ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

PROGRESSIV INFORMATICS TECHNOLOGIES

UDC 621.391

Evseev S. P.[1], Tomashevskyy B. P.[2]

[1]Ph.D, Associate Professor of Information Systems Department of Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

[2]Ph.D, Leading Research Assistant, Senior Researcher of the Research Department of Missile Troops and Artillery of the Scientific Center of Land Forces, Kharkiv, Ukraine

TWO-FACTOR AUTHENTICATION METHODS THREATS ANALYSIS

The article considers basic methods of two-factor authentication system constructing on the basis of the use of cryptographic mechanisms to ensure the reliability, of formed authenticators, the risk of various methods of online attacks against a variety of two-factor authentication systems is estimated, as well as a system PassWindow is considered, which provides two-factor authentication on the unique ability of the matrix to transmit information in such a way that it is deciphered only to the imposition of the physical signs of the intended recipient pattern and barcode pattern obtained by digital network devices, resistance to the analysis is provided by a unique barcode card pattern generation as unique statistical images, a sequence of characters, or as more extended in an animated version.

The object of the research is the process of improving the integrity and authenticity of data packets in banking transactions security protocols on the basis of two-factor authentication methods. The subject of the study is methods and algorithms of integrity control and authenticity of data packets in banking transaction security protocols on the basis of two-factor authentication methods.

The aim of the paper is to increase the integrity and authenticity of data packets in banking transactions security protocols, a banking transaction, threat assessment on two-factor authentication methods. A comparative analysis of various systems with two-factor authentication PassWindow system in opposition to various Internet attack scenario is being carried out. An effective method for monitoring a practical two-factor authentication PassWindow system in its application to the banking system.

Keywords: two-factor authentication, online attacks, social engineering.

NOMENCLATURE

ID is an unique digital number of a user;

OTP is a password that is valid for only one login session or transaction, on a computer system or other digital device;

PIN is a numeric password shared between a user and a system, that can be used to authenticate the user to the system;

RSA is one of the first practicable public-key cryptosystems widely used for secure data transmission;

SMS is a text messaging service component of mobile communication systems.

INTRODUCTION

Existing authentication systems are based on a user submitting a static pair ID / password to the computer. However, in this case, the pair may have been compromised due to the negligence of users or the possibility for a fraud to guess passwords over [1–4]. Significant time intervals during which the password and the identifier are unchanged, allows applying various methods of interception and selection. To improve the security of a computer system administrators restrict the validity period of passwords, but in a typical case, this time limit is weeks and months, which is quite enough for an malefactor. A radical considers implementing two-factor authentication system, when the system asks a user to provide her with «what you know» (name and possibly a PIN-code), and «what you have» – any hardware identifier associated with the user [1, 2].

The purpose of the article is the investigation of the main methods for constructing two-factor authentication systems, risk analysis of different methods of online attacks against two-factor authentication systems based on the PassWindow system. A comparative analysis of the various two-factor authentication systems in opposition to various Internet attack scenarios is conducted.

1 PROBLEM STATEMENT

Currently, the Internet has become a primary method of communication of our modern life. It will undoubtedly be the main tool for the implementation of shopping and other financial operations. The appearance of these technologies has created a concomitant demand for authentication methods that are based not only on the traditional cryptographic methods (encryption, hashing, digital signature), but also on the methods based on usage of several factors to ensure the authenticity of the person

DOI 10.15588/1607-3274-2015-1-7

performing the financial transaction. Two-factor security system is based on the fact that a user in addition that one knows the password to access a specific user name («login») owns a tool for the corresponding access key. The latter can be an electronic security certificate stored on a computer or received on a personal phone SMS with a verification code or a fingerprint reader scanned by an electronic card reader device [1].

2 REVIEW OF THE LITERATURE

Strict (two-factor) authentication methods are most commonly used in the financial sector however may be used in almost any other field. The main methods of constructing two-factor authentication systems are given in Fig. 1 and can be classified as following [3].

1. Software to identify a specific PC. A special program is installed in a computer, which sets in it a cryptographic token. Then, the authentication process will involve two factors: the password and token embedded in the PC. As the marker is always stored on the computer, to logon the user only needs to enter login and password.

2. Biometrics. The use of biometrics as a secondary factor identification is carried out by identifying the physical characteristics of the person (fingerprint, iris, etc.).

3. Disposable e-mail- or SMS-password. Use of this password as a secondary identification factor is possible by sending second disposable password to one's registered e-mail address or mobile phone.

4. One-time password token. User is presented with the device that generates constantly changing passwords. It is these passwords which are entered by the user in addition to the usual passwords during the authentication process.

5. External control. This method assumes a call from the bank on a pre-registered phone number. The user must enter the password via the phone, and only after that he will get access to the system.

6. Identification using gadgets. This kind of identification is carried out by placing a cryptographic tag on any user's device (e.g. USB-drive, iPad, memory card, etc.). During registration, the user must connect the device to a PC.

7. Card with a scratch-off layer. The user is issued a card with PIN-code, which can be used only once.

The analysis has shown that in the banking systems tend to use two-factor authentication systems based on disposable e-mail- or SMS-passwords, and various types of tokens.

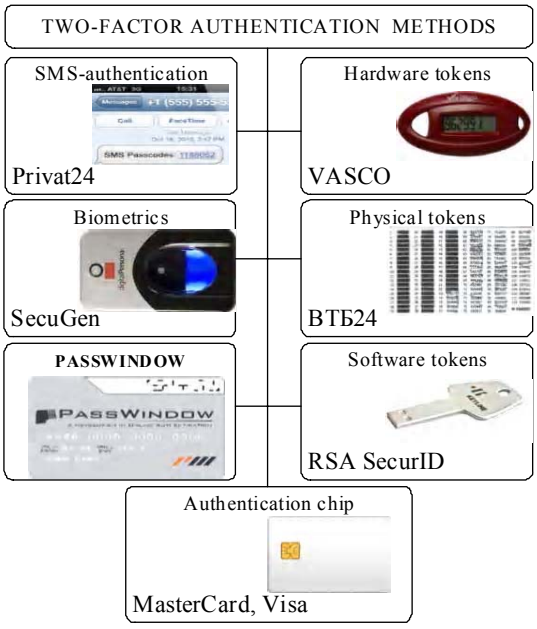


Figure 1 – Basic two-factor authentication systems

3 MATERIALS AND METHODS

Today several companies offer two-factor authentication systems based on the generation of OTP (One-Time Password – OTP), including RSA Security, VASCO Data Security and ActivIdentity.

To implement it the different types of OTP generators are used. OTP Generator is a standalone portable electronic device that can generate and display on a built-in LCD screen digital codes. For a generation of VASCO's Digipass devices one-time password generation mechanism is based on the cryptographic TripleDES conversion of data set consisting of 40 bits of the current time and the 24-bit data vector which are unique for every for each access identifier. The resulting conversion is visible on the display in the form of six or eight decimal digits is read visually and manually entered by the user as a password in response to the authentication application. Frequency of password change thus is 36 sec., so user receives truly a one-time password to login [4].

On the server part of computer system this password is compared with the password generated by the server itself by the same algorithm with the use of the current time on server clock and unique device data that is stored in a special database. In case of coincidence of passwords user is granted with access to the system. Fig. 2 shows the operation of the two-factor authentication systems of VASCO company.

Let concider the authentication based on PassWindow. PassWindow is a way to provide two-factor authentication in the online environment. It includes two matrix parts which are a physical key with a printed pattern on a plastic plate and a digital barcode template presented in the form of an image on an ordinary electronic display, such as a laptop or mobile device display. They generate a unique one-time password and a set of numbers for a particular transaction for a user, when they overlap each other. This password is then used for online authentication and transaction authentication. Information about a specific transaction is included in these figures, such as an account number or amount of the intended

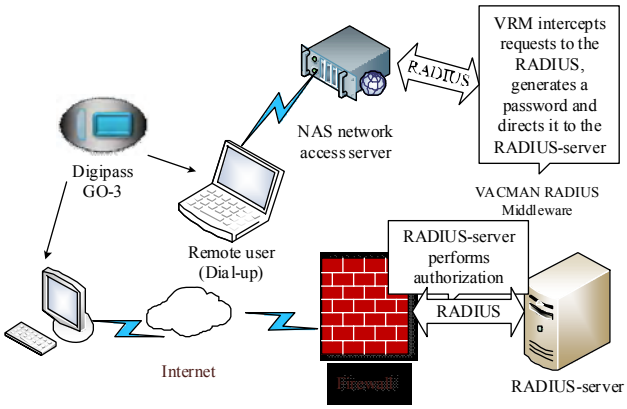


Figure 2 – The principle of operation of two-factor authentication systems of VASCO company

transaction that allows the user to visually confirm the authenticity of the received authentication request. These features make PassWindow one of the very few currently available authentication mechanisms, which provides a robust and accurate protection against the latest network security threats MITM (Man-In-The-Middle) attacks [4].

PassWindow technology is based on the unique ability of the matrix to transmit information so as that it stands only to the imposition of the physical signs pattern of the intended recipient (the user has this information already) after which the barcode template is displayed (challenge pattern) on the electronic network devices, such as computer, smartphone, etc. The combination of the key and the barcode template shows the encoded information only to a single user, moreover a full template preview is only possible from direct view. Any act of barcode interception via electronic devices means that leaked information will not be sufficient to let an attacker know the secret key of the user template during the whole activity term of the card.

Barcode PassWindow templates can exist as unique static images or a sequence of characters in the form of more extended animated version, which is the main topic of this paper. These animated barcodes consist of a sequence of static patterns, each of them contains the encoded characters or have no meaning and simply dynamically add an entropy to the entire pattern. Barcode patterns sequences are dynamically generated by the authentication server so that each of them is unique (and hence it has a sense) only when used together with the key to which it fits. Any interference or counterfeiting of a barcode template will be passively presented to the user in the form of appearance of combinations in a pattern that does not meet the expectations, for example, randomly placed segments that do not contain any characters, random numbers, missing or excessive numbers that appear within a template or performing the verification of data that does not refer to the active transaction.

Any alphanumeric code can be reliably transmitted using the PassWindow method, however the current implementation of the method is aimed at the transfer of short strings of random numbers for their use as a one-time password in conjunction with the figures which identify uniqueness of user authentication transaction. Once a user confirms that the unique information within a transaction encoded in the bar code corresponds to the desired, one can complete the transaction by entering the appropriate one-time password. The main stages of PassWindow are presented in Fig. 3.

Construction and safety profile of transaction authentication codes can be changed dynamically in order to meet a wide range of online authentication specific tasks.

Let concider the safety assessment of two-factor authentication systems.

Analysis of modern authentication systems showed that their security is measured by dividing the difference between the cost and benefits to the attacks on the value of the attacker's protection. So, expensive, though more secure methods, such as cryptographic PKI-units with their own secured communication channels of screens and keyboards are evaluated so low on the scale of security, whereas the banking system is still mainly based on the cheapest and apparently the least secure way of using PIN-codes and

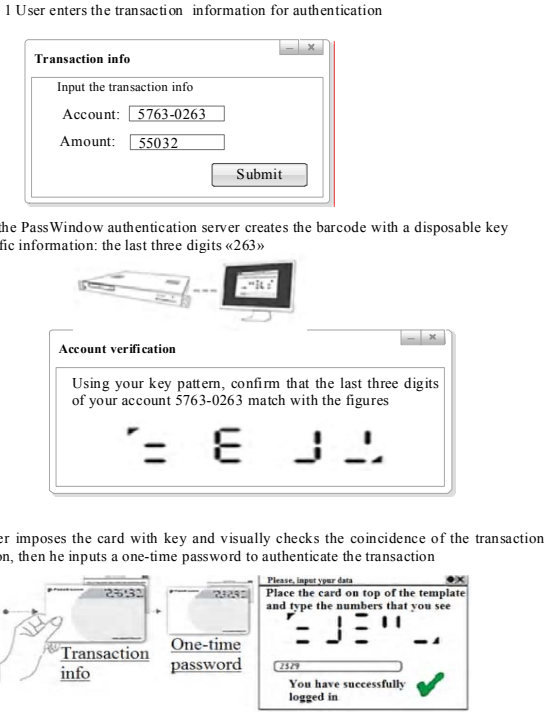


Figure 3 – The main stages of PassWindow

passwords. Total cost and complexity of deploying such devices often outweighs the benefit of their ultra-high security.

Network security threats can be classified into network attacks (information from a remote agent) and local attacks that originate from malicious software already installed on the client system, such as Trojans, rootkits, and so on. Frequently authentication safety assessments are primarily focused on network attacks assuming that the user terminal (i.e. tablet PC, laptop or mobile device) is a protected platform [11–14]. Nevertheless the attacker commonly gains full access to the victim's PC through hidden communication processes remaining from malware that use unpatched security holes in the licensed software.

The common attack methods are:

– compromised online databases – collected information stored in merchant databases is stolen;

– man in the middle / phishing – a third party intercepts and impersonates the client and server to the respective other to record and/or alter their communications;

– social engineering attacks – customers are deceived into revealing their private details to a hacker;

– man in the browser – malware is installed on the victim's computer to report network activity, keystrokes, and screen capture data to the attacker allowing interception during fund transfers in which funds can be unwittingly diverted by altering the information displayed in the user's browser;

– brute-force cracking of user passwords – the server is polled with every possible password combination;

– simple theft – authentication details written down or on a card can be physically taken and copied;

– shoulder surfing – an attacker can surreptitiously watch the user enter their transaction details.

4 EXPERIMENTS

The analysis of PassWindow security threats has shown that the most effective threat is analytic attack on the secret

key (card bar-code). To succeed the algorithm three to five monitoring sessions (OTP Bank transfer by client) have to be accomplished.

Plastic cards monitoring algorithm consists of the following steps.

1. Monitoring of the channel and receiving data by sessions.

2. Transfer data to the indicator class (as binary code), which can be operated as an object (indicator class represents the array of 7 ones / zeros).

3. Verification of the possibility to form «digits» in every position of the card (cycle by all sessions). Inside the cycle a new cycle for each sequence begins, in turn each indicator appears as «true» (we believe that it has a figure in itself).

Inside the cycle the verification is being conducted and if the current position is «true», then a version in which inverted generator indicator is written is being created and in case it is «wrong», position of the indicator is recorded. After each cycle within a single sequence the intersection of the previous versions of the sequence is executed and if all the sequences in the current session had been crossed then we release them, i.e. the end leaves (options) are reviewed and their copies are thrown out.

4. Review of all the sequences in all sessions. The intersection of letters between sessions serially (the first session from the second is a result from the intersection of the third session, etc.). After each intersection adjacent session leaves the leaves are «clean» from copies.

5. The intersection of all session letters among themselves. Cycle through all the letters so each option (leaf) is checked for input by generator data, if it has a conflict with some of the indicators then this letter (option) is discarded. As a result, there will be only one option which does not conflict with any of the sequences of all the sessions.

6. Displaying the final version of output.txt in binary formatted string.

Plastic PassWindow cards monitoring algorithm is shown in Fig. 4.

5 RESULTS

Designation SMS-systems or two-factor authentication based on mobile phones is a mistake, a more precise term is «out-of-band» authentication. Nevertheless with the spread of GSM, smartphones and tablets connected to the network, even this safety advantage may be lost if a user transaction authentication is performed on the mobile device itself. In addition, the growth of unwanted software for mobile devices now allows an attacker to gain access to the authentication codes sent via SMS, not only with the traditional interception by a malicious software [5], but also by intercepting and decrypting data sent over the GSM-network telecommunications [6]. Mobile devices authentication attacks are performed successfully even without such technologies. Instead, an attacker simply impersonating a user of the device, and requests all SMS messages to be sent to another phone number for the entire attack period [3]. Another authentication method uses the camera a mobile device to read the barcode image on the user's workstation, which is coded with the OTP information about the transaction. This method contains the mistake of assuming that the operating system on the user's mobile device is not exposed to such a vulnerability to malicious software, like all other forms of software working with the network [8].

In the case of biometric authentication user data are available for online authentication.

However, biometric authentication devices can not communicate from local devices or network without being confronted by malicious programs and / or «Man in the middle» attacks [9]. This method is also impossible to re-edit after the attacker has posed oneself as a user by using biometric authentication.

Biometric authentication provides a user-friendly way of generating online user name, but listening to the network and a compromised device, the overall safety performance of such methods is not better than when using normal user name and password.

Electronic hardware tokens come in several types and include various security authentication functions.

The most commonly hardware tokens generate one-time passwords (OTP) using cryptographic algorithms with an internal secret key, or, more often, the secret key is generated on the basis of common values of the synchronized system time. User reads the displayed numbers on a device and manually enters them into one's terminals to cross-reference with the authentication server.

This simple method of generating electronic OTP is vulnerable to attacks by an «intermediary» because users are obliged to disclose the OTP without the means of checking the authentication context.

In response, many token manufacturers have added a small digital keypad, significantly increased the token size, but allowing the user to enter information about specific transactions that have been encrypted with a secret key before the user inputs the result to one's terminal. This is a type of verification or signature of a transactions and it does provide some protection against «Man in the middle» attack.

Nevertheless, this method is still vulnerable to attacks using laborious manual process of a transaction signing. Time and attention necessary to perform a manual operation are successfully used to distract the user from the context of the transaction information that one accepts, and, consequently, attacks can be successfully committed on a massive scale [10–11].

Printed OTP lists / number grids. An older method of providing one-time password is printed lists of randomly generated passcodes or transaction authorization codes on a sheet of paper or a sketch-card. Each access code is requested in sequence and is used to authenticate a transaction.

Alternatively, printing the symbol table can be used, and an authentication server will issue a bar code, prompting the characters located in certain coordinates.

Both methods use the keys and the signals that may be communicated verbally. This allows an attacker to ask the user to the next valid code by malware using social engineering and phishing attacks. Moreover, the relatively low lists or grids entropy requires frequent keys change in order to prevent repeated code request by an attacker.

These techniques are vulnerable to the full range of «Man in the middle» attacks for the same reasons that all the authentication methods with an unknown context.

For the sake of PassWindow vulnerability testing against such an attack, was created an hacking algorithm, which tries to use these principles to perform this analysis.

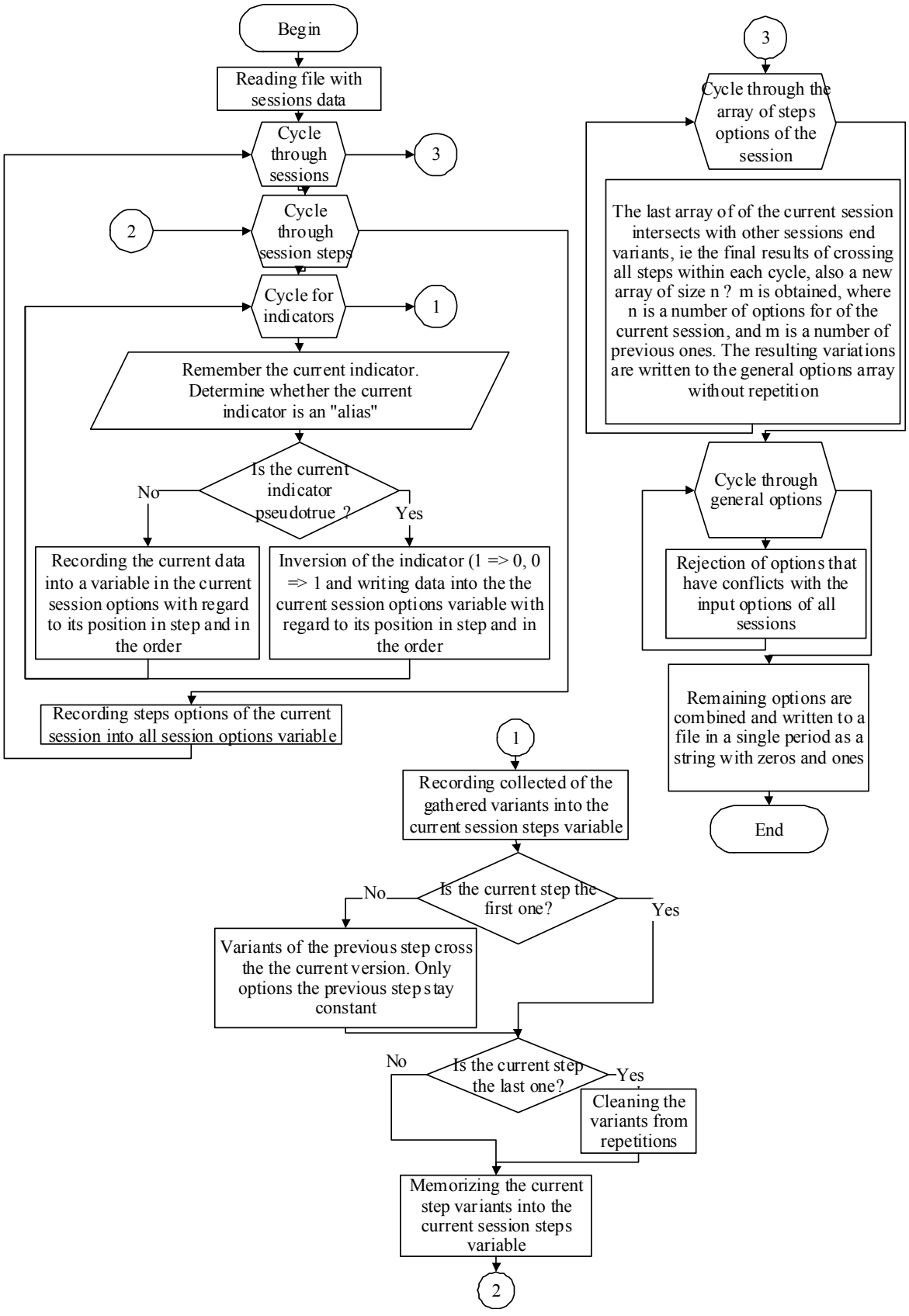


Figure 4 – Plastic PassWindow cards monitoring algorithm

The algorithm itself uses the technique of brute force. It begins by generating all combinations with the result that the numbers are the result that can be placed in the template.

For example, a six-figure result in the pattern of 14-columns provides the following options (among others):

2 – 5 – 7 – 2 – 4 – 3 – – –

2 – 5 – 7 – 2 – 4 – – 3 – –

2 – 5 – 7 – 2 – 4 – – – 3 –
2– – 5– – 7 – 2 – 4 – – 3.

Each combination is estimated by well-known barcode to calculate whether he could imagine the digit in the request or not.

Segments can either be present, if they are necessary to build the solution or not, if they must be absent for it, or may be unknown, if the segment is far from the digit, or imposed on the barcode bit.

After a separate set of combinations for each interception, the algorithm looks for the incompatibility between the combinations. It takes the first combination of the first set, comparing it in turn with each of the combinations of the second set. If it is incompatible with each combination of the second group, the combination is discarded.

Compatibility check continues so that each combination in each set is compared with the combinations of each other set. If the combination is discarded, then each subsequent set needs to be revised. By sorting and analysing sufficient number of interceptions algorithm is able to derive the key pattern with sufficient reliability.

However, this attack requires a significant amount of interceptions by an attacker: 20–30 in case of small patterns, hundreds of templates for large, several thousand in the case of using the method in the animation mode of increased security.

Thus, the PassWindow safety is not so much the complexity of the algorithm needed to solve it, as the systemic extracting enough information from the target difficulties. If PassWindow used correctly, there is a high probability that the necessary information may not be available, even for the most experienced hackers.

Let concider the Fake (weakened) PassWindow barcodes.

An attacker can try to weaken the protection, changing the frame rate of real (intercepted) barcode before delivering weakened (simplified) bar code to the user. This method reduces the entropy of the bar code in order to change details that could facilitate the analysis intercepting of requests / responses. However, clearly the damaged barcode passively alerts the user to attempt an attack, causing his suspicions about the use of computing and communication channels.

However, this attack requires a considerable amount of interceptions by an attacker: from 20 to 30 in case of small templates and hundreds for large ones, several thousand in the case of using the method in the animation mode with advanced security mode [1].

Thus PassWindow security is not so much the complexity of the algorithm required to solve it, but the difficulties in the system problems of sufficient information retrieval from the target. If PassWindow is used correctly, there is a high probability that the required information may not be available even for the most experienced hackers.

The authors offer their algorithm of PassWindow system monitoring, which allows in 3–5 sessions of transmission of OTP passwords to get a unique card barcode of a user that almost leads to destruction of the safety of the banking system.

6 DISCUSSION

Hypothetical attacks on authentication means PassWindow.

Man in the middle and phishing attacks (MITM) involve a third party intercepting communications between a client and server, impersonating each to the respective other and intercepting, recording, and/or altering communications between them [12].

Phishing is a kind of MITM attack that usually involves a fake login screen for well-known online services that reports login details to the attacking third party before seamlessly forwarding the user to their desired destination, unaware that their authentication details have been compromised to be used maliciously later [13].

This attack method is the most effective one. Standard methods for one-time password (OTP) are unable to provide protection because the OTP itself is simply passed to an attacker, together with any other relevant information, such as user name and password.

PassWindow solves this problem by providing a passive check at the transaction level to ensure that the user knows about the authenticity of the transaction, which one performs to enter OTP at the completion of this transaction. Thus, PassWindow protects transactions against fraudulent MITM attacks and provides authentication both ways from the user to the server and the server to the user.

Let concider the Social engineering attacks.

Social engineering involves the customer being convinced to reveal their private details, and in the case of hardware tokens, their OTPs.

A PassWindow key pattern is not easily communicated verbally or by typing, thereby eliminating the most convenient telephone social engineering attacks that are used against electronic hardware tokens, a method that is called «vishing» [14]. These attacks are based on the person who calls the user and impersonating an authorized service representative.

An oral request is made to read a valid authorization code from the authentication device of victim that supposedly allow the caller to identify, for example, «an important confidential information». It is unlikely that an attacker will try to extract the PassWindow key combination from the client this way, as it is difficult to explain in words the visual characteristics of the PassWindow matrix segment.

Man in the browser or hacker infiltration. When an attacker receives reports from the malware installed in the victim's computer and detects that the victim is accessing their financial institution's website, the software alters the form data in the browser such that a different amount of funds are transferred to a different account – usually a 'mule' account. The owner of the mule account then transfers this money to the attacker.

Verification information about the transaction taking place can be encoded into the PassWindow challenge pattern. This can assure the user, for example, that the funds are being transferred to the correct account.

Let concider the Simple theft.

The only way for a PassWindow key pattern to be revealed and duplicated is by directly copying the card in one's immediate possession. This possibility is reduced by the introduction of a tint that can be printed over the pattern, hindering attempts at photography and photocopying.

However, because PassWindow should be used as the second factor in the authentication strategy, mere knowledge of the key pattern is insufficient for fraudulent authentication without also knowing the victim's username and password.

Shoulder surfing. While probably the most mundane of the 'hacking methods', PassWindow is secure against 'shoulder surfing' – surreptitiously watching the user enter their transaction details. Because the key/challenge solution

is a one-time password, the shoulder surfer cannot benefit from knowing it.

Again, a tint printed over the key pattern on the card renders the pattern itself invisible to anyone but the user.

Direct attack on a PassWindows authentication server. An attacker can try to directly attack a PassWindows authentication server, to disrupt the integrity of the PassWindow authentication procedure. The PassWindow authentication server uses very simple and limited communication protocol, and the entire authentication processing is performed on the server. Its functionality is limited to the creation of the barcode image data and receiving short access codes and user IDs, and eventually making a response (yes / no) to the authentication request. In addition, different authentication strategies run queries speed and response duration. This basic digital communications with the authentication server give a small opportunity for an attacker to directly occupy the server in any effective manner, which may lead to a successful access.

Let concider the Analytic attack on the secret key.

An attacker can try to bring a printed the PassWindow key combination of a user through the analytical (e.g. statistical or algebraic) attack. This can be done using a complex program «attack of the man in the middle» or malicious programs installed locally on the basis of monitoring that will allow to intercept PassWindow barcodes and appropriate user responses. With the time, as the attacker accumulates these pairs of request / response, one can potentially get some idea about the PassWindow key template through the analysis of the captured data.

CONCLUSIONS

In this paper, the theoretical generalization of major the increase principles of integrity and authenticity of data packets in security banking transactions protocols based on authentication methods of the two-factor authentication.

Scientific novelty lies in the fact that, for the first time proposed mathematical tools and program implementation of the PassWindow system monitoring allows to get a unique barcode of the user's card for 3–5 OTP passwords transmission sessions, which almost leads to destruction of the banking system safety.

ACKNOWLEDGEMENTS

Work was executed within the concept of the National Informatization Program, approved by the Law of Ukraine «On the Concept of National Informatization Program» dated 4 February 1998 № 75/98-VR.

Concept (Principles of Public Policy) of the National Security of Ukraine, adopted by the Supreme Council of Ukraine on 16 January 1997 № 3/97-VR.

Tactical and technical task for research work: – № 36B113 «Development of methods for improving efficiency of transmission and protection of information in telecommunication systems».

REFERENCES

1. Evaluation of hypothetical attacks against PassWindow [Electronic resource] / S. O'Neil // PassWindow – 2009. – Access mode: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
2. Двухфакторная Аутентификация [Электронный ресурс], *Aladdin,* 2014, Режим доступа: http://www.aladdin-rd.ru/solutions/authentication.
3. Настройка двухфакторной аутентификации [Электронный ресурс], *Citrix,* 2012, Режим доступа: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru.
4. Семь методов двухфакторной аутентификации [Электронный ресурс], *ITC.ua*, 2007, Режим доступа: http://www.infosecurityrussia.ru/news/29947.
5. Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication [Electronic resource] / E. Chickowski // Information week – 2010. – Access mode: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495.
6. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication [Electronic resource] / E. Barkan, E. Biham, N. Keller // ACM digital library. – 2008. – Access mode: http://dl.acm.org/citation.cfm?id=1356689.
7. $45k stolen in phone porting scam [Electronic resource] / Brett Winterford // ITnews – 2011. – Access mode: http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0.
8. Zeus Banking Trojan Hits Android Phones [Electronic resource] / M. J. Schwartz // Information week. – 2011. – Access mode: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909.
9. Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth [Electronic resource] / [C. Zeitz, T. Scheidat, J. Dittmann; at all.] // Proceedings of SPIE. – 2008. – Access mode: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632.
10. Trojan Writers Target UK Banks With Botnets [Electronic resource] // TechWorld. – 2010. – Access mode: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets.
11. Belgian court found fraud in Internet banking [Electronic resource] / Het Belang Van Limburg // PassWindow – 2010. – Access mode: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
12. Network Forensic Analysis of SSL MITM Attacks [Electronic resource] // NETRESEC Network Security Police Service – 2011. – Access mode: http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks.
13. Internet Banking Targeted Phishing Attack [Electronic resource] // Metropolitan Police Service – 2005. – Access mode: http://www.webcitation.org/5ndG8erWg.
14. Spike in phone phishing attacks [Electronic resource] / Brian Krebs // KrebsOnSecurity – 2010. – Access mode: http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks.

Article was submitted 07.11.2014.
After revision 21.11.2014.

Евсеев С. П.[1], Томашевский Б. П.[2]

[1]Канд. техн. наук, доцент кафедры информационных систем Харьковского национального экономического университета им. С. Кузнеца, Харьков, Украина

[2]Канд. техн. наук, ведущий научный сотрудник, старший научный сотрудник научно-исследовательского отдела ракетных войск и артиллерии научного центра сухопутных войск, Харьков, Украина

ИССЛЕДОВАНИЕ УГРОЗ МЕТОДОВ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

В статье рассматриваются основные методы построения системы двухфакторной аутентификации на основе использования криптографических механизмов обеспечения криптостойкости, формируемых аутентификаторов, оценивается риск различных методов онлайн-атак против различных систем двухфакторной аутентификации, а также рассматривается система PassWindow, обеспечивающая двухфакторную аутентификацию на уникальной способности части матриц передавать информацию таким образом, что она расшифровывается только при наложении физического шаблона знаков предполагаемого получателя и шаблона штрих-кода, получаемых через

электронно-сетевые устройства пользователей, стойкость к анализу обеспечивается уникальностью формирования шаблона штрих-кода карточки в виде уникальных статистических изображений, последовательности символов или в виде более расширено анимационной версии.

Объектом исследования является процесс повышения целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций на основе методов двухфакторной аутентификации. Предметом исследования являются методы и алгоритмы контроля целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций на основе методов двухфакторной аутентификации.

Целью работы является повышение целостности и аутентичности пакетов данных в протоколах безопасности банковских транзакций, оценка угроз на методы двухфакторной аутентификации. Проводится сравнительный анализ различных систем двухфакторной аутентификации с системой PassWindow в сфере противостояния различным интернет-сценариям атак. Предлагается эффективный практический метод мониторинга системы двухфакторной аутентификации PassWindow при ее применении в банковских системах.

Ключевые слова: двухфакторная аутентификация, онлайн-атаки, социальная инженерия.

Евсеев С. П.[1], Томашевский Б. П.[2]

[1]Канд. техн. наук, доцент кафедри інформаційних систем Харківського національного економічного університету ім. С. Кузнеця, Харків, Україна

[2]Канд. техн. наук, провідний науковий співробітник, старший науковий співробітник науково-дослідного відділу ракетних військ та артилерії наукового центру сухопутних військ, Харків, Україна

ДОСЛІДЖЕННЯ ЗАГРОЗ МЕТОДІВ ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ

У статті розглядаються основні методи побудови системи двофакторної аутентифікації на основі використання криптографічних механізмів забезпечення криптостійкості, аутентифікаторів, які формуються, оцінюється ризик різних методів онлайн-атак проти різних систем двофакторної аутентифікації, а також розглядається система PassWindow, що забезпечує двофакторну аутентифікацію на унікальній здатності частини матриць передавати інформацію таким чином, що вона розшифровується тільки при накладенні фізичного шаблону знаків передбачуваного одержувача і шаблону штрих-коду, одержуваних через електронно-мережеві пристрої користувачів, стійкість до аналізу забезпечується унікальністю формування шаблону штрих-коду картки у вигляді унікальних статистичних зображень, послідовності символів або у вигляді більш розширено анімаційної версії.

Об'єктом дослідження є процес підвищення цілісності та автентичності пакетів даних у протоколах безпеки банківських транзакцій на основі методів двофакторної аутентифікації. Предметом дослідження є методи та алгоритми контролю цілісності та автентичності пакетів даних у протоколах безпеки банківських транзакцій на основі методів двофакторної аутентифікації.

Метою роботи є підвищення цілісності та автентичності пакетів даних у протоколах безпеки банківських транзакцій, оцінка загроз на методи двофакторної аутентифікації. Проводиться порівняльний аналіз різних систем двофакторної аутентифікації з системою PassWindow у сфері протистояння різним інтернет-сценаріями атак. Пропонується ефективний практичний метод моніторингу системи двофакторної аутентифікації PassWindow при її застосуванні в банківських системах.

Ключові слова: двофакторна аутентифікація, онлайн-атаки, соціальна інженерія.

REFERENCES

1. Sean O'Neil Evaluation of hypothetical attacks against PassWindow [Electronic resource], *PassWindow*, 2009, Access mode: http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
2. Dvuxfaktornaya Autentifikaciya [Electronic resource] // Aladdin – 2014. – Access mode: http://www.aladdin-rd.ru/solutions/authentication.
3. Nastrojka dvuxfaktornoj autentifikacii [Electronic resource] // Citrix – 2012. – Access mode: http://support.citrix.com/proddocs/topic/web-interface-impington/nl/ru/wi-configure-two-factor-authentication-gransden.html?locale=ru.
4. Sem' metodov dvuxfaktornoj autentifikacii [Electronic resource] // ITC.ua – 2007. – Access mode: http://www.infosecurityrussia.ru/news/29947.
5. Chickowski, Ericka Man In The Mobile Attacks Highlight Weaknesses In Out-Of-Band Authentication [Electronic resource], *Information week*, 2010, Access mode: http://www.darkreading.com/risk/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication/d/d-id/1134495.
6. Elad Barkan, Eli Biham, Nathan Keller Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication [Electronic resource], *ACM digital library*, 2008, Access mode: http://dl.acm.org/citation.cfm?id=1356689.
7. Brett Winterford $45k stolen in phone porting scam [Electronic resource], *Itnews*, 2011, Access mode: http://www.itnews.com.au/News/282310,45k-stolen-in-phone-porting-scam.aspx/0.
8. Schwartz, Mathew J. Zeus Banking Trojan Hits Android Phones [Electronic resource], *Information week*, 2011, Access mode: http://www.informationweek.com/mobile/zeus-banking-trojan-hits-android-phones/d/d-id/1098909.
9. Christian Zeitz; Tobias Scheidat; Jana Dittmann; Claus Vielhauer; Elisardo González Agulla; Enrique Otero Muras; Carmen Garc a Mateo; José L. Alba Castro Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth [Electronic resource], *Proceedings of SPIE*, 2008, Access mode: http://spie.org/Publications/Proceedings/Paper/10.1117/12.767632.
10. TechWorld Trojan Writers Target UK Banks With Botnets [Electronic resource], 2010, Access mode: http://news.techworld.com/security/3228941/trojan-writers-target-uk-banks-with-botnets.
11. Het Belang Van Limburg Belgian court found fraud in Internet banking [Electronic resource], *PassWindow*, 2010, Access mode, http://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.
12. Network Forensic Analysis of SSL MITM Attacks [Electronic resource], *NETRESEC Network Security Police Service*, 2011, Access mode: http://www.netresec.com/?page=Blog&month=2011-03&post=Network-Forensic-Analysis-of-SSL-MITM-Attacks.
13. Internet Banking Targeted Phishing Attack [Electronic resource], *Metropolitan Police Service,* 2005, Access mode: http://www.webcitation.org/5ndG8erWg.
14. Brian Krebs Spike in phone phishing attacks [Electronic resource], *KrebsOnSecurity*, 2010, Access mode: http://krebsonsecurity.com/2010/06/a-spike-in-phone-phishing-attacks.

UDC 681.3.06 (0.43)

Korol O. G.

Lecturer of Department of Information Systems, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine

ENHANCED MAC ALGORITHM BASED ON THE USE OF MODULAR TRANSFORMATIONS

The article considers the choice of cycle functions in the provable persistent key universal hashing scheme, proposed model and method of forming codes of integrity and authenticity of data on the basis of modular transformations, computational complexity reduce algorithm of the hashing schemes implementation using cyclic functions. The object of the research is the process of improving the integrity and authenticity of data packets in security protocols of telecommunication networks. The subject of the study are models, methods and algorithms for monitoring the integrity and authenticity of data packets in security protocols of telecommunication networks. The purpose of the study is to increase the integrity and authenticity of data packets in security protocols of telecommunication networks. The developed enhanced method of forming a cascade MAC differs from the known (algorithm UMAC) using modular hashing on the last stage of the MAC forming that provides high collision properties of strictly universal hashing and safety performance at the level of modern means of demonstrable strength protection. Were obtained estimates of the computational complexity of the formation of the MAC using modular hashing, found, that with comparable rates of resistance the complexity of modular hashing exceeds by 1–2 orders of known schemes based on block symmetric ciphers. However, the use of modular transformations provides provable security and high collision properties of strictly universal hashing.

Keywords: codes of integrity and authenticity of data, a modular transformation, universal classes of hash functions.

NOMENCLATURE

gcd(x, y) is a greatest common divisor of x and y;
D is a dispersion;
f is a composition of f_1 and f_2;
f_1 is a set of functions performing the mapping $X \to U$;
f_2 is a set of functions performing the mapping $U \to Y$;
m is a mathematical expectation;
H is a set of functions f;
H_0 is an initialization vector;
H_1 is a set of functions f_1;
H_2 is a set of functions f_2;
k is a number of elements in binary representation of n;
Key is a key rule;
L is a bit processor;
m_i is a i-bit in binary representation of n;
n is an exponent ;
$O(n)$ is a computational complexity;
p is a large prime integer;
q is a large prime integer;
U is a set of u numbers;
u is a count of numbers in set U;
X is a set of n numbers;
x is a number to be raised;
Y is a set of m numbers;
α is a generator of the ring of integers Z_p;
ε is a fixed accuracy;
$\vee$ is a bitwise logical OR operation;
$\perp n$ is a save lesser n-bits of m-bit result operation;
$\oplus$ is a modulo 2 (XOR).

INTRODUCTION

Studies have shown that the use of modular transformations allows realizing of provably resistant information hashing that satisfies the collisional properties of universal hash functions. Demonstrably safe level of strength is justified by reducing the problem of finding the source and / or the problem of recovering the secret key data to the solution of one of the well-known complexity-theoretic problems [1–3, 6].

At the same time, as shown by studies [1–3, 6], the universal hashing using modular transformations has a significant drawback – high computational complexity of the formation of the hash codes. In fact, for each information unit must perform a modular exponentiation that under transformation module appropriate orders significantly increases the time hashing information sequence. A promising direction in this regard is the development of multilayer universal hashing circuits using modular transformations on the last, the final stage of the hash code formation. This is as shown below, on the one hand provides a high collision properties of the resulting codes of integrity and authenticity of data generation circuit, on the other hand – provides high performance and provable strength level used transformations.

1 PROBLEM STATEMENT

The use of multilayer hash key circuits allows building of effective mechanisms for monitoring the integrity and authenticity of information in telecommunication systems and networks. However, the known multilayer structure (for example, the algorithm UMAC) together with the high speed and the cryptographic strength when applying a cryptographic transformation layer (using symmetric block cipher) lose universal hash properties, which leads to deterioration of the properties of the collision properties of generated message authentication codes. The purpose of the study is to develop a method of forming codes of integrity and authenticity of data based on provably resistant hash key that allows providing high levels of security and with applying certain restrictions on the modular transformations provide high collisional properties.

2 REVIEW OF THE LITERATURE

The analysis of [6–9] shows that the modular transformations are used today in the construction of keyless hash functions. Thus, in the fourth part of the international standard ISO/IEC 10118-4 defined two keyless hash function MASH-1 and MASH-2, which use modular arithmetic, namely the modular exponentiation to construct hash [9]. The very name of functions MASH-1 and MASH-2 occurs

DOI 10.15588/1607-3274-2015-1-8

from abbreviated Modular Arithmetic Secure Hash (secure hashing based on modular arithmetic), emphasizing the use of modular transformations in the formation of the hash image.

Table 1 shows the results of a comparative analysis of performance of some keyless hash functions, including the hash function on the modular arithmetic MASH-1 and MASH-2 [7].

The analysis showed that the major drawback of hash functions MASH-1 and MASH-2 is the low hash code formation rate. In fact, it is determined by the speed of RSA-like encryption, which is 2–3 orders of magnitude slower than modern block symmetric ciphers. However, due to the presence of the possibility of using the existing modular arithmetic hardware and software used in asymmetrical RSA-like cryptosystems, as well as because of the possibility of providing a provable strength level (on the classification of security models NESSIE) considered keyless hash MASH-1 and MASH-2 were standardized [7, 9, 16].

3 MATERIALS AND METHODS

Development of a universal key hashing method with demonstrable strength based on modular transformations.

In the basis of the proposed universal key hashing method with provable strength is the use of modular transformations, providing reduction of the problem of finding the inverse image or a secret key in hashing scheme to one of the well-known complexity-theoretic problems. Such a justification of strength by security models classification NESSIE is considered to be provable security, thus emphasizing the reducibility cryptanalysis to one of the well-known computationally intractable in a given time complexity-theoretic problems [6]. Table 2 shows the results of studies of cyclic functions: the first column contains the complexity-theoretical problem of the function, the second column shows the cyclic function analytical record, in the third column – estimate of the calculating complexity of the cyclic function values, the fourth – estimate of computational complexity of the function inverting (strength estimation).

Studies have shown that the most appropriate solution should obviously consider the use of the cyclic function, the problem of inverting which is associated with the solution of the complexity-theoretic problem of the extraction of square roots modulo n.

Under certain restrictions on the values of the composite module n this computational complexity inverting problem comparable to the problems of factorization and discrete logarithms. At the same time, the direct calculation of the

Table 1 – A comparative analysis of some keyless hash functions

The hash function	The length of hash	Applied conversion	Processing speed	Security model (by NESSIE)
SHA-2	256, 384, 512	logical and arithmetic	108..109 bit/sec	Practical Security
Whirlpool	512	In finite Galois fields	107..108 bit/sec	Practical Security
GOST 34311-95	256	Block symmetric encryption	107..108 bit/sec	Practical Security
RIPEMD-160	160	logical and arithmetic	108..109 bit/sec	Practical Security
MASH-1	*	Modular squaring	105..106 bit/sec	** «Provable» Security
MASH-2	*	Modular exponentiation 28+1 = 257	104..105 bit/sec	** «Provable» Security

* Determined by the dimension of the conversion module.

** If the parameters of the modular exponentiation comply with the limits for RSA-like systems.

Table 2 – Estimate of the complexity of some complexity-theoretic problems

Complexity-theoretic problem	Candidates for the construction of the cyclic function	Estimate of the computing complexity	Estimate of the inverting complexity
Integer factorization problem	$f(x_i, H_{i-1}) = x_i H_{i-1}$, Function is defined over large prime numbers $x_i = p$ and $H_{i-1} = q$	$O(n^2)$, where $n = \lceil \log_2 p \rceil + \lceil \log_2 q \rceil$	$L_N(\alpha,\beta) = \exp\left((\beta + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right)$ For the field number of the general form of the inverting complexity $L_N\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right)$, For a field number of a special type $N = a^b + c$ the complexity of the inversion is $L_N\left(\frac{1}{3}, \sqrt[3]{\frac{32}{9}}\right)$
RSA problem	$f(x_i, H_{i-1}) = (x_i \oplus H_{i-1})^e \bmod (N)$, $\gcd(e, \varphi(p,q)) = 1$, $N = pq$	$O(\log_2 e)$ multiplications, the fast exponentiation algorithm	
The discrete logarithm problem	$f(x_i, H_{i-1}) = \left(\alpha^{x_i \oplus H_{i-1}}\right) \bmod (p)$, α – generator Z_p	$O(\log_2 n)$ multiplications, the fast exponentiation algorithm, $O(n^3)$ for $\alpha = 2$, where $n = \lceil \log_2 p \rceil$	$\min\left\{\sqrt{p}, L_N(\alpha,\beta)\right\}$, where $L_N(\alpha,\beta) = \exp\left((\beta + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\right)$ For a primitive field $GF(p)$ the complexity of the inversion is $\min\left\{\sqrt{p}, L_N\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right)\right\}$, For a primitive field $GF(2^m)$ the inversion complexity is $L_N\left(\frac{1}{3}, 1.4\right)$
Diffie-Hellman problem	$f(x_i, H_{i-1}) = \left(\alpha^{x_i \oplus H_{i-1}}\right) \bmod (p)$, α – generator Z_p	$O(n^3)$ for $\alpha = 2$, where $n = \lceil \log_2 p \rceil$	

values of $a \equiv \left(x^2\right) \bmod(n)$ requires significantly fewer operations.

It should be noted, however, that the use of a quadratic cycle function does not lead to construction of a universal hashing. Next to the computational complexity is a cyclic function

$$f\left(x_i, H_{i-1}\right) = \left(x_i \oplus H_{i-1}\right)^e \bmod(N), \qquad (1)$$

inversion problem which is associated with the solution of the complexity-theoretic problem in RSA, where

$$\gcd\left(e, \varphi(p,q)\right) = 1,\ N = pq\,.$$

Thus, the use of cyclic function (1) based on modular exponentiation allows to construct a provably resistant universal hash function only under the constraints on the value of the modular exponent and absolute value of the change.

Another candidate for the cyclic function in the iterative hashing scheme is a function of the form:

$$f\left(x_i, H_{i-1}\right) = \left(\alpha^{x_i \oplus H_{i-1}}\right) \bmod(p), \qquad (2)$$

inversion problem which is associated with the solution of the complexity-theoretic problem of the discrete logarithm.

Use of a cyclic function ensures the construction of provably resistant hash, collision properties which satisfy the conditions of universality.

Thus, studies have shown that for the construction of universal hash information with provable security level should be used the cyclic function of the form (1) or of the form (2).

Development of algorithms for iterative key hashing with demonstrable strength based on modular transformations.

Iterative key hash algorithms with demonstrable strength based on the use of modular transformations is based algorithm MASH-1, subject to change initialization vectors and use of the above cyclic functions satisfying certain restrictions on used modular transformations.

Iterative key hashing scheme using cyclic function (1) developed by analogy with the scheme in Section 2 *NH* hashing is shown in Fig. 1. An algorithm for calculating the hash value based on the cyclic function (1) differs from the algorithm MASH-2, basically, by system settings and the determination of constants.

Using the cyclic function (2), the inversion problem of which is based on the solution of the complexity-theoretic problem of the discrete logarithm, construct the following hashing scheme (see Fig. 2).

Designed algorithms differ from the keyless hash algorithms MASH-1 and MASH-2 basically, by system settings and the determination of constants. In addition, the proposed schemes are key hashing, as the secret key data used interchangeable initialization vector H_0 = Key. For applied modular transformations in key hashing cyclic function imposed limitations discussed above.

Thus, the proposed universal hashing method using modular transformations allows formation of authenticators (hashes) to provide the required performance security. Designed algorithms allow practically implement the proposed hashing schemes in software and in hardware form.

4 EXPERIMENTS

Development of proposals for the implementation of the iterative hash key with demonstrable strength using modular transformations.

The proposed universal hashing method is an iterative scheme of formation of the hash code with the cyclic function, built using modular transformations. To ensure high collision properties of universal hashing proposed cyclic function must be implemented with the use of the expressions (1) or (2) with the corresponding constraints on the modular transformations.

The analysis shows that the most expensive from a computational point of view the operation in the implementation of cycle functions (1) and (2) is the operation of modular exponentiation. With the direct exponentiation operations through the chain of multiplications, computational complexity of the implementation of such cyclic functions increases in proportion to the exponent, i.e. for the construction of x the power n generally needs $n-1$ multiplications:

$$x^n = \underbrace{x \cdot x \cdot x \cdot \ldots \cdot x}_{n-1 \text{ multyplications}}\,.$$

An asymptotic estimate of the computational complexity of this exponentiation operation implementation is $O(n)$ multiplications.

To reduce the computational complexity of the implementation of the hashing scheme using cyclic functions (1) and (2) algorithm applied for fast

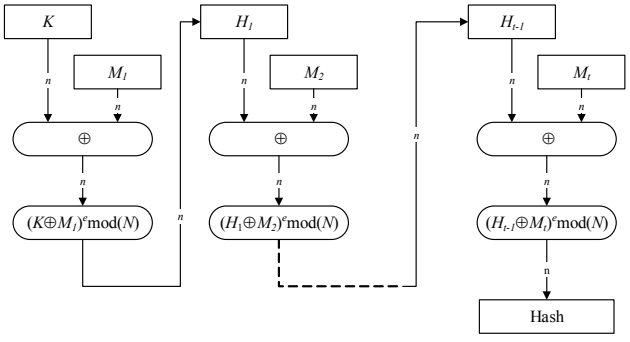


Figure 1 – Iterative key hashing scheme using the expression (1)

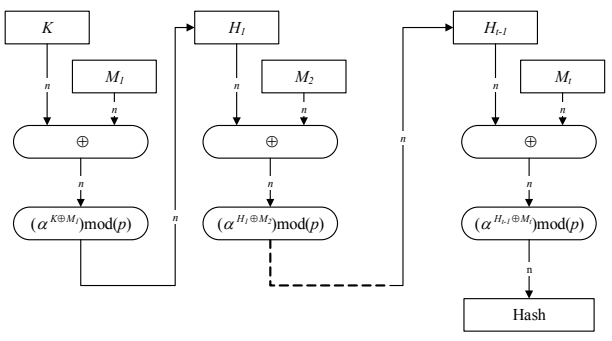


Figure 2 – Iterative key hashing scheme using the expression (2)

exponentiation, which is based on the representation of x^n in the following form:

$$x^n = x^{((...((m_k \cdot 2+m_{k-1})\cdot 2+m_{k-2})\cdot 2+...)\cdot 2+m_1)\cdot 2+m_0} =$$

$$= ((...(((x^{m_k})^2 \cdot x^{m_{k-1}})^2...)^2 \cdot x^{m_1})^2 \cdot x^{m_0}, \quad (3)$$

where $(m_k, m_{k-1},...,m_0)$ – binary representation of n, i.e. $m_i \in \{0,1\}$ and

$$n = m_k \cdot 2^k + m_{k-1} \cdot 2^{k-1} + ... + m_1 \cdot 2 + m_0. \quad (4)$$

Rearranging the factors in the representation of x^n we obtain the following expression:

$$x^n = x^{m_0} \cdot (x^2)^{m_1} \cdot (x^{2^2})^{m_2} \cdot (x^{2^3})^{m_3} \cdot ... \cdot (x^{2^k})^{m_k},$$

which implies that for the construction of a number x to the power of n required to implement at most k operations of squaring and at most k operations of multiplication, where $k+1$ – number of elements in the binary number n, i.e. $k = (\log_2 n) - 1$. Thus, the computational complexity of calculating the asymptotic x^n can be estimated as $O(\log_2 n)$.

The above algorithm can significantly speed up the computation of cyclic functions (1) and (2) underlying the proposed method of universal hashing. Table 3 shows the dependence of the implementation complexity of the operation of exponentiation through a chain of multiplications and through the representation (3), (4), indicating the minimum necessary order of the conversion module to achieve the required level of security.

The data in the second row of table 3 shown using the equivalence conditions (on computational complexity) of the squaring and multiplication operations.

Analysis of the data in table 4 shows that the implementation of the proposed universal hashing method through a traditional exponentiation algorithm computationally unattainable. The number of multiplications to be executed to compute a value of the cyclic function, even at the lowest level of security (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) exceeds the capabilities of most modern computer systems.

The last row of table 3 is, in fact, is the computational complexity estimate of the proposed hashing scheme. Thus, at the lowest level of strength (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) to calculate one value of cyclic function takes no more than 2046 operations multiplications. For a sufficient level of strength (cardinality of the set of key data BSC equal to 2128) relevant to the national standard encryption USA FIPS-197 (AES), to calculate the cyclic function need to do no more than 6142 multiplications. For high-level strength (cardinality of the set of key data BSC equal to 2256), corresponding to the current domestic standard symmetric cryptoconversion GOST 28147-89, to calculate the cyclic function does not need to perform more than 30718 multiplications.

Developing a model of MAC cascade formation using modular transformations and justification of practical recommendations on its use.

The article proposes a cascade formation model of codes of integrity and authenticity of data (MAC) using the modular transformations. The proposed model is based on a multi-layer universal hashing circuit using the last, the final stage of modular transformations.

Properties of multilayer (composite) design is best explained with the help of mappings language [4, 5]. Let X, Y, U are sets of n, m, u elements, $n < m < u$. H_1 is a set of functions f_1 performing the mapping $X \to U$ and H_2 is a set of functions f_2 performing the mapping $U \to Y$. Then $H = H_2 \circ H_1$ is a set of functions f, which is the composition $f = f_1 \circ f_2$.

Characteristics of a multilayered structure presented by the results of the following theorem [1–3].

Theorem 1. The composition of the universal hash functions class $\varepsilon_1 - U(N_1, n, u)$ and strictly universal hash functions class $\varepsilon_2 - SU(N_2, u, m)$ is strictly a universal class with parameters $\varepsilon - SU(N_1 N_2, n, m)$, where $\varepsilon = \varepsilon_1 + \varepsilon_2 - \varepsilon_1 \varepsilon_2$.

Thus, using the composition of authentication codes algorithms that are equivalent to an algorithm for computing the universal and strictly universal hash functions classes we obtain a multi-layer scheme for generating MAC [11–15]. Properties thus generated codes of integrity and authenticity of data will satisfy the properties of strictly universal class of hash functions.

In the method of forming codes of integrity and authenticity of data, the first layers are proposed to be realized with traditional UMAC high-speed but cryptographically weak universal hashing schemes algorithm, the last layer is proposed to implement using the developed safe (cryptographically strong) strictly universal hashing scheme based on the modular transformations.

Formally, the proposed cascade formation scheme of codes of integrity and authenticity of data shown in Fig. 3.

The main part of the information data is processed first layers of universal hashing. Formed as a result of such conversion hash code on the last processed final stage cryptographically strong universal hash function based on the modular transformation.

Thus, based on the proposed scheme, MAC formation using modular transformations is used:

– on the first layers high-speed universal hashing methods (NH-hashing, polynomial hashing, Carter-Wegman hashing) are used;

– on the last layer secure strictly universal hashing based on modular transformations (using cyclic functions (1) and / or (2)) is used.

Table 3 – Dependence of the implementation complexity regarding the exponentiation method

Exponentiation method	Procedure for conversion module / equivalent length of symmetric cryptographic algorithm key		
	1024 / 80	3072 / 128	15360 / 256
Through a series of multiplications	10308	10924	104623
Fast exponentiation algorithm	2046	6142	30718

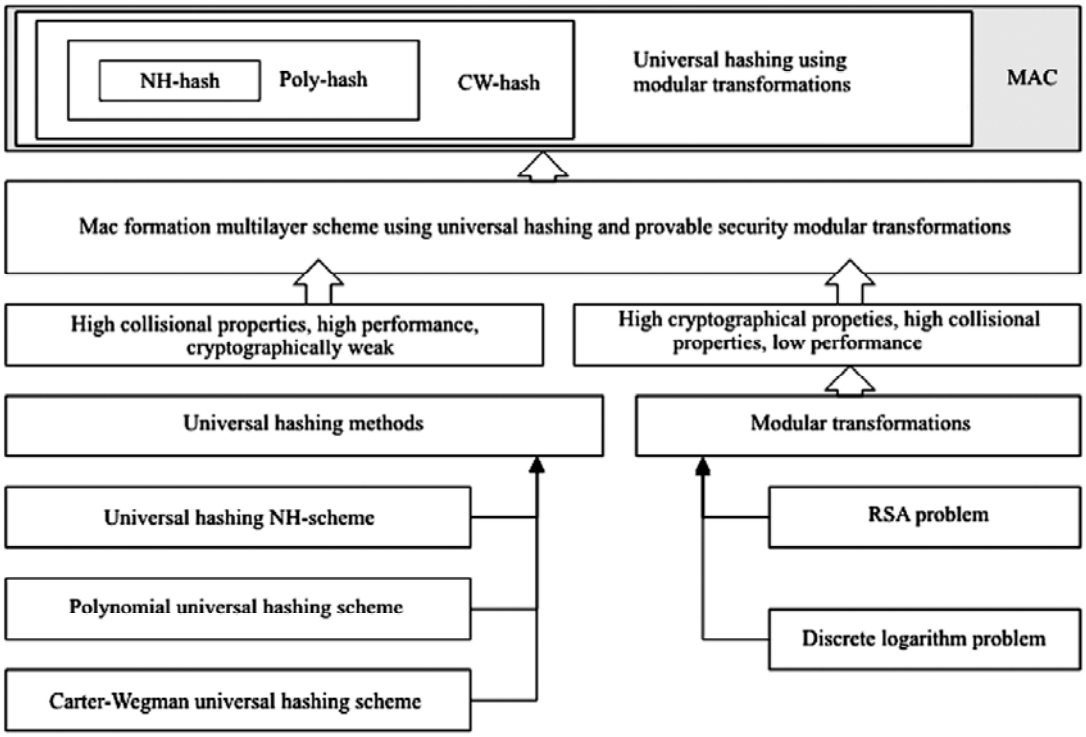


Figure 3 – Proposed cascade formation scheme control codes of integrity and authenticity of data using the modular transformations

The work [3] proposes technique of statistical studies of collisional properties of MAC, in particular, introduces statistical indicators characterizing the collision properties of forming circuit of control codes integrity and authenticity of data, allowing using methods of probability theory and mathematical statistics to obtain estimates with prescribed confidence interval and the required accuracy.

Experimental studies of collisional properties of message authentication codes UMAC for the relevant sections of the conversion:

– in the first stage investigate collision properties of a mini-version of the universal hashing. To do this, the theoretical estimates of the number of generated hash codes collisions occurring in the course of the experiment must be confirmed;

– in the second stage conduct an experimental study of the properties of pseudo-conflict substrates based on analysis of the properties of the reduced Baby-Rijndael cipher model. Similar studies in the available literature aren't described, appear to be carried out by us for the first time;

– in the third stage conduct an experimental study of the properties of collision properties generated by using mini-UMAC integrity and authenticity of data control. This is the most important part of the research, as it would answer the question of maintaining the properties of universal hashing after application of the cryptographic transformation of the information layer.

Estimates of the number of collisions generated elements will be carried out focusing on the universal hashing collision properties. In fact, we need to confirm or refute the hypothesis of the saving of universal hashing collision properties at all stages of generating of the mini-UMAC control codes of integrity and authenticity of data.

5 RESULTS

Consider a cyclic functions MASH-1 and MASH-2 for the construction of the key universal hash functions and hash option when the initial state (initialization vector) is given by some key rule, i.e. choose H_0 = Key. In this case, we have a certain class of hash functions, depending on the parameter Key. For experimental studies selected the following parameters: $p = 17,\ q = 19,\ N = 323$. Study were to verify the conditions of universal hashing with exhaustive search of all the values of initialization vectors $(\text{Key} = 0, ..., 2^m - 1, m = 8)$ for a sample of the population values of information blocks. The results obtained are summarized in table 3.

Thus, studies have shown that the application of transformations using modular arithmetic allows to build universal and strictly universal hash functions classes,

Table 3 – The results of studies of collisional properties of a key hashing algorithms built on the basis of MASH-1 and MASH-2 by changing the values of the initialization vector secret key

	Based algorithm MASH-1	Based algorithm MASH-2
$\widetilde{m}(n_1)$	41.42	0
$\widetilde{D}(n_1)$	42.74	0
$P_\partial = P(\lvert\widetilde{m}(n_1) - m(n_1)\rvert < 5)$	0.98	≈ 1
$\widetilde{m}(n_2)$	3.99	1
$\widetilde{D}(n_2)$	0.01	0
$P_\partial = P(\lvert\widetilde{m}(n_2) - m(n_2)\rvert < 0.025)$	0.99	≈ 1
$\widetilde{m}(n_3)$	0.26	0.31
$\widetilde{D}(n_3)$	0.21	0.22
$P_\partial = P(\lvert\widetilde{m}(n_3) - m(n_3)\rvert < 0.1)$	0.97	0.97

which on one hand allow high collision properties, on the other hand, under certain restrictions on the value of the modular exponential ensure high security and the applicability of the model demonstrable strength.

For comparison with other key hashing schemes in terms of the resistance and performance will take the following assumptions. Let one multiplication operation on numbers with the order of 2^m requires $\left\lceil \frac{m}{L} \right\rceil$ operations of bitwise modulo two addition (XOR). This assumption is most often used when evaluating the complexity of the cryptographic algorithms implementation. In this case, the estimate of $\left\lceil \frac{m}{L} \right\rceil$ gives the approximate number of L-bit processor cycles necessary for the implementation of the one multiplication operation of numbers the bit length of which does not exceed m. At the same time, hashing using modular transformations process immediately $m/8$ information data bytes.

Table 4 shows the results of comparative studies of the performance of key hashing schemes for fixed security performance. Speed is expressed in an S amount of the 32-bit processor cycles necessary for generating one byte of the output data. Security indicator was fixed over the length of the secret key the attacker needed to hack. For schemes on modular arithmetic the equivalent length of the key block symmetric cryptographic algorithm is shown (see. Table 2).

The data presented in Table 4 show that the use of modular transformations for solving the key hashing problems significantly increases the computational complexity and reduces algorithms speed by 1–2 orders of magnitude. At the same time, the proposed key hashing schemes have provably resistant safety level (problem of finding the hashing key or the inverse image is reduced to solving a certain complexity-theoretic problem). In addition, it was shown above that such authentication schemes satisfy the properties of universal hashing to ensure the high collision characteristics of the generated MAC.

Table 5 shows a comparison of the computational complexity of some hash functions. Data on performance for the proposed MAC scheme with modular transformations are given for the minimum level of persistence (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) and a sufficient level of strength (for modular transformations equivalent length block symmetric cipher key is 128 bits). Length of the MAC generated is 80, and 128 bits, respectively.

For all the functions listed in Table 5 (except the proposed using modular transformations) specific complexity of the codes of integrity and authenticity of data is not dependent on the amount of data processed. For the proposed model using a modular transformations specific complexity with increase of length of data to be processed is reduced. So for a high level of strength (equivalent length block symmetric cipher key is 128 bits) already for data blocks of 32768 bytes is comparable to well-known and used in network security protocols, algorithms form the MAC. For the lowest level of strength (cardinality of the set of key data block symmetric cipher is equal to 2^{80}) the proposed scheme of codes of integrity and authenticity of data cascade formation using modular transformations already for data packets of 2048 bytes is not inferior in performance used to date the formation of the MAC algorithm in network security protocols, including protocols IPsec.

6 DISCUSSION

Analysis of the data presented in Table 3 allows claiming the adequacy of the experimental results. For fixed accuracy ε were obtained high values of confidence probability that indicates the validity and reliability of the results according to their statistical properties of the entire population of data.

Analyze the results of statistical studies and compare them with the theoretical estimates: with $P_{amount} \cdot |H| = 1$ (the first criterion), with $|H|/|B| = 1$ (the second criterion) and with $P_{amount} \cdot |H| = 1$ (the third criterion).

As seen from the data in Table 3 realization of a key hashing scheme based on MASH-1 algorithm when replacing the values of the initialization vector with the secret key does not enable high collision properties. The number of collisions occurring substantially above the upper theoretical limit on both the first and the second criterion, consequently, this structure is not a universal hashing

Table 4 – Estimation of the complexity of hashing algorithms in the S number of the 32-bit processor cycles per byte of data processed

Hash function	Resilience (key length)	Number pf cycles S
SHA-2 (512)	512	80
SHA-2 (256)	256	64
SHA-1	160	80
RIPEMD-160	160	160
MD5	128	64
Modular arithmetic hashing	80	512
	128	1536
	256	7680

Table 5 – Estimate of the complexity of different MAC forming schemes

Algorithm	The length of the input data, bytes					
	2048	4096	8192	16384	32768	65536
HMAC-MD5 (128 bits)	9	9	9	9	9	9
HMAC-RIPE-MD (160 bits)	27	27	27	27	27	27
HMAC-SHA-1 (160 bits)	25	25	25	25	25	25
HMAC-SHA-2 (512 bits)	84	84	84	84	84	84
CBC MAC-Rijndael (128 bits)	26	26	26	26	26	26
CBC MAC-DES (64 bits)	62	62	62	62	62	62
Proposed MAC scheme using modular transformations (80 bits)	38	22	14	10	8	7
Proposed MAC scheme using modular transformations (128 bits)	294	150	78	42	24	15

scheme and so, is not a strictly universal hashing scheme. This result was obtained with a high confidence level $P_\partial = P(|\tilde{m}(n_i) - m(n_i)| < \varepsilon) > 0.9$ for high precision. So for the first criterion the confidence interval was 41.42 ± 5 (confidence level 0.98), for the second criterion the confidence interval was 3.99 ± 0.025 (confidence level 0.99), and for the third criterion the confidence interval was 0.26 ± 0.1 (confidence level 0.97). The key hashing scheme based on MASH-1 algorithm by changing the values of the initialization vector with the secret key satisfies only the third criterion ($\tilde{m}(n_3) = 0.26$).

The use of key hashing based on MASH-2 algorithm when replacing the values of the initialization vector with the secret key by contrast provides high collision characteristics of universal hashing. For all three criteria resulting estimates are below the upper theoretical limit $\tilde{m}(n_i) < 1,\ i = 1, 2, 3$. This statement is confirmed with almost 100% probability. So for the first and the second dispersion criterion value $D(n_1)$ and $D(n_2)$ that characterize the dispersion of the hash rules values (MAC formation rules), with the equalities (3.1) and (3.2) with respect to their mathematical expectations $m(n_1)$ and $m(n_2)$ respectively, equals to zero which means the identity of the results obtained in all tests and practically certain that $m(n_1) = 0,\ m(n_2) = 0$. The resulting estimate for the third criterion also lies below the upper theoretical estimation ($\tilde{m}(n_3) = 0.31$) and this value is confirmed with high confidence level of $P_\partial = P(|\tilde{m}(n_3) - m(n_3)| < 0.1) = 0.97$ for fixed precision (confidence interval is 0.31 ± 0.1).

The explanation for this behavior of the modular transformations in the MASH-1 and MASH-2 schemes lies in the chosen parameters of the modular exponent. Thus, for the MASH-1 algorithm cyclic function (4.3) assumes the value of the modular exponent e = 2 that always breaks the condition (4.5). In the algorithm MASH-2 exponent is set $e = 2^8+1 = 257$ that for the chosen parameters $p = 17,\ q = 19,\ N = 323$ satisfies the constraint (4.5): $\gcd(e, \varphi(N)) = \gcd(257, 288) = 1$. Therefore, the key hashing built on the basis of modular transformations in some cases allows to provide for the universal properties and strictly universal hashing. To perform these properties condition (3.5) is necessary to be performed which a scheme for the selected parameters on the basis of the algorithm MASH-2 shows.

CONCLUSIONS

In this paper were obtained the theoretical generalization and new solution of scientific-applied problem, which is to develop and research of models and methods of effective mechanisms for monitoring the integrity and authenticity of data packets while minimizing the number of CPU cycles per byte of information to process to provide the necessary reliability and data security in telecommunications networks.

Scientific novelty of the work is following.

1. For the first time to analyze the collision properties of the codes monitoring the integrity and authenticity an approach is suggested based on the creation of scale models (mini version) algorithms of UMAC, which allows them to retain the algebraic structure.

2. For the first time mathematical apparatus and methods for the analysis of statistical studies of collisional properties are suggested which allows to determine the distribution of codes formed on the entire set of key data and obtain estimates of collisional properties with the required accuracy.

3. For the first time model and method of forming codes of integrity and authenticity of data using at the final stage cryptographically strong strictly universal hash function based on modular transformations. The proposed solution provides high collision properties of strictly universal hashing, low computational complexity and high security performance at the level of modern means of cryptographic protection with provable security.

Practical advice on building a cascade formation schemes of MAC based on modular hashing was justified the implementation of which will ensure the delivery time information packet to 0.5 sec; safe time more than 200 years; the probability of imposing a false message is not more than 10^{-25}; the probability of message modification message is not more than 10^{-25}. The usage of the developed models and methods of forming the MAC to control the integrity and authenticity of data packets in security protocols of telecommunication networks and internal payment banking systems.

ACKNOWLEDGEMENTS

The work is supported by the scientific research project «Prospective study of methods and mechanisms to ensure the integrity and authenticity of data circulating in the internal payment system of commercial bank» № 58/2008 and scientific research project «Development of methods of expediting the transfer and protection of information in telecommunication systems» № 36B113.

REFERENCES

1. Stinson D. R. Some constructions and bounds for authentication codes / D. R. Stinson // J. Cryptology. – 1988. – № 1. – P. 37–51.
2. Stinson D. R. The combinatorics of authentication and secrecy codes / D. R. Stinson // J. Cryptology. – 1990. – № 2. – P. 23–49.
3. Кузнецов А. А. Исследование коллизионных свойств кодов аутентификации сообщений UMAC / А. А. Кузнецов, О. Г. Король, С. П. Евсеев // Прикладная радиоэлектроника. – Харьков : Изд-во ХНУРЭ, 2012. – Т. 11, № 2. – С. 171–183.
4. Hoholdt T. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound / T. Hoholdt // The first steps, IEEE Trans. Info. Theory. – 1997. – 135 p.
5. Maitra S. Further constructions of resilient Boolean functions with very high nonlinearity / S. Maitra, E. Pasalic // Accepted in SETA. – May, 2001.
6. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 504 с.
7. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004 – Version 0.15 (beta), Springer-Verlag.
8. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. / В. Столлингс : пер. с англ. – М. : Вильям, 2001. – 672 с.
9. Король О. Г. Исследование методов обеспечения аутентичности и целостности данных на основе односторонних хеш-функций / О. Г. Король, С. П. Евсеев // Науково-технічний журнал «Захист інформації». – 2008. – Спецвипуск (40). – С. 50–55.
10. Bierbrauer J. Authentification via algebraic-geometric codes [Electronic resource] / J. Bierbrauer. – Access mode : http:// www.math.mtu.edu/~jbierbra/ potpap.ps.
11. Bierbrauer J. On families of hash function via geometric codes and concatenation / J. Bierbrauer, T. Johansson, G. Kabatianskii // Advances in Cryptology – CRYPTO 93. Lecture Notes in Computer Science. – 1994 – № 773. – P. 331–342.
12. Bierbrauer J. Universal hashing and geometric codes [Electronic resource] / J. Bierbrauer. – Access mode : http://www.math.mtu.edu/ ~jbierbra/ hashco1.ps.

13. Black J. «UMAC: Fast and provably secure message authentication», Advances in Cryptology. / J. Black, S. Halevi, H. Krawczyk, T. Krovetz, P. Rogaway // CRYPTO '99, LNCS, Springer-Verlag, 1999. – Vol. 1666 – P. 216–233.
14. Carter J. L. Universal classes of hash functions / J. L. Carter, M. N. Wegman // Computer and System Scince. – 1979. – № 18. – P. 143–154.
15. Krovetz T. UMAC – Message authentication code using universal hashing. IETF Internet Draft, draft-krovetz-umac-02.txt [Electronic resource]. – Access mode: www.cs.ucdavis.edu/~rogaway/umac, 2004.
16. NESSIE consortium «NESSIE Security report» Deliverable report D20 – NESSIE, 2002. – NES/DOC/ENS/WP5/D20 [Electronic resource]. – Access mode: http://www.cryptonessie.org/.

Article was submitted 07.11.2014.
After revision 21.11.2014.

Король О. Г.
Преподаватель кафедры информационных систем, Харьковский национальный экономический университет им. С. Кузнеца, Харьков, Украина

УСОВЕРШЕНСТВОВАННЫЙ АЛГОРИТМ MAC, ОСНОВАННЫЙ НА ИСПОЛЬЗОВАНИИ МОДУЛЯРНЫХ ПРЕОБРАЗОВАНИЙ

Обосновывается выбор цикловых функций в схеме доказуемо стойкого ключевого универсального хеширования, предлагается модель и метод формирования кодов контроля целостности и аутентичности данных на основе модулярных преобразований, алгоритм снижения вычислительной сложности реализации схем хеширования с использованием цикловых функций. Объектом исследования является процесс повышения целостности и аутентичности пакетов данных в протоколах безопасности телекоммуникационных сетей. Предметом исследования являются модели, методы и алгоритмы контроля целостности и аутентичности пакетов данных в протоколах безопасности телекоммуникационных сетей. Целью работы является повышение целостности и аутентичности пакетов данных в протоколах безопасности телекоммуникационных сетей. Разработанный усовершенствованный метод каскадного формирования MAC-кодов отличается от известного (алгоритм UMAC) применением модулярного хеширования на последнем этапе формирования MAC, что позволяет обеспечить высокие коллизионные свойства строго универсального хеширования и показатели безопасности на уровне современных средств защиты доказуемой стойкости. Получены оценки вычислительной сложности формирования MAC с использованием модулярного хеширования, установлено, что при сравнимых показателях стойкости сложность модулярного хеширования превышает на 1–2 порядка известные схемы на основе блочных симметричных шифров. Тем не менее, применение модулярных преобразований обеспечивает доказуемый уровень безопасности и высокие коллизионные свойства строго универсального хеширования.

Ключевые слова: коды контроля целостности и аутентичности данных, модулярные преобразования, универсальные классы хеширующих функций.

Король О. Г.
Викладач кафедри інформаційних систем, Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна

ВДОСКОНАЛЕНИЙ АЛГОРИТМ MAC, ЗАСНОВАНИЙ НА ВИКОРИСТАННІ МОДУЛЯРНИХ ПЕРЕТВОРЕНЬ

Обгрунтовується вибір циклових функцій у схемі доказово стійкого ключового універсального хешування, пропонується модель і метод формування кодів контролю цілісності та автентичності даних на основі модулярних перетворень, алгоритм зниження обчислювальної складності реалізації схем хешування з використанням циклових функцій. Об'єктом дослідження є процес підвищення цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж. Предметом дослідження є моделі, методи та алгоритми контролю цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж. Метою роботи є підвищення цілісності та автентичності пакетів даних у протоколах безпеки телекомунікаційних мереж. Розроблений удосконалений метод каскадного формування MAC-кодів відрізняється від відомого (алгоритм UMAC) застосуванням модулярного хешування на останньому етапі формування MAC, що дозволяє забезпечити високі колізійні властивості суворо універсального хешування і показники безпеки на рівні сучасних засобів захисту доказової стійкості. Отримано оцінки обчислювальної складності формування MAC з використанням модулярного хешування, встановлено, що при порівнянних показниках стійкості складність модулярного хешування перевищує на 1–2 порядки відомі схеми на основі блокових симетричних шифрів. Проте, застосування модулярних перетворень забезпечує доказовий рівень безпеки і високі колізійні властивості суворо універсального хешування.

Ключові слова: коди контролю цілісності та автентичності даних, модулярні перетворення, універсальні класи хешуючих функцій.

REFERENCES

1. Stinson D. R. Some constructions and bounds for authentication codes, *J. Cryptology,* 1988, No. 1, pp. 37–51.
2. Stinson D. R., The combinatorics of authentication and secrecy codes, *J. Cryptology,* 1990, No. 2, pp. 23–49.
3. Kuznecov A. A., Korol' O. G., Evseev S. P. Issledovanie kollizionnyx svojstv kodov autentifikacii soobshhenij UMAC, *Prikladnaya radioe'lektronika.* Xar'kov, Izd-vo XNURE', 2012, Vol. 11, No. 2, pp. 171–183.
4. Hoholdt T. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps, *IEEE Trans. Info. Theory*, 1997, 135 p.
5. Maitra S., Pasalic E. Further constructions of resilient Boolean functions with very high nonlinearity, *Accepted in SETA,* May, 2001.
6. Kuznecov O. O. Evseev S. P., Korol' O. G. Zaxist informacií v informacijnix sistemax. Xar'kov, Vid. XNEU, 2011, 504 p.
7. Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004, Version 0.15 (beta), Springer-Verlag.
8. Stollings V. per. s angl. Kriptografiya i zashhita setej: principy i praktika, 2-e izd. Moscow, izdatel'skij dom «Vil'yam», 2001, 672 p.
9. Korol' O. G., Evseev S. P. Issledovanie metodov obespecheniya autentichnosti i celostnosti dannyx na osnove odnostoronnix xesh-funkcij, *Naukovo-texnichnij zhurnal «Zaxist informacii»*, Specvipusk (40), 2008, pp. 50–55.
10. Bierbrauer J. Authentification via algebraic-geometric codes [Electronic resource], Access mode : http://www.math.mtu.edu/~jbierbra/ potpap.ps.
11. Bierbrauer J., Johansson T., Kabatianskii G. On families of hash function via geometric codes and concatenation, *Advances in Cryptology – CRYPTO 93. Lecture Notes in Computer Science*, 1994, No. 773, pp. 331–342.
12. Bierbrauer J. Universal hashing and geometric codes [Electronic resource], Access mode : http://www.math.mtu.edu/~jbierbra/ hashco1.ps.
13. Black J., Halevi S., Krawczyk H., Krovetz T., Rogaway P. «UMAC: Fast and provably secure message authentication», Advances in Cryptology, CRYPTO '99, LNCS, Springer-Verlag, 1999, vol. 1666, pp. 216–233.
14. Carter J. L., Wegman M. N. Universal classes of hash functions, *Computer and System Science,* 1979, No. 18, pp. 143–154.
15. Krovetz T. UMAC – Message authentication code using universal hashing. IETF Internet Draft, draft-krovetz-umac-02.txt [Electronic resource]. Access mode: www.cs.ucdavis.edu/~rogaway/umac, 2004.
16. NESSIE consortium «NESSIE Security report». Deliverable report D20. NESSIE, 2002. NES/DOC/ENS/WP5/D20 [Electronic resource]. Access mode: http://www.cryptonessie.org/.

UDC 004.93

Pupeikis R.

Ph.D., Associate Professor, Major Researcher of Department of Recognition Processes, Vilnius University, Vilnius, Lithuania

REVISED FAST FOURIER TRANSFORM

The problem of realisation of the Discrete Fourier Transform in on-line is analysed because of non-efficient consuming a time for a new recalculation of spectrum samples if one discrete-time signal sample or even some small portion of samples in period are replaced by new sample or by new samples, respectively. Using Fast Fourier Transform (FFT) procedure it is assumed that some signal samples in the respective period available for processing digitally are updated by a sensor in real time. It is urgent for every new sample that emerges to have a new spectrum. The ordinary recalculation of spectrum samples even with highly efficient Cooley-Tukey FFT algorithm is not suitable due to speedy varying in time real process to be observed. The idea is that FFT procedure should not be recalculated with every new sample, it is needed just to modify it when the new sample emerges and replaces the old one. We retrieve the recursive formulas for FFT algorithms that refer to the spectrum samples modification. In a case of appearing one new sample, the recursive algorithm calculates a new spectrum samples by simple addition of a residual between an old and new samples, multiplied on respective row of Fourier 'code' matrix, to a vector of old spectrum samples. An example of 8-point FFT is presented.

Keywords: digital signal processing, discrete Fourier transform, fast Fourier transform.

NOMENCLATURE

DSP is a digital signal processing;

DFT is a discrete Fourier transform;

FFT fast Fourier transform;

$\{x(n)\}$ is a discrete-time real valued signal or sequence of real numbers;

L is a length of a real valued signal;

n is a number of signal sample;

$X(\omega)$ is a Fourier transform of a discrete-time signal;

j is the imaginary unit;

ω is an angular frequency;

$X(k)$ is a spectrum sample;

k is a number of spectrum sample;

N is a general number of spectrum or signal samples;

W_N^{kn} is is a periodic function with only N different values;

$x_{old}(l)$ is an old l-th sample of real valued signal;

$x_{new}(l)$ is a new l-th sample of real valued signal;

$X_{old}(k)$ is an old k-th sample of spectrum;

$X_{new}(k)$ is a new k-th sample of spectrum.

INTRODUCTION

The continuous-time Fourier series are broadly used in theory as well as in practice where functions are continuous. DFT can be treated as its discrete-time counterpart. DFT has also been implemented digitally in the area of filter synthesis, image processing, various audio and video signal developments, and many types of spectrum analyzers that compute sampled power spectra and frequency response functions. The properties of ordinary DFT are accurately described. On the other hand, it is known that ordinary DFT involves a lot of redundant calculations. Therefore, usually, ordinary DFT algorithm is replaced by highly efficient computer procedures, known as FFT algorithms. Also there is a considerable amount of literature available on DFT and FFT, mentioned here just a few (e.g. [1–9]) that are coupled with DSP. However, some problems, encountered with FFT applications to measured samples of signals, are not generally understood [3], especially, analysing varying in the time processes, e.g. if some portion of samples or even one sample in the given period is replaced by new samples or one sample, respectively, and for each such real time case we have to obtain a new spectrum. Therefore, it is needed to modify DFT and FFT in order to recalculate only some products of the Fourier 'code matrix' with the respective samples replaced. The next section introduces the statement of the problem to be solved. In Section 3 we worked out the recursive equations that allow to modify the ordinary FFT procedure. Examples are presented in Section 4. Section 5 contains conclusions.

1 PROBLEM STATEMENT

Consider a discrete-time finite duration real-valued signal $\{x(n)\}$ of length L (i.e., $\{x(n)\} = 0$ for $n < 0$ and $n \geq L$) that has the Fourier transform

$$X(\omega) = \sum_{n=0}^{L-1} x(n) e^{-j\omega n} \quad \forall \omega \in \overline{0,2\pi}, \tag{1}$$

where the upper and lower indices in the summation reflect the fact that $\{x(n)\}$=0 outside the range of $0 \leq n = 0 \geq L-1$. Here j is the imaginary unit. When we sample $\{X(\omega)\}$ at equally frequencies $\omega_k = 2\pi k / N \ \forall k \in \overline{0, N-1}$, with $N \geq L$, the resultant samples are as follows:

$$X\{(k)\} = X\left(\frac{2\pi k}{N}\right) = \sum_{n=0}^{N-1} x(n) e^{-j2\pi kn/N}. \tag{2}$$

For convenience the upper index in the sum has been increased from $L-1$ to $N-1$ since $\{x(n)\} = 0$ for $n \geq L$. Here N is the general number of samples of the basic real valued signal $\{x(n)\}$ under consideration. The relation in eq. (2) is called DFT of $\{x(n)\}$ and is used for transforming the sample sequence $\{x(n)\}$ into a sequence of frequency samples $X\{(k)\}$ of length N. Rewriting eq. (2) in the form

$$X\{(k)\} = \sum_{n=0}^{N-1} x(n) W_N^{kn} \quad \forall k \in \overline{0, N-1}, \tag{3}$$

DOI 10.15588/1607-3274-2015-1-9

$$W_N^{kn} = e^{-j2\pi kn/N}, \quad (4)$$

one can realize that the integer product kn repeats for different combinations of k and n, and that W_N^{kn} is a periodic function with only N different values. Therefore, various fast and efficient DFT algorithms without redundant calculations were worked out [1–9]. Frequently, the FFT is computed by decimating the sample sequence $\{x(n)\}$ into sub-sequences until 2-point DFT's remain.

Assume that the frequencies analysis of real-time streaming sensor data $\{x(n)\}$ is needed. The aim of the paper is to work out an recursive approach that would update the spectrum samples given in eq. (3) as fast as possible with a sensor's sample that emerges, without anew recalculation of spectrum samples by FFT algorithm.

2 REVIEW OF THE LITERATURE

Recursive methods are important for the property that observations of time-varying phenomenon by their use can be processed by computer in real time. Hence, they may be applied in on-line monitoring and analysis of generally time-varying processes, and also combined with on-line control strategies to produce adaptive control algorithms. Some of them were used to the parametric identification of nonlinear Wiener systems [10]. Recursive procedures can be effective by processing various characteristics of stacionary as well as nonstacionary random processes and systems [11].

It is well-known that the most important area of DSP includes searching for different characteristics of signals and systems in frequency domain. Here more popular are DFT and various FFT procedures. However, as it is emphasized in [3], that the use of the DFT with the digitized signals are not generally understood. For example, ordinary DFT requires that in the given period *N* all samples ought to be fixed. Indeed, the author of this paper has not found any published work that addresses the recursive calculation of the DFT or FFT on an *N*-point complex valued function, when the samples of the varying in the time signal are observed by sensor. On the other hand, it is known that the processes, functioning in real life are dynamic and time-varying.

Therefore, it is important to work out procedures based on ordinary DFT that allow us to find spectrum samples, when some samples of discrete-time signal in the respective period, available for processing digitally, are updated by a sensor in real time.

3 MATERIALS AND METHODS

It is not efficient to recalculate the basic spectrum samples anew, if only one signal sample or even a small portion of new samples emerges continuously, especially, when speed is a main issue. Then, the computation time can become prohibitive, in spite of the fact that FFT requires only $N\log_2 N$ complex multiplications and complex additions to compute each of the N spectral samples. In such a case, it is important to work out an approach for modifying FFT in order to decrease the calculation time significantly. Let us retrieve now recursive formulas for recalculating the basic spectrum samples $X(k)\ \forall k \in \overline{0, N-1}$ partly, when a new sample $x_{new}(l)$ appears in the given N samples of a signal $x(n)\ \forall n \in \overline{0, N-1}$ while the respective old one vanishes. For real valued $x(n)\ \forall n \in \overline{0, N-1}$ eq.(3) can be rewritten as

$$X_{old}(k) = X_{old}\left(\frac{2\pi k}{N}\right) = \sum_{n=0}^{N-1} x_{old}(n) W_N^{kn}, \quad (5)$$

or

$$X_{new}(k) = X_{new}\left(\frac{2\pi k}{N}\right) = \sum_{n=0}^{N-1} x_{new}(n) W_N^{kn}, \quad (6)$$

if only the old and new samples of the sequence $\{x(n)\}$ are used, respectively. Here $x_{old}(l)$, $x_{new}(l) \forall l \in \overline{0, N-1}$ are *l*-th old and new samples, $X_{old}(k)$, $X_{new}(k)\ \forall k \in \overline{0, N-1}$ are values of the old and new samples in frequency domain, correspondingly.

Suppose now that in eq. (6) all the new samples are equivalent to the old ones, except, the sample $x_{new}(l)$. Then, we can rewrite eq. (6) as follows

$$X_{new}(k) = \sum_{n=0}^{l-1} x_{old}(n) W_N^{kn} + x_{new}(l) W_N^{kl} + \sum_{n=l+1}^{N-1} x_{old}(n) W_N^{kn}\ \forall k \in \overline{0, N-1}.$$

Subtracting the values $X_{old}(k)$ from $X_{new}(k)$ $\forall k \in \overline{0, N-1}$ we obtain the relationship of the form

$$\begin{bmatrix} X_{new}(0) - X_{old}(0) \\ X_{new}(1) - X_{old}(1) \\ \vdots \\ X_{new}(N-2) - X_{old}(N-2) \\ X_{new}(N-1) - X_{old}(N-1) \end{bmatrix} = [x_{new}(l) - x_{old}(l)] \begin{bmatrix} W_N^{l0} \\ W_N^{l1} \\ \vdots \\ W_N^{l(N-2)} \\ W_N^{l(N-1)} \end{bmatrix}.$$

It can also be rewritten in the recursive form

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ \vdots \\ X_{new}(N-2) \\ X_{new}(N-1) \end{bmatrix} = \begin{bmatrix} X_{old}(0) \\ X_{old}(1) \\ \vdots \\ X_{old}(N-2) \\ X_{old}(N-1) \end{bmatrix} + [x_{new}(l) - x_{old}(l)] \begin{bmatrix} W_N^{l0} \\ W_N^{l1} \\ \vdots \\ W_N^{l(N-2)} \\ W_N^{l(N-1)} \end{bmatrix}, \quad (7)$$

assuming that a new sample $x_{new}(l)$ emerges and replaces the old one $x_{old}(l)$.

Suppose now that in eq. (6) all the new samples are equivalent to the old ones, except a some portion of new samples $x_{new}(l), x_{new}(l+1),..., x_{new}(l+p-2), x_{new}(l+p-1)$, that appears in the given *N* samples of signal $\{x(n)\}$, while the respective portion of the old samples vanishes. In such a case, the final expression can be rewritten recursively

$$X_{new}(k) = X_{old}(k) + \sum_{m=l}^{l+p-1} [x_{new}(m) - x_{old}(m)] W_N^{km}\ \forall k \in \overline{0, N-1},$$

or in extended form

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ \vdots \\ X_{new}(N-2) \\ X_{new}(N-1) \end{bmatrix} = \begin{bmatrix} X_{old}(0) \\ X_{old}(1) \\ \vdots \\ X_{old}(N-2) \\ X_{old}(N-1) \end{bmatrix} + [x_{new}(l) -$$

$$- x_{old}(l)] \begin{bmatrix} W_N^{l0} \\ W_N^{l1} \\ \vdots \\ W_N^{l(N-2)} \\ W_N^{l(N-1)} \end{bmatrix} + \ldots + [x_{new}(\upsilon) - x_{old}(\upsilon)] \begin{bmatrix} W_N^{\upsilon 0} \\ W_N^{\upsilon 1} \\ \vdots \\ W_N^{\upsilon(N-2)} \\ W_N^{\upsilon(N-1)} \end{bmatrix}. \quad (8)$$

Here $\upsilon = l + p - 1$.

4 EXPERIMENTS

Let us describe now two experiments that are carried out while analysis of recursive FFT. In both experiments we consider the discrete-time periodic signal

$$x(n) = \{\ldots 24, 8, 12, 16, 20, 6, 10, 14, \ldots\}. \quad (9)$$

By inspection, the period $N = 8$. DFT is computed according to

$$X(k) = \sum_{n=0}^{7} x(n) \exp(-j\frac{2\pi}{8}nk), \forall k \in \overline{0,7}\ . \quad (10)$$

or in a form

$$\begin{bmatrix} X(0) \\ X(1) \\ X(2) \\ X(3) \\ X(4) \\ X(5) \\ X(6) \\ X(7) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a(1-j) & -j & b(1+j) & -1 & b(1-j) & j & a(1+j) \\ 1 & -j & -1 & j & 1 & -j & -1 & j \\ 1 & b(1+j) & j & a(1-j) & -1 & a(1+j) & -j & b(1-j) \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & b(1-j) & -j & a(1+j) & -1 & a(1-j) & j & b(1+j) \\ 1 & j & -1 & -j & 1 & j & -1 & -j \\ 1 & a(1+j) & j & b(1-j) & -1 & b(1+j) & -j & a(1-j) \end{bmatrix} \begin{bmatrix} 24 \\ 8 \\ 12 \\ 16 \\ 20 \\ 6 \\ 10 \\ 14 \end{bmatrix}, \quad (11)$$

using Fourier 'code' matrix. Here a=0.7071 and $b = -a$. Afterwards, the spectrum samples $X(0), X(1),\ldots,X(7)$ are determined by FFT using *Matlab* as follows: *fft*([24, 8, 12, 16, 20, 6, 10, 14], 8). The spectrum samples are: $X(0)$= 110, $X(1)$= 4 – 4.83j, $X(2)$= 22 + 16j, $X(3)$ = 4 – 0.83j, $X(4) = 22$, $X(5) = 4 + 0.83j$, $X(6) = 22 - 16j$, $X(7) = 4 + 4.83j$.

In the first experiment we change in (11), firstly, fourth sample, and, secondly, the sixth one. Suppose that a new fourth sample '25' comes in (9), and the old one '20' goes out. Then, the system of linear complex valued equations (10) is of the form

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ X_{new}(2) \\ X_{new}(3) \\ X_{new}(4) \\ X_{new}(5) \\ X_{new}(6) \\ X_{new}(7) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a(1-j) & -j & b(1+j) & -1 & b(1-j) & j & a(1+j) \\ 1 & -j & -1 & j & 1 & -j & -1 & j \\ 1 & b(1+j) & j & a(1-j) & -1 & a(1+j) & -j & b(1-j) \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & b(1-j) & -j & a(1+j) & -1 & a(1-j) & j & b(1+j) \\ 1 & j & -1 & -j & 1 & j & -1 & -j \\ 1 & a(1+j) & j & b(1-j) & -1 & b(1+j) & -j & a(1-j) \end{bmatrix} \begin{bmatrix} 24 \\ 8 \\ 12 \\ 16 \\ 25 \\ 6 \\ 10 \\ 14 \end{bmatrix}.$$

Afterwards, the spectrum samples $X_{new}(0), X_{new}(1),\ldots,X_{new}(7)$ are recalculated anew by Matlab: *fft*([24, 8, 12, 16, 25, 6, 10, 14], 8). Their values now are: $X_{new}(0)$= 115, $X_{new}(1)$= –1 – 4.83j, $X_{new}(2)$= 27 + 16j, $X_{new}(3)$= –1 – 0.83j, $X_{new}(4)$= 27, $X_{new}(5)$= –1 + 0.83j, $X_{new}(6)$= 27 – 16j, $X_{new}(7)$= –1 + 4.83j. The same spectrum samples $X_{new}(0), X_{new}(1),\ldots,X_{new}(7)$ can be determined recursively by eq. (7) as follows

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ X_{new}(2) \\ X_{new}(3) \\ X_{new}(4) \\ X_{new}(5) \\ X_{new}(6) \\ X_{new}(7) \end{bmatrix} = \begin{bmatrix} 110 + (5)\cdot 1 \\ 4 - 4.83j + (5)\cdot(-1) \\ 22 + 16j + (5)\cdot 1 \\ 4 - 0.83j + (5)\cdot(-1) \\ 22 + (5)\cdot 1 \\ 4 + 0.83j + (5)\cdot(-1) \\ 22 - 16j + (5)\cdot 1 \\ 4 + 4.83j + (5)\cdot(-1) \end{bmatrix} = \begin{bmatrix} 115 \\ -1 - 4.83j \\ 27 + 16j \\ -1 - 0.83j \\ 27 \\ -1 + 0.83j \\ 27 - 16j \\ -1 + 4.83j \end{bmatrix}.$$

It is obvious, that in both cases we obtain the same set values of $X(0), X(1),\ldots,X(7)$, respectively. Suppose now that just after finishing recursive calculations the new sixth sample with values '5' come in the set of samples (9) and the respective old one with values '10' go out. Then, the previous values of $X_{new}(0), X_{new}(1),\ldots,X_{new}(7)$ can be treated now as old ones, i.e. $X_{old}(0) = X_{new}(0), X_{old}(1) = X_{new}(1),\ldots,X_{old}(6) = X_{new}(6), X_{old}(7) = X_{new}(7)$, respectively. The current values of $X(0), X(1),\ldots,X(7)$ are treated as $X_{new}(0), X_{new}(1),\ldots,X_{new}(7)$. They can be obtained by the recursive formula

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ X_{new}(2) \\ X_{new}(3) \\ X_{new}(4) \\ X_{new}(5) \\ X_{new}(6) \\ X_{new}(7) \end{bmatrix} = \begin{bmatrix} 115 + (-5)\cdot 1 \\ -1 - 4.83j + (-5)\cdot j \\ 27 + 16j + (-5)\cdot(-1) \\ -1 - 0.83j + (-5)\cdot(-j) \\ 27 + (-5)\cdot 1 \\ -1 + 0.83j + (-5)\cdot j \\ 27 - 16j + (-5)\cdot(-1) \\ -1 + 4.83j + (-5)\cdot(-j) \end{bmatrix} = \begin{bmatrix} 110 \\ -1 - 9.83j \\ 32 + 16j \\ -1 + 4.17j \\ 22 \\ -1 - 4.17j \\ 32 - 16j \\ -1 + 9.83j \end{bmatrix}.$$

Let us check now the previous recursive FFT by the ordinary one using *Matlab*: *fft*([24, 8, 12, 16, 20, 6, 5, 14], 8). The spectrum samples are:

$$X(0) = 110,\ X(1) = -1 - 9.83j,\ X(2) = 32 + 16j,$$
$$X(3) = -1 + 4.17j,\ X(4) = 22,\ X(5) = -1 - 4.17j,$$
$$X(6) = 32 - 16j, X(7) = -1 + 9.83j. \quad (12)$$

It is assumed in the second experiment that both samples in (9) emerge at the same time. They appear just after calculations performed with initial set of samples (9). The new fourth and sixth samples with values '25' and '5' come in (9) and the respective old ones with values '20' and '10' go out. Then, eq. (11) obtains the form

$$\begin{bmatrix} X(0) \\ X(1) \\ X(2) \\ X(3) \\ X(4) \\ X(5) \\ X(6) \\ X(7) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a(1-j) & -j & b(1+j) & -1 & b(1-j) & j & a(1+j) \\ 1 & -j & -1 & j & 1 & -j & -1 & j \\ 1 & b(1+j) & j & a(1-j) & -1 & a(1+j) & -j & b(1-j) \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & b(1-j) & -j & a(1+j) & -1 & a(1-j) & j & b(1+j) \\ 1 & j & -1 & -j & 1 & j & -1 & -j \\ 1 & a(1+j) & j & b(1-j) & -1 & b(1+j) & -j & a(1-j) \end{bmatrix} \begin{bmatrix} 24 \\ 8 \\ 12 \\ 16 \\ 25 \\ 6 \\ 5 \\ 14 \end{bmatrix},$$

According eq. (8) recursive 8-point FFT expression is

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ X_{new}(2) \\ X_{new}(3) \\ X_{new}(4) \\ X_{new}(5) \\ X_{new}(6) \\ X_{new}(7) \end{bmatrix} = \begin{bmatrix} 110+(5)\cdot 1+(-5)\cdot 1 \\ 4-4.83j+(5)\cdot(-1)+(-5)j \\ 22+16j+(5)\cdot 1+(-5)\cdot(-1) \\ 4-0.83j+(5)\cdot(-1)+(-5)\cdot(-j) \\ 22+(5)\cdot 1+(-5)\cdot 1 \\ 4+0.83j+(5)\cdot(-1)+(-5)\cdot j \\ 22-16j+(5)\cdot 1+(-5)\cdot(-1) \\ 4+4.83j+(5)\cdot(-1)+(-5)(-j) \end{bmatrix} = \begin{bmatrix} 110 \\ -1-9.83j \\ 32+16j \\ -1+4.17j \\ 22 \\ -1-4.17j \\ 32-16j \\ -1+9.83j \end{bmatrix}. \quad (13)$$

Thus, the results (13) given by the recursive FFT of the form (7) are coincident with the results (12) that are obtained by ordinary FFT using Matlab standard function *fft*. Let us analyse now the recursive FFT using the special form

$$\begin{bmatrix} X(0) \\ X(1) \\ X(2) \\ X(3) \\ X(4) \\ X(5) \\ X(6) \\ X(7) \end{bmatrix} = \begin{bmatrix} G(0)+W_8^0 H(0) \\ G(1)+W_8^1 H(1) \\ G(2)+W_8^2 H(2) \\ G(3)+W_8^3 H(3) \\ G(0)-W_8^0 H(0) \\ G(1)-W_8^1 H(1) \\ G(2)-W_8^2 H(2) \\ G(3)-W_8^3 H(3) \end{bmatrix},$$

of ordinary FFT for the given period N. Here

$$G(k) = \sum_{n=0}^{3} x(2n) W_4^{kn}, \; H(k) = \sum_{n=0}^{3} x(2n+1) W_4^{kn},$$

$$\forall k = 0, 1, 2, 3.$$

Suppose that a new fourth sample '25' comes in the set, given by the initial eq. (9), and the old sample '20' goes out. At the same moment, every value of $G(k)\ \forall k \in \overline{0,3}$ changes, while corresponding value of $H(k)\ \forall k \in \overline{0,3}$ remains the same. Then, one can obtain

$$\begin{bmatrix} X_{new}(0) \\ X_{new}(1) \\ X_{new}(2) \\ X_{new}(3) \\ X_{new}(4) \\ X_{new}(5) \\ X_{new}(6) \\ X_{new}(7) \end{bmatrix} = \begin{bmatrix} G(0)+(5)\cdot 1+W_8^0 H(0) \\ G(1)+(5)\cdot(-1)+W_8^1 H(0) \\ G(2)+(5)\cdot 1+W_8^2 H(0) \\ G(3)+(5)\cdot(-1)+W_8^3 H(0) \\ G(0)+(5)\cdot 1-W_8^0 H(0) \\ G(1)+(5)\cdot(-1)-W_8^1 H(1) \\ G(2)+(5)\cdot 1-W_8^2 H(2) \\ G(3)+(5)\cdot(-1)-W_8^3 H(3) \end{bmatrix} = \begin{bmatrix} X_{old}(0) \\ X_{old}(1) \\ X_{old}(2) \\ X_{old}(3) \\ X_{old}(4) \\ X_{old}(5) \\ X_{old}(6) \\ X_{old}(7) \end{bmatrix} + 5 \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}.$$

This relationship is coincident with the formula (7), too.

5 RESULTS

It follows from the 8-point DFT example with real-valued samples set (9), that recursive FFT on an 8-point complex valued function, requires 8 operations (here operation is defined as one complex valued multiplication plus an one complex valued addition [3]) if one new sample comes in, and twice more both operations, if a portion of two samples emerges.

6 DISCUSSION

Thus, N-point DFT requires N complex-valued operations if one new sample emerges in a period, and $2N$ operations if a portion of two samples goes in, respectively. On the other hand, direct computation of the DFT on an N-point complex valued function requires NI operations to recalculate all N spectrum samples. Calculations increase even four times if twice increases the general number of samples to be processed. The Cooley-Tukey algorithm, that belongs to the class of FFT algorithms, takes approximately $N \log 2\, N$ operations [12, 13]. It is known [4], that for small values of N (say, 32 to 128) the FFT is important. For large values of N (1024 and above), the FFT is incredibly more efficient. For example, FFT is even hundred times faster than DFT, when N = 1024. Nevertheless, recalculation of spectrum samples by FFT is not only nonracional but also nonefficient if one sample emerges replacing an old one. In such a case, recursive calculation by (7) is much more effective. In order to change old spectrum samples the recursive FFT requires only 1024 operations on an 1024-point complex valued function, while the ordinary FFT requires 10 times more by anew their recalculation.

CONCLUSIONS

For discrete-time signals the DFT coefficient values have been proposed to recursively determine if one new signal sample or new portion of samples emerge in the given period of a realization replacing the old sample or old portion of samples, respectively. The number of operations for their speedy calculating is essentially reduced by the original recursive expression in comparison with the ordinary DFT or FFT equations (2), (3), respectively, used in the case of fixed values of samples $x(n)\ \forall n \in 0, N-1$ in a fixed period N. An example, presented here, has shown us the efficiency of the recursive approach, too. Therefore, it is not rational to recalculate frequency samples by ordinary DFT or even FFT algorithms if only one sample in the given period or if some small portion of samples is replaced by new sample or some new samples, respectively. The recursive FFT approach could be effective, especially, in real-time applications when speed of calculations is the main issue.

ACKNOWLEDGEMENTS

The work is supported by the state budget scientific research project of Institute of Mathematics and Informatics of Vilnius University «Analysis, recognition, optimization and control of nonlinear systems and signals of complex structure» (registration number 2AP1.46) and by an European Commission Funded Project «Comenius MP» running from November 2012 to October 2014 (№ 526315-LLP-2012-CY-COMENIUS-CMP).

REFERENCES

1. Deziel J. P. Applied introduction to digital signal processing / J. P. Deziel. – New Jersey : Prentice Hall, Inc., 2000. – 388 p.
2. Gonzalez R. C. Digitale Image Processing / R. C. Gonzalez. – New Jersey : Prentice Hall, Inc., 2007. – 976 p.
3. Oppenheim A. V. Discrete-time signal processing / A. V. Oppenheim, R. W. Shafer. – New Jersey : Prentice Hall, Inc., 2009. – 1120 p.
4. Proakis J. G. Digital signal processing. Principles, algorithms, and applications / J. G. Proakis, D. G. Manolakis. – New Jersey : Prentice Hall, Inc., 2006. – 1004 p.
5. Proakis J. G. Student manual for digital signal processing with Matlab / J. G. Proakis, V.K. Ingle. – New Jersey : Prentice Hall, Inc., 2006. – 264 p.
6. Lyons R. G. Understanding digital signal processing / R. G. Lyons. – New Jersey : Prentice Hall, Inc., 2010. – 984 p.
7. Richardson M. H. Fundamentals of the discrete Fourier transform / M. H. Richardson // Sound & Vibration Magazine. – 1978. – March. – P. 1–8.
8. Smith S. W. Digital signal processing. A practical guide for engineers and scientists / S.W. Smith. – San Diego : California Technical Publishing, 2003. – 640 p.
9. Pupeikis R. Vaizdu apdorojimo Matlab'o terpėje pagrindai / R. Pupeikis. – Vilnius : Technika, 2008. – 107 p.
10. Pupeikis R. Self-tuning minimum variance control of linear systems followed by saturation nonlinearities in a noisy frame / R. Pupeikis / / International Journal of Robust and Nonlinear Control. – 2014. – Vol. 24, № 2. – P. 313–325. DOI: 10.1002/rnc.2888
11. Казлаускас К. Цифровые системы обработки данных. Монография./ К. Казлаускас, Р. Пупейкис. – Вильнюс : Мокслас, 1991. – 220 с.
12. Cooley J. W. An algorithm for the machine calculation of complex Fourier series/ J. W. Cooley, J. Tuke // Mathematics Computation. – 1965. – Vol. 19 – P. 297–301.
13. Brigham E. Fast Fourier transform and its applications / E. Brigham. – New Jersey : Prentice Hall, Inc., 1988. – 446 p.

Article was submitted 15.12.2014.
After revision 25.12.2014.

Пупейкис Р.
Канд. техн. наук, доцент, старший сотрудник отдела процессов распознавания, Вильнюсский университет, Вильнюс, Литва

ИСПРАВЛЕННОЕ БЫСТРОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ

Проблема реализации дискретного преобразования Фурье в режиме он-лайн анализируется из-за неэффективных затрат времени для нового пересчета отсчетов спектра, если отсчет одного сигнала с дискретным временем или даже небольшая часть отсчетов в периоде заменены на новый отсчет или новые отсчеты, соответственно. Использование процедуры быстрого преобразования Фурье (БПФ) предполагает, что некоторые отсчеты сигнала в соответствующем периоде, доступные для цифровой обработки, обновляются с помощью датчика в режиме реального времени. Это актуально для каждого нового отсчета, который приводит к получению нового спектра. Обычный пересчет отсчетов спектра даже с высокоэффективным алгоритмом БПФ Кули-Тьюки не подходит из-за быстро изменяющегося во времени наблюдаемого реального процесса. Идея заключается в том, что процедура БПФ не должна пересчитываться с каждым новым отсчетом, нужно просто модифицировать его, когда новый отсчет появляется и заменяет старый. Получены рекуррентные формулы для алгоритмов БПФ, которые относятся к модификации отсчетов спектра. В случае возникновения одного нового отсчета, рекурсивный алгоритм вычисляет новые отсчеты спектра простым добавлением к вектору старых отсчетов спектра разности между старыми и новыми отсчетами, умноженной на соответствующий ряд матрицы «кода» Фурье. Приведен пример 8-точечного БПФ.

Ключевые слова: цифровая обработка сигналов, дискретное преобразование Фурье, быстрое преобразование Фурье.

Пупейкіс Р.
Канд. техн. наук, доцент, старший співробітник відділу процесів розпізнавання, Вільнюський університет, Вільнюс, Литва

ВИПРАВЛЕНЕ ШВИДКЕ ПЕРЕТВОРЕННЯ ФУР'Є

Проблема реалізації дискретного перетворення Фур'є в режимі он-лайн аналізується через неефективні витрати часу для нового перерахунку відліків спектру, якщо відлік одного сигналу з дискретним часом або навіть невелика частина відліків в періоді замінені на новий відлік або нові відліки, відповідно. Використання процедури швидкого перетворення Фур'є (ШПФ) припускає, що деякі відліки сигналу у відповідному періоді, доступні для цифрової обробки, оновлюються за допомогою датчика в режимі реального часу. Це актуально для кожного нового відліку, який призводить до отримання нового спектра. Звичайний перерахунок відліків спектру навіть з високоефективним алгоритмом ШПФ Кулі-Тьюки не підходить через швидко мінливого у часі спостережуваного реального процесу. Ідея полягає в тому, що процедура ШПФ не повинна перераховуватися з кожним новим відліком, потрібно просто модифікувати його, коли новий відлік з'являється і замінює старий. Отримано рекурентні формули для алгоритмів ШПФ, які відносяться до модифікації відліків спектру. У разі виникнення одного нового відліку, рекурсивний алгоритм обчислює нові відліки спектру простим додаванням до вектора старих відліків спектру різниці між старими і новими відліками, помноженої на відповідний ряд матриці «коду» Фур'є. Наведено приклад 8-точкового ШПФ.

Ключові слова: цифрова обробка сигналів, дискретне перетворення Фур'є, швидке перетворення Фур'є.

REFERENCES

1. Deziel J. P. Applied introduction to digital signal processing. New Jersey: Prentice Hall, Inc., 2000, 388 p.
2. Gonzalez R.C. Digitale Image Processing. New Jersey, Prentice Hall, Inc., 2007, 976 p.
3. Oppenheim A. V., Shafer R. W. Discrete-time signal processing. New Jersey, Prentice Hall, Inc., 2009, 1120 p.
4. Proakis J. G., Manolakis D. G. Digital signal processing. Principles, algorithms, and applications. New Jersey, Prentice Hall, Inc., 2006, 1004 p.
5. Proakis J. G., Ingle V. K. Student manual for digital signal processing with Matlab. New Jersey : Prentice Hall, Inc., 2006, 264 p.
6. Lyons R. G. Understanding digital signal processing. New Jersey, Prentice Hall, Inc., 2010, 984 p.
7. Richardson M. H. Fundamentals of the discrete Fourier transform, *Sound & Vibration Magazine,* 1978, March, pp. 1–8.
8. Smith S. W. Digital signal processing. A practical guide for engineers and scientists. San Diego, California Technical Publishing, 2003, 640 p.
9. Pupeikis R. Vaizdu apdorojimo Matlab'o terpėje pagrindai. Vilnius, Technika, 2008, 107 p.
10. Pupeikis R. Self-tuning minimum variance control of linear systems followed by saturation nonlinearities in a noisy frame, *International Journal of Robust and Nonlinear Control,* 2014, Vol. 24, No. 2, pp. 313–325. DOI: 10.1002/rnc.2888
11. Kazlauskas K., Pupejkis R. Cifrovye sistemy obrabotki dannyh. Monografija. Vil'njus, Mokslas, 1991, 220 p.
12. Cooley J. W., Tuke J. An algorithm for the machine calculation of complex Fourier series, *Mathematics Computation*, 1965, Vol. 19, pp. 297–301.
13. Brigham E. Fast Fourier transform and its applications. New Jersey, Prentice Hall, Inc., 1988, 446 p.

УДК 004:528.71

Гнатушенко В. В.[1], Кавац О. О.[2], Шевченко В. Ю.[3]

[1]Д-р техн. наук, професор, професор кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпропетровськ, Україна
[2]Канд. техн. наук, доцент, доцент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпропетровськ, Україна
[3]Аспірант Дніпропетровського національного університету імені Олеся Гончара, м. Дніпропетровськ, Україна

ПІДВИЩЕННЯ ПРОСТОРОВОГО РОЗРІЗНЕННЯ БАГАТОКАНАЛЬНИХ АЕРОКОСМІЧНИХ ЗОБРАЖЕНЬ ВИСОКОГО ПРОСТОРОВОГО РОЗРІЗНЕННЯ НА ОСНОВІ ГІПЕРСФЕРИЧНОГО ПЕРЕТВОРЕННЯ

У роботі вирішено актуальне завдання розробки інформаційної технології підвищення візуальної якості багатоканальних аерокосмічних зображень високого просторового розрізнення. Об'єктом дослідження є процес злиття панхромного та мультиспектрального фотограмметричних сканерних зображень, отриманих координатно-чутливими сенсорами у видимому та інфрачервоному діапазонах електромагнітного проміння. Предмет дослідження становлять методи попередньої та синергетичної обробки багатоканальних даних для поліпшення якості результуючого зображення та зменшення кольорових спотворень. Мета роботи: автоматизоване підвищення просторового розрізнення первинного багатоканального зображення та в порівнянні з існуючими методами усунення спектральних спотворень в локальних областях. Крім того, пропонована технологія дозволить ефективно проводити подальше розпізнавання й оперативний моніторинг об'єктів інфраструктури. У роботі запропоновано нову інформаційну технологію злиття багатоканальних аерокосмічних зображень на основі HSV-конвертування і гіперсферичного перетворення кольору, що дозволяє поліпшити просторове розрізнення первинного цифрового зображення й уникнути спектральних спотворень. Це досягається, зокрема, за рахунок попередньої еквалізації первинних знімків, оброблення даних у локалізованих спектральних базисах, оптимізованого за інформаційними характеристиками, та використання інформації, яку містить зображення інфрачервоного діапазону. Розроблено програмне забезпечення, що реалізує запропонований підхід. Проведено експерименти з дослідження властивостей запропонованого алгоритму. Експериментальні оцінки проведені на восьмиканальних зображеннях, отриманих супутником World-View-2. Результати тестування підтвердили, що запропонований підхід дозволяє досягти високої спектральної та просторової якості багатоканальних зображень та перевершує існуючі методи.

Ключові слова: сканерне зображення, вейвлет-перетворення, гіперсферичне перетворення, інформативність, злиття.

НОМЕНКЛАТУРА

ERGAS – relative Dimensionless Glabal Error;
HCT – hyperspherical color transform;
HSV – hue, saturation, value;
ICA – independent component analysis;
MUL – multispectral image;
NIR – near infrared channel;
SSIM – structure similarity;
PAN – panchromatic image;
RGB – red, green, blue;
ДЗЗ – дистанційне зондування Землі;
КА – космічний апарат;
I – інтенсивність яскравості;
θ – кутові змінні;
Band – канали мультиспектрального зображення;
N – номер каналу зображення.

ВСТУП

Методологія обробки і дешифрування даних дистанційного зондування Землі (ДЗЗ) давно і добре опрацьована. Широкий комерційний доступ до супутникових даних високого розрізнення відкрив багато нових можливостей для їх використання. Типовий набір даних з апаратури ДЗЗ, встановленої на супутниках, включає мультиспектральне зображення (MUL) в трьох і більше каналах видимого та інфрачервоного діапазонів і панхромне зображення (PAN) у видимому діапазоні [1]. Панхромне зображення має зазвичай більш високу просторову роздільну здатність, ніж мультиспектральне. Актуальною областю сучасних наукових досліджень є синергетична обробка (злиття) таких фотограмметричних даних декількох каналів з метою одержання штучного зображення із покращеними показниками інформативності у порівнянні із первинними знімками та їх подальший аналіз [1–4].

На сьогоднішній день одними із найсучасних супутників високого просторового розрізнення є WorldView-2 та WorldView-3. Апаратура цих супутників має дуже схожі технічні характеристики. Мультиспектральний сенсор VNIR WorldView-3 незначно відрізняється своїми можливостями від сенсора WorldView-2, відмінність – тільки в трохи більшому розрізненні. КА WorldView-3 дозволяє вести космічну зйомку з роздільною здатністю до 0,31 м. У багатоспектральному режимі роздільна здатність системи становить 1,2 м, а в ближній ІЧ-ділянці спектра – 3,7 м. Додавання нового ІЧ-діапазону зажадало включення додаткового 8-канального модуля з ІЧ-детекторами в конструкцію оптичної системи супутника. Зазначимо, що знімки WorldView-3 вже зробили свій вплив на Міністерство торгівлі США, яке прийняло рішення зняти обмеження, що розповсюджувалися на комерційне використання супутникових фотографій, на яких відображені об'єкти з фізичними розмірами менше 50 см. Вже сьогодні DigitalGlobe може продавати зображення з 40-сантиметровим розрізненням, а в наступному році компанія отримає дозвіл на продаж знімків з роздільною здатністю до 31 см. Останні дослідження показали, що 8-канальна зйомка впевнено забезпечує підвищення точності дешифрування на 15–30% порівняно з традиційною 4-канальною зйомкою [5]. Але існуючі рішення проблеми підвищення інформативності первинних багато-

DOI 10.15588/1607-3274-2015-1-10

канальних даних орієнтовані переважно на збільшення їх візуальної якості без урахування фізичних механізмів фіксації видової інформації, розроблялися для мультиспектральних знімків оптичного діапазону і тому мають ряд недоліків, основними з яких є суттєві колірні спотворення зображень [1–4]. Таким чином виникає необхідність розробки нових методів обробки первинних восьмиканальних аерокосмічних зображень для якісного і кількісного збільшення їх інформативності.

Метою роботи є розробка нової технології автоматизованого підвищення просторового розрізнення первинного багатоканального зображення й усунення спектральних спотворень в локальних областях.

1 ПОСТАНОВКА ЗАДАЧІ

У якості вхідних даних використовуються восьмиканальні знімки супутника WorldView-2. Необхідно розробити нову технологію підвищення інформативності аерокосмічних зображень, що дозволить одержати багатоспектральні зображення більш високого просторового розрізнення без втрати спектральної інформації. Основою технології є гіперсферичне перетворення кольору. Алгоритм поєднає в собі переваги заміщення компонент і багатомасштабного аналізу. Будуть отримані кількісні оцінки якості синтезованих мультиспектральних зображень такі як: ентропія, SSIM, ERGAS, Quality index та інші [6, 7]. Зазначені метрики дозволять оцінити якісні показники первинного та обробленого зображень.

2 ОГЛЯД ЛІТЕРАТУРИ

Аерокосмічні зображення фіксованого об’єкту (сцени), одержані у різних спектральних інтервалах, мають різну просторову та радіометричну розрізненість і внаслідок цього суттєво розрізняються за просторовими розподілами яскравості. Разом з тим, кожне таке зображення має окрему інформаційну значущість щодо подання характеристик об’єкту (сцени).

Використання кольору для відображення даних ДЗЗ є одним із найбільш важливих аспектів, що пов’язані з обробкою зображення. Колір можна використовувати не тільки для відображення мультиспектральних знімків, але і для вилучення з них необхідної інформації (розпізнавання).

При описі сприйняття кольорового зображення, як правило, не користуються такими поняттями як відносна доля червоного, зеленого чи синього кольору. Саме тому вихідні кольорові компоненти RGB корисно перетворювати у компоненти, що відповідають тону, насиченості та інтенсивності (HSV). Саме таке перетворення є основою відомих методів підвищення якості цифрових зображень [1–5, 8].

Нажаль окреме використання існуючих методів підвищення просторового розрізнення багатоканальних зображень, таких як HSV, ICA, Color Normalized Brovey, Grama-Schmidt, PC Spectral Sharpening, не дає прийнятного результату [6, 8 10].

Спільною та основною проблемою, пов’язаною зі злиттям сканерних зображень, отриманих сучасними аерокосмічними системами, є істотне колірне порушення. Причиною таких спотворень є той факт, що існуючи алгоритми головним чином розроблялися для об’єднання зображень супутника SPOT. На відміну від відповідних характеристик зазначеного кос-мічного апарату довжина панхром-хвилі сучасних супутників (IKONOS, QuickBird, Worldview-2 та ін.) була розширена від видимого до ближнього інфрачервоного діапазону.

Найбільш близькою до нашого дослідження є робота [11], але в ній автори не використовують перехід до HSV-простору, здійснюють за іншим правилом заміну яскравісної компоненти при гіперсферичному перетворенні та застосовують «a trous» – алгоритм, що в разі значних відмінностей контрастних характеристик первинних зображень неминуче призводить до посилення неінформативної шумової складової одного зображення до рівня суттєвих структурних особливостей іншого зображення.

3 МАТЕРІАЛИ ТА МЕТОДИ

В даній роботі ми пропонуємо алгоритм, заснований також на гіперсферичному перетворенні (НСТ), який вільний від зазначених вище недоліків і здатний ефективно працювати з будь-якою кількістю вхідних каналів мультиспектрального зображення. Крім того, на окремих кроках технології реалізовані такі методи обробки, як зважене усереднення, адаптивна гістограмна еквалізація, метод HSV та пакетне вейвлет-перетворення. Схема запропонованого алгоритму подана на рис. 1. Розглянемо основні етапи перетворення первинних багатоканальних зображень.

1. Завантажуємо фотограмметричні знімки супутника WorldView-2: панхромне – PAN, мультиспектральне – MUL (Coastal, Blue, Green, Yellow, Red, Red Edge, NIR1, NIR 2).

2. Виконуємо масштабування мультиспектрального (MUL) зображення до розмірів панхромного (PAN) знімка методом інтерполяції зі згладжувальним фільтром, що створює піксель як середньозважене пікселів, що містяться в області, яка опинилася під фільтром. Цей процес формує зображення з плавними переходами в сірому рівні [1].

3. Оскільки характерною рисою більшості фотограмметрических зображень є значна питома вага темних ділянок і порівняно мале число ділянок з високою яскравістю, тому наступним етапом пропонується провести еквалізацію мультиспектрального і панхромного зображень, за допомогою якої коригуємо первинні зображення, вирівнявши інтегральні площі ділянок з різними яскравостями. Пропонуємо використовувати адаптивну гістограмну еквалізацію [10].

4. Перетворюємо зображення з формату RGB в кольорову систему HSV [9]. Для панхромного зображення таке перетворення здійснюється з попереднім вибором у якості окремих R-, G-, B-компонент полутонового PAN-зображення. Для мультиспектрального зображення таке перетворення здійснюється з попереднім вибором у якості окремих R-, G-, B-компонент відповідних зображень 5-го, 3-го та 2-го каналів.

5. Замінюємо яскравісну V-компоненту мультиспектрального зображення MUL_{HSV} V-компонентою панхромного зображення PAN_{HSV}.

6. Здійснюємо зворотне перетворення отриманого на попередньому етапі зображення з формату HSV в кольорову систему RGB. Отримане зображення MUL_{RGB} вже буде мати підвищене просторове розрізнення у порівнянні з первинним знімком у натуральних кольорах.

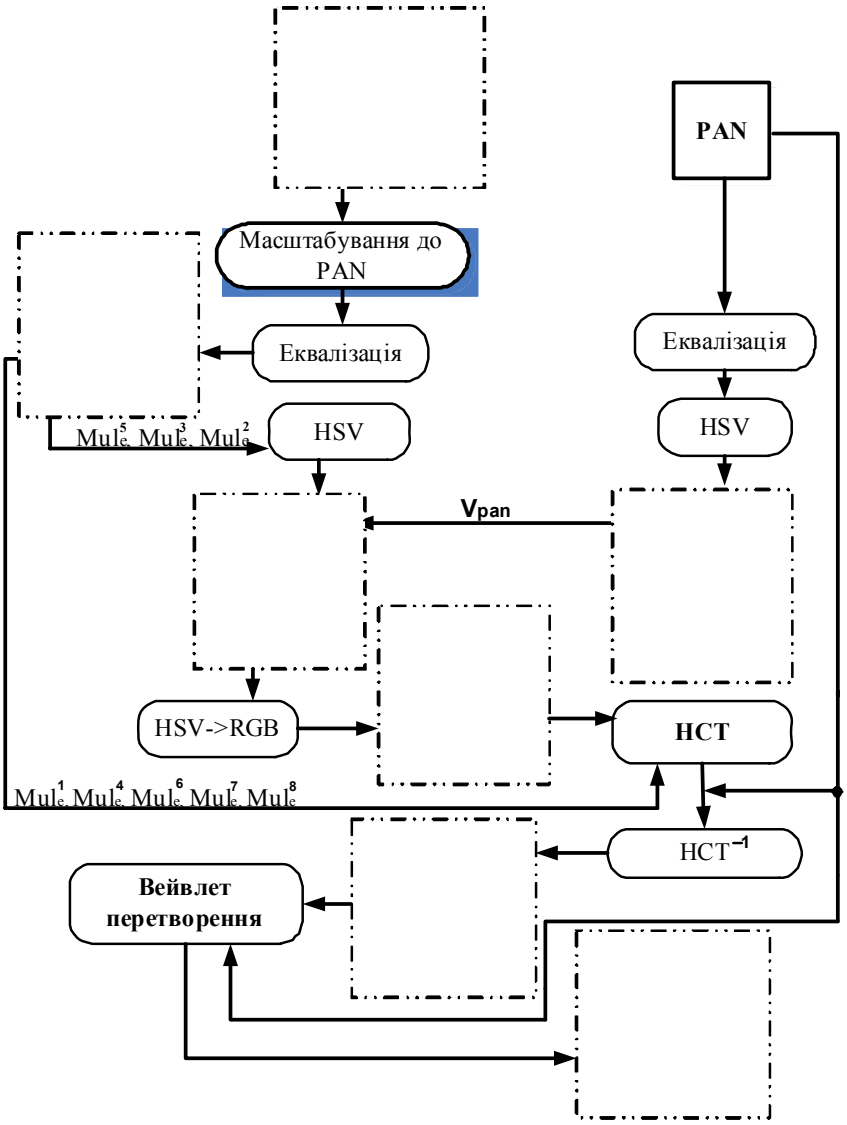


Рисунок 1 – Схема алгоритму

7. Перетворюємо восьмиканальне мультиспектральне зображення, що складається з MUL_{RGB} і зображень 1, 4, 6, 7, 8-го каналів після еквалізації) в гіперсферичний колірний простір, який задається формулами (1)–(4) [11]:

$$I = \sqrt{Band_1^2 + Band_2^2 ... + Band_N^2}\,, \qquad (1)$$

$$\theta_1 = \arctan\left(\frac{\sqrt{Band_N^2 + Band_{N-1}^2 ... + Band_2^2}}{Band_1}\right), \qquad (2)$$

$$\theta_{N-2} = \arctan\left(\frac{\sqrt{Band_N^2 + Band_{N-1}^2}}{Band_{N-2}}\right), \qquad (3)$$

$$\theta_{N-1} = \arctan\left(\frac{Band_N}{Band_{N-1}}\right). \qquad (4)$$

8. Замінюємо яскравісну *I*-компоненту багатоканального зображення панхромним зображенням PAN.

9. Застосовуємо зворотне HCT-перетворення та отримуємо результат MUL_{HST} за формулами (5)–(8):

$$Band_1 = I\cos\theta_1\,, \qquad (5)$$

$$Band_2 = I\sin\theta_1\cos\theta_2\,, \qquad (6)$$

$$Band_{N-1} = I\sin\theta_1\sin\theta_2 ... \sin\theta_{N-2}\cos\theta_{N-1}\,, \qquad (7)$$

$$Band_N = I\sin\theta_1\sin\theta_2 ... \sin\theta_{N-2}\sin\theta_{N-1}\,. \qquad (8)$$

10. Перетворюємо отримане зображення MUL_{HST} в первинну кольорову модель.

11. Застосовуємо вейвлет-перетворення [12]. Розклад відповідних каналів яскравості багатоканального зображення здійснюється до заданого рівня декомпозиції за оптимального пакетного вейвлет-базису у відповідності з обраною функцією інформаційної вартості (критерієм інформативності), обчислюваної відносно коефіцієнтів вейвлет-розкладу вершини-пращура та вершин всіх його нащадків. Далі здійснюємо формоутворення нових складових розкладу згідно з обраним правилом об'єднання

коефіцієнтів, зворотний пакетний вейвлет розклад та перехід до вихідної кольорової метрики [10]. Отримуємо результат RES у вигляді восьмиканального зображення з підвищеним просторовим розрізненням без втрат спектральної інформації.

4 ЕКСПЕРИМЕНТИ

Виконаємо експериментальне дослідження ефективності розробленого методу на основі гіперсферичного перетворення. Для цього будемо використовувати кількісні оцінки якості синтезованих мультиспектральних зображень: ентропія, SSIM, ERGAS, Quality index та ін. [6, 7].

Для реалізації окремих етапів запропонованого алгоритму та його порівняння з відомими методами використовувались програмний продукт для обробки даних ДЗЗ ENVI 5.0 і пакет для інженерних розрахунків Matlab 12.0 [13]. В програмному комплексі ENVI 5.0 використано методи HSV, PCA, Grama-Shmidt, Color Normalized (Brovey) та еквалізація. В пакеті Matlab 12.0 нами програмно реалізовано та здійснено гіперсферичне та вейвлет-перетворення, а також розрахунок кількісних оцінок ефективності методів: ентропії, SSIM, ERGAS, Quality index.

5 РЕЗУЛЬТАТИ

На рис. 2а подано фрагмент панхромного зображення до обробки, на рис. 2б – первинне мультиспектральне зображення з вибором у якості окремих R-, G-, B-компонент відповідних зображень 5-го, 3-го та 2-го каналів. На рис. 2в подано фрагмент мультиспектрального зображення після обробки запропонованим у роботі алгоритмом. Для його RGB-візуалізації також використано 5-й, 3-й та 2-й канали.

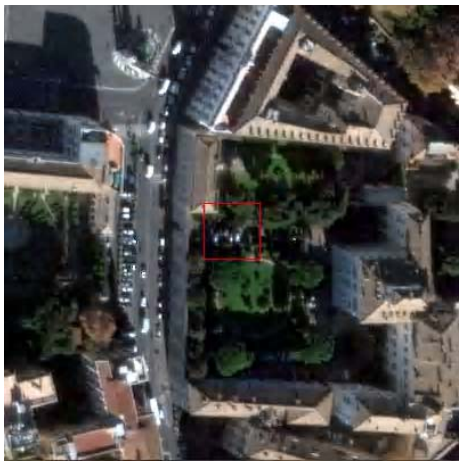
У табл. 1 наведено розраховані значення ентропії, оцінені для первинних мультиспектрального та панхромного зображень, а також для синтезованого багатоканального зображення за запропонованим методом (розмір фрагментів зображень 500×500 пікселів). У табл. 2 наведені значення ERGAS і SSIM для синтезованих мультиспектральних зображень, отриманих окремо відомими методами злиття (PCA, Grama-Shmidt, HSV, Wavelet) і запропонованим у роботі методом.

6 ОБГОВОРЕННЯ

Як видно із табл. 1, запропонований метод дійсно підвищує інформативність мультиспектрального зображення, оскільки значення ентропії в порівнянні з вхідними даними є вищим. З результатів табл. 2 можна бачити, що найефективнішим методом злиття зображень є запропонований метод (RES). На це вказує значення безрозмірної глобальної помилки ERGAS, що є найменшим (ERGAS=1,52) у порівнянні з існуючими методами і свідчить про мінімальну «кількість» спектральних спотворень фотограмметричних сканерних зображень. Про ефективність розробленої технології також свідчать отримані значення індексу SSIM, який визначає структурну схожість двох зображень (еталонного та синтезованого зображення). Структурна схожість розуміється нами як подібність геометричних структур зображень, яка інваріантна до розподілів їхньої яскравості та контрастності. Просторовий розподіл яскравості зображення, отриманого після обробки, зрозуміло, відрізняється від первин-

а

б



в

Рисунок 2 – Фрагменти зображень: а – первинне панхромне, б – первинне мультиспектральне, в – синтезоване після обробки запропонованим алгоритмом

Таблиця 1 – Кількісні значення ентропії

Зображення	Значення ентропії
Панхроматичне (Pan)	7,2932
Мультиспектральне (Mul)	7,2719
Синтезоване зображення **(RES)**	**7,5118**

Таблиця 2 – Порівняльний аналіз ефективності методів

Метод	Метрика ERGAS	SSIM
PCA	2,21	0,768
Grama-Shmidt	1,95	0,831
HSV	2,48	0,672
Wavelet	1,89	0,875
Запропонований (**RES**)	**1,52**	**0,982**

ного, що випливає із самого факту обробки, спрямованої на підвищення інформативності видових даних. При цьому принципове значення має збереження структури первинного зображення в обробленому знімку, інваріантному щодо яскравості й контрастності обробленого знімка (як параметрів, які пов'язані з «зовнішніми факторами», наприклад, чутливістю датчика видової інформації). Нами у якості еталонного зображення було взято панхроматичне зображення, що з набору багатоспектральних даних має найбільш високе просторове (структурне) розрізнення.

Таким чином, аналіз результатів свідчить про те, що синтезоване зображення високого просторового розрізнення з максимальною інформативністю забезпечує комплексування саме за запропонованою технологією з попередньою еквалізацією первинних зображень.

ВИСНОВКИ

У роботі вирішено актуальну задачу автоматизованого підвищення просторового розрізнення первинних багатоканальних зображень.

Наукова новизна роботи полягає у розробці нового методу злиття багатоканальних аерокосмічних зображень на основі HSV-конвертування і гіперсферичного перетворення кольору, що дозволяє поліпшити просторову здатність первинного цифрового зображення й уникнути спектральних спотворень в локальних областях. У порівнянні з існуючими методами злиття запропонована інформаційна технологія дозволяє підвищити інформативність багатоканального зображення без істотних колірних спотворень. Це досягається, зокрема, за рахунок попередньої еквалізації первинних знімків, оброблення даних у локалізованих спектральних базисах, оптимізованого за інформаційними характеристиками, та використання інформації, яку містить зображення інфрачервоного діапазону.

Практична цінність отриманих результатів полягає в тому, що розроблене програмне забезпечення, яке реалізує запропонований метод, дозволяє покращувати інформативність первинного цифрового зображення. Це дозволяє в свою чергу підвищувати достовірність подальшого розпізнавання об'єктів і виділення затінених ділянок на цифровому зображенні високого просторового розрізнення.

Перспективи подальших досліджень полягають у проведені подальших досліджень, пов'язаних з компенсацією впливу низки факторів, які суттєво впливають на просторову та радіометричну розрізненість багатоканальних аерокосмічних зображень, а також визначенням можливості забезпечення заданої достовірності подальшого розпізнавання об'єктів земної поверхні.

ПОДЯКИ

Роботу виконано в рамках держбюджетної науково-дослідної роботи Міністерства освіти і науки України «Математичні моделі та методи ідентифікації та тематичної обробки багатоспектральних растрових зображень» (№ Держ. реєстрації 0112U000187).

СПИСОК ЛІТЕРАТУРИ

1. Шовенгедт Р. А. Дистанционное зондирование. Методы и модели обработки изображений / Р. А. Шовенгердт. – М. : Техносфера, 2010. – 560 с.
2. Pohl C. Review article multisensor image fusion in remote sensing: Concepts, methods and applications / C. Pohl, J. L. van Genderen // International Journal Remote Sensing. – 1998. – № 19. – P. 823–854. DOI: 10.1080/014311698215748.
3. A Survey of Classical Methods and New Trends in Pansharpening of Multispectral Images / [I. Amro, J. Mateos, M. Vega, R. Molina, A. K. Katsaggelos] // EURASIP Journal on Advances in Signal Processing. – Vol. 1/79. – P. 79. DOI: 10.1186/1687–6180–2011–79.
4. Zhang J. Multi-source remote sensing data fusion: Status and trends / J. Zhang // International Journal of Image and Data Fusion. – 2010. – № 1. – P. 5–24. DOI: 10.1080/19479830903561035.
5. Padwick C. WorldView-2 pan-sharpening / C.Padwick, M. Deskevich, F. Pacifici, S. Smallwood // ASPRS: Conference, San Diego, California, 26–30 April, 2010: proceedings. – San Diego, 2010. – P. 99–103.
6. Wang Z. Image Quality Assessment: From Error Visibility to Structural Similarity / Z. Wang, A. C. Bovik, H. R. Sheikh, E.P. Simoncelli // IEEE Transactions on Image Processing. – 2004. – Vol. 13, No. 4.– P. 600–612. DOI: 10.1109/TIP.2003.819861.
7. Wald L. Quality of High Resolution Synthesised Images: Is There a Simple Criterion? / L. Wald // Fusion of Earth Data: Merging Point Measurements, Raster Maps and Remotely Sensed Images: Third Conference, Sophia Antipolis, 26–28 January 2000: proceedings. – Sopia Antipolis, France, 2011. – P. 99–103.
8. Zhang Y. An IHS and wavelet integrated approach to improve pan-sharpening visual quality of natural color IKONOS and QuickBird images / Y. Zhang, G. Hong // International Journal of Image and Data Fusion. – 2005. – № 6. – P. 225–234. DOI: 10.1016/j.inffus.2004.06.009.
9. Гнатушенко В. В. Злиття аерокосмічних зображень високого просторового розрізнення на основі HSV-перетворення та вейвлет-декомпозиції / В. В. Гнатушенко, В. Ю. Шевченко // Вісник ХНТУ. – 2014. – № 2 (47). – С. 100–105.
10. Гнатушенко В. В. Інформаційна технологія підвищення просторової розрізненості цифрових супутникових зображень на основі ICA- та вейвлет-перетворень / В. В. Гнатушенко, О. О. Кавац // Вісник Національного університету «Львівська політехніка», серія «Комп'ютерні науки та інформаційні технології». – 2013. – № 771. – С. 28–32.
11. Li X. Hyperspherical color transform based pansharpening method for WorldView-2 satellite images/ X. Li, H. Mingyi, L. Zhang // Industrial Electronics and Applications: 8th IEEE Conference, Melbourne, Australia, 19–21 June 2013: proceedings. – Melbourne, 2013. – P. 520. DOI: 10.1109/ICIEA.2013.6566424.
12. Малла С. Вейвлеты в обработке сигналов / Пер. с англ. Я. М. Жилейкина. – М. : Мир, 2005. – 671 с., ил.
13. Гонсалес Р. Цифровая обработка изображений в среде MATLAB / Р. Гонсалес, Р. Вудс, С. Эддинс. – М. : Техносфера, 2006. – 616 с.

Стаття надійшла до редакції 09.12.2014.
Після доробки 25.12.2014.

Гнатушенко В. В.[1], Кавац О. О.[2], Шевченко В. Ю.[3]

[1]Д-р техн. наук, профессор, профессор кафедры информационных технологий и систем Национальной металлургической академии Украины, г. Днепропетровск, Украина

[2]Канд. техн. наук, доцент, доцент кафедры информационных технологий и систем Национальной металлургической академии Украины, г. Днепропетровск, Украина

[3]Аспирант Днепропетровского национального университета имени Олеся Гончара, г. Днепропетровск, Украина

ПОВЫШЕНИЕ ПРОСТРАНСТВЕННОГО РАЗРЕШЕНИЯ МНОГОКАНАЛЬНЫХ АЭРОКОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ ВЫСОКОГО ПРОСТРАНСТВЕННОГО РАЗРЕШЕНИЯ НА ОСНОВЕ ГІПЕРСФЕРИЧНОГО ПРЕОБРАЗОВАНИЯ

В работе решена актуальная задача разработки информационной технологии повышения визуального качества многоканальных аэрокосмических изображений высокого пространственного разрешения. Объектом исследования является процесс слияния панхромного и мультиспектрального фотограмметрических сканерных изображений, полученных координатно-чувствительными сенсорами в видимом и инфракрасном диапазонах электромагнитного излучения. Предмет исследования составляют методы предварительной и синергетической обработки многоканальных данных для улучшения качества результирующего изображения и уменьшения цветовых искажений. Цель работы: автоматизированное повышение пространственного разрешения первичного многоканального изображения и по сравнению с существующими методами устранение цветовых искажений в локальных областях. Кроме того, предлагаемая технология позволит эффективно проводить дальнейшее распознавание и оперативный мониторинг объектов инфраструктуры. В работе предложена новая информационная технология слияния многоканальных аэрокосмических изображений на основе HSV-конвертирования и гиперсферического преобразования цвета, которая позволяет улучшить пространственное разрешение первичного цифрового изображения, избежав при этом спектральных искажений. Это достигается, в частности, за счет предварительной эквализации первичных снимков, обработки данных в локализованных спектральных базисах, оптимизированной по информационным характеристикам, и использования информации, содержащейся в изображении инфракрасного диапазона. Разработано программное обеспечение, реализующее предложенный подход. Проведены эксперименты по исследованию свойств данного алгоритма. Экспериментальные оценки проведены на восьмиканальных изображениях, полученных спутником WorldView-2. Результаты тестирования подтвердили, что предложенный подход позволяет достичь высокого спектрального и пространственного качества многоканальных изображений и превосходит существующие методы.

Ключевые слова: сканерное изображения, вейвлет-преобразование, гиперсферическое преобразования, информативность, слияние.

Hnatushenko V. V.[1], Kavats O. O.[2], Shevchenko V. Yu.[3]

[1]Dr. of Sc., Professor, Professor of Department of Information Technologies and Systems, National Metallurgical Academy of Ukraine, Dnepropetrovsk, Ukraine

[2]PhD, Associate Professor, Associate Professor of Department of Information Technologies and Systems, National Metallurgical Academy of Ukraine, Dnepropetrovsk, Ukraine

[3]Post-graduate student, Dnipropetrovsk National University named by Oles Honchar, Dnepropetrovsk, Ukraine

IMPROVEMENT THE SPATIAL RESOLUTION OF MULTICHANNEL AEROSPACE HIGH SPATIAL RESOLUTION IMAGES ON THE BASE OF HYPERSPHERICAL TRANSFORM

In this paper we solve an actual problem of development of information technology to improve the visual quality of multi-channel space images of high spatial resolution. The object of the research is the process of fusing panchromatic and multispectral photogrammetric images obtained coordinate-sensitive sensors in the visible and infrared regions of the electromagnetic radiation. The subject of research are methods make preliminary and synergistic multi-channel data processing to improve the quality of the resulting image and reduce the color distortion. The purpose of the work is to increase the spatial resolution of the automated primary multi-channel images and compared with existing methods of eliminating color distortion in the local areas. In addition, the proposed technology will effectively carry out further recognition and real-time monitoring infrastructure. In the paper we propose a new information pansharpening technology based on HSV-converting and hyperspherical color conversion, which allows not only to improve the spatial resolution of the primary digital image, but also avoid the spectral distortion. This is achieved, in particular, by image pre-equalization, data processing localized spectral bases, optimized performance information, and the information contained in the infrared image. The software implementing proposed method is developed. The experiments to study the properties of the proposed algorithm are conducted. Experimental evaluation performed on eight-channel images obtained WorldView-2 satellite. Test results confirmed that the proposed approach can achieve high spectral and spatial quality multichannel images and outperforms existing methods.

Keywords: scanner images, the wavelet transform, hyperspherical color transform, informative, pansharpening.

REFERENCES

1. Shovengedt R. A. Distancionnoe zondirovanie. Metody i modeli obrabotki izobrazhenij. Moscow. Tehnosfera, 2010, 560 p.
2. Pohl C. J., Van Genderen L. Review article multisensor image fusion in remote sensing: Concepts, methods and applications, *International Journal Remote Sensing,* 1998, No. 19, pp. 823–854. DOI: 10.1080/014311698215748.
3. Amro I., Mateos J., Vega M., Molina R., Katsaggelos A. K. A Survey of Classical Methods and New Trends in Pansharpening of Multispectral Images, *EURASIP Journal on Advances in Signal Processing,* Vol. 1/79, P. 79. DOI: 10.1186/1687–6180–2011–79.
4. Zhang J. Multi-source remote sensing data fusion: Status and trends, International Journal of Image and Data Fusion, 2010, No. 1, pp. 5–24. DOI: 10.1080/19479830903561035.
5. Padwick C., Deskevich M., Pacifici F., Smallwood S. WorldView-2 pan-sharpening, *ASPRS: Conference*, San Diego, California, 26–30 April, 2010: proceedings. San Diego, 2010, pp. 99–103.
6. Wang Z., Bovik A. C., Sheikh H. R., Simoncelli E. P. Image Quality Assessment: From Error Visibility to Structural Similarity, *IEEE Transactions on Image Processing.* 2004, Vol. 13, No. 4, pp. 600–612. DOI: 10.1109/TIP.2003.819861.
7. Wald L. Quality of High Resolution Synthesised Images: Is There a Simple Criterion? *Fusion of Earth Data: Merging Point Measurements, Raster Maps and Remotely Sensed Images: Third Conference*. Sophia Antipolis, 26–28 January 2000, proceedings. Sopia Antipolis, France, 2011, pp. 99–103.
8. Zhang Y., Hong G. An IHS and wavelet integrated approach to improve pan-sharpening visual quality of natural color IKONOS and QuickBird images, *International Journal of Image and Data Fusion,* 2005, No. 6, pp. 225–234. DOI: 10.1016/j.inffus.2004.06.009.
9. Hnatushenko V. V., Ju V.Shevchenko Zlittja aerokosmichnih zobrazhen' visokogo prostorovogo rozriznennja na osnovi HSV-peretvorennja ta vejvlet-dekompozicij, *Visnik HNTU,* 2014, No. 2 (47), pp. 100–105.
10. Hnatushenko V. V., Kavac O. O. Informacijna tehnologija pidvishhennja prostorovoï roziznenosti cifrovih suputnikovih zobrazhen' na osnovi ISA- ta vejvlet-peretvoren', *Visnik Nacional'nogo universitetu «L'vivs'ka politehnika», serija «Komp'juterni nauki ta informacijni tehnologiï»*, 2013, No. 771, pp. 28–32.
11. Li Xu, Mingyi He, Zhang Lei Hyperspherical color transform based pansharpening method for WorldView-2 satellite images, *Industrial Electronics and Applications: 8th IEEE Conference, Melbourne, Australia, 19–21 June 2013: proceedings*. Melbourne, 2013, pp. 520. DOI: 10.1109/ICIEA.2013.6566424.
12. Malla S. Vejvlety v obrabotke signalov. Per. s angl. Ja. M. Zhilejkina. Moscow, Mir, 2005, 671 p.
13. Gonsales R., Vuds R., Jeddins S. Cifrovaja obrabotka izobrazhenij v srede MATLAB. Moscow, Tehnosfera, 2006, 616 p.

УПРАВЛІННЯ У ТЕХНІЧНИХ СИСТЕМАХ

УПРАВЛЕНИЕ В ТЕХНИЧЕСКИХ СИСТЕМАХ

CONTROL IN TECHNICAL SYSTEMS

UDC 004.21

Bayas M. M.

Post-graduate student of Department of Computer Systems of Institute of Automation, Electronics and Computer Systems, Vinnitsia National Technical University, Ukraine. Senior lecturer of «Universidad de la Península de Santa Elena», Ecuador

DEVELOPMENT OF A COORDINATION METHOD FOR EFFECTIVE DECISION-MAKING IN A HIERARCHICAL MULTILEVEL INDUSTRIAL SYSTEM

In modern conditions of manufacturing the ever increasing size of enterprises leads to objective changes in the interdependence of their subordinated structures. The resulting complexity requires modernization of the process management systems. One important direction task in this modernization is the development of effective methods of coordination. Therefore, this article addresses the problem of coordination in decision making among a group of autonomous production units. The object of study is the local decision making process on a dairy plant, which operate with three production lines. The subject of study is the coordination of operations when there is only one packaging machine. The objective of this work is to increase the overall effectiveness index of a system of production units by means of optimal resource allocation and synchronization of operations of technological processes. For effective coordination it is proposed a method that ensures the optimization of processes while considering the particular preferences of each local decision-making unit. For each subordinated decision unit or coordinator, an objective function measures the effectiveness of the subprocesses activities. The coordinator affects the lower-level decision-making so that the performance of the whole system is optimized. It incorporates a hierarchical multilevel system for the management of activities, and the detailed mathematical modeling of the sequencing of operations. The method proposed is based on the theory of fuzzy sets and fuzzy logic. The decision-making process is accomplished by a minimax estimation of the membership functions. The coordinated operations give as result a higher global effectiveness. Additionally, for the comparison of preferences, the normalized criteria of effectiveness based on the technological characteristics of each process are suggested.

Keywords: coordination of subprocess, fuzzy method, hierarchical multilevel system, decision-making.

NOMENCLATURE

opt is an optimal (desired or acceptable) value of the performance of the whole system for the problem being solved;

B_i is a volume of buffer i;

B_{maxi} is a maximum capacity of the temporary stores;

C is a production cost;

E is a effectiveness criterion of the system;

eff_i is a value of a normalization constant;

K_0 is a central coordinator;

$K_{1–3}$ are the subordinated coordinators;

K_4 is a coordinator of the packing device;

P is a revenue;

p_i is a performance of the production lines;

p_u is a performance of the packing device;

R_r is a finished product;

R_o is a raw material;

R_{0i} is a coordination vector (resource allocation);

S is a vector of sequencing of activities;

T is a completion time;

t_{01} is a start time of the first subprocess;

t_{0u} is a start time of operation of the packing and transfer device;

t_{li} is a buffer i loading time;

t_f is a moment of completion of the process;

t_{ui} is a buffer i unloading time;

t_{fu} is an end time of operation of the packing and the transfer device;

t_{pi} is a processing time;

X_{oi} is a decision vector (raw material request);

α_i, λ_i are coordination variables;

σ_{pi} is a measure that takes into account the statistical characteristics of the subprocess.

DOI 10.15588/1607-3274-2015-1-11

INTRODUCTION

In modern conditions of manufacturing the ever increasing size of enterprises leads to objective changes in the interdependence of their subordinated structures. The resulting complexity requires modernization of the process management systems. One important direction task in this modernization is the development of effective methods of coordination.

The objective of this paper is to increase the overall effectiveness index of a system of production units by means of optimal resource allocation and synchronization of operations of technological processes.

1 PROBLEM STATEMENT

Given a system comprised of a set of subprocesses (production lines) $<SP_1, SP_2, ..., SP_n>$ with the inputs (raw material) $<R_{01}, R_{02}, ... , R_{0n}>$ intermediate outputs (produced units) $< R_{r1}, R_{r2}, .. R_{ri} >$ and the following restrictions: buffers $<B_1, B_2, ..., B_n>$; production line performances $< p_1, p_2, ... p_n>$, performance of a shared single packing and transfer mechanism p_u. Taking into account the physical and technical constraints the problem of system coordination is to find a decision vector $< R_{01}, R_{02}, ... , R_{0n} >$ in order to obtain $E = F(\text{eff}_i) \rightarrow \text{opt}$, where in E is the effectiveness criterion of the system and eff_i the effectiveness criteria of the different subprocesses.

As the object of study let's consider the problem of coordination of local decisions of a dairy plant, which produces three types of dairy products. The technological process of preparation and packaging of milk is a complex technological task automation, which should provide some technological operations: receiving, separation, homogenization, normalization, packaging and packing. Each operation is a time-consuming process that requires continuous monitoring. The objective of the management system is the coordination of the operations when there is only one packaging machine. The presence of only one packaging device makes it very difficult the parallel operation of all the lines, and therefore it leads to downtime and loss of profits. Figure 1 shows the typical scheme of coordination of the dairy plant.

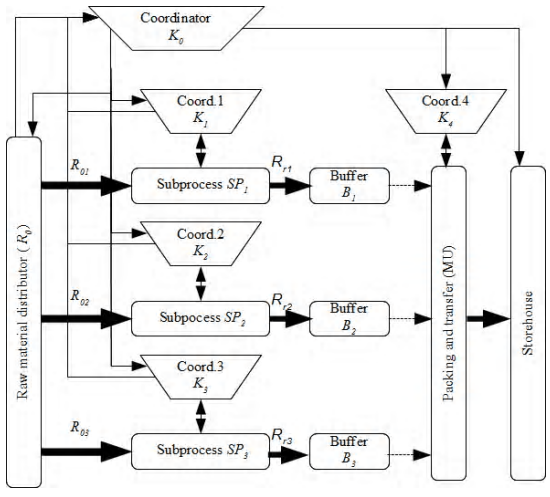


Figure 1 – Scheme of coordination: ➡ – mass flow, → – data flow, ➞ – subprocess pending for packing and transfer

2 REVIEW OF THE LITERATURE

The problem of development of science-based hierarchical management systems becomes relevant in a continuous adaptation of modern industries to external changes. It is important to highlight the Mesarovic's theory of management of hierarchical multilevel systems [1] among one of the most significant developments in the field of hierarchical structures of a different nature. Also significant contributions were made in the work of the following researchers, T. Malone and K. Crowston, A. A. Voronin, S. P. Mishin, V. N. Burkova, D. A. Novikov, M. B. Gubko, M. J. Beckmann and several other researchers [2–9]. The basis of most of these works on classical is the methods of mathematical programming, game theory, the theory of dynamic systems. The study of hierarchical systems has a number of basic problems of operation and control. In particular, the problem of decomposition of the system, the task of coordinating the system, the task of accounting for uncertainty of parameters and variables in hierarchical decision-making systems are of interest [10].

The coordination method of the multi-level hierarchical system, of course, has an impact on its most important characteristics, such as efficiency, reliability, and cost. Therefore, the determination of the optimal coordination method is an important task in the design of complex process control systems [1–10].

The principal methods focus mostly on iterative and non-iterative algorithms for deterministic coordination. However, the variety of problems of coordination, the large size of the problem, the uncertainty in estimating the state of the coordinated processes requires further research. In particular, the published studies do not consider the problem of resource allocation in relation to the task of synchronizing parallel processes [10–13].

3 MATERIALS AND METHODS

The main task in the development of a multi-level system is the specification of system elements. In the simplest case, a coordinator K can be modeled by input/output relation $K \subset I \times O$, I is the set of inputs and O the set of outputs. In most cases, the mapping from one set to another is not expressed explicitly. The input and output variables and parameters of the coordinators are showed in fig. 2.

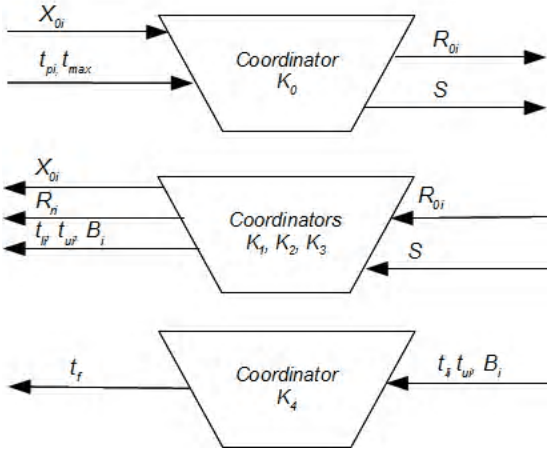


Figure 2 – Coordinators' input and output variables and parameters

One key factor in process management systems is the performance analysis. This analysis ensures that the system meets the technical requirements; the final products are delivered on time, and manufactured within reasonable costs. For each subordinated decision unit or coordinator, an objective function *eff*, measures the effectiveness of the subprocesses activities and is a function of the sub-systems input and output variables. The objective of the coordinator is to affect the lower-level decision-making so that the performance of the whole system is optimized. Having a performance index for each subprocess allows to make the sub-system decision-making problems independent from each other and to remove the possible «conflicts» caused by the interconnections between the sub-systems.

The full use of productive capacity is an objective optimization of industrial processes. The amount of resources allocated to each subprocess determines the degree of utilization. However, if the assignment exceeds the performances then the lines work in low-efficiency regimes. The efficiency criterion must, therefore, consider these factors, equation (1):

$$eff_i = eff_{0i} \exp\left[\frac{-\left(\frac{X_i}{p_i} - T\right)^2}{\sigma_{pi}}\right]. \quad (1)$$

One of the issues when measuring effectiveness criteria of the different subprocesses concerns the scale, fig. 3. Scaling coefficients are used to represent all numerical quantities to comparable orders of magnitude; in this case they are normalized to one.

To formalize the effectiveness criterion of the packing and transfer device, it is necessary to formulate the model of the process, a Gantt chart is shown in fig. 4.

A wide range of problems, including the coordination of production activities are solved using search methods. These methods aim to find an optimal solution within a search space Ω, defined by a series of constraints. In most cases, the search requires high computational costs. Analytical methods, such as gradient-based methods are not applicable when the space is multidimensional search or the task has a combinatorial nature. For this reason researchers prefer heuristic methods such as genetic algorithms or random search methods [10, 12–14].

Then the criterion of effectiveness of the packing machine can be written as follows in the equation (2):

$$eff_4 = \frac{\sum_{i=1}^{n} \frac{R_{ri}}{p_u}}{t_{fu} - t_{ou}}. \quad (2)$$

The task of the coordinator of the packing machine is to minimize coefficient eff_4. The sequencing of the operations is carried out as follows:

1. Finding the number k of subprocesses that can work in parallel, equation (3):

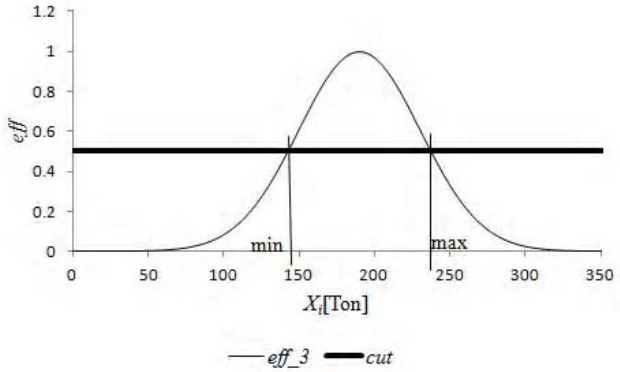


Figure 3 – Effectiveness criteria of the different subprocesses

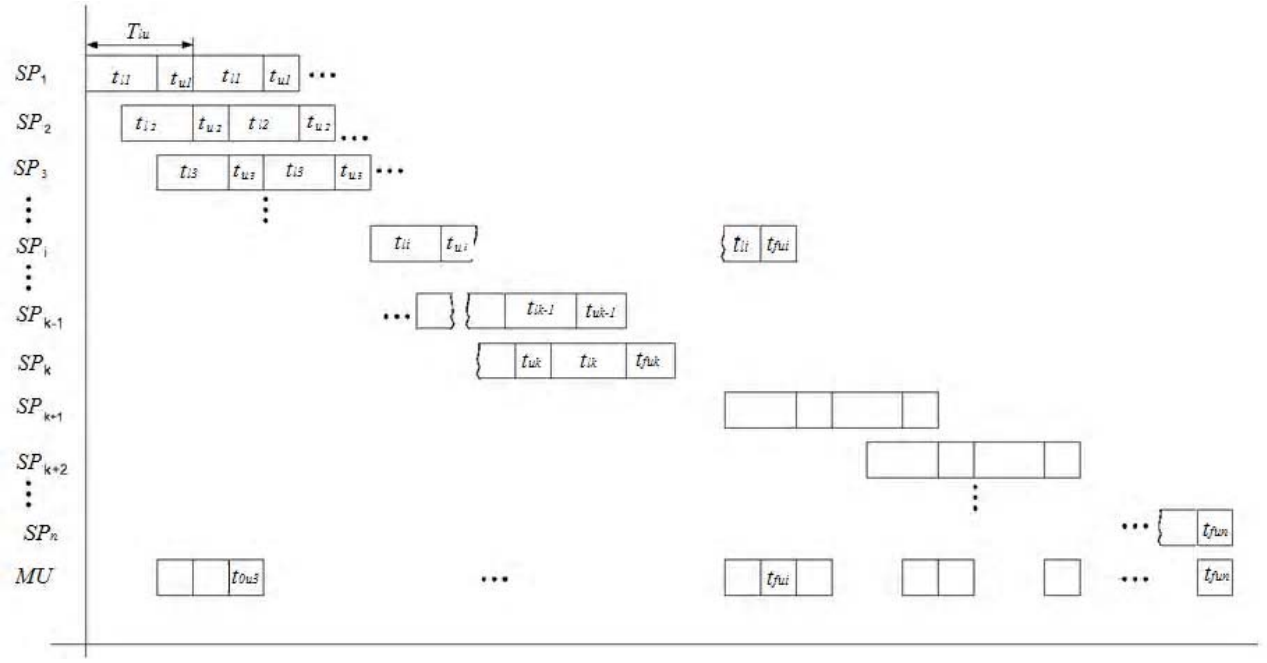


Figure 4 – Model of the process

$$\sum_{i=1}^{r\in(1,n)} p_i = p_i \le p_u < \sum_{i=1}^{k+1} p_i. \quad (3)$$

2. The k subprocesses are sequenced according to the value of the buffer load time so that if $t_{li} > t_{lj}$ then $t_{0i} < t_{0j}$,

3. The remaining $n–k$ subprocesses are sequenced from the lowest to the highest according to the buffer loading time.

4. The start time of the subprocess $k+1$ is equal to equation (4):

$$\max_{i\in(1,k)} (t_{fi}) - t_{l(k+1)}. \quad (4)$$

For the calculation of the start time and final time of operations, the following procedure is proposed:

Let to consider the parallel processes. The start time of the process is equal to the start time of the first subprocess $t_{01}=0$, and the start time for the i subprocess is given equation (5):

$$t_{\substack{oi \\ i\in(1,k)}} = (i-1)T - \sum_{j=2}^{i} t_{lj}. \quad (5)$$

where T_{lu} is the sum of t_{li} and t_{ui}. The completion time of the sub-processes is written as $t_{fi}=t_{oi}+t_{pi.}$ And the process time t_{pi} is given by equation (6):

$$t_{pi} = \frac{R_{ri}}{p_i}. \quad (6)$$

From these equations, the completion time of the parallel subprocesses k is given by equation (7):

$$t_{f\max} = t_{\substack{0i \\ i=\arg(t_{p\max})}} + \max_{i\in(1,k)} \frac{R_{ri}}{p_u}. \quad (7)$$

For subprocesses $n–k$, that work in series, the start time and the completion time are calculated by equations (8) and (9):

$$t_f(k+j) = t_0(k+j) + t_p(k+j), \quad (8)$$

$$t_0(k+j) = t_{fk} - t_l(k+j). \quad (9)$$

Therefore,

$$t_{fn} = k\, t_{f\max} - \sum_{i=k+1}^{n} t_{li} + \sum_{i=k+1}^{n} t_{pi}, \quad (10)$$

The start time of the packing device $t_{ou}=t_{l1}$ and the completion time $t_{fu}=t_{fn}$.

A number of sub-processes can work in parallel if the conditions illustrated in fig. 5 are met by equation (11):

$$\begin{cases} t_{li} + t_{ui} = T_{lu}, \\ \sum tui = T_{lu}, \\ \sum_{i=1}^{n} t_{li} = (k-1)\sum_{i=1}^{k} t_{ui}. \end{cases} \quad (11)$$

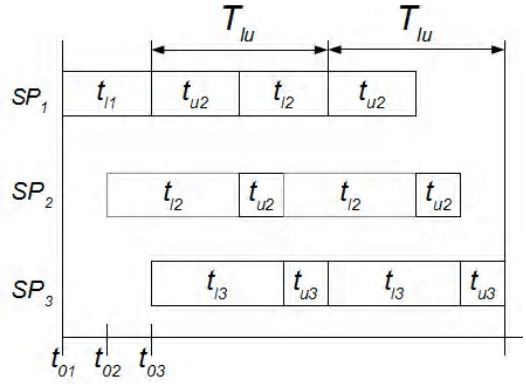


Figure 5 – Gant diagram of the analysis for the completion time of the subprocesses

The coordination can be achieved through the variation of the quantities stored in temporary spaces and the variation of the performance of the lines. By the introduction of the coordination variables α_i for temporary store B_i and λ_i for machines performance, equation (11) can be rewritten in the parametric form as the equation (12):

$$\begin{cases} T_{lu} = f(\alpha_i, \lambda_i), \\ s.t. \\ \sum_{i=1}^{n} \frac{\alpha_i B\max_i}{\lambda_i, p_i} = (n-1)\sum_{i=1}^{n} \frac{\alpha_i B\max_i}{p_u \lambda_i, p_i}. \end{cases} \quad (12)$$

Thus, the coordination task is reduced to finding a vector $X(\alpha_i, \lambda_i)$, which satisfies the above-mentioned conditions:

$$\begin{cases} \min\left|\sum t_l(\alpha_i, \lambda_i) - (n-1)\sum t_u(\alpha_i, \lambda_i)\right|, \\ s.t. \\ \alpha \in [\alpha_{\min}, \alpha_{\max}], \\ \lambda \in [\lambda_{\min}, \lambda_{\max}] \end{cases} \quad (13)$$

The values $\alpha_{\min}$, $\alpha_{\max}$, $\lambda_{\min}$, $\lambda_{\max}$, ensure that the subprocesses operate in the rank of better efficiency. Equation (13) is solved either by genetic algorithms or a random search method, based on sampling and local search.

As the criterion for evaluating the effectiveness of the upper-level coordinator, it is proposed the relationship between the net profit and maximum completion time in the equation (14):

$$E = \frac{P - C}{T}. \quad (14)$$

It is worth noting that the execution time T depends on the amount of raw material, designated by each line and its technical parameters. Thus, the selected criterion is a function of the resources allocated to each line and the sequencing of operations.

The overall decision-making is based on the coordination of the decision of the subprocesses. These decisions are the result of the optimization procedures. The value of optimization problems can be modiыed with a set of weight coefficients, in order to make the subprocesses decision problems independent from each other.

When designing complex systems, there is often ambiguity in one or more of the following elements: constraints, demands or objectives. This imprecision arises because of the scarcity of information or the same nature of processes, which does not allow a satisfactory formulation of the design goals, and thus the inability to assess the relative importance objectives.

4 EXPERIMENTS

To coordinate the making decision process of the object of this study it applied the proposed a mechanism based on fuzzy sets [11]. Formulating a fuzzy coordination problem entails developing membership functions м for each constraint and each objective. It is important that the membership functions are normalized to comparable value, usually 1. The membership function of a subprocess is the coordination function of that subprocess. On the other hand, the criteria of effectiveness, which act as the degree of satisfaction of the subprocess is the coordination function.

It is desirable to find a solution that maximizes the value of each criterion. However, such a situation occurs only in ideal cases, therefore, for real problems a compromise solution is required. This leads to the need to specify the sequence of application of the criteria and the relative importance. The minimax criterion for the solution of the decision-making problem allows overcoming the disadvantages that appear when applying the additive and multiplicative indicators. The intersection of the membership function of subprocesses objectives, including the upper-level coordinator, yields the membership function of the system:

$$\mu_g = \min(\mu_0, \mu_1, \mu_2, ..., \mu_n). \quad (15)$$

The value that maximizes the global decision is defined as follows:

$$\max_{x \in X} \mu_g(x) = \max_{x \in X} \min \mu_g(\mu_0, \mu_1, \mu_2, ..., \mu_n). \quad (16)$$

The block diagram shows the management process, with the resolution of optimization problems of local subprocesses and the coordination of the isolated solutions.

1. Begin.
2. Selection of the solution vector.
3. Selection of weight coefficients.
4. For i=1 to n subprocess:

a) assigning solution vector to lower levels subsystems;
b) solution of local optimization problems;
c) calculation of membership functions.

5. End for.
6. Calculation of the global membership function μ_g.
7. If $\mu_g < \min\mu_g$ repeat from step 2.
8. End.

5 RESULTS

Figures 6 and 7 show the evolution of the values of the coefficient of effectiveness as a function of the iterations of the process of coordination. The top figure corresponds to system index and lower figure to subprocesses. At the point of coordination, all subprocesses operate within the ranges

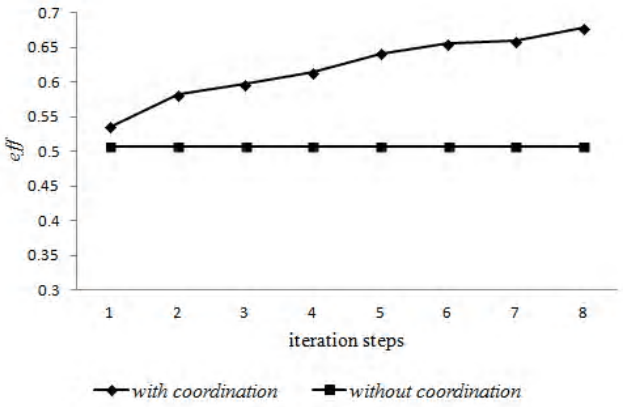


Figure 6 – Coefficient of effectiveness of system with coordination and without coordination

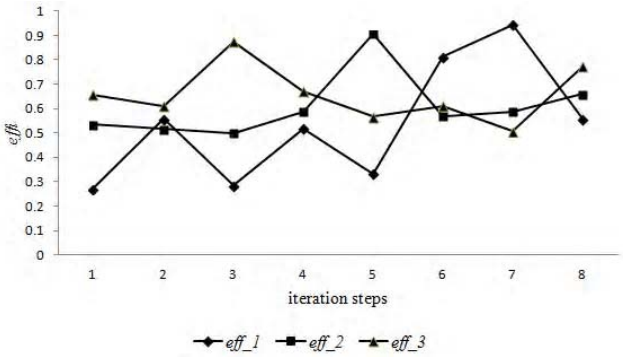


Figure 7 – Coefficient of effectiveness of subprocesses

set forth in the optimization process and under these conditions the overall effectiveness is higher for the case with coordination compared with the case without coordination.

6 DISCUSSION

The results fully support that coordination has a positive effect on the performance of control systems. However, the determination of the effectiveness criteria exerts a large influence on the results. For example, if to take the balance of the criteria of effectiveness as the stopping condition then in the second iteration the program would have stopped. This fact would have led to a suboptimal result as it is clearly illustrated in Figures 6–7. Another important aspect that we have found is the stability of the algorithm. Even though, the behavior of the curves for the indices of effectiveness for each subsystem seems to be erratic, the overall result has a monotonous improvement in each iteration. The method was developed with the characteristics and peculiarities of a specific application under certain conditions; therefore is necessary to take into consideration these conditions for other applications.

CONCLUSION

A fuzzy method for the coordination of the activities of a dairy plant was developed. It incorporates a hierarchical multilevel system for the management of activities, and the detailed mathematical modeling of the sequencing of operations. The decision-making process was accomplished by a minimax estimation of the membership functions. The coordinated operations give as result a higher global effectiveness.

ACKNOWLEDGMENTS

This work was supported by the grant «The Ministry of Higher Education, Science, Technology and Innovation» SENESCYT «Ecuador, and is sponsored by the University of Santa Elena» «UPSE», Ecuador.

REFERENCES

1. Месарович М. Теория иерархических многоуровневых систем / М. Месарович, Д. Мако, И. Такахара. – М. : Мир, 1973. – 344 с.
2. Ладанюк О. А. Автоматизированное управление взаимосвязанными подсистемами технологических комплексов пищевых производств: дисертаційна робота на здобуття наукового ступеню канд. техн. наук / О. А. Ладанюк. – К. : 1996. – 176 с.
3. Бурков В. Н. Основы математической теории активных систем / В. Н. Бурков. – М. : Наука, 1977. – 255 с.
4. Новиков Д. А. Механизмы функционирования многоуровневых организационных систем. / Д. А. Новиков. – М. : Фонд «Проблемы управления», 1999. – 150 с.
5. Beckmann M. Management production function and the theory of the firm / M. Beckmann // Journal of Economic Theory. – 1977. – № 14 – P. 1–18.
6. Goubko M. V. Optimal hierarchies of control for cost functions presentable as sum of homogenous functions. / M. V. Goubko // Automation and Remote Control. – 2010. – Vol. 71, № 9.– P. 1913–1926.
7. Mishin S. P. Optimal stimulation in multilevel hierarchical structures. / S. P. Mishin // Automation and Remote Control 65, 2004. – № 5. – P. 768–789.
8. Воронин А. А. Оптимальные иерархические структуры / А. А Воронин, С. П. Мишин. – М. : ИПУ РАН, 2003. – 210 с.
9. Malone T. W. The interdisciplinary study of coordination / T. W. Malone, K. Crowston // ACM Comput. Surveys. – 1994. – Vol. 26, № 1. – P. 87–119.
10. Dubovoy V.M. Decision-making in the management of branched technological processes: monograph / V. M. Dubovoy, G. Y. Derman, I. V. Pylypenko, M. M. Bayas. – Vinnitsa : VNTU, 2013. – 223 c.
11. Системний аналіз складних систем управління : навч. посіб. / [А. П. Ладанюк, Я. В. Смітюх, Л. О. Власенко та ін.]. – К. : НУХТ, 2013. – 274 с.
12. Bayas M. M. Efficient Resources Allocation in Technological Processes Using Genetic Algorithm / M. M. Bayas, V. M. Dubovoy // Middle-East Journal of Scientific Research. – 2013. – Vol. 14, № 1. – P. 1–4. DOI: 10.5829/idosi.mejsr.2013.14.1.16313.
13. Bayas M. M. Efficient Resources Allocation in Technological Processes Using an Approximate algorithm based on Random Walk / M. M. Bayas, V. M. Dubovoy // International Journal of Engineering and Technology. – 2013. – Vol. 5, № 5. – P. 4214–4218.
14. Байас М. М. Координация решений о распределении ресурсов на основе генетического алгоритма / М. М. Байас, В. М. Дубовой // Інформаційні технології та комп'ютерна інженерія. – 2014. – № 2. – С. 4–12.

Article was submitted 07.11.2014.
After revision 22.12.2014.

Байас М. М.

Аспирант кафедры компьютерных систем управления, Винницкий национальный технический университет, Винница; преподаватель «Universidad de la Península de Santa Elena», Эквадор

РАЗРАБОТКА КООРДИНАЦИОННОГО МЕТОДА ДЛЯ ЭФФЕКТИВНОГО ПРИНЯТИЯ РЕШЕНИЙ В ИЕРАРХИЧЕСКОЙ МНОГОУРОВНЕВОЙ ПРОМЫШЛЕННОЙ СИСТЕМЕ

В условиях современного производства происходят объективные изменения в функционировании промышленных предприятий, что связано с ростом их размеров и сложностью во взаимозависимости подчиненных структур. Поэтому на предприятии необходима модернизация систем управления процессами. Одним из важных заданий в этой модернизации является разработка эффективных методов координации. Поэтому в данной статье рассматриваются проблемы координации в принятии решений в группе автономных производственных единиц. Объектом исследования являются процессы принятия локальных решений на молокозаводе, на котором работает три производственные линии. Предметом исследования является координация операций, когда имеется только одна упаковочная машина. Цель данной работы – увеличить общий индекс эффективности системы производственных единиц за счет оптимального распределения ресурсов и синхронизации операций технологического процесса. Для эффективной координации предлагается метод, который обеспечивает оптимизацию процессов при рассмотрении конкретных предпочтений каждого локального блока принятия решений. Для каждого подчиненного блока принятия решений или координатора, целевая функция измеряет эффективность деятельности подпроцессов. Координатор влияет на процесс принятия решений более низкого уровня, так что производительность системы в целом оптимизируется. Координатор содержит иерархическую многоуровневую систему для управления деятельностью, а также детальное математическое моделирование последовательности операций. Предложенный метод основан на теории нечетких множеств и нечеткой логики. Процесс принятия решений осуществляется посредством минимаксной оценки функций принадлежности. Координированные операции дают в качестве результата более высокую глобальную эффективность. Кроме того, для сравнения предпочтений предложены нормированные критерии эффективности, основанные на технологических характеристиках каждого процесса.

Ключевые слова: координация подпроцесса, нечеткий метод, иерархическая многоуровневая система, принятие решений**.**

Байас М. М.

Аспирант кафедри комп'ютерних систем управління, Вінницький національний технічний університет, Вінниця; викладачка «Universidad de la Península de Santa Elena», Еквадор

РОЗРОБКА КООРДИНАЦІЙНОГО МЕТОДУ ДЛЯ ЕФЕКТИВНОГО ПРИЙНЯТТЯ РІШЕНЬ В ІЄРАРХІЧНІЙ БАГАТОРІВНЕВІЙ ПРОМИСЛОВІЙ СИСТЕМІ

В умовах сучасного виробництва відбуваються об'єктивні зміни у функціонуванні промислових підприємств, що пов'язано з ростом їхніх розмірів і складністю у взаємозалежності підлеглих структур. Тому на підприємстві необхідна модернізація систем керування процесами. Одним з важливих завдань у цій модернізації є розробка ефективних методів координації. Тому в даній статті розглядаються проблеми координації в прийнятті рішень у групі автономних виробничих одиниць. Об'єктом дослідження є процеси прийняття локальних рішень на молокозаводі, на якому працює три виробничі лінії. Предметом дослідження є координація операцій, коли є тільки одна пакувальна машина. Мета даної роботи – збільшити загальний індекс ефективності системи виробничих одиниць за рахунок оптимального розподілу ресурсів і синхронізації операцій технологічного процесу. Для ефективної координації пропонується метод, що забезпечує оптимізацію процесів при розгляді конкретних переваг кожного локального блоку прийняття рішень. Для

кожного підпорядкованого блоку прийняття рішень або координатора, цільова функція вимірює ефективність діяльності підпроцесів. Координатор впливає на процес прийняття рішень більш низького рівня так, що продуктивність системи в цілому оптимізується. Координатор містить ієрархічну багаторівневу систему для керування діяльністю, а також детальне математичне моделювання послідовності операцій. Запропонований метод заснований на теорії нечітких множин і нечіткої логіки. Процес прийняття рішень здійснюється за допомогою мінімаксного оцінювання функцій належності. Координовані операції дають як результат більш високу глобальну ефективність. Крім того, для порівняння переваг запропоновані нормовані критерії ефективності, засновані на технологічних характеристиках кожного процесу.

Ключові слова: координація підпроцесу, нечіткий метод, ієрархічна багаторівнева система, прийняття рішень.

REFERENCES

1. Mesarovich M., Mako D., Takahara I. Theory of hierarchical multilevel systems. Moscow, Mir, 1973, 344 p.
2. Ladanyuk O. A. Automated control of interconnected subsystems technological systems of food production: disertatsiyna robot zdobuttya Naukova stage cand. tehn. Sciences. Kiev, 1996, 176 p.
3. Burkov V. N. Foundations of the mathematical theory of active systems. Moscow, Nauka, 1977, 255 p.
4. Novikov D. A. Mechanisms of multilevel organizational systems. Moscow, Foundation «Problems of Control», 1999, 150 p.
5. Beckmann M. Management production function and the theory of the firm, *Journal of Economic Theory,* 1977, No. 14, P. 1–18.
6. Goubko M. V. Optimal hierarchies of control for cost functions presentable as sum of homogenous functions, *Automation and Remote Control*, 2010, Vol. 71, No. 9, pp. 1913–1926.
7. Mishin S. P. Optimal stimulation in multilevel hierarchical structures, *Automation and Remote Control 65*, 2004, No. 5, pp. 768–789.
8. Voronin A. A., Mishin S. P. Optimal hierarchical structure. Moscow, ICS RAS, 2003, 210 p.
9. Malone T. W., Crowston K. The interdisciplinary study of coordination, *ACM Comput. Surveys,* 1994, Vol. 26, No. 1, pp. 87–119.
10. Dubovoy V. M., Derman G. Y., Pylypenko I. V., Bayas M. M. Decision-making in the management of branched technological processes: [monograph]. Vinnitsa, VNTU, 2013, 223 c.
11. Ladanyuk A. P. Smityuh Y., Vlasenko L. O. [that in.]. Systemic analiz folding systems upravlinnya: navch. posib. Kiev, NUHT, 2013, 274 p.
12. Bayas M. M., Dubovoy V. M. Efficient Resources Allocation in Technological Processes Using Genetic Algorithm, *Middle-East Journal of Scientific Research*, 2013, Vol. 14, No. 1, pp. 1–4. DOI: 10.5829 / idosi.mejsr.2013.14.1.16313.
13. Bayas M. M., Dubovoy V. M. Efficient Resources Allocation in Technological Processes Using an Approximate algorithm based on Random Walk, *International Journal of Engineering and Technology*, 2013, Vol. 5, No. 5, pp. 4214–4218.
14. Bayas M. M., Dubovoy V. M. Coordination resource allocation decisions based on genetic algorithm, *Informatsiyni tehnologiï that Komp'yuterniy inzheneriya,* 2014, No. 2, pp. 4–12.

Наукове видання

Радіоелектроніка,

інформатика,

управління

№ 1/2015

Науковий журнал

Головний редактор – д-р фіз.-мат. наук В. В. Погосов

Заст. головного редактора – д-р техн. наук С. О. Субботін

Комп'ютерне моделювання та верстання — С. В. Зуб
Редактор англійських текстів — С. О. Субботін

Оригінал-макет підготовлено у редакційно-видавничому відділі ЗНТУ

Свідоцтво про державну реєстрацію
КВ № 6904 від 29.01.2003.

Підписано до друку 15.06.2015. Формат 60×84/8.
Папір офс. Різогр. друк. Ум. друк. арк. 9,99.
Тираж 300 прим. Зам. № 632.

69063, м. Запоріжжя, ЗНТУ, друкарня, вул. Жуковського, 64

Свідоцтво суб'єкта видавничої справи
ДК № 2394 від 27.12.2005.