot i \cdot j}{n}, \quad c_{i,j} = \frac{1}{n} \cdot \sin\frac{2 \cdot \pi \cdot i \cdot j}{n} \quad (3)$$

If you use constant coefficients that are calculated by formulas (3), the basic formulas (1) can be simplified to the following form [4]:

$$\forall i \in \{0,1,..,n-1\} : g_i = \sum_{j=0}^{n-1} a_{ij} \cdot x_j, \; q_i = \sum_{j=0}^{n-1} c_{ij} \cdot x_{ij} \quad (4)$$

It needs to organize a secure Fourier transform: encrypt the values x0, x1, ... xn-1, which are transmitted to the cloud. Consider that in the cloud values v0, v1, ... vn-1 and w0, w1, ... wn-1 are being calculated using formulas (4) and go back to the user who has to restore the real values g0, g1, ... gn-1 and q0, q1, ... qn-1.

As noted above, the implementation of DFT on remote computer multiprocessor systems offers great possibilities for parallelization of computational process. Theoretically, when using an unlimited number of processors, multiply operations can be performed simultaneously by 2·n2 processors.

In addition, to form 2·n sums according to formulas (4) it needs to perform log2n sum operations on 2·n processors. Doing so, theoretically minimal execution time T0 of DFT on remote computer multiprocessor systems are determined by the formula:

$$T_0 = t_a \cdot \log_2 n + t_m, \quad (5)$$

where tm is the time for performing the floating-point multiplication and ta is the time for performing the floating-point adding.

When performing a DFT on single processor, then the Fourier transform is usually characterized by the number of multiples and additions that needs to perform during the process of the transformation. Number of multiplies for implementation of DFT is n2, and the number of additions is n·(n-1) [6]. The numerical value of T1 time execution of DFT on a single processor is determined by the following formula:

$$T_1 = t_m \cdot n^2 + t_a \cdot n \cdot (n-1) \quad (6)$$

.

Considering the fact that for modern processors, the time to perform an floating-point multiplication operation is many times greater than the time when the floating-point addition operation is performed, the attraction of remote multiprocessor computing systems with use of the cloud technologies capabilities allows speeding up the calculations in ξ times when DFT is performed. Numerical value ξ can be determined by substitution (5) and (6) to the following formula:

$$\xi = \frac{T_1}{T_0} \approx \frac{t_m \cdot n^2}{t_m + t_a \cdot \log_2 n} \quad (7)$$

.

If we take into account that the execution time of the multiplication is about 30 times longer than the execution time of the addition, then, according to the formula (7) when n = 16 the value of ξ is 226, and when n = 256 ξ is equal to 51739.

In practice, digital signal processing DFT is often implemented in the form of fast Fourier transform, which allows to reduce the number of multiplication and addition operations by using the properties of symmetry of the Fourier transform coefficients. When using a fast Fourier transform (FFT), amount of floating-point multiplication operations same as amount of floating-point addition operations are both equal to n2/2 [7].

There are two important conclusions to draw from:

The usage of remote multiprocessor computing systems to speed up the calculating of DFT gives a significant effect in terms of accelerating the computations, that is important for practical use which function in real-time mode.

The efficiency of using remote multiprocessor computing systems in frames of cloud technologies to accelerate the computational implementation of DFT is increasing as the size of the transformation is increased.

To realize these benefits provided by the modern cloud technologies, we need to develop a method that makes it impossible to get unauthorized access to the numerical values of the signal simples while running DFT over the signals on remote and out of user control computer systems.

One of the powerful reserves that can be used for the faster calculation of the discrete Fourier transform is cloud technologies. They provide the user with the global network access to virtually unlimited computing resources. These opportunities are actively used in solving a wide range of important tasks.

One of the main cloud technologies disadvantages, that significantly restricts their use, is the possibility of unauthorized access to user data during their processing the data on the remote computing capacities. A significant number of works deal with the problem of user data protecting on distance processing systems in recent years [7, 8, 9]. The fact of the matter is that there is no single approach to data protection in the procedure of their processing. Accordingly, there can't be a single homomorphic algorithm for data encryption, on which calculations on remote smoked capacities are performed.

This means that the homomorphic signal encryption algorithm should depend on the nature of their remote processing operations.

Accordingly, almost all homomorphic encryption researches solve the problem of data protection only for certain classes of computing problems [10].

The above analysis of the computational procedures that is fundamental for the discrete Fourier transform showed that for the algebraic basis of the homomorphic signal encryption can be used additive or multiplied operations, and operation of modulatory arithmetic in a traditional algebra.

When using modular arithmetic [11], each of the signal X samples: x0,x1,…,xn-1 is added to the additive mask r0,r1,…,rn-1 in such a way that the remote system is transmitted to the set of additive disguised samples: x0+r0, x0+r1,…,xn-1+rn-1. When this happens the values of masks are chosen in order that (r0+r1+…+rn-1) mod Z = 0, where Z is the private key of homomorphic encryption.

Then, with the remote execution of a discrete Fourier transform according to formula (4), the obtained results can be represented in the form:

$$\forall i \in \{0,1,...,n-1\} : g_i' = \sum_{l=0}^{n-1} (x_{il} + r_l) \cdot a_{il} = \sum_{l=0}^{n-1} x_{il} \cdot a_{il} + \sum_{l=0}^{n-1} r_l \cdot a_{il} =$$
$$= g_i + \beta \cdot Z; \quad q_i' = \sum_{l=0}^{n-1} (x_{il} + r_l) \cdot c_{il} = \sum_{l=0}^{n-1} x_{il} \cdot c_{il} + \sum_{l=0}^{n-1} r_l \cdot c_{il} = q_i + \gamma \cdot Z, \tag{8}$$

where β and γ are an integer. In other words, from the formula (8) it follows that the result of the remote processing is the sum of the real component of the spectral representation and some number that is targeted is divided without a remainder into the private key Z. Accordingly, the decryption of the received data is carried out in the following form:

$$\forall i \in \{1,2,...,n\} : g_i = g_i' \bmod Z, \; q_i = q_i' \bmod Z. \tag{9}$$

The disadvantage of the described well-known method is the high complexity of the decrypting implementation. In fact, for each of this spectral representation component there must be performed a division operation for finding a remainder according to the formula (9).

The work [12] introduces the method for encryption of signal, which remotely performs the discrete Fourier transform. In this case, the data encryption uses replication operations based on modular exponential derivation. This allows to flexibility in adjust the safety level of remote discrete Fourier transform implementation. In addition, in the development proposed the effective mechanisms of controlling the functional correctness of the remote discrete Fourier transform in the uncontrolled computing platforms. At the same time, using modular exponential as a mechanism for encryption markedly complicates the choice of keys and causes the considerable computing complexity of discrete Fourier transform realization, which is several times greater than the complexity of discrete Fourier transform realization with formula (4). Generations of keys is significant problem in the proposed method, which also requires significant computing resources. Supposing that the keys are used repeatedly, it results a security level decreasing, due to the fact that it opens to the attacker wider abilities to crack the cipher code. Usage of single use key in the proposed method leads to an increase in computing resources costs for discrete Fourier transform.

3. Purpose and objectives of research

The aim of the research is to increase the efficiency of the protected implementation of the discrete Fourier transform on remote computer systems.

Research objectives are determined by the aim and are as follows:

- Investigation of possible options for homomorphic encryption of signal samples before their transmission to the cloud, as well as decryption of the results obtained. Choosing the most effective option.
- Development of a method for secure implementation of the discrete Fourier transform on remote computer systems based on additive homomorphic encryption of signal samples.
- Theoretical and experimental study of the effectiveness of the method of secure implementation of discrete transformations in the cloud both in terms of the level of security and in terms of the achievable processing acceleration.

4. The method of the protected discrete Fourier transform implementation on remote multiprocessor computer systems

Since the operations that make up the discrete Fourier transform can be reduced to addition operations, the most natural way to hide signals by the sample is to add the components of the secret key to them. So, the basic idea of the proposed method is that each encrypted signal sample δj, j∈{0, 1,…,n-1} can be presented as a sum or deviation of two values: real signal sample and components of the secret key:

$$\forall j \in \{0,1,...,n-1\} : \delta_j = x_j + b_j, \tag{10}$$

where B= {b0,b1,…,bn-1} is the value of the carrier signal, whose components make up the secret key. To increase the level of protection of samples of real signals during their remote processing, it is proposed to use several carrier signals, which form a set Ω of κ elements Ω = {B1, B2, …, Bκ}. This carrier signal is correlated with the values of the results of the Fourier transform of: Θ = {V1, V2, …,Vκ} and Ψ = {W1, W2, …, Wκ}. In this way, the numerical values of sets items Θ and Ψ are calculated according to the following formulas:

$$\forall i \in \{0,1,...,n-1\}, l \in \{1,2,...,\kappa\} : v_{li} = \sum_{j=0}^{n-1} a_{ij} \cdot b_{lj}, w_{li} = \sum_{j=0}^{n-1} c_{lj} \cdot b_{lj} \tag{11}$$

.

The values of the bias signals that make a set Ω are chosen in such a way for the most distort of the dominant character type of useful signal X. For each area of practical usage of digital signal processing, the characteristic properties of the signal spectrum can be identified. Accordingly, the carrier signals must be selected in such a way as to distort the spectrum of these signals as much as possible. After selecting the set Ω the components of sets Θ and Ψ are calculated using formulas (11) with the image of the results in the memory. It should be noted that these calculations are realized in a non-critical time mode using the user's computing platform.

The proposed method of homomorphic encryption assumes the following sequence of actions

When the DFT is carried out over the signal X, set by the n values of its simples (x1, x2, …, xn) follows out the next action order:

Randomly, one of the carrier signals is selected from a set of Ω. Without losing the generalization, you can assume that the number of the chosen carrier signal in set Ω is h.

Bias values are calculated δ0, δ1, …, δn-1 of the X signal simples relatively to the selected Bh carrier signal according to the following formula (10).

The resulting values δ0, δ1, …, δn-1 are sent to a remote computer system.

A remote computer system performs a DFT for over a set of simples δ0, δ1, …, δn-1 according to formulas:

$$\forall i \in \{0,1,2,...,n-1\} : s_j = \sum_{j=0}^{n-1} a_{i,j} \cdot \delta_j, z_j = \sum_{j=0}^{n-1} c_{i,j} \cdot \delta_j \tag{12}$$

.

The remote computer system returns to the user the calculated values of s0, s1,…, sn-1 and z0, z1, …,zn-1.

The user restores the real values of the X signal spectral representation components: g0, g1, …,gn-1 and q0, q1, …,qn-1 with the following transformations:

$$\forall j \in \{0,1,...,n-1\} : g_j = s_j - v_{hj}, \quad q_j = z_j - w_{hj}. \tag{13}$$

The correctness of the results can be proved by the following calculations:

$$\forall i \in \{0,1,\ldots,n-1\}:$$

$$\begin{aligned} g_i &= \sum_{j=0}^{n-1} \alpha_{ij} \cdot x_j = \sum_{j=0}^{n-1} a_{ij} \cdot (\delta_j - b_{hj}) = \sum_{j=0}^{n-1} a_{ij} \cdot \delta_j - \sum_{j=0}^{n-1} a_{ij} \cdot b_{hj} = s_i - v_{hi} \\ q_i &= \sum_{j=0}^{n-1} c_{ij} \cdot x_j = \sum_{j=0}^{n-1} c_{ij} \cdot (\delta_j - b_{hj}) = \sum_{j=0}^{n-1} c_{ij} \cdot \delta_j - \sum_{j=0}^{n-1} c_{ij} \cdot b_{hj} = z_i - w_{hj} \end{aligned} \quad (14)$$

.

It can be seen from the transformations (14) that the term-by-term results as a result of the proposed computational procedure correspond to the results of the discrete Fourier transform over the original signal samples.

When using the developed procedure on the side of the remote computer system there is only a set of signals X (δ0, δ1, …, δn-1) relatively to the selected carrier signal which without knowledges of a given carrier signal cannot be recovered. Because the Bq carrier signal counts are calculated and stored on the user's side, signal X is practically impossible to recover on the side of the system that performs the remote DFT procedure.

The security level of the signal, which is transmitted in the form of an array of samples to the remote computer system, is largely determined by the choice of the carrier signal. The choice of the carrier signal should be carried out in such a way that the selection of the signal samples x0, x1, x2, ..., xn-1 from the samples δ0,δ1,δ2,…,δn-1 of the mixture of signals and the spectrum components s0,s1,s2, …,sn-1 and z0,z1,z2, …,zn-1 required the greatest possible resources.

With a random selection of samples b0,b1,b2, …,bn-1 of the carrier signal, its spectral components have approximately the same values (white noise). This makes it easier to fit the spectrum of the real signal x0,x1,x2, …,xn-1 by removing white noise.

Experimental studies have shown that more efficient is the random generation of the components s0,s1,s2, …,sn-1 of the real component and z0,z1,z2, …,zn-1 of the imaginary component of the spectrum. In this case, the samples of the carrier signal are calculated by the inverse discrete Fourier transform.

5. Evaluation of the developed method effectiveness

Efficiency assessment should include two conditions:

- Security level against illegal access attempts on signal reports, which is determined by the volume of resources required to violate the protection.
- The calculation acceleration coefficient ξ, which is determined by the formula (7). In this formula (7), the value of T0 is replaced by T0′ - the total time for performing the discrete Fourier transform on a remote computer system, which is determined by formula (5) and the time for performing encryption and decryption operations - Tcd: T0′= T0 + Tcd.

As a result of the proposed remote DFT procedure on the user's side, in the process of implementing p.2, we get only n additional operations, as part of formula calculations (10), as well as in the implementation of p. 6 we get 2·n subtractions operations according to the formula (13). All other DFT operations are carried out on a remote computer system. Thus, the numerical value of the time spent on the performing encryption and decryption operations on the user platform Tcd is determined as Tcd = 3·n·ta. Correspondently T0′= T0 + Tcd = tm + ta·(3·n +log2n).

In accordance with formulas (7) the proposed method acceleration factor ξ′ will be calculated as follows:

$$\xi' = \frac{T_1}{T_0'} = \frac{t_m \cdot n^2 + t_a \cdot n \cdot (n-1)}{t_m + t_a \cdot (3 \cdot n + \log_2 n)} . \quad (15)$$

For example, if we take into account that the execution time of the multiplication is about 30 times longer than the execution time of the addition, the numerical value of the acceleration factor ξ' with the proposed method of remotely protected DFT, calculated by formula (15), is $\xi'= 34.6$ for n=8 and $\xi'= 1206$ for n=128.

The real value of the acceleration coefficient ξ'' for the implementation of the discrete Fourier transform when using the proposed method is somewhat lower. This is because the user can apply the Fast Fourier Transform technology. This allows you to significantly reduce the value of T1. The formula for calculating the acceleration coefficient is as follows:

$$\xi'' = \frac{T_1'}{T_0'} = \frac{t_m \cdot n \cdot \log_2 n + t_a \cdot n}{t_m + t_a \cdot (3 \cdot n + \log_2 n)}. \quad (16)$$

Calculated by formula (16) the acceleration factor ξ'' with the proposed method is $\xi''= 26$ for n=8 and $\xi''= 64$ for n=128.

Formulas (15,16) did not take into account the time of data delivery to remote computing systems and the time of returning the results to the user. Full consideration of the corresponding times reduces the real value of the acceleration coefficient ξ. However, in practice it is usually not a single signal that is processed, but a stream of signals. At the same situation, the time of transporting data over the network practically does not affect the rate of signal processing and the real data are close to theoretical estimates by (15,16).

The level of data protection provided by the proposed method is determined by the ability of an attacker to reconstruct them at the place of their processing, that is, on a remote computer system. This means that from the set of samples $\delta 0,\delta 1,\ldots,\delta n-1$ it is necessary to restore set of values of the true signal samples x0,x1,…,xn-1. To do this, he needs to know the set of carrier signal samples b0,b1,…,bn-1. If a different carrier signal are used for each processed signal, then the task of reconstructing the useful signal requires of the resources, the costs of which make this process economically unfeasible for the vast majority of practical applications.

However, in reality, the number of reference signals is limited by the value κ. That can do possible the situation in which the same carrier signal was used for homomorphic encryption of several signals. If the attacker does not know any set of samples of the true signal, then it is practically impractical to reconstruct the rest of the signals.

The situation changes if an attacker in one way or another can obtain information about the value of the X0 signal samples. This possibility can arise if an attacker illegally connects to one of the terminal devices that generate the signal. For example, an attacker can illegally connect to the output of one of the surveillance cameras. In this case, an attacker using set $\delta 0,\delta 1,\ldots,\delta n-1$ can restore the samples of one of the carrier signals: b0,b1,…,bn-1.

Accordingly, an attacker will be able to recover that part of the signals that is encrypted using the specified carrier signal. This attack will be successful only if the attacker is able to match the samples x0,x1,…,xn-1 of the signal X0, which he became aware of with the encrypted sample $\delta 0,\delta 1,\ldots,\delta n-1$.

However, when using modern cloud technologies that redistribute processing tasks across different computer systems, this is difficult to do. Therefore, the attack described above will be more effective if the attacker has control over the data transmission channel. To avoid this situation, additional encryption of the sample streams using streaming or symmetric block ciphers can be recommended.

An effective way to increase the level of data security, over which the discrete Fourier transform is performed remotely, is the use of linear combinations of reference signals for homomorphic encryption.

6. Conclusion

As a result of the research, a new method of the protected discrete Fourier transform implementation on remote computer systems has been proposed. The peculiarity of the developed method is the use of additive encryption. A sequence of pre-formed carrier signals is used as an additive mask. Real and imaginary components that are calculated on the user's computer are used to decrypt the values obtained from the remote system.

As a result of the research, it was proved that parallelization of the calculations of the discrete Fourier transform reduces the processing time of information by one-two oders. Theoretically and experimentally proved the effectiveness of encryption: the resources of modern computer systems do not correspond to the level that is needed to perform the selection of additive mask.

The proposed method can be used effectively in systems that use real-time signal processing.

References

1. Armbrust M. A view of cloud computing / M. Armbrust, A. Fox, R. Griffith, R. Katz, A.A. Konwinski // International Journal Computer Technology.-2013.- No.4.- PP.50-58.
2. Bianchi T. On the Implementation of the Discrete Fourier Transform in the Encrypted Domain / T. Bianchi, A. Piva, and M. Barni // IEEE Transactions on Information Forensics and Security,- 2009.-Vol. 4, - no.1, - PP. 86–97.
3. Nakonechny A.J. Signal processing using modern cloud technologies / A.J. Nakonechny, P.G. Pazan // Visnik of the National University "Lviv Polytechnic", series Automation, measurement and control.-2015.- Vol. 821.- PP.8-16.
4. Texas Instruments. TMS320F2812 Digital Signal Processor. Implementation Tutorial.-2013.- 122 P.
5. Markovskyi O.P. Secure Modular Exponentiation in Cloud Systems/ O.P. Markovskyi, N. Bardis, S.J. Kirilenko // Proceeding of the Congress on Information Technology. Computationnal and Experimental Physics (CITCEP 2015), 18-20 December 2015, Krakow. Poland. – PP.266-269.
6. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – Issue 4. – 2012. – №3. – PP. 169-180.
7. Guduguntla Sandeep, S.P.V.Subba Rao. Radix 4 Fast Fourier Transform Using New Distributive Arithmetic// International Journal of Recent Technology and Engineering.- 2019.- vol. 8.- pp.11-15.
8. Xia Z.. Towards privacy-preserving content-based image retrieval in cloud computing / Z. Xia, Z, Y. Zhu, X. Sun, Z.Qin, K. Ren // IEEE Trans. Cloud Comput. – 2018.- No.6,- PP. 276–286.
9. Hamdi Hassen. Distributed Fast Fourier Transform (DFFT) on MapReduce Model for Arabic Handwriting Feature Extraction Technique via Cloud Computing Technologies / Hamdi Hassen, Khemakhem Maher // IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT).- 2014.- PP.33-39.
10. Li L. Separable Data-Hiding Scheme for Encrypted Image to Protect Privacy of User in Cloud / Lin Li, W.Lifang, S. Tun-Qing, C. Chin-Chen // Symmetry.- 2019,- No.11.- PP. 1-14.
11. Markovskyi O.P. The method of accelerated secure image filtering on remote computer systems / O.P. Markovskyi, I.O.Gymenuk, Alireza Miratаei, J.I. Turoshanko, M.O. Voloshuk // Telecommunication and information technology.- 2019,- Vol.65.-no.4.- PP.99-110.
12. Bujbarova M.F. Method for protected Fourier transforms on remote distributed computer systems / M.F.Bujbarova, Y.M. Vynogradov, V.Y. Priymak // Visnik of National Technical University of Ukraine "KPI" Informatics, Control and Computer Engineering.- 2016.- Vol. 65,- PP.64-71.