Institute of Information and
Computational Technologies

ISSN : 2788-7677 (Online)
ISSN : 2788-7987 (Print)

ADVANCED TECHNOLOGIES AND COMPUTER SCIENCE

2020
№2

www.atcs.iict.kz

Institute of Information and Computational Technologies,

Advanced Technologies and computer science

№2

Almaty 2020

Institute of Information and Computational Technologies,

Advanced Technologies and computer science

The publisher, the authors, and the editors are safe to assume that the advice and information in this journal are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published works and institutional affiliations.

28 Shevchenko str., Almaty,Republic of Kazakhstan
7 (727) 272-37-11
atcs@iict.kz

About the Journal

Advance technologies and computer science is a bilingual scientific peer-reviewed, interdisciplinary, electronic journal of open access, including thematic areas:

- Section **"Applied mathematics, computer science and control theory"** includes papers describing modern problems in these areas.
- Section **"Information and telecommunication technologies"** also includes the following topics:
  - Data transmission systems and networks.
  - Internet technologies.
  - Cloud technologies.
  - Parallel computing.
  - Distributed computing.
  - Supercomputer and cluster systems.
  - Big data processing (Big-data).
  - Geographic Information Systems and Technologies.
- In the section **"Artificial intelligence technologies"** in addition to technology, there are works on topics:
  - Intelligent Management Systems.
  - Speech technology and computer linguistics.
  - Pattern Recognition and Image Processing.
  - Bioinformatics and biometric systems.
  - Human-machine interaction.
  - Machine learning.
  - Intelligent Robotic Systems.
- The section **"Information Security and Data Protection"** also covers topics:
  - Software and hardware information protection.
  - Mathematical methods for ensuring information security of complex systems.
- The section **"Modeling and optimization of complex systems and business processes"** may include:
  - Computational mathematics, numerical analysis and programming, mathematical logic.
  - Theory of Statistics.
  - Statistical Methods.

Editorial Team

Chief Editor

Editorial team

Contents

UDC 004.716

Analysis of eSIM technologies and Wi-Fi offloading algorithms

A.K. Atabekov, K.S. Duisbekova
IIT University, Information System

Importance Nowadays embedded SIM (eSIM) become more popular technology and it aims to overcome the traditions plastic SIM cards, while it is actual technical implementation was developed many years ago. Also data traffic over cellular networks shows the current exponential growth, which is increasing annually by an order of magnitude and has already exceeded voice traffic. This increase in the need for information traffic leads to the fact that light-emitting diodes need solutions to enhance the provision of capabilities, as a result of which offloading traffic to Wi-Fi is one of the ways to increase full capabilities. Despite the fact that offloading on Wi-Fi networks has matured over the years, operators face various problems in realizing this task.

Objectives In this article, we will talk about the meaningful problems when offloading information traffic on a Wi-Fi network. Also, we will investigate eSIM technology, it's processes and its use in practical aspects. How this virtual SIM card technology is used nowadays and in which variations and implementations we can meet it.

Methods The research involves the methods of logical and comparative analysis.

Results Offloading mobile data is expected to become a key industry segment in the near future due to the unprecedented growth rate of data traffic on mobile networks. Wi-Fi offloading has evolved into a mature offloading solution. Most carriers around the world have begun deploying Wi-Fi offload solutions. However, there are a number of problems that must be correctly addressed in order to create a successful unloading mechanism. Key issues include spatial and temporal estimates for unloading, planning and deployment issues, choice of backhaul, device limitations, and charging mechanisms. Such problems can be properly addressed by the joint efforts of all participants in the value chain of mobile data transmission. We can see that there are a high variety of virtual SIM technologies used in different implementations, which are somehow differ in implementation of provisioning and storing SIM profile. During the analysis of virtual SIM technologies it was find out that the most popular and secure for nowadays are eSIM technology for provisioning SIM profiles OTA that was set a new standard related to embedded Subscribed Identity Module. Future work enclosed in the developing of personal router that works on eSIM technology and developing personal algorithm for Wi-Fi offloading to seamless switching between cellular data and Wi-Fi.

Keywords: Wi-Fi offloading, embedded SIM, data traffic, mobile data

Intoduction

The number of smartphone subscription connections at the global level has reached three billion, and within the last 5 years, data traffic has increased over 40-fold. According to a Cisco report [1], smartphone-based data traffic is predicted to exceed eightieth of total knowledge traffic generated on mobile networks by 2020.

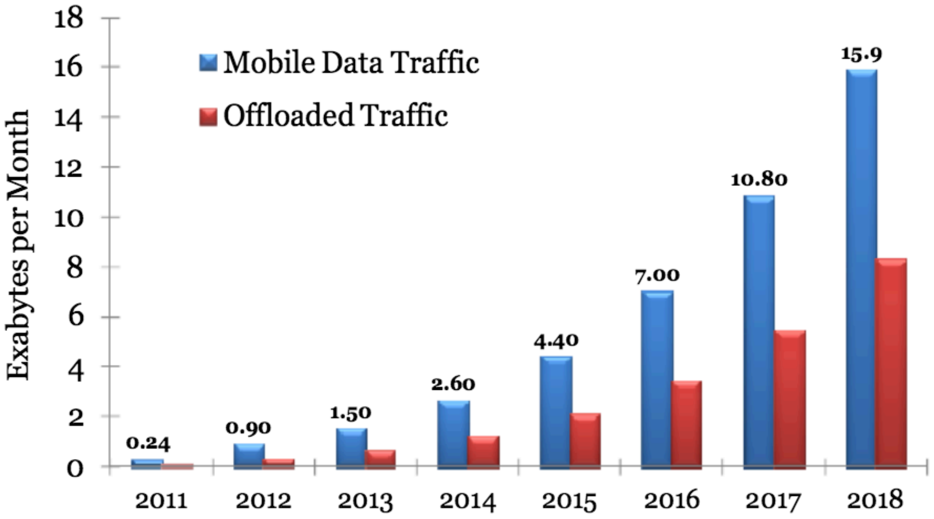


Figure 1 – Global mobile data traffic along with current and predicted offloaded data [1]

This unexampled growth of data traffic may be attributed to variety of things. The widespread adoption of Machine-to-Machine (M2M) [2] technologies across a variety of industries is another conducive issue. Wi-Fi offloading technology transfers part of the cellular network load to Wi-Fi network via the Wi-Fi access points. Network suppliers are searching for methods that specifically offload the cellular data traffic into Wi-Fi (IEEE 802.11) systems to adjust the heap and improve organize execution. A few designs dependent on Proxy Mobile IPv6 (PMIPv6) have been proposed to support seamless mobile data offloading. According to the article “Cellular Meets WiFi: Traffic Offloading or Resource Sharing”[3] traffic offloading and resource sharing are two common methods for delivering cellular data traffic over unlicensed bands. Author in [4] describes SIM evaluation and over the years, the device of physical SIM cards has not changed much. Of course, they decreased in size: Mini-SIM 25 x 15 mm, Micro-SIM 15 x 12 mm, Nano-SIM 12.3 x 8.8 mm. However, SIM cards retained functionality and compatibility, regardless of format. And you still need to insert a small plastic card into your phone or tablet to connect to the mobile network. Every cubic millimeter of a smartphone matters when you try to create increasingly complex electronics. At first they abandoned the 3.5 mm audio jack, now the relative large SIM card to manufacturers seems an anachronism. Phones without SIM cards have existed for a long time - they were used in DAMPS and CDMA-800 networks. However, such devices were tied to the communication standard: it was impossible to change the number or connect to another operator, simply by inserting another SIM-card into your phone. GSM phones without a SIM slot were introduced several years ago. Connecting such devices to mobile communications is carried out without buying an embedded card - the operator and tariff are selected in the device settings. The SIM card in the form of a chip is sealed into the device at the stage of its manufacture. The advantages of such a solution are obvious: when traveling, it’s much easier to switch to the local operator’s network, the problem with different sizes of SIM cards disappears, and even free up space for new smartphone functions. Samsung Gear S2 3G was the first device supporting eSIM (Embedded SIM), however, the technology gained wide popularity after the release of Apple Watch Series 3 (sales of the new model of Apple watches were twice as high as Series 2). Apple's solution could not do without interesting features: eSIM in Watch 3 works only with the iPhone - while the iPhone and Apple Watch must connect to the same mobile operator. Embedded SIM (eSIM) become more popular technology and it aims to overcome the traditions plastic SIM cards, while it is actual technical implementation was developed many years ago. Currently we can see that IOT devices, smart watches and mobile phone manufacturers as Samsung and Apple start to implement the eSIM technology to their products. But there are also other device and gadget manufacturers that start using over the air SIM provisioning technologies. In this article, we will talk about the meaningful problems when offloading information traffic on a Wi-Fi network. Also, we will investigate eSIM technology, it's processes and its use in practical aspects. How this virtual SIM card technology is used nowadays and in which variations and implementations we can meet it.

Materials and methods

The research involves the methods of logical and comparative analysis. For the comparative analysis of virtual SIM technology these technologies were investigated.

Built-in eSIM technology offers an elegant, reliable and virtually infinitely scalable solution for legacy SIM card calls in IoT applications. ESIM is still a physical SIM, but instead of being removable, it is constantly soldered to the device. Authorized users can access profiles and other data in eSIM and update them using a wireless SIM card provisioning (RSP) solution[5]. The problem of SIM cards exists not only for smartphones, but also for smart things. Therefore, ARM has developed iSIM for all IoT devices. New technology allows you to embed a SIM card in processors to save even more space. The developed ARM card occupies "a fraction of one square millimeter." For comparison, eSIM, although smaller than nano-SIM, still occupies 6 x 5 mm of space in the phone. The technology is intended primarily for small IoT devices - for example, for wireless sensors that need to transmit data using mobile communications. ARM's goal is to minimize the cost of these products. In the future, technology can be used in other devices, including smartphones. eSIM and iSIM solves the problems that current physical SIM card solution has:

- Small in size. 5 × 6 millimeters ESIM is about half the size of a Nano SIM card, which is 12 × 8.8 millimeters. iSIM measures in nanometers, part of a Nano SIM card. This further reduction in size gives device manufacturers greater design flexibility and reduces their manufacturing costs.
- Can be controlled remotely. You can remotely manage profiles to change networks or update settings on virtually any number of eSIM devices using RSP technology.
- Proof of hacking. You cannot quit and accidentally step on eSIM.
- Proof of theft. You cannot steal eSIM.

It can be argued that eSIM was a revolutionary innovation, as it significantly reduced the cost and complexity of managing physical SIM cards, which makes IoT scalable. As a result, companies that deploy a large number of IoT devices are not tied to their original network operator or its pricing and access policies. iSIM strengthens and expands these and other qualities, and also eliminates some of the disadvantages of eSIM. The main innovation of iSIM is that it transfers the functionality of the SIM card to the device's permanent hardware array. However, unlike eSIM, iSIM no longer uses a separate processor; nor does it require a significant fraction of the hardware footprint of the device[6]. Instead, iSIM allows equipment manufacturers and processor companies to design system-on-a-chip (SOC) architectures that combine the functionality of a SIM card with an existing embedded processor and cellular modem[7]. There are also another implementations such as softSIM and cloudSIM. SoftSIM are a conceptual capability in a device. It can be provisioned remotely over the air. There is no SIM at all in the divice. The provisioning information is held in memory as a part of other computing equipment. Most of phone companies are against these because they are perceived as more exposed of question of hacking. But currenltly we can see softSIM solution from KnowRoaming company that is implemented in ZTE and Alcatel phones. Building on SIM Security Benefits eSIM offers another major enhancement that benefits every mobile device: security. Physical SIM cards have always been more secure than software standards, since hardware systems are inherently more difficult to crack. eSIM and iSIM are difficult to steal, which increases the reliability and integrity of the devices that use them. iSIM then relies on eSIM and SIM security credentials. Located in a secure enclave in a system-on-a-chip (SoC) system, it provides the root of confidence for the mobile network, made possible by an additional level of authentication. This reuse is especially useful in payment, identification, and critical infrastructure applications. The advantage of iSIM it all comes down to cost because iSIM devices require fewer components, assembling them is cheaper. And, as a rule, the simpler design of iSIM also leads to the creation of more reliable and, therefore, less expensive devices. Per unit cost advantage of iSIM can be small. But when an organization purchases hundreds of thousands of IoT devices at the same time, such a small cost reduction can result in significant savings. The cost advantage of iSIM is becoming more important given the growing market for IoT devices, which must be very small, reliable, and inexpensive to use.

Results

Offloading mobile data is expected to become a key industry segment in the near future due to the unprecedented growth rate of data traffic on mobile networks. Wi-Fi offloading has evolved into a mature offloading solution. Most carriers around the world have begun deploying Wi-Fi offload solutions. However, there are a number of problems that must be correctly addressed in order to create a successful unloading mechanism. Key issues include spatial and temporal estimates for unloading, planning and deployment issues, choice of backhaul, device limitations, and charging mechanisms. Such problems can be properly addressed by the joint efforts of all participants in the value chain of mobile data transmission. We can see that there are a high variety of virtual SIM technologies used in different implementations, which are somehow differ in implementation of provisioning and storing SIM profile. During the analysis of virtual SIM technologies it was find out that the most popular and secure for nowadays is eSIM technology for provisioning SIM profiles OTA that was set a new standard related to embedded Subscribed Identity Module. But we should keep in mind the cost advantage of iSIM is becoming more important given the growing market for IoT devices, which must be very small, reliable, and inexpensive to use. Future work enclosed in the developing of personal router that works on eSIM technology and developing personal algorithm for Wi-Fi offloading to seamless switching between cellular data and Wi-Fi.

References

[1] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2018-2023. Date Views 02.06.2019 www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[2] Wu, G., Talwar, S., Johnsson, K., Himayat, N., Johnson, K. D., 2017. M2M: From Mobile to Embedded Internet. IEEE Communications Magazine, 49(4).

[3] Qimei, C., Y. Guanding, S. Hangguan, M. Amine and Y. Geoffrey, 2018. Cellular Meets WiFi: Traffic Offloading or Resource Sharing?. IEEE Transactions on Wireless Communications, 15(5): 3354-3367.

[4] Vahidian, E., Evolution of the SIM to eSIM, NTNU Norwegian University of Science and Technology, Jan. 21, 2013, core.ac.uk/download/pdf/52107393.pdf.

[5] GSMA embedded sim specification - a single common and global specification to accelerate growth in m2m. Date Views 01.03.2020 www.gsma.com/iot/wp-content/uploads/2014/10/GSMA-Embedded-SIM-Specification-flyer.pdf.

[6] Unlocking Secure IoT Device Connectivity with iSIM. Date Views 04.03.2020 www.gsma.com/esim/blog-from-arm-unlocking-secure-iot-device-connectivity-with-isim.

[7] ARM Glossary – eSIM, iSIM and remote SIM provisioning. Date Views 03.03.2020 www..arm.com/glossary/esim-isim.

UDC 004.056
IRSTI 81.93.29

Pipeline multiplier of polynomials modulo with analysis of high-order bits of the multiplier

M. Kalimoldayev[1], S. Tynymbayev[2], M. Ibraimov[3], M. Magzom[1], Y. Kozhagulov[3], T. Namazbayev[3], Waldemar Wójcik[4]

[1]Institute of Information and computational technologies, Almaty, Kazakhstan,
[2]Almaty University of Power Engineering and Telecommunication, Almaty, Kazakhstan,
[3]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[4]Lublin Technical University, Poland

ORCID iD and E-mail: 0000-0003-0025-8880, mnk@ipic.kz; 0000-0002-9326-9476, s.tynym@mail.ru; 0000-0002-8049-3911, margulan.ibraimov@kaznu.kz; 0000-0002-9380-1469, magzomxzn@gmail.com; 0000-0001-5714-832X, kazgu.kz@gmail.com; 0000-0002-2389-2262, tirnagog@mail.ru, waldemar.wojcik@pollub.pl

Abstract. Among public-key cryptosystems, cryptosystems built on the basis of a polynomial system of residual classes are special. Because in these systems, arithmetic operations are performed at high speed. There are many algorithms for encrypting and decrypting data presented in the form of polynomials. The paper considers data encryption based on the multiplication of polynomials modulo irreducible polynomials. In such a multiplier, the binary image of a multiply polynomial can serve as a fragment of encrypted text. The binary image of the multiplier polynomial is the secret key and the binary representation of the irreducible polynomial is the module.

Existing sequential polynomial multipliers and single-cycle matrix polynomial multipliers modulo do not provide the speed required by the encryption block. The paper considers the possibility of multiplying polynomials modulo on a Pipeline in which architectural techniques are laid in order to increase computing performance.

In the conclusion of the work, the time gain of the multiplication modulo is shown by the example of the multiplication of five triples of polynomials. Verilog language was used to describe the scheme of the Pipeline multiplier. Used FPGA Artix-7 from Xilinx companies.

The developed Pipeline multiplier can be used for cryptosystems based on a polynomial system of residual classes, which can be implemented in hardware or software.

Keywords: Polynomial system of remainder classes, irreducible polynomials, remainder former, Pipeline modular multiplier.

Introduction

There are two approaches to multiplying polynomials modulo. At the first approach, multiplying modulo in two stages is performed [1, 2]. At the first stage, polynomials are multiplied, at the second stage, polynomials multiple by irreducible polynomials modulo. If at the first stage of multiplication polynomials are possible to accelerate on matrix circuits, then the accelerated of them multiplying modulo is difficult. At the second approach, process of multiplying modulo is divided into steps, and at each step of the multiplication polynomials is combined with the operation of reduction irreducible polynomials modulo. While, of multiplying polynomials are performed on a sequential circuit starting with the analysis of high-order [3] or left-most [4] bits of the polynomial multiplier.

To improve performance, one-clock multipliers of polynomials modulo with a matrix structure were developed [5, 6].

The matrix structures of parallel multipliers have the potential improving performance - the possibility of pipelining, which is a prospective architectural technique [7].

Main part

During pipelining, the multiplying operation is divided into a finite number of sub-operations, and each sub-operation is performed at its own Pipeline stage, with all Pipeline stages are working of parallel. The results obtained at the *i* - th stage are transferred for further processing to the (*i*+1)-th Pipeline stage. Transmit of information from stage to stage is through the buffer memory located between them.

A stage that have accomplished of its sub-operation remember the result in the buffer memory and can start processing the next portion of the sub-operation data, while the next Pipeline stage uses the data stored in the buffer memory located at its output. Synchronization of the Pipeline is provided by clock pulses, the period of which is determined by the slowest Pipeline stage and the delay in the buffer memory element.

In a Pipeline multiplier of N stages, the multiplying data modulo can be input with an interval of N times less than for a matrix multiplier. Output results appear at the same pace.

A diagram of an N-stage of the Pipeline for multiplying a polynomial-multiplicand A(x) by a polynomial-multiplier B(x) modulo an irreducible polynomial P(x) shown in Figure 1.

The first Pipeline stage contains logical block diagram AND1 and buffer registers RgA.1, RgR_0, RgB.1and RgP.1. The second and next Pipeline stages contain logical blocks-former of partial remainders ($PRF_N \div PRF_{N-1}$). The second and other Pipeline stages have individual buffer registers. For example, the buffer registers of the second Pipeline stage are the registers RgA.2, RgR_1, RgB.2 and RgP.2. The buffer register of the N-stage is the Rg.N-1 register, in this diagram the registers RgA, RgB and RgP are the input Pipeline registers, where before the start of operations on the next triples of polynomials $A(x)_i$, $b(x)_i$ and $P(x)_i$, the *i*-th triple of polynomials is accepted.

Upon the first clock pulse CP1 is provided, the first triple of polynomials A, B, P from the input registers are transferred to the first stage of buffer registers. In the process this transfer, the contents input register RgA logical are multiplied by the high-order bit b_{i-1} polynomial-multiplier $B_1(x)$. The result of operations $A_1(x)\&b_{i-1}=R_0$ written to the first stage of buffer register RgR_0, and $A_1(x)$, $P_1(x)$ are accepted in the RgA.1 and RgP.1 registers.

According to the clock signal CP1, the second triple of polynomials A2(x), B2(x) and P2(x) are received to place of the first triples $A_1(x)$, $B_1(x)$ and $P_1(x)$ in the input registers. Upon the signal CP2 is provided, the contents of the input registers are transferred to the first stage of buffer registers, the contents of the first stage are transferred to the second stage of buffer registers RgA.2, RgR_1, RgB.2 and RgP.2. While, in the first Pipeline stage operation $A_2(x)\ \&b_{i-1} = R_0$ is performed, reaches in RgR register. The buffer registers RgA.1, RgP.1 will receive the corresponding contents of RgA (A_2) and RgP (P_2).

During the action of the second pulse of CP2 in PRF.1, the operation and the calculation of the remainder $R_1 = (2R_0 \oplus A_1\&b_{i-2}) \bmod P_1$ saved in the buffer register RgR_1 are performed.

The clock signal CP2 into the input registers receives the polynomials of the third triples of polynomials $A_3(x)$, $B_3(x)$ and $P_3(x)$. Upon the third clock signal CP3 is provided, the third triples of polynomials $A_3(x)$, $B_3(x)$ and $P_3(x)$, will be processed by the logical blocks of the first stage (AND1), the second triples of polynomials $A_2(x)$, $B_2(x)$, and $P_2(x)$, will be processed by the logical blocks of the second stage PRF.1, the logic blocks of the third stage PRF.2 will process the first triples of polynomials $A_1(x)$, $B_1(x)$ and $P_1(x)$.

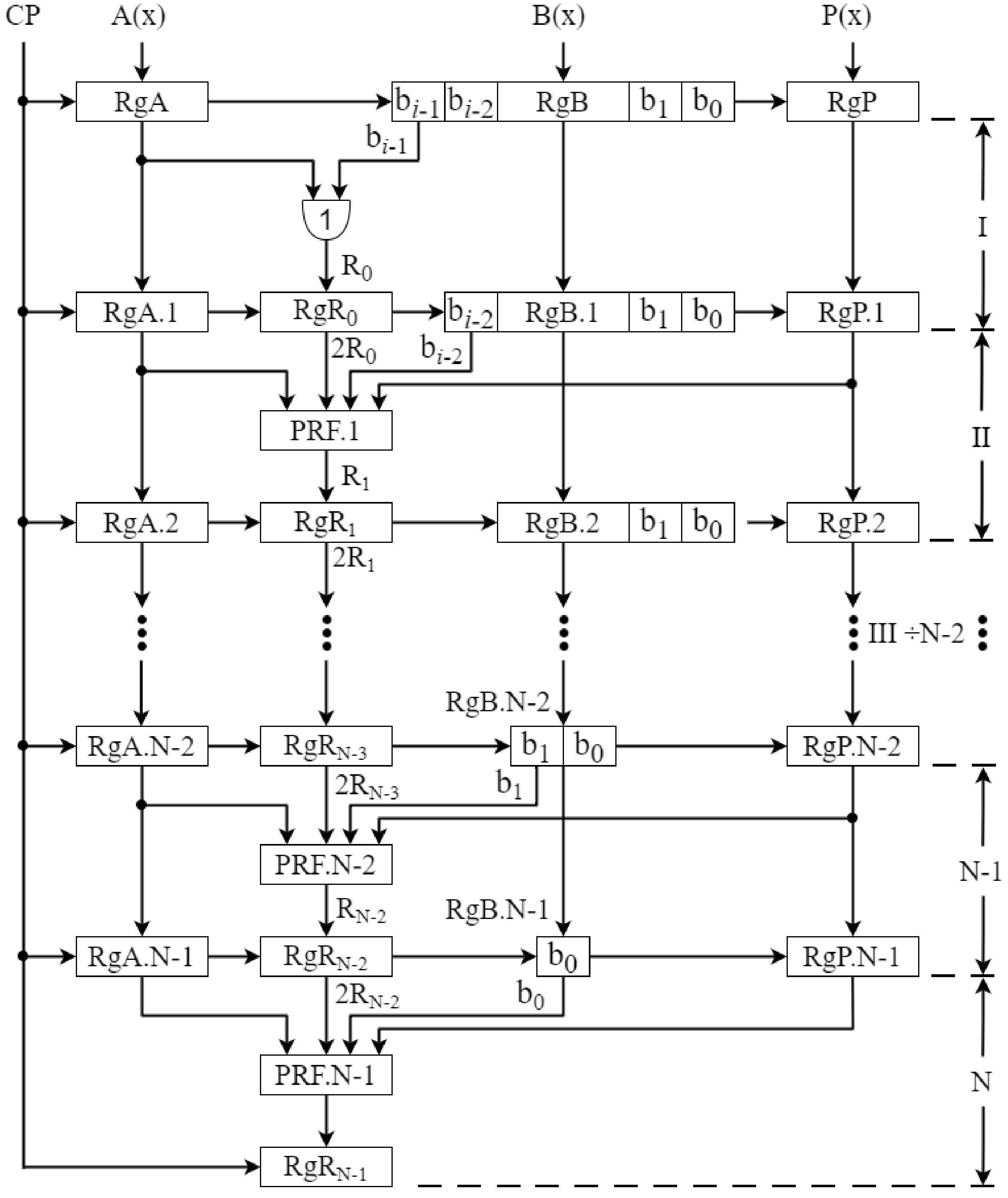


Figure 1 – Pipeline multiplier of polynomials modulo starting with analysis of high-order bit of the multiplier

Upon the N-clock pulse CP.N is provided, the contents of the input registers polynomials $A_N(x)$, $B_N(x)$ and $P_N(x)$ will reaches to the first stage buffer registers, the contents of the first stage buffer registers to the second stage buffer registers, etc.

The results of processing the polynomials $A_1(x)$, $B_1(x)$ and $P_1(x)$ from the N-1 stage buffer registers will moved to the N-stage buffer register – Rg.N-1, while in PRF.N-1

$R_{N-1} = [(2R_{N-1} \oplus A_1(x)\&b_0)]mod P_1$ is calculated, which is the result of multiplying modulo $[A_1(x)*B_1(x)]modP_1(x)$. The input registers receive the triples of polynomials $A_{N+1}(x)$, $B_{N+1}(x)$ and $P_{N+1}(x)$ with a clock signal CP.N.

Upon the clock pulses N+1, N+2, N+3, etc. is provided on the output Pipeline register Rg.N-1, the results of multiplying of triples of polynomials will be formed:

$$R_{N-1} = [A_{N+1}(X) * B_{N+1}(X)]\ mod\ P_{N+1}$$
$$R_{N-1} = [A_{N+2}(X) * B_{N+2}(X)]\ mod\ P_{N+2}$$
$$\vdots$$
$$R_{N-1} = [A_{N+k}(X) * B_{N+k}(X)]\ mod\ P_{N+k}$$

Figure 2 shows the structure of the PRF*i*. The central adder modulo 2 is the Add.2 adder.

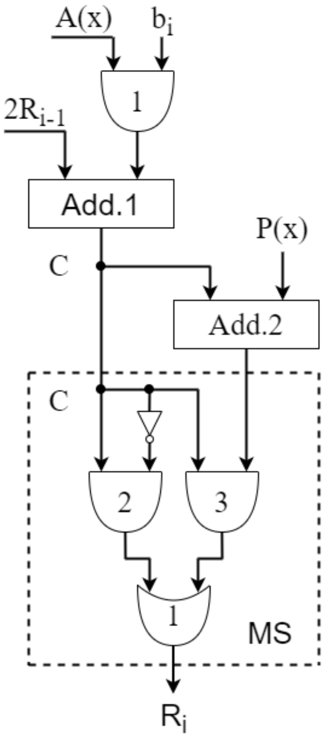


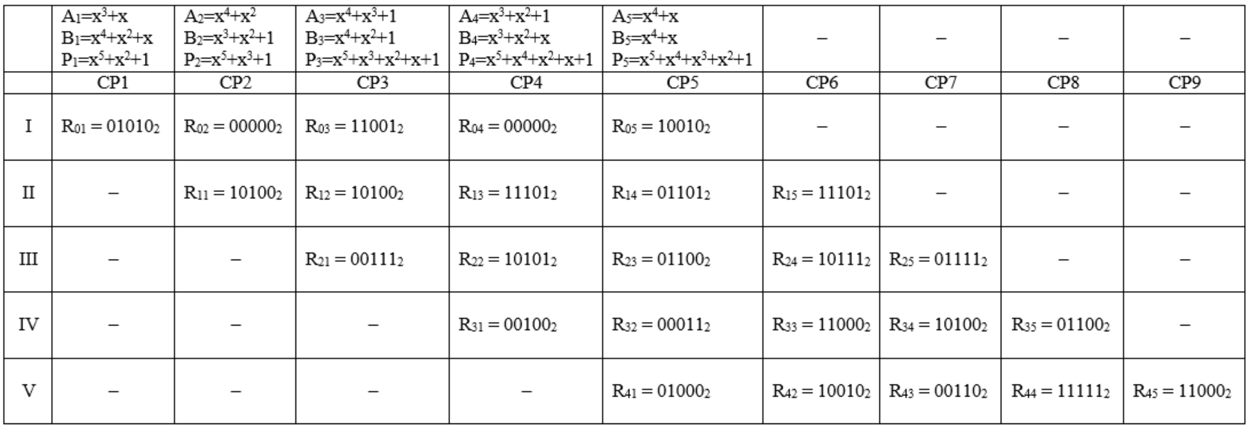
Figure 2 – PRF*i* structure

The results of the sum modulo of two $2R_{i-1} \oplus A(x)b_i$ is provided to the left inputs is performed by the adder modulo of two Add.1. The value of P (x) is provided to the right inputs of Add.2. If, at the same time $C = 2R_{i-1} \oplus A(x)b_i > P(x)$ then in the high-order bit of the sum C the value $C_h = 1$ is formed. With this signal, block of diagram AND3, the result of adding $C \oplus P(x)$ at the output of Add.2 forming R_i is output. If $C = 2R_{i-1} \oplus A(x)b_i < P(x)$, $C_h = 0$. Then the value $C = 2R_{i-1} \oplus A(x)b_i$ by the signal $C_h = 1$ by the block of diagram AND2 the output is $C = R_i$.

Consider the example of multiplying polynomials modulo on a five-stage Pipeline. Let:

$A_1 = x^3+x = 01010_2$; $B_1 = x^4+x^2+x = 10110_2$; $P_1 = x^5+x^2+1 = 100101_2$;
$A_2 = x^4+x^2 = 10100_2$; $B_2 = x^3+x^2+1 = 01101_2$; $P_2 = x^5+x^3+1 = 101001_2$;
$A_3 = x^4 + x^3 + 1 = 11001_2$; $B_3 = x^4 + x^2 + 1 = 10101_2$; $P_3 = x^5+x^3+x^2+x+1 = 101111_2$;
$A_4 = x^3 + x^2 + 1 = 01101_2$; $B_4 = x^3 + x^2 + x = 01110_2$; $P_4 = x^5 + x^4 + x^2 + x + 1 = 110111_2$;
$A_5 = x^4 + x = 10010_2$; $B_5 = x^4 + x = 10010_2$; $P_5 = x^5 + x^4 + x^3 + x^2 + 1 = 111101_2$.

The results of multiplying polynomials $A_1(x) \div A_5(x)$ by $B_1(x) \div B_5(x)$ modulo $P_1(x) \div P_5(x)$ are shown in figure 3.



	$A_1=x^3+x$ $B_1=x^4+x^2+x$ $P_1=x^5+x^2+1$	$A_2=x^4+x^2$ $B_2=x^3+x^2+1$ $P_2=x^5+x^3+1$	$A_3=x^4+x^3+1$ $B_3=x^4+x^2+1$ $P_3=x^5+x^3+x^2+x+1$	$A_4=x^3+x^2+1$ $B_4=x^3+x^2+x$ $P_4=x^5+x^4+x^2+x+1$	$A_5=x^4+x$ $B_5=x^4+x$ $P_5=x^5+x^4+x^3+x^2+1$	–	–	–	–
	CP1	CP2	CP3	CP4	CP5	CP6	CP7	CP8	CP9
I	$R_{01} = 01010_2$	$R_{02} = 00000_2$	$R_{03} = 11001_2$	$R_{04} = 00000_2$	$R_{05} = 10010_2$	–	–	–	–
II	–	$R_{11} = 10100_2$	$R_{12} = 10100_2$	$R_{13} = 11101_2$	$R_{14} = 01101_2$	$R_{15} = 11101_2$	–	–	–
III	–	–	$R_{21} = 00111_2$	$R_{22} = 10101_2$	$R_{23} = 01100_2$	$R_{24} = 10111_2$	$R_{25} = 01111_2$	–	–
IV	–	–	–	$R_{31} = 00100_2$	$R_{32} = 00011_2$	$R_{33} = 11000_2$	$R_{34} = 10100_2$	$R_{35} = 01100_2$	–
V	–	–	–	–	$R_{41} = 01000_2$	$R_{42} = 10010_2$	$R_{43} = 00110_2$	$R_{44} = 11111_2$	$R_{45} = 11000_2$

Figure 3 – The results of multiplying polynomials $A_1(x) \div A_5(x)$ by $B_1(x) \div B_5(x)$ modulo $P_1(x) \div P_5(x)$

From this figure 3

$R_{41} = [A_1(x) \cdot B_1(x)]$ *mod* $P_1 = 01000_2$, is corresponds to a polynomial: $R_{41} = x^3$;
$R_{42} = [A_2(x) \cdot B_2(x)]$ *mod* $P_2 = 10010_2$, is corresponds to a polynomial: $R_{42} = x^4 + x$;
$R_{43} = [A_3(x) \cdot B_3(x)]$ *mod* $P_3 = 00110_2 = x^2 + x$;
$R_{44} = [A_4(x) \cdot B_4(x)]$ *mod* $P_4 = 11111_2 = x^4 + x^3 + x^2 + x + 1$;
$R_{45} = [A_5(x) \cdot B_5(x)]$ *mod* $P_5 = 11000_2 = x^4 + x^3$.

In this figure 3, R_{ij} are the numbers of intermediate remainders $i(i = 0 \div 4)$ and the numbers of triples of numbers j, where $j = 1 \div 5$.Consider the time value. The multiplying time of polynomials without a Pipeline is determined by the formula:

$$T_{w.c} = NKT_K,$$

where K – the number of triples of polynomials to be multiplying,
N – The number of Pipeline stages,
T_K – the duration of the clock period, which is determined by the ratio $T_K = T_{PRF} + T_{BRg}$,
where T_{PRF} – partial remainder formation time,
T_{BRg} – time of recording of the processing results to buffer registers.

The runtime of operations on K input polynomial streams (triples of polynomials) at N Pipeline stages or with a clock period T_K is determined by the ratio [9]:

$$T_{NK} = \big(N + (K - 1)\big)T_K.$$

The time value is determined by the formula:

$$C = \big(NK - (N + K - 1)\big)T_K.$$

For our example,

$$C = \big(NK - (N + K - 1)\big)T_K = (25 - 9)T_K = 16T_K$$

The timing diagram and the results of the multiplying modulo the above triples of numbers on a five-stage Pipeline are shows in Figure 4. Verilog HDL is used to describe the circuit of the Pipeline multiplier. Artix-7 from Xilinx as the Field Programmable Gate Array (FPGA) was chosen.

As shown in the Figure 4, the first triple of polynomials $A_1(x)$, $B_1(x)$, $P_1(x)$ from the Pipeline input registers to the buffer registers of the first stage with the first clock signal CP1 are transferred. In this case, the partial remainder $R_{01} = 01010_2$ is calculated by the logical block of the first stage.

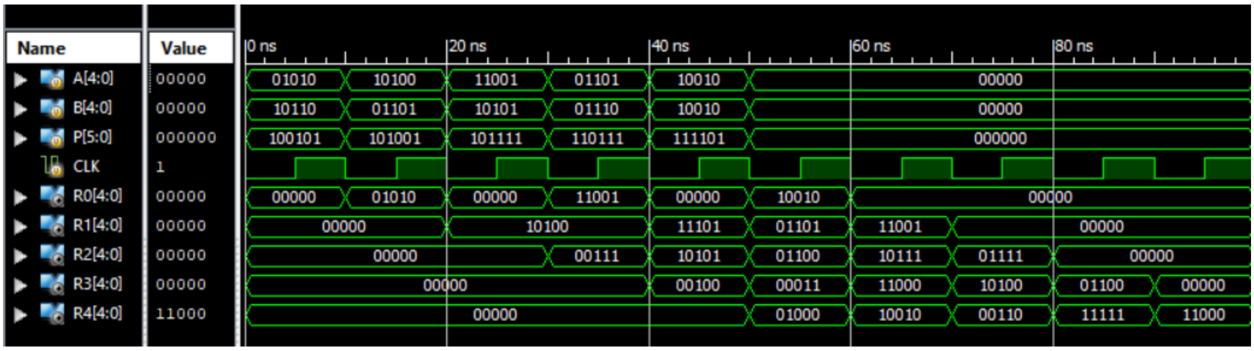


Figure 4 – The timing diagram of the Pipeline circuit

During the action of the second clock signal CP2, the second triple of polynomials $A_2(x)$, $B_2(x)$, $P_2(x)$ from the Pipeline input registers are transferred to the first stage buffer register, the contents of the first stage buffer registers are transferred to the second stage buffer registers. In this case, at the first stage $R_{02} = 00000_2$, at the second stage of the Pipeline, the remainder $R_{11} = 10100_2$ is calculated.

Upon the third clock pulse CP3 is provided from the Pipeline input registers, the triple of polynomials $A_3(x)$, $B_3(x)$, $P_3(x)$ are transferred to the first stage buffer registers, the contents of the first stage buffer registers are transferred to the second stage buffer registers, also the contents of the second stage buffer registers are transferred to the third stage buffer registers. While, a partial remainder $R_{03} = 11001_2$ is formed in the first stage of the Pipeline, $R_{12} = 10100_2$ and $R_{21} = 00111_2$ respectively are formed in the second and third stages of the Pipeline.

After the fourth clock pulse CP4 is provided, triple of polynomials $A_4(x)$, $B_4(x)$, $P_4(x)$ enter the inputs of the first stage of the Pipeline, the partial remainder $R_{04} = 00000_2$ is calculated of the first stage of the Pipeline, the remaining residues $R_{13} = 11101_2$, $R_{22} = 10101_2$, $R_{31} = 00100_2$ are formed on the other three stages.

Upon the fifth pulse CP5 is provided, triple of polynomials $A_5(x)$, $B_5(x)$, $P_5(x)$ enter the inputs of the first stage of the Pipeline, and at the first, second, third and fourth stages partial remainders $R_{05} = 10010_2$, $R_{14} = 01101_2$, $R_{23} = 01100_2$, $R_{32} = 00011_2$, $R_{41} = 01000_2$ are formed.

Upon the sixth pulse CP6 is provided to the inputs of the first stage of the Pipeline, polynomials are not provided and the remainders $R_{15} = 11101_2$, $R_{24} = 10111_2$, $R_{33} = 11000_2$, $R_{42} = 10010_2$ are formed on the corresponding 2, 3, 4, 5 stages of the Pipeline.

After the seventh pulse CP7 is provided the remainders $R_{25} = 01111_2$, $R_{34} = 10100_2$, $R_{43} = 00110_2$ in the 3, 4, 5 stages of the Pipeline are calculated.

The eighth clock pulse CP8 the remainders $R_{35} = 01100_2$, $R_{44} = 11111_2$ in stages 4, 5 are formed.

The ninth clock pulse CP9 completes the work of the Pipeline and in the fifth stages of the Pipeline the remainder R_{45} is calculated, which is the result $R_{45} = [A_5(x) * B_5(x)]modP_5(x)$.

Pipeline multiplier of polynomials modulo with analysis of high-order bits of the multiplier

M. Kalimoldayev, S. Tynymbayev, M. Ibraimov, M. Magzom,
Y. Kozhagulov, T. Namazbayev, Waldemar Wójcik

REFERENCES

1. Magzom M. *Development and research of cryptosystems for information security in decentralized networks.*PhD Dissertation [Razrabotka i issledovanie kriptosistem zashchity informatsii v detsentralizovannykh setiakh. PhD Dissertation]. -Almaty, 2017 (In Russian)

2. Tynymbayev S., Kapalova N. Polynomial multipliers on the module of irreducible polynomials sequential action [Umnozhitel' polinomov po moduliu neprivodimykh polinomov posledovatel'nogo deistviia]. *Materials of the 2nd international scientific-practical conference "Informatics and applied mathematics"*. Almaty 2017 (In Russian)

3. Kalimoldayev M., Tynymbaev S., Magzom M., Ibraimov M., Khokhlov S., Sydorenko V. Polynomials Multiplier under Irreducible Polynomial Module for High-Performance Cryptographic Hardware Tools. *Proc. Of 15th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer*. Kherson, Ukraine, June 12-15, 2019,pp. 729-757

4. Kalimoldayev M., Tynymbayev S., Kapalova N. Polynomial multipliers on the module of irreducible polynomials. *Bulletin of National Academy of Sciences of the Republic of Kazakhstan.* Volume 4, Number 368 (2017), pp. 48-53

5. Kalimoldayev M., Tynymbayev S., Gnatyuk S., Ibraimov M., Magzom M. The device for multiplying polynomials modulo an irreducible polynomial. *News of The National Academy of Sciences of the Republic of Kazakhstan Series of Geology and Technical Sciences.* Volume 2, Number 434 (2019), pp. 199-205

6. Tynymbayev S., Berdibayev R., Omar T., Gnatyuk S., Namazbayev T., Adilbekkyzy S. Devices for multiplying modulo numbers with analysis of the lower bits of the multiplier. *Bulletin of National Academy of Sciences of the Republic of Kazakhstan.* Volume 4, Number 380 (2019), pp. 38-45

7. Tsil'ker, B. Ia., & Orlov, S. A. (2011). *Organization of computers and systems: A textbook for high schools* [Organizatsiia EVM i sistem: Uchebnik dlia vuzov]. SPb.: Piter, 2011. 688 p. (In Russian)

IRSTI 49.40.01
UDC 004.92

Using wavelet transform in image processing

E. Daiyrbayeva[2], F. Murzin[3], A. Yerimbetova [1,2], A. Toigozhinova[2]
[1]Institute of Information and Computational Technologies,Almaty, Kazakhstan
[2]Kazakh academy of transport and communications named after M. Tynyshpaev,
Almaty, Kazakhstan
[3]A.P. Ershov Institute of Informatics Systems SB RAS, Novosibirsk, Russia
[1]nurbekkyzy_e@mail.ru, [3]aigerian@mail.ru,[4]aynur_t@mail.ru
[1]ORCID ID: https://orcid.org/0000-0002-4255-5456
[2] ORCID ID: https://orcid.org/0000−0002−4644−5406
[3]ORCID ID: https://orcid.org/0000-0002-2013-1513
[4]ORCID ID: https://orcid.org/0000-0002-0305-2776

Abstract. At the present stage of globalization, the problem of information security remains relevant. It is necessary to commend the work of scientists in the areas of the possibility of delivering information in a confidential form by various methods. This issue is one of the priority areas in the field of steganography.

This article discusses the possibility of using a wavelet transform for processing (improving) digital images by transferring them to the transformation domain, and after processing - restoration using the inverse transformation operation. Computer image processing involves the processing of digital images using a PC or specialized devices built on digital signal processors. In this case, image processing is understood not only to improve the visual perception of images, but also to classify objects that are performed during image analysis.

The wavelet transform provides the most visual and informative picture of the results of the experiment, allows you to clear the original data from noise and random distortions, and even "by eye" to notice some features of the data and the direction of their further processing and analysis.

Keywords: images, wavelet transform, noise, steganography.

New efficient methods of image processing became possible with the development of the theory of wavelets, which, in comparison with the Fourier transform, allow us to represent with much greater accuracy the smallest features of functions, images and signals, up to discontinuities of the first kind (jumps), with their binding to time or space coordinates. The term "wavelet" was introduced by Alex Grossman and Jean Morlet in the mid-1980s in relation to the analysis of seismic and acoustic signals. Currently, wavelets are used in image recognition tasks, in the processing and synthesis of various signals, in the analysis of images of different nature, for compressing large amounts of information.

Wavelet (born of wavelet - small wave, ripple,. also a surge, often - wavelet) - a mathematical function that analyzes the different frequency components of the data. The graph of the function looks like wave-like oscillations with amplitude decreasing to zero far from the origin.

The ideas of the theory of wavelets arose when a sufficient number of experimental data series appeared, the processing of which by the standard and well-developed method of the Fourier transform showed its limitations for finding regularities in them.The rapid development of computer technology also played a role, which made it possible to numerically solve such problems that were simply inaccessible before.

Practically important wavelets are traditionally defined as functions of a single real variable with real values. Depending on the mathematical model (structure, scope, structure the field of possible values and transformations) distinguish between discrete and continuous wavelets. Since the decomposition of signals in the wavelet basis is carried out using floating-point arithmetic, errors occur, the magnitude of which depends on the degree of approximation of the signal.

Using wavelet transform in image processing

E. Daiyrbayeva, F. Murzin, A. Yerimbetova, A. Toigozhinova

Images of various types are increasingly being used both for scientific and applied purposes and in everyday life. Many information transformation and data analysis tasks involve image processing and transmission. Accuracy of results depends on image quality.

Digital imaging continues to evolve today. In many industrial and scientific-applied fields, there are various tasks of digital image processing. Many questions have a complete solution. This refers to the problems of filtering, segmentation, object recognition in images, multimedia information processing, and digital television signal evaluation [1].

In computer systems, when the recipient of information is a person, methods of image enhancement are of great importance, which make it possible to increase the visibility of interesting details in the image. In addition, in the preprocessing of images performed in automatic computer systems, preprocessing of images also plays an important role, which makes it possible to form the space of objects' attributes [2].

The images obtained at the output of the optoelectronic converters are distorted by noise. When analyzing objects against a complex background, the background is also a hindrance. The weakening of interference is achieved by filtering. Filtering is done in the spatial or frequency domain, depending on the application.

Computer image processing involves processing digital images using computers or specialized devices based on digital signal processors. In this case, image processing is understood not only to improve the visual perception of images, but also to classify objects, performed in the analysis of images [3].

To carry out digital image processing, it is necessary to convert the continuous (analog) image signal into a digital array. This transformation involves performing two transformations. The first transformation is the replacement of a real continuous image with a set of samples at discrete times, such a transformation is called sampling. The second is the transformation of a continuous set of image signal values into a set of quantized values, such a transformation is called quantization.

The main stages of digital image processing are shown in fig. 1.

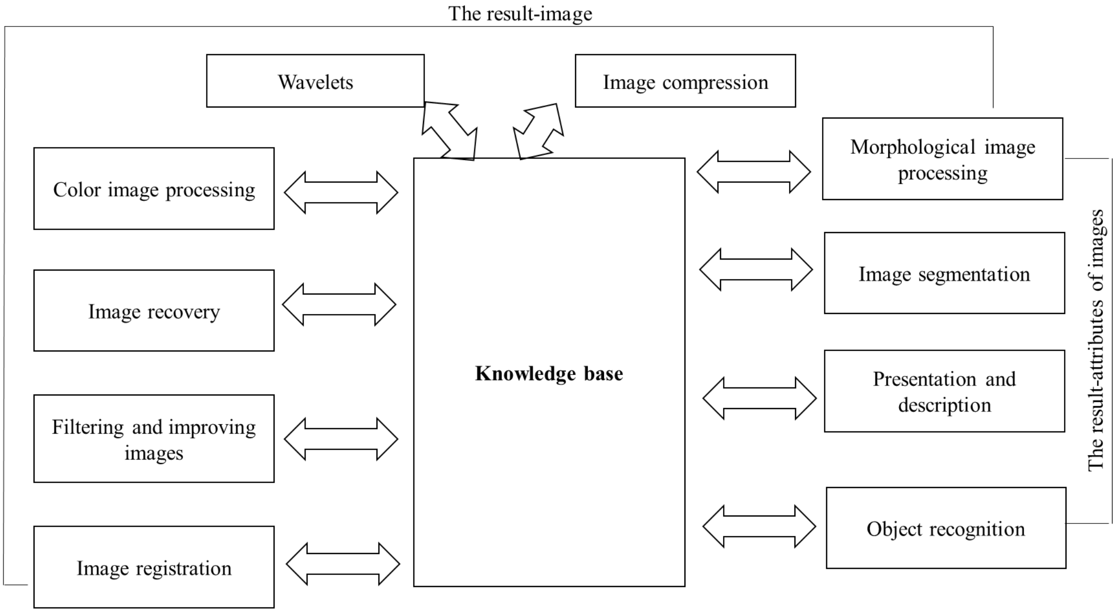


Figure - 1. Main stages of digital image processing

Analyzing the literature in this area, we can identify the following: the almost complete absence of methods for embedding compression-resistant multimedia data. One of the transformations that allows such embedding is the discrete wavelet transform [2,3]. As is known, a set of wavelets in their time or frequency representation can approximate a complex signal or image, both perfectly accurate and with some error. Wavelets have clear advantages in representing local features of functions and implicitly taking into account the features of the psychophysiological model of perception. Because of this, they are widely used for feature analysis, compression, and reconstruction of complex signals. We show that their application in the development of a steganography method focused on achieving maximum throughput (hidden transmission and storage of information) can solve the main problems of steganography, namely: minimizing introduced distortions and resistance to attacks by a passive attacker [4].

Wavelets are a generalized name for temporal functions that have the form of wave packets of one form or another, localized along the axis of the independent variable (t or x) and capable of shifting along it or scaling (compression-stretching). Wavelets are created using special basic functions - prototypes that specify their type and properties [5].

An image consisting of two dots with $\{x_1, x_2\}$. brightness is used. These values can be replaced by the mean a and half-difference d:

$$a = \frac{(x_1 + x_2)}{2}, d = \frac{(x_1 - x_2)}{2}$$

The "wavelet transform" of the original $\{x_1, x_2\}$ sequence is the $\{a, d\}$ sequence, knowing which you can restore the original values

$$x_1 = a + d, x_2 = a - d$$

In this view, information is not added or lost. But such a replacement can be useful if the values of x_1 and x_2 are close. In this case, the difference d is small and less memory can be used to store it, or you can drop d altogether and replace the "image" $\{x_1, x_2\}$ with an approximation of $\{a\}$. Thus, image compression is obtained. The restored image is $\{a, a\}$.

Considered a large "image" $\{x_1, x_2, x_3, x_4\}$. Average values and differences are calculated.

$$\begin{aligned} a_{1,0} &= \frac{(x_1 + x_2)}{2}, a_{1,1} = \frac{(x3 + x4)}{2} \\ d_{1,0} &= \frac{(x1 - x2)}{2}, d_{1,1} = \frac{(x_3 - x_4)}{2} \end{aligned} \tag{1}$$

Received a new representation $\{a_{1,0}, a_{1,1}, d_{1,0}, d_{1,1}\}$ "image", which contains the same values as the original. If you delete the numbers $d_{1,0}, d_{1,1}$, you get a compressed image of $\{a_{1,0}, a_{1,1}\}$. Applying the same procedure to the remaining image, you can write (2)

$$a_{0,0} = \frac{(a_{1,0} + a_{1,1})}{2}, d_{0,0} = \frac{a_{1,0} - a_{1,1}}{2} \tag{2}$$

or

$$a_{0,0} = \frac{a_{1,0} + a_{1,1}}{2} = \left(\frac{x_1 + x_2}{2} + \frac{x_3 + x_4}{2} \right) \Big/ 2 = \frac{x_1 + x_2 + x_3 + x_4}{4} \tag{3}$$

$$d_{0,0} = \frac{a_{1,0} - a_{1,1}}{2} = \left(\frac{x_1 + x_2}{2} - \frac{x_3 + x_4}{2} \right) \Big/ 2 = \frac{x_1 + x_2 - x_3 - x_4}{4} \tag{4}$$

Neglecting $d_{0,0}$, you can write the entire image $\{x_1, x_2, x_3, x_4\}$ with an image consisting of one number $\{a_{0,0}\}$ – with the average value of the brightness of all pixels. A value of $a_{0,0}$ represents the most approximate level of image information; information at the lowest resolution.

The values $\left\{a_{1,0}, a_{1,1}\right\}$, taken together, represent information at the next higher resolution level. They are expressed through $\left\{a_{0,0}, d_{0,0}\right\}$ by the formulas (5)

$$a_{1,0} = a_{0,0} + d_{0,0}, a_{1,1} = a_{0,0} - d_{0,0} \tag{5}$$

The original pixel values / luminances of $\left\{x_1, x_2, x_3, x_4\right\}$ represent the highest image resolution. These values can be restored by calling (6)

$$x_1 = a_{1,0} + d_{1,0}; x2 = a_{1,0} - d_{1,0}; x3 = a_{1,1} + d_{1,1}; x4 = a_{1,1} - d_{1,1} \tag{6}$$

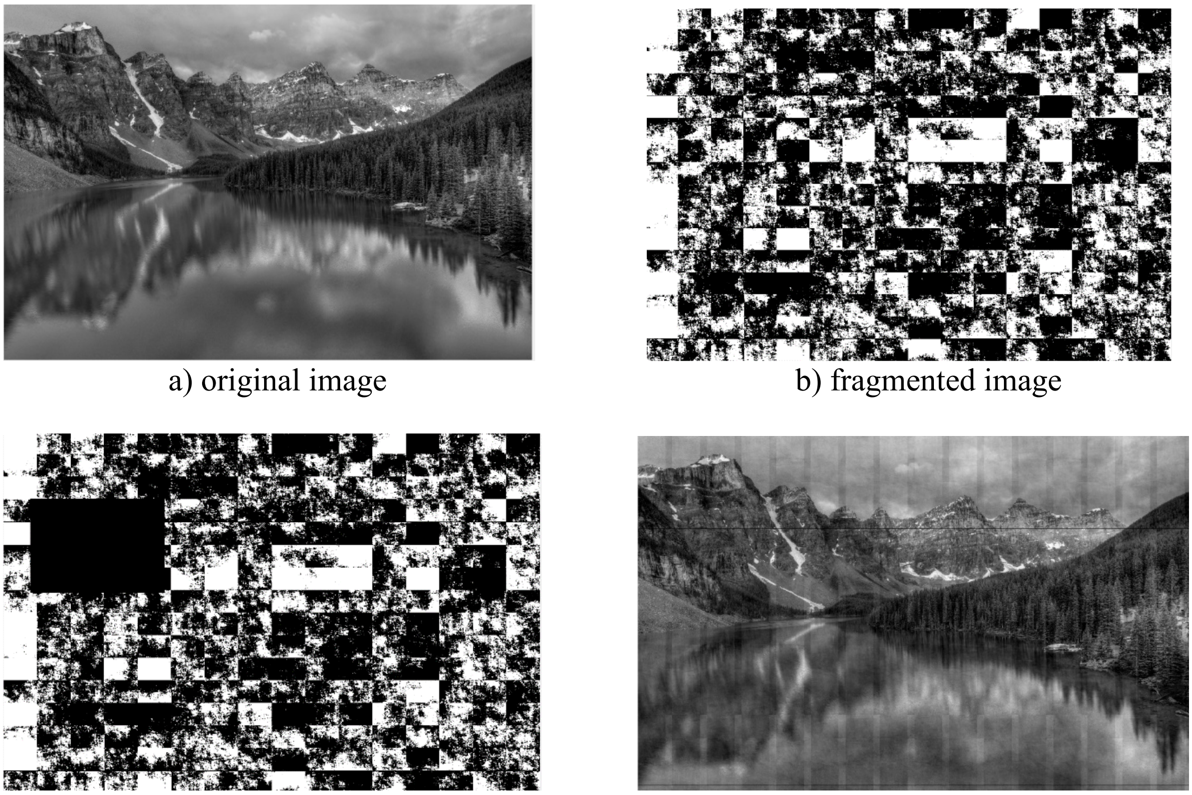
Taking into account, (1), (3) and (4), the "wavelet transform" of the original image is determined by the formulas (7):

$$\begin{gathered} a_{0,0} = \frac{x_1 + x_2 + x_3 + x_4}{4}, d_{0,0} = \frac{x_1 + x_2 - x_3 - x_4}{4} \\ d_{1,0} = \frac{x_1 - x_2}{2}, d_{1,1} = \frac{x_3 - x_4}{2} \end{gathered} \tag{7}$$

Based on the above, as an example (1-7), several images were tested, with different sizes of data shown in fig.2, here are the results of some experiments ("Nature" with a resolution of 1024 × 1024 pixels) [5,6].

The result of the wavelet transform is an ordinary array of numerical coefficients. This form of representation of information about the image is very convenient, because numerical data is easy to process. So, the image processing takes place in two stages – the first stage is compression with loss of information (wavelet transform), the second-the usual data archiving. To restore the image, you must repeat all the steps in reverse order. First, the value of the coefficients is restored, and then, using the inverse wavelet transform, an image is obtained.

The presented computer program functions as follows: first, the file is read into the pixel matrix then the program does a standard wavelet transform of the image and saves the result to a file. The results can be seen in Figure 2 (b-e).

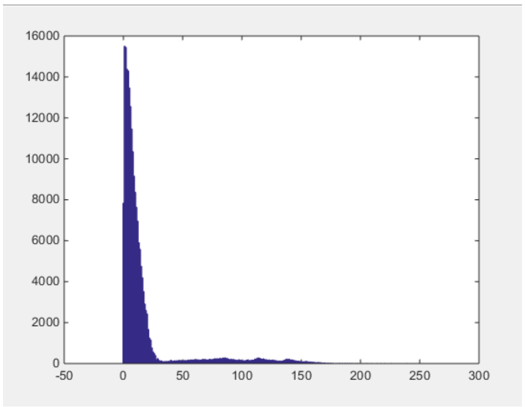


a) original image

b) fragmented image

c) fragmented image with noise

d) Conversion result



e) histogram

Figure - 2. Test results

Image quality can be determined by statistical, spectral, and brightness characteristics of the image. In most practical applications, quality is considered as a measure of the proximity of two images: real and ideal, or transformed and original.

Image enhancement. In computer systems, the source images and data processing results are displayed as an image on the screen, with the recipient of the information being an observer. The procedure that provides this representation is called visualization. It is desirable to use processing to give the output image such qualities that would make its perception by a person as comfortable as possible [2].

Eliminating noise in an image the need for noise reduction occurs if the noise level significantly degrades the image quality, preventing you from extracting useful information from it.To suppress noise, it is necessary to know its structure, which can often be estimated only from the image itself.

Conclusion. In recent years, when digital systems are increasingly replacing analog image processing systems, it is very important to master modern computer methods for describing and processing images.

Several images have been tested with different data sizes to be hidden. The program allows you to compare the original and resulting images, both visually and by calculating the signal-to-noise ratio, which allows you to mathematically evaluate a person's visual perception. Software experiments were carried out in the MatLab system.

Acknowledgments

This research has been is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP08857179)

References

[1] R. Gonsales, R. Vuds. Tsifrovaya obrabotka izobrazheniy [in Russian: Digital image processing]-// M.: Tekhnosfera, 2005.

[2] R. Gonsales, R. Vuds. [in Russian: Eddins Digital Image Processing in Matlab]-// M.: Tekhnosfera, 2006.

[3] R. Ibrahim and T.S. Kuan, Steganography imaging system (SIS): hiding secret message inside an image, Lecture Notes in Engineering and Computer Science: Proceedings of The World Congress on Engineering and Computer Science 2010, San Francisco, USA, 2010, pp. 144-148.

[4] V.T.Fisenko, T.YU.Fisenko. Komp'yuternaya obrabotka i raspoznavaniye izobrazheniy [in Russian: Computer processing and image recognition] ucheb. Posobiye. - //SPb: SPbGU ITMO, 2008. – 192 s.

[5] P.G. Dolya. Metody obrabotki izobrazheniy [in Russian: Image processing methods]-// Khar'kovskiy Natsional'nyy Universitet mekhaniko – matematicheskiy fakul'tet 2013.

[6] P.G Dolya. Matematicheskiye metody obrabotki izobrazheniy [in Russian: Mathematical methods of image processing]-//Khar'kovskiy Natsional'nyy Universitet mekhaniko– matematicheskiy fakul'tet 2014.

UDC 004.056.5
SRSTI 81.93.29

CRYPTOGRAPHIC ATTACK TO ENCRYPTION ALGORITHM “AL01” BY THE BOOMERANG METHOD

K.S .Sakan[1,2], K.T.Algazy[1,2]
[1]Institute of Information and Computational Technologies SC MES RK, Almaty, Kazakhstan,
[2]Kazakh National University named after al-Farabi, Almaty, Kazakhstan
E-mail: kairat_sks@mail.ru, kunbolat@mail.ru

Abstract. This paper describes the implementation of a cryptographic attack by the boomerang method on the "AL01" block symmetric algorithm, one of the encryption algorithms which are developed at the Institute of information and computational technologies of the SC MES RK.

This method allowed for successful attacks on many ciphers previously recognized as resistant to classical differential cryptanalysis. There are modifications of this cryptanalysis method: an amplified boomerang attack and a rectangle attack (this method is covered in this paper). In some cases, the use of this attack method can significantly reduce the amount of required data. Also this attack is applicable to algorithms with a heterogeneous structure of rounds. As with the method of differential cryptanalysis, the practical application of the boomerang attack is limited by the high requirements for processing time and data volume. Taking into account the basic properties of the differential cryptanalysis and based on the conclusions of other scientific works, the necessary minimum number of a set of quartets of open and corresponding closed texts is determined. The article concludes that the proposed cryptographic algorithm is highly resistant to this type of cryptographic attack.

Keywords: symmetric encryption algorithms, requirements for encryption algorithms, basic methods of cryptanalysis, boomerang attack.

Introduction. The strength of an encryption algorithm is its permissible degree of resistance to differential cryptographic attacks. There are certainly resistant (or theoretically persistent), provably resistant, and presumably resistant crypto algorithms. Similarly, one can distinguish between the stability of the crypto algorithm itself, the stability of the protocol, and the stability of the key distribution generation algorithm [1]. Supposedly resistant crypto algorithms are based on the complexity of solving a particular mathematical problem that is not reduced to well-known. Examples are the ciphers GOST 28147-89, AES, FEAL [2].

The boomerang attack is a cryptographic attack on a block cipher based on differential cryptanalysis methods. The attack algorithm was published in 1999 by UC Berkeley professor David Wagner, who used it to crack the COCONUT98, Khufu, and CAST-256 ciphers. Further, this method has found wide theoretical application in reliability assessments in many block ciphers. The boomerang method allows to attack some of the algorithms that are resistant to classical differential cryptanalysis, significantly reducing the amount of data required for analysis.

Cryptographic attack to encryption algorithm "AL01". The main point of the study is to find the sets of open quartets and their corresponding ciphertexts, and their minimum necessary layer to continue the analysis. As you know, the data encryption block of the "AL01" algorithm consists of the following transformations: linear transformation - bitwise addition operation (XOR), nonlinear transformation S-replacement block. As already described in the scheme of the encryption algorithm "AL01", the number of rounds is eight [3]. When using a boomerang attack, the completes scheme of algorithm *E is* divided into two consecutive parts of equal complexity: into two parts, 2 round seach *E0* and *E1,* such that $E = E_0{}^\circ E_1$, where $^\circ$ - operation of concatenation. We can this structure describe in function form: $E(M) = E_1(E_0(M))$.

The basic idea behind the boomerang attack is to use two short effective differentials instead of one long differential, trying to do better than the traditional differential attack [4]. Let the function *E₀* has differential characteristic α → β with probability *p*, and the function *E₁* :γ → δ with probability *q*. This work uses a rectangle-style boomerang attack, but the name of the boomerang attack is saved.

Figure 1 shows a rectangular boomerang structure with *E₀* and *E₁,*quartets plaintext ciphertext quartets and related differentials, α, β, γ and δ. The essence of the analysis is to find the correct quartets of texts, the analysis of which will lead to finding the secret key. By a correct quartet of texts, we will call a pair of a quartet of open and closed texts (P_1, P_2, P_3, P_4) and (C_1, C_2, C_3, C_4), for which the difference of the sum modulo 2 of the plain text P_1 and P_2, coincides with the difference of the sum modulo 2 of the plaintext P_3 and P_4, and at the same time the sum modulo 2 of the two corresponding closed texts C_1 and C_3 coincides with the difference of the sum mod 2 of the plain text C_2 and C_4. The adversary encrypts a set of plaintext pairs with a difference α and collects quartets that satisfy the requirements $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$ and $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$. In this case, the following three conditions must be met, namely [5]:

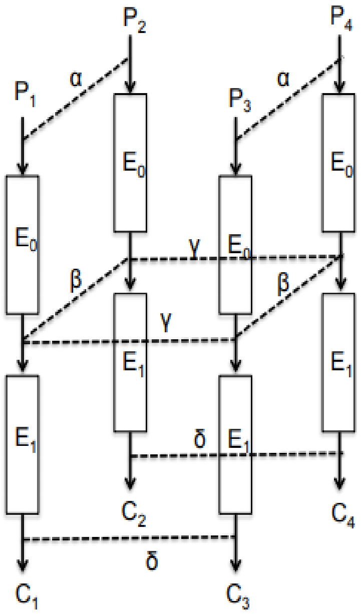


Fig 1. Rectangle-style boomerang

$$E_0(P_1) \oplus E_0(P_2) = E_0(P_3) \oplus E_0(P_4) = \beta,$$

$$(P_1) \oplus E_0(P_3) = \gamma,$$

$$C_1 \oplus C_3 = C_2 \oplus C_4 = \delta.$$

The probability of success of a boomerang attack is determined by a simple estimate $p_0 \geq Pr(\alpha \rightarrow \beta) * Pr(\gamma \rightarrow \delta) = pq$. It was noted that the probability of *p* and *q* can be increased by using multiple characteristic differentials with respect to *E₀* and *E₁*:

$$\hat{p} = \sqrt{\sum\nolimits_{\gamma} Pr^2\,(\alpha \rightarrow \beta)}\ ,$$

$$\hat{q} = \sqrt{\sum\nolimits_{\gamma} Pr^2\,(\gamma \rightarrow \delta)}.$$

It is known that if the with the length of the encryption block *n*-bit the in equality is:

$$\hat{p}\hat{q} > 2^{-n/2},$$

then ciphertexts can be distinguished from random texts. Further, the number of correct quartets *t* is calculated by the formula:

$$t = N^2 2^{-n} \hat{p}^2 \hat{q}^2,$$

where *N* is the number of plain text quartets.

We consider a truncated version of the analysis of the algorithm: the number of rounds will be two, according to the first round, functions E_0, on the second - E_1. As mentioned above, the "AL01" algorithm uses two primitives: linear – addition 2 modulo (XOR operation) and nonlinear – S-box, which maps one byte to another byte. One round consists of 16 rows, where each byte of the row is defined as the value of the S-box, the input parameter of which is the result of the XOR operation to two bytes of the previous row and the round key. The main primitive that affects the differentials is the S-box. Further, we will consider the change in the differential after each series.

Consider the worst case: the best suitable differential characteristic is when α is the difference between the plaintext P_1 and P_2 is minimal and differs with only one last bit:α=0x00000000000000000000000000000001. Taking into account the algorithm scheme and performing the S-box differential analysis, after each row we obtain the probability of obtaining the necessary characteristics for the analysis (Table 1) [6].

Table 1. Probability of obtaining the necessary characteristics for analysis

Round No	Series	The number of effective unequal S-blocks	Probability
Round 1	Series 1	2	$\frac{4}{256} = 2$
	Series 2	3	2^{-12}
	Series 3	4	2^{-18}
	Series 4	5	2^{-24}
	Series 5	6	2^{-30}
	Series 6	7	2^{-36}
	Series 7	8	2^{-42}
	Series 8	9	2^{-48}
	Series 9	10	2^{-54}
	Series 10	11	2^{-60}
	Series 11	12	2^{-66}
	Series 12	13	2^{-72}
	Series 13	14	2^{-78}
	Series 14	15	2^{-84}
	Series 15	16	2^{-90}
	Series 16	16	2^{-192}
	p- overall probability after Round 1		2^{-192}

We carry out the same procedure for the 2nd round with respect to the suitable differential $E_0(P_1)$ and $E_0(P_3)$. Here, we also assume that the best differential:

$$\gamma = E_0(P_1) \oplus E_0(P_3) = 0x00000000000000000000000000000001.$$

e.g. $E_0(P_1)$ and $E_0(P_3)$ is minimal and differs with only one last bit.

Taking into account the symmetry of E_0 and E_1, we obtain the probability $q = 2^{-192}$. Since the computing power of the computer does not allow us to consider all possible variants of differentials, we restrict ourselves to $\hat{p} = p$ and $\hat{q} = q$.

Therefore, the probability of success of a rectangle-type boomerang attack is extremely small:

$$p_0 \geq Pr(\alpha \to \beta) * Pr(\gamma \to \delta) \approx pq \approx 2^{-392}.$$

Now let us determine the number of required plaintext quartets N to obtain one correct quartet. Assuming that $t = 1$, we calculate

$$N^2 2^{-n} \hat{p}^2 \hat{q}^2 = 1.$$

Since the length of the encryption block is n=128, it follows that $N = 2^{455}$. For at least one correct quartet for two-round “AL01” algorithm will need about 2^{455} quartets plaintext. Given that this estimate is carried out before the two-round algorithm, the subsequent analysis steps do not make sense, since the complexity of the calculation and the number of optimal numbers of correct quartets increase rapidly with increasing rounds.

Conclusion. Summing up, it shows that the complexity of the analysis on two rounds becomes greater than the complexity of a complete search and it makes no sense to apply the analysis. Therefore, it is considered that the proposed “AL01” encryption algorithm is cryptographically resistant to the attack by the boomerang method. Our results showed that the attack poses no threat to the full-round "AL01" algorithm, but helps us understand the differential behavior and its strength in a boomerang attack.

As well as for the method of differential cryptanalysis, the practical application of this attack in terms of computational complexity is strictly limited by high requirements for processing time and data volume. Therefore, the boomerang attack was mainly applied to ciphers with the least number of rounds when evaluating the strength of algorithms. The algorithm is a theoretical achievement of evaluating algorithms.

The presented works were carried out at the expense of the funding of the grant funding project AP08856426 for scientific research for 2020-2022 years “Development and research of an encryption algorithm and creation of a software and hardware complex for its implementation”.

Reference:

1. Rostovtsev A. G., Mikhailova N. V. Methods of cryptanalysis of classical ciphers//. A. G. Rostovtsev, N. V. Mikhailova - M.: Nauka, 1995. 208 p.

2. Introduction to Cryptanalysis. Cryptanalysis of symmetric cryptosystems: block ciphers //2012.url:https://docplayer.ru/36057626-Vvedenie-v-kriptoanaliz-kriptoanaliz-simmetrichnyh-kriptosistem-blochnye-shifry.html(in Russian)

3. Report of scientific-research work «Development of software and software-hardware means for cryptographic protection of information during its transmition and storage in general-purpose infocommunication systems and networks», BR05236757, 2020.

4. D. Wagner, The boomerang attack in Fast Software Encryption, FSE’99 (L. R. Knudsen, ed.), vol. 1636 of Lecture Notes in Computer Science, pp. 156–170, Springer-Verlag, 1999.

5. J. Chen, A. Miyaji, Differential Cryptanalysis and Boomerang Cryptanalysis of LBlock, International Conference on Availability, Reliability and Security CD-ARES 2013: Security Engineering and Intelligence Informatics, pp 1-15, volume 8128, Regensburg, Germany, September 2-6, 2013.

6. Dyusenbayev D.S., Sakan K.S., Cryptographic attack on the "Qamal" algorithm using the boomerang method // Materials of the international scientific-practical conference "Actual problems of information security in Kazakhstan". – 2020. – P. 123-129 (in Russian).

IRSTI 50.37.23; 50.41.25
UDC 51.74; 627.85

Water level monitoring system in hydraulic structures

T. Mazakov[1], P. Kisala[2], N. Issimov[3] and G. Ziyatbekova[4]
[1,3] RSE Institute of Information and Computational Technologies MES RK CS,
Almaty, Kazakhstan
[2]Lublin Technical University, Poland
[1,4]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[1]tmazakov@mail.ru, 3p.kisala@pollub.pl, [3]int_nurdaulet@mail.ru, [4]ziyatbekova@mail.ru
[1]ORCID ID: https://orcid.org/0000-0001-9345-5167
[4]ORCID ID: https://orcid.org/0000-0002-9290-6074

Abstract. The article is devoted to the creation of a system for monitoring the water level in hydraulic structures (HS) to prevent a dam break. The article discusses a system for monitoring the water level in hydraulic structures, which allows real-time information on the relative humidity and air temperature, on the distance from the crest of the dam to the water surface in the reservoir. The general characteristics of the problem and the formulation of research tasks are given. On the basis of microprocessor technology and sensor sensors, an autonomous microcomputer system for transmitting climate data has been developed. A program for monitoring breakout factors in real time has been developed. Based on the information received, the system makes it possible to estimate the predicted time for the increase in the volume of the water level from the current to the critical level and inform the population about the state of the reservoir. The task is analyzed and the main problems that may arise in the course of its solution are identified. The advantages and disadvantages of the described methods are highlighted.

Keywords: monitoring system, dam, water level sensor, breakthrough waves, water resources, hardware-software complex, hydraulic structure.

Introduction. The purpose of water resources monitoring is to obtain data from repeated observations of the elements of water resources, carried out for their assessment, according to a certain plan, using modern methodologies for measuring parameters and collecting data. It allows you to obtain information regarding the current state of water resources and assess trends in changes in their characteristics, as well as predict the limits of possible changes. Monitoring of water resources includes monitoring of water bodies (surface, underground), water management systems and structures, monitoring of water use, etc. Water resources monitoring method is intended for water specialists to assess and manage water resources. The water resources monitoring system creates information support for the management of the country's water fund. The main provisions of the formation of the monitoring system: a complex approach; continuity of monitoring in space and time; using common methodological approaches; organization of a monitoring system based on geographic information systems (GIS); the system should be open for practical linkage with other systems; focus on computer technology for collecting storage and processing data [1].

Monitoring of water resources in Kazakhstan is characterized by a number of problems, the main of which: insufficient funding, low coverage of the country by the observation network, collection of information is carried out separately and in small quantities, outdated equipment and methods for collecting and analyzing the information received, poorly equipped observation posts, disunity of the monitoring network of various departments, weak research support for the development of a water monitoring system. To solve the above problems of the development of water resources monitoring in Kazakhstan, it is necessary to introduce the following measures: determination of the required information for various water users and natural ecosystems; creation of a unified system for monitoring water resources based on GIS technologies and with the participation of all stakeholders; improving the quality of scientific research of the features of the monitoring system of the Republic of Kazakhstan.

Implementation. For practical applications, systems are being developed for monitoring the state of water bodies in real time, based on the automation of the process of collecting and processing information. Basically, the automated monitoring systems use the following sensors: inclometric; streams; deformation; temperature; pressure per pound; water level [2-4].

During the operation of hydrotechnical facilities, in particular in the mountains, the destruction of the pressure head of the hydraulic units is one of the most dangerous cases of accidents, which lead to the cystic, ecological and socio-logical, a also significantly affecting the ecology of the downstream of hydropower plants. For information monitoring systems, it is necessary to ensure the collection of data in real time.

The water level measuring equipment can be different. To ensure the functioning of the system, the measuring equipment will be interfaced with the data transmission subsystem and the power supply subsystem. The conjugation of these systems will allow monitoring the water level in moraine lakes, the location of which is extremely difficult to access. The technical means that measure the water level must be able to receive data from sensors with different periodicity [5-7]. As was said above, the data arriving from the measuring equipment will be transmitted to the data collection and processing center by means of low-orbit space communication systems.

The accumulated data will be transferred to situational centers and used by special services for forecasting possible floods and floods, calculating water consumption and for other purposes. The monitoring system can be linked to other automated systems, for example, systems for the intake and discharge of water on the webs of hydroelectric power plants, alarm systems, and other functional interconnected systems. The introduction of a water level monitoring system will allow for the prevention of emergencies.

The main information for monitoring the risk of dam failure is the data from the water level sensor. Additional information is provided by data received from temperature and precipitation sensors.

The unit for receiving and transmitting current information is implemented in the form of sensors about water level, humidity and temperature and is located on the crest of the dam. The sensors are connected to the Arduino microprocessor [8-10], which provides preliminary processing of the data coming from the sensors and transfers them for further processing.

To measure the water level in the reservoir, we used an ultrasonic sensor US-015, which works by sending sound waves at a certain frequency.

Specifications US-015:

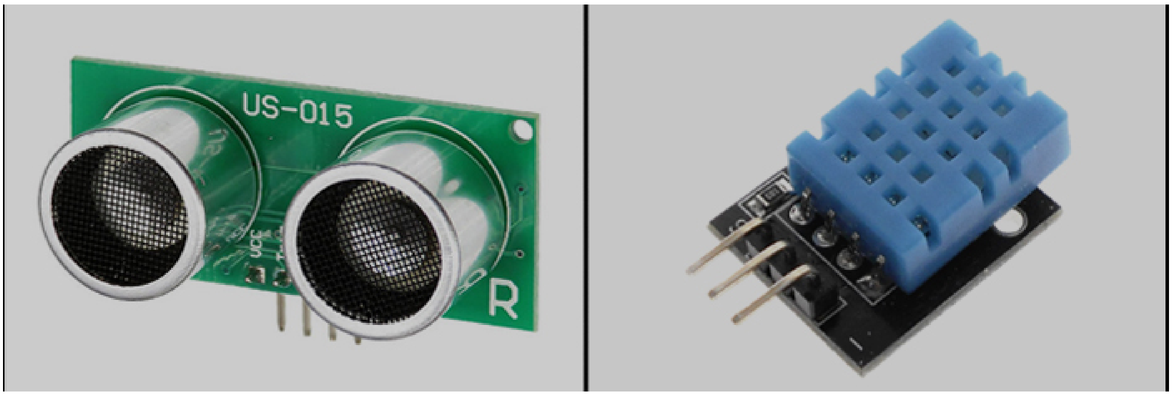
- Supply voltage: 5 V;
- Power consumption: 20 mA;
- Standby current consumption: 2.2 mA;
- Measurement angle: 15°;
- Measuring distance range: 2 - 700 cm;
- Accuracy: 0.3 cm + 1%.

To measure the temperature and the presence of precipitation, a DHT11 sensor was used, which has one digital output, therefore, readings can be taken no more often than once every 1-2 seconds.

DHT11 characteristics:

- Power and I/O 3-5V;
- Determination of humidity 20-80% with 5% accuracy;
- Determination of temperature 0-50 degrees with 2% accuracy;
- The sampling rate is no more than 1 Hz (no more than once every 1 sec.).

Figures 1 and 2 show the type of sensors used, their design and layout.



а) Sensor US-015 б) DHT11 sensor

Figure 1 - Type of sensors: a) water level sensor US-015 and b) temperature and humidity sensor DHT11

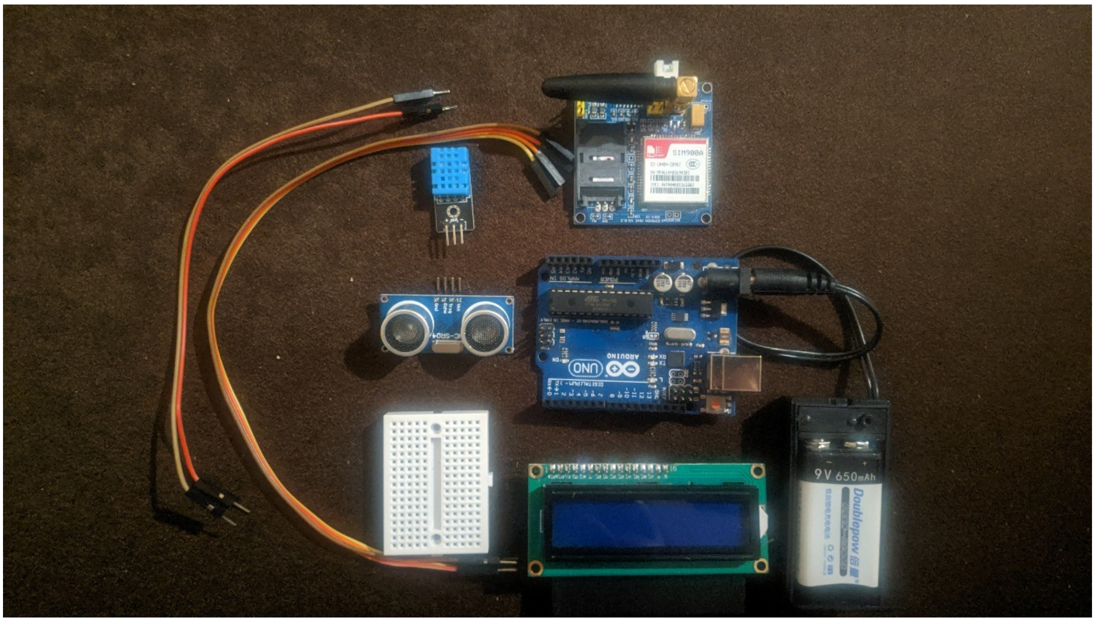


Figure 2 - Composition of sensors detecting information on climate and water level

Catastrophic flooding, which is the result of a hydrodynamic accident, consists in the rapid flooding of the area by a breakout wave. Hydraulic structures can be breached due to natural forces (earthquake, hurricane, landslide, etc.), structural defects, violations of operating rules, impact of floods, destruction of the dam base, etc. During the breakthrough of the hydraulic structures, a gap (closure channel, passage) is formed, through which the water flows from the upper downstream to the lower one and the formation of a breakthrough wave. Breakthrough wave is the main striking factor of this type of accident, characterized by wave height and speed [11, 12].

In [13], it was found that the following hydroelectric complex parameters and the conditions of propagation of a breakthrough wave in the downstream most significantly affect the h_{max} values: reservoir volume before the accident (W_{water}), reservoir depth at the dam before the accident (H_0), roughness of the upstream wall (n_0), the amount of opening of the gap (B_{gap}), water flow in the downstream of the hydroelectric facility before the accident (Q_0), the distance from the damsite to the observation site (L). The dependence of the maximum flooding depth on the main influencing factors was obtained and presented in general form by the expression:

$$\mathrm{h}_{\max} = 2{,}51\,\frac{H_0^{0,98}\,n_0^{0,02}\,Q_0^{0,05}}{W_{water}^{0,05}\,L^{0,13}} \tag{1}$$

The limits of applicability of formula (1) are indicated: reservoir volume (W_{water}) – from 50 to 5000 thousand m^3; depth of water upstream of the dam (H_0) – from 2 to 20 m; water flow in the downstream of the hydraulic facility before the accident (Q_0) – from 1 to 100 m^3/s; reservoir length – from 0.8 to 2 km, if there is no backup from the downstream hydraulic structures; distance from the dam site to the considered section (L) from 0.5 to 50 km; roughness (n_0) from 0.02 to 0.2.

In addition, the formula (1) has the following disadvantages:

1) missing parameter – the amount of opening of the gap (B_{gap}),

2) the volume of the reservoir before the accident (W_{water}) is placed in the denominator, which leads to a contradiction to the basics of hydrology – "a larger volume of reservoir filling leads to a decrease in the breakthrough wave".

In [14], due to the limitations of the applicability of the formula (1), it was proposed to use the dependence (2) proposed by V.I. Volkov to determine the maximum depth of flooding:

$$\mathrm{h}_{\max} = 0{,}34\mathrm{H}_0\left(\frac{L}{\mathrm{H}_0}\right)^{-0,13} \tag{2}$$

As a disadvantage of the formula (2), it should be noted that it does not use such important parameters of the hydraulic structures as the reservoir volume before the accident (W_{water}), the amount of opening of the gap (B_{gap}). This fact greatly narrows the applicability of this formula.

To correct these shortcomings, the article proposes the following approach.

The maximum depth $\mathrm{h}_{\max}$ is sought in the form

$$\mathrm{h}_{\max} = \alpha_0 \mathrm{B}_{gap}^{\alpha_1}\mathrm{H}_0^{\alpha_2}\mathrm{W}_{water}^{\alpha_3}\mathrm{L}^{-\alpha_4}\cos\theta, \tag{3}$$

where $\boldsymbol{\theta}$ – is the angle of inclination of the earth (relief) at a distance L.

In the formula (3) all the coefficients $\boldsymbol{\alpha_i > 0, i = \overline{0,4}}$.

Let n = 4 be the number of information parameters of hydraulic structures that affect the size of the breakthrough wave; $x = (x_0, \dots, x_n)$ – the vector whose components characterize the hydraulic structures.

For the convenience of further calculations, we will accept

$y = \mathrm{h}_{\max};\ x_0 = 1,\ x_1 = \mathrm{B}_{gap};\ x_2 = \mathrm{H}_0;\ x_3 = W_{water};\ x_4 = L.$

We introduce the following designations:

m– the number of versions (situations);

X_{ij} – the value of the i-th parameter in the j-th version,

where$i = \overline{0,n}$, $j = \overline{1,m}$.

Y_j – maximum breakthrough wave depth in the j –th situation, where $j = \overline{1,m}$.

Then formula (3) can be rewritten in the form:

$$Y_0 = \alpha_0 * \left(\prod_{k=1}^{3} x_k^{\alpha_k}\right) * x_4^{-\alpha_4} \tag{4}$$

$$Y = Y_0 * cos(\theta)$$

Formula (4) corresponds to the optimization problem, where the coefficients α_k, are unknown, which determine the influence of the k–th information parameter on the overall result.

We will take the logarithm of the expression (4):

$$l\,n(Y_0) = \alpha_0 + \sum_{k=1}^{3} \alpha_k\, l\,n(x_k) - \alpha_4 l\,n(x_4) \tag{5}$$

The coefficients α_k in formula (5) can be found from the minimum condition for the functional

$$S\ = \sum_{j=1}^{m} \left(l\,n(Y_{0j}) - \alpha_0 - \sum_{k=1}^{3} \alpha_k\, l\,n(X_{kj}) + \alpha_4 l\,n(X_{4j}) \right)^2 \tag{6}$$

We introduce the set

$$A = \{0 \leq \alpha_i \leq 10\} \tag{7}$$

It is easy to show that A is a convex closed set in R^m space.

The algorithm for finding the coefficients of functional (6).

Step 1. The minimum of functional (6) is found by the least square method, by reducing to a system of linear algebraic equations of the form

$$\text{C}\beta = d$$

Where C – (n+1)*(n+1) – the matrix, $d - (\text{n} + 1) -$ the vector made up of values $l\,n(Y_{0j}), l\,n(X_{kj}), k\ = \overline{0, n},\ \ j = \overline{1, m}.$

If all elements of the vector $\beta_i > 0$,= $\overline{0, n}$, then we take $\alpha_i\ =\ \beta_i, i = \overline{0, n}$ and go to step 5.

Step 2. Denote by α_i^n the n-th approximation for calculating the coefficient α_i.

As a zero approximation, we select

$$\alpha_i^0 = \begin{cases} \beta_i,\ if\beta_i\ > 0 \\ \varepsilon,\ if\beta_i\ \leq 0 \end{cases}.$$

Here $\varepsilon > 0$ – is a sufficiently small number.

Step 3. The minimum of the functional (6) is defined on the set (7).

Let's build an iterative process

$$\alpha_i^{n+1} = \Pi_\text{A}(\alpha_i^n - \gamma_n S'(\alpha_i^n)) \tag{8}$$

Here Π_A – projection operator onto the set A. The coefficients $\gamma_n\ \geq 0$, the determine the step length at the n-th stage, can be found from the condition

$$S(\ \alpha_i^n - \gamma_n S'(\alpha_i^n)) = \min_{\gamma \in R} S\left(\alpha_i^n - \gamma S'(\alpha_i^{k,n})\right)$$

or in the process of splitting the step.

Step 4. Discrepancy is sought $r = min_i\left(abs(\alpha_i^{n+1} - \alpha_i^n)\right)$.

If $r < \varepsilon$, then go to step 5. Otherwise, increase the iteration number and go to step 2.

Step 5. Algorithm completion.

The convergence of the proposed algorithm is provided by the following theorem.

Theorem 1. Let the set A be convex and closed. Then the sequence $\{\alpha_i^n\}$, defined by the formula (8) converges to the solution of the problem of minimizing the functional (6) on the set (7).

Proof. Since the set A is convex and closed, the functional (6) is convex and differentiable, then any limit point of the sequence $\{\alpha_i^n\}$ is the minimum point [15].

Based on the available information about the breakthroughs, 30 versions of parametric data were prepared. Based on this information, the following formula is obtained:

$$\mathrm{h_{max}} = 1{,}34 * H_0^{0{,}55} B_{gap}^{0{,}32} W_0^{0{,}04} L^{-1{,}4} \cos\,(\theta) \qquad (9)$$

In the formula (9), the volume of the reservoir (W_{water}) is measured in millions of m^3; the water depth in the upstream wall of the dam ($\mathrm{H_0}$) is in m;the amount of opening of the gap (B_{gap}) – in m; the distance from the dam site to the observation site (L) - in km; θ is measured in degrees.

Conclusion. The analysis of existing methods of solutions and the formulation of problems for monitoring hydrological processes. The general characteristics of the problem and the formulation of research tasks are given. On the basis of microprocessor technology and sensor sensors, an autonomous microcomputer system for transmitting climate data has been developed. A program for monitoring breakout factors in real time has been developed [16].

The model problem (events that took place in Kyzylagash village of the Almaty region of the Republic of Kazakhstan) shows the effectiveness of the developed mathematical model of predicting the consequences of a dam break.

In the spring of 2010, a tragedy overtook the Almaty region - a flood, with human casualties and destruction. The reign of the elements occurred as a result of the break of the dam. And also in 2014 the same tragedy was repeated in the Karaganda region. These alarming situations for all the peoples of the country served as a serious lesson in preventing similar situations in the future These alarming situations for all the peoples of the country served as a serious lesson in preventing similar situations in the future. To improve the operational safety of equipping hydraulic structures, it is necessary to develop recommendations with modern instrumentation, equipment and means [17, 18].

Acknowledgements. The work was carried out at the expense of grant funding of scientific research for 2018-2020 under the project AP05131027 «Development of biometric methods and information protection tools».

References

1. Mazakov T.Zh., Jomartova Sh.A., Kisala P., Ziyatbekova G.Z. Problems and measures for the development of monitoring of water resources // Bulletin of KazNRTU, 2020. – № 2 (138). – P. 365-369.
2. Shtork S.I., Vieira N.F., Fernandes E.C. On the identification of helical instabilities in a reacting swirling flow. – Fuel, 2008. – Vol. 87. – No. 10-11. – P. 2314-2321.
3. Coleman, Stephen. Dittrich, Andreas; Koll, Katinka; Aberle, Jochen; Geisenhainer, Peter (Hg.) Fluvial sediment transport and morphology: views from upstream and midstream. River Flow. Karlsruhe: Bundesanstalt für Wasserbau, 2010. – P. 11-22.
4. Hydraulic structures. Textbook for universities. – M.: Publishing house of the Association of building universities, 2008. – Part 1. – 576 p.
5. Kotyuk A.F. Sensors in modern dimensions. - M.: «Radio and communication», 2006. - 96 p.

6. Freiden J. Modern sensors. – M.: «Technosphere», 2005. – 592 p.

7. Aleinikov A.F. Gridchin V.A. Tsapenko M.P. Sensors (promising areas of development). – Novosibirsk: NSTU, 2001. – 176 p.

8. Aliaskar M.S., Dzhomartova Sh.A., Ziyatbekova G.Z., Isimov N.T., Amirkhanov B.S., Mazakova A.T. Autonomous microprocessor system for transmitting climatic data // Bulletin of KazNRTU im. K.I. Satpayev. – Almaty, 2019. – No. 1 (131). – P. 371-377.

9. Karvinen T., Karvinen K., Valtokari V. Making sensors: projects of sensor devices based on Arduino and RaspberryPi. – M.: LLC «I.D. Williams», 2017. – 432 p.

10. Vavilov V.D., Timoshenkov S.P., Timoshenkov A.S. Macrosystem sensors of physical quantities. – M.: Technosphere, 2018. – 550 p.

11. Arefyev N.V., Mikhalev M.A., Skvortsova A.S. General erosion of the channel and lowering of the water level in the downstream // Environmental Engineering, 2008. – No. 1. – P. 83-87.

12. Klimovich V.I., Prokofiev V.A. The calculation of the parameters of the breakthrough wave and the definition of the border of the flood zone during the accident at the ash disposal site // Hydrotechnical construction, 2001. – No. 1. – P. 38-44.

13. Sekisova I.A. Development and testing of a system for assessing the state of hydraulic structures of river low-pressure hydroelectric facilities // Dis. Cand. tech. sciences for special. 05.23.07. – Moscow, 2008. – P. 230.

14. Chernykh O.N., Volkov V.I., Altunin V.I. Safety problems of the territories of the lower reaches of the capital's ponds // Environmental engineering, 2017.– No. 1. – P. 47-55.

15. Sukharev A.G., Timokhov A.V., Fedorov V.V. Course optimization methods. – M.: Nauka, 1986. – P. 328.

16. Jomartova Sh.A., Mazakov T.Zh., Isimov N.T. Mazakova A.T. Real-time forecasting program // Bulletin of the National Engineering Academy of the Republic of Kazakhstan. – 2017. – No. 4 (66). – P. 27-32.

17. T.Zh. Mazakov, P. Kisala, Sh.A. Jomartova, G.Z. Ziyatbekova, N.T. Karymsakova. Mathematical modeling forecasting of consequences of damage breakthrough // News of the National Academy of Sciences of the Republic of Kazakhstan. Series of Geology and Technical Sciences. – 2020. – Vol. 5, No 403. – P. 116-124. URL: https://doi.org/10.32014/2020.2518-170X.111 (online; accessed: 11.12.2019).

18. T. Mazakov, Sh. Jomartova, G. Ziyatbekova, M. Aliaskar. Automated system for monitoring the threat of waterworks breakout // Journal of Theoretical and Applied Information Technology, 2020. – Vol. 98, – No 15. – P. 3176-3189. ISSN: 1992-8645, E-ISSN: 1817-3195.

Funding
The authors received no direct funding for this research.