Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center

Viktor Grechaninov[a], Hennadii Hulak[b], Volodymyr Sokolov[b], Pavlo Skladannyi[b], and Nataliia Korshun[b]

[a] Institute of Mathematical Machines and Systems, Kyiv, Ukraine
[b] Borys Grinchenko Kyiv University, Kyiv, Ukraine

Abstract

In modern conditions of abrupt changes in the military-political situation, the problem of ensuring the security and cyber protection of computer systems of situational centers of critical infrastructure facilities are acquired particular importance. Information systems of situational centers of critical infrastructure need meticulous attention to methods and tools. The paper presents an analysis of the components of cybersecurity and dependability. The research is based on the ontological approach to their mutual impact, determining the features of the complex influence of random errors and deliberate attacks. Based on the analysis of the attributes of dependability and cybersecurity, a game model is proposed. In addition to the cyber-attack entity, the approach considers another allied player entity, accidental factors of artificial and natural origin. However, implementing these factors can destroy the computer system's software and/or hardware platforms. However, it can also significantly affect the level of technical and cryptographic protection of the system. It is shown that it is necessary to ensure trust in the design procedures, configuration management, and safe installation, which are potential steps for implementing loopholes. Using the concept of a tuple of information elements in the framework of the proposed game model, a single criterion of dependability and cybersecurity of the computer (specifically, information) system of the situation center is formulated. A generalized model of dependability and cyber protection of the information system of the situation center of the critical infrastructure facility has been built. The given model allows a complex estimation of the dependability capacity of situational centers.

Keywords

Cybersecurity of the situation center, criterion of dependability, criterion of confidentiality, reliability of critical infrastructure.

1. Introduction

The complex and multifaceted challenges facing Critical Infrastructure Information Center (CIS) information systems require meticulous attention to methods and tools. Such approaches are used to provide the necessary services that can be guaranteed to be trusted. Conceptual principles for the interrelation of dependability and security of information systems are given in [1]. The main attributes of information systems, such as accessibility, reliability, security, integrity, maintainability, etc., are defined. In addition to accessibility and integrity, security is also associated with privacy. The main provisions of the study are supplemented by additional definitions that address threats to reliability and security (faults, errors, failures), their attributes, and means of achieving them (fault prevention, fault tolerance, forecasting, and troubleshooting). In particular, the "tree" of the listed essences is proposed in [2], represented in Fig. 1.

Emerging Technology Trends on the Smart Industry and the Internet of Things, January 19, 2021, Kyiv, Ukraine
EMAIL: grechaninov@nas.gov.ua (V. Grechaninov); h.hulak@kubg.edu.ua (H. Hulak); v.sokolov@kubg.edu.ua (V. Sokolov); p.skladannyi@kubg.edu.ua (P. Skladannyi); n.korshun@kubg.edu.ua (N. Korshun)
ORCID: 0000-0001-6268-3204 (V. Grechaninov); 0000-0001-9131-9233 (H. Hulak); 0000-0002-9349-7946 (V. Sokolov); 0000-0002-7775-6039 (P. Skladannyi); 0000-0003-2908-970X (N. Korshun)

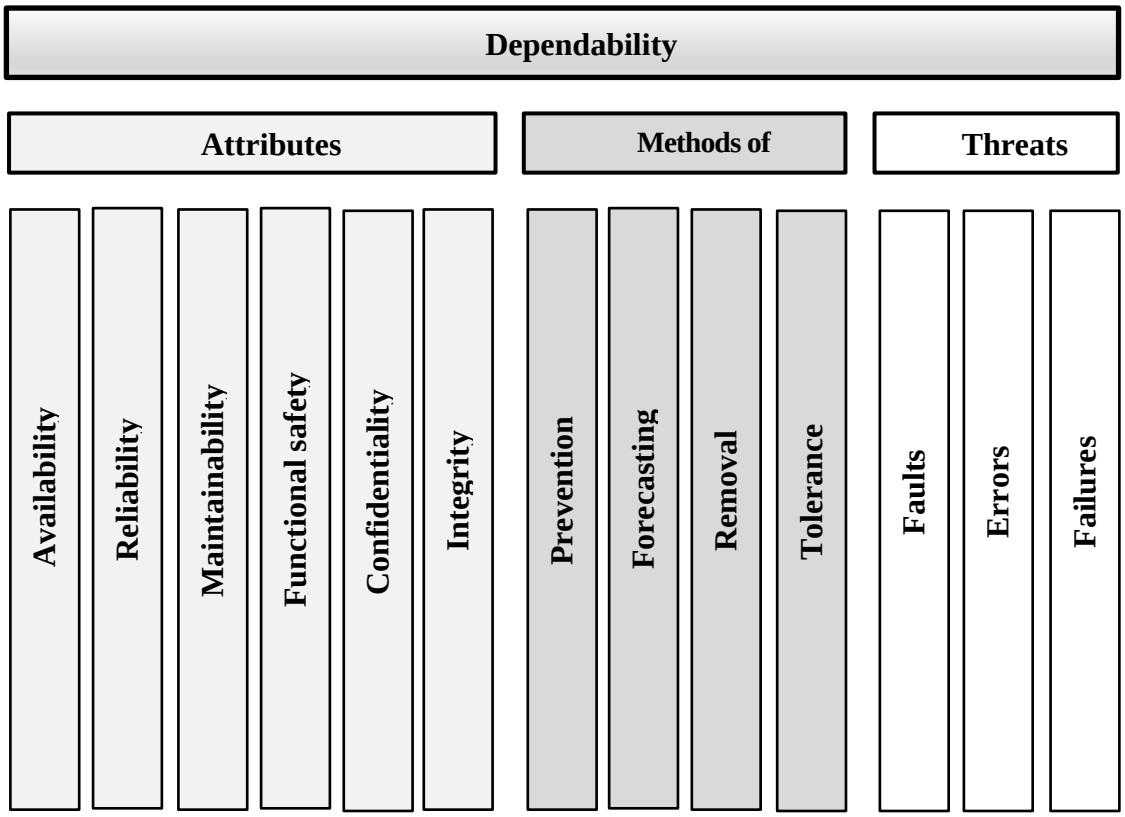

Figure 1: Tree of components of security and protection [3]

From the tree, it can be seen that dependability includes a whole set of attributes, methods of security, and threats.

With the growing power and frequency of cyberattacks, the essential elements for studying the problems of security and cyber protection are their owners and attackers. Both sides are the subject of information conflict over computer systems. On the one hand, owners expect these systems to provide services that can be reasonably trusted. On the other hand, sure attackers or groups, including those supported by certain political or financial circles, try to harm the owners of computer systems.

The subjects of information conflict and their interaction remain insufficiently described and studied. The scientific problem of cybersecurity of critical infrastructure information systems and situational centers that control the security of such systems remains unresolved. Therefore, research on the development of the structure of entities involved in information conflict and the formalization of models of security and cybersecurity is relevant.

2. Work Review and Problem Statement

Automatic collection, analysis, and preparation of security data are proposed to overcome the scalability of information systems effectively. The difficulties of this approach are due to the limitations of autonomous cybersecurity networks. Defining players and their roles will overcome such difficulties. The paper [4] presents the research results on where and why the human factor seems indispensable.

The article [5] presents the structure of intelligent decision support systems based on the situation center. The intelligent subsystem of the situational center allows solving problems based on various sources of information, taking into account uncertainty. Nevertheless, the presented block diagram does not take into account the formalization of the roles of the attacker.

Separate issues of security threats to situational centers are presented in [6]. The proposed solutions only partially help to combat threats. Increasing the capacity of the situation center equipment or additional training only partially solves the problem of exponential growth in the number of attacks.

The work [7] describes a mathematical model for rapid state analysis and forecasting national security. The proposed method of training specialists in national security seems to be the most adequate

for today's challenges. It allows setting up a learning process for staff of situation centers. However, still, the method considers the problem one-sidedly and lacks a comprehensive approach.

The study builds a model of the state of dependability of a computer system, clarifies certain concepts and the structure of dependability attributes, formulates the principles of dependability, and analyzes current issues related to the creation of dependability of computer systems. In [8], the analysis of complex tasks arising at the life cycle stages of dependability of computer systems was carried out. In particular, the issues of quality assessment of such systems were studied.

Similar studies of various aspects of building and evaluating the quality of dependability of computer systems without a detailed analysis of information security mechanisms [9]. In particular, the attributive model of system dependability was studied in [10], and also a complex analysis of the essential attributes and metrics of system dependability was carried out.

Ensuring the safety of information security tools, particularly cryptographic computer systems, was first studied in [11]. In particular, a method of assessing the reliability of digital signature computer systems based on elliptical curves is proposed. It is proposed to define the warranty of such systems as the probability that the signature will not be broken during the mission.

For the first time, this paper proposes a quantitative approach to assessing the level of confidentiality in reputable computer systems that can be applied to information systems for a variety of purposes, including critical infrastructure. In [12], primary attention is paid to security issues. Moreover, in [13] - the quality of cryptographic transformations in the event of accidental failures, errors, and failures of hardware and software platforms of cryptographic information security is analyzed. A similar problem is considered in [14], where the issue of ensuring confidentiality is guaranteed systems is considered without reference to specific mechanisms of information protection.

The harmonized standard DSTU ISO / IEC 19790 [16] sets out the security objectives of crypto modules, which are associated with dependability but are not identified with it. The standard requires the detection of failures and errors in the module and the prevention of negative consequences of these adverse events, eliminating the possibility of unauthorized modification of cryptographic functions and data of the module. There are also additional restrictions: replacement, input, or removal of keys and other security-critical parameters, ensuring the proper work of the module in the specified mode, and so on.

Regarding scientific research on providing the security and safety of special-purpose information systems, it is possible to pay attention to the publication [17]. In this paper, we consider it an interdependent factor, but the dependence function is not defined. In [18], special-purpose systems are also considered, with the components of information system security and characteristics of their possible defeat in case of attacks on the system.

With the increasing number and growth of cyberattacks, there is a need to ensure the sustainable operation of unique information systems. Thus, despite the significant number of scientific publications in the construction and operation of guaranteed information systems and means of information protection, there is no practical model of counteraction. There is a separate description of the requirements for information systems used in situational centers of the national security and defense sectors.

Since the first massive cyberattacks on critical infrastructure, the issue of regulatory norms to ensure the security of computer systems and information security has become paramount. In particular, the Resolution of the Cabinet of Ministers [15] defines the organizational and technical requirements for cyber security in critical infrastructure. It also sets out different requirements for ensuring the availability and resilience of the components of the relevant systems but does not link this to the broader concept of “dependability” [19–21].

There is an urgent scientific and practical task of developing general security and cyber protection model, which would take into account the antagonistic behavior of the system owner, on the one hand, and the attacker (or random factors), on the other. All this suggests that it is appropriate to conduct a study on the model of the antagonistic matrix game.

3. Purpose and Objectives of the Study

The work aims to analyze the components of cybersecurity and dependability. The research is based on the ontological approach to their mutual influence. It is meant to determine the features of the complex impact of random errors and deliberate attacks on the components of the CPC. A separate issue remains to construct a generalized model for dependability and cyber security of relevant information systems. This will make it possible to form a criterion for determining the interdependence of security and dependability factors and minimize the functions of cybersecurity in the design of new systems. The practical component of the study is aimed at determining the criteria of dependability and cybersecurity.

The following tasks were set to achieve this goal:

- To define ontologies of essences of information conflict.
- Build a model of dependability and cyber protection.

4. Materials and Methods of Research

The object of study is explained by considering that any image transferring operation through a noisy medium will corrupt the original image with some unrequired noise; the operation for removing noise from this corrupted image may take different scenarios and ways. The denoising process is evaluated using some performance index such as peak signal to noise ratio.

In this paper it is required to apply a new proposed wavelet based thresholding method for denoising image and improve its PSNR over other traditional methods. The subject of study is the image denoising methods used in recent researches and a comparative study among them using some comment performance index. The purpose of the work is to improve the image quality using wavelet based denoising method with new proposed thresholding technique known as siny-soft wavelet thresholding.

5. Problem Statement, Materials, and Methods

Through most of the image transportation operation the image will face some types of noise, so in order to keep the original image qualified, it is recommended to denoise the noisy image prior to impellent further processing on it, in order not to get bad results and conclusions.

So in this paper a new proposed thresholding method is implemented for image denoising based wavelet transformation in order to enhance the image quality.

Recent years, many researches deal with new methods for signal and image denoising. Some researches for image denoising can be summarized as follows. Novel denoising method known as adaptive non local means with method for noise thresholding, such that image quality can be improved with about PSNR 33.8 dB [22].

Other researches in biomedical engineering deals with ultrasound rental images and use curvelet and contourlet transformations in order to reduce the noise from the corrupted image [23].

Wavelet based researches play an important rule in the image denoising, one of the recent paper proposed a self-adaptive hierarchical threshold algorithm and make a comparative study for it with a global threshold selection algorithm. Self-adaptive method shows a better performance due to tracking for noise level rate instantiously with threshold selection at each level [24].

Another authors proposed another techniques for noise reduction in image enhancement. Garrote, SCAD, mixed and FDR rules are some methods used in their papers for denoising images and signals. The results for their process are qualified using SNR and MSE performance measures [25].

Other comparative study for different wavelet based denoising algorithms was introduced by researchers with several thresholding techniques such as visushrink, sure shrink, Bayes shrink, and feature adaptive shrinkage. All these techniques are evaluated using PSNR as a quantitate performance index [26, 27].

Bivariate shrinkage rule is also proposed by researchers who proposed using the advantage of both types for dual tree and orthogonal wavelet transform in their complex form to improve the shrinkage model significantly [28], to define the criteria of multimedia colors [29, 30].

The core for any comparison study is the suitable selection for a common performance index and dimension for evaluated parameters. So in denoising methods PSNR and MSE represent the most popular performance measure in this field. When considering wavelet denoising technique for image quality enhancement, there are different threshold selection rules and various thresholding methods in the literature of wavelet analysis.

Although the wavelet image denoising procedure can be summarized by three steps:

1. Calculation for wavelet transform coefficient for the image with suitable wavelet mother function, decomposing level, and simple wavelet or wavelet packet tree technique.
2. Thresholding the coefficients using some of the thresholding method with proper selected threshold based on some statistical rules relating to the estimated noise level.
3. Reconstruct the denoised image using the threshold coefficients and the same used wavelet mother function and levels.

6. Experiments

In this work, at the beginning a simple comparison for various wavelet mother functions based denoising techniques was established and tabulated in Table 1. After considering these different wavelet mother functions, Biorthogonal 5.8 wavelet mother function showed the best results among the compared mother functions when using a peak signal to noise ratio PSNR as a popular performance index. In this experiment three values for the noise variance are examined which are 10, 20, and 30. Lena image is used as a test image with 256×256 dimensions, and additive white Gaussian noise adopted and added to the original signal in order to evaluate the proposed thresholding method.

Table 1

Comparison for various wavelet functions at different nose levels

Wavelet	Db6	Sym6	Coif6	Bior 5.8
σ		PSNR Value		
10	31.46	34.73	33.23	40.12
20	29.07	31.58	31.65	38.31
30	27.29	28.78	28.78	35.78

Then a proposed wavelet based denoising algorithm is evaluated using siny-soft thresholding with suitable selected threshold. The PSNR results for some denoising methods in literature are taken from corresponding researches and tabulated in Table 2 for further comparison with the proposed siny-soft thresholding.

In this paper, a new wavelet based thresholding method is suggested as shown in Fig. 1 in order to improve the quality for the image under test. The proposed method can considered as a manipulation for the classical soft thresholding method, after addition for sinusoidal signal in the region out of the dead zone yielding a new siny-soft thresholding function. In addition to that, two fine tuning coefficients are augmented in the proposed thresholding equation to control the value and scale for the sinusoidal peaks in the passband region.

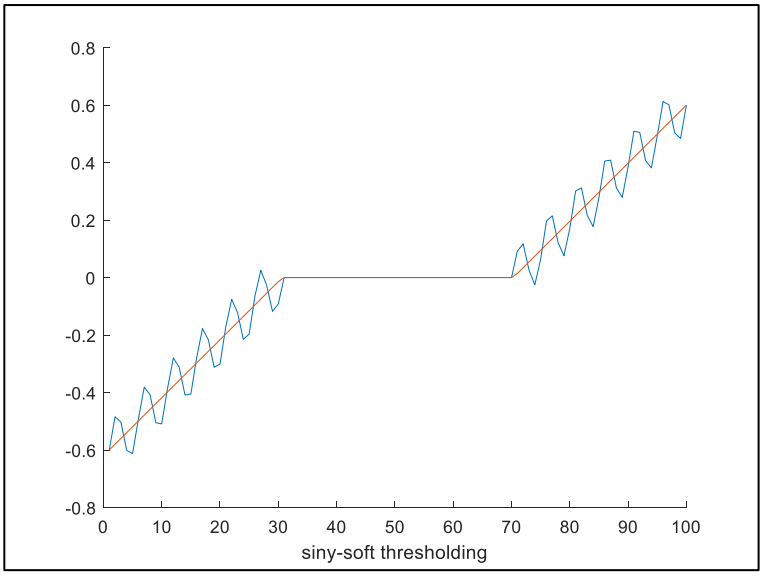

Figure 1: Proposed Siny-soft wavelet thresholding

Table 2

Comparison for various denoising methods with the proposed method

σ	10	20	30
Method		**PSNR Value**	
WT [22]	27.36	24.97	23.97
GBFMT [22]	33.07	29.23	27.19
WFRT [22]	33.23	28.94	26.71
ANLMNT [22]	33.80	30.34	28.11
Curvlet [23]	36.27	—	—
Contourlet [23]	39.84	—	—
Wavelet hierarchical threshold [24]	—	22.82	—
Wavelet global threshold [24]	—	21.40	—
Visu hard rule [25]	21.50	18.55	16.21
Visu soft rule [25]	18.60	15.95	14.23
Visu garrote rule [25]	20.10	16.91	15.6
Visu SCAD rule [25]	19.03	15.95	14.13
Visu Mixed rule [25]	23.12	19.23	17.01
Visu hard [26]	35.35	34.19	33.64
Visu soft [26]	34.45	33.71	33.27
B-M hard [26]	35.52	34.7	33.98
B-M soft [26]	34.64	34.24	33.85
Sime-soft [26]	36.29	34.31	33.10
SURE [26]	33.46	33.22	33.00
Bayes [26]	37.29	35.85	34.97
FAS [26]	36.78	34.73	33.45
Mean filtering [26]	36.07	33.63	32.13
Median filtering [26]	34.79	32.14	30.62
ST [27]	31.28	—	24.52
HT [27]	32.69	—	24.52
POAC [27]	30.09	—	24.53
Bayes shrink [28]	33.32	30.17	28.48
Adapt shrink [28]	31.07	—	—
HMT [28]	33.84	30.39	28.35
Lawmap [28]	34.10	30.89	29.05
Proposed in [31]	33.94	30.73	28.94
Complex [28]	35.34	32.40	30.54

Proposed in [32]	34.36	31.19	29.41
SI-adaptshr [28]	—	32.12	—
CHMT [28]	34.90	—	—
The system in [33]	34.96	31.72	—
The system in [33]	35.31	32.31	—
Our proposed work (siny-soft)	40.12	38.31	35.78

Here under some of mathematical models for the well-known thresholding method in corresponding with the proposed method:

Soft thresholding

$$Q_j=\begin{cases}\left[sign\,(W_j)(|W_j|-\lambda)\right] & |W_j|\geq\lambda\\ 0 & |W_j|<\lambda\end{cases} \quad (1)$$

Hard thresholding

$$Q_j=\begin{cases}W_j & |W_j|\geq\lambda\\ 0 & |W_j|<\lambda\end{cases} \quad (2)$$

Siny- Soft thresholding

$$Q_j=\begin{cases}\left[sign\,(W_j)(|W_j|-\lambda)\right] & |W_j|>\lambda\\ +asin(b\pi W_j) & \\ 0 & |W_j|\leq\lambda\end{cases} \quad (3)$$

where Q_j is an output signal from wavelet thresholding at level j, W_j is an input signal to wavelet thresholding at level j, λ is a threshold.

7. Results

The simulation results for Matlab program demonstrates that wavelet based siny-soft thresholding technique improves the noise reduction and denoising performance in term of PSNR.

Referring to Table 1, three values for noise level are used to artificially corrupt the original image. Various wavelet mother functions are examined and compared using five decomposing level and proposed siny-soft thresholding with universal threshold.

From Table 1 biorthogonal 5.8 wavelet function is succeed as compared to other used functions, so further analysis for wavelet denoising will use this mother function in order to compare this new proposed method to other methods listed in the researches and literature.

Table 2 shows the summarized results for more than 11 references which were used image denoising with different methods and techniques. Three noise level are considered and PSNR values for about 30 experiment's by other researchers, our proposed method showed a good results for denoising for different noise level which are PSNR about 37.12, 35.31, and 33.78 dB for noise variance of 10, 20, and 30 respectively.

Results for denoising are also demonstrated by Fig. 2–5 which shows the enhancement for Lena image in three cases for various noise levels.

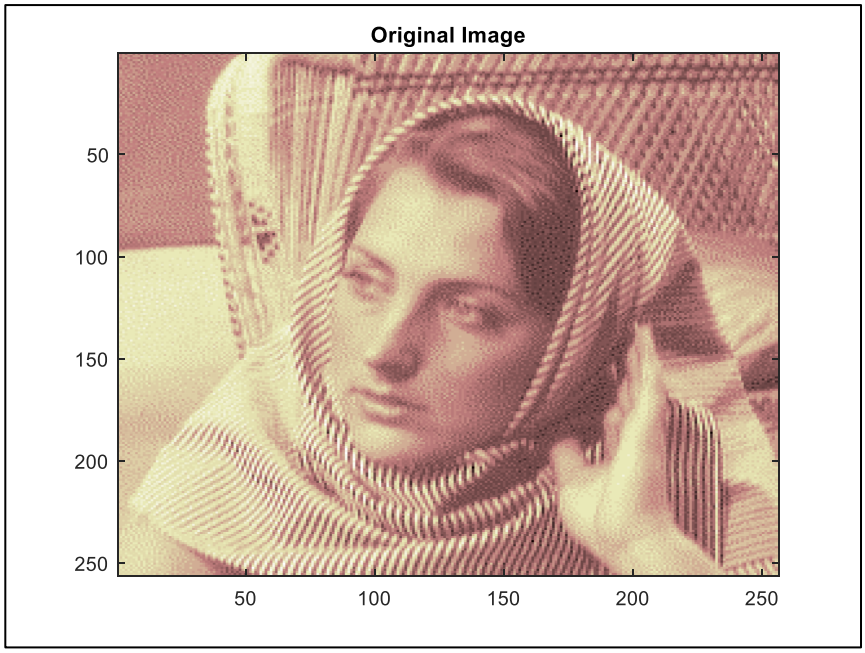

Figure 2: Original noiseless Lena image

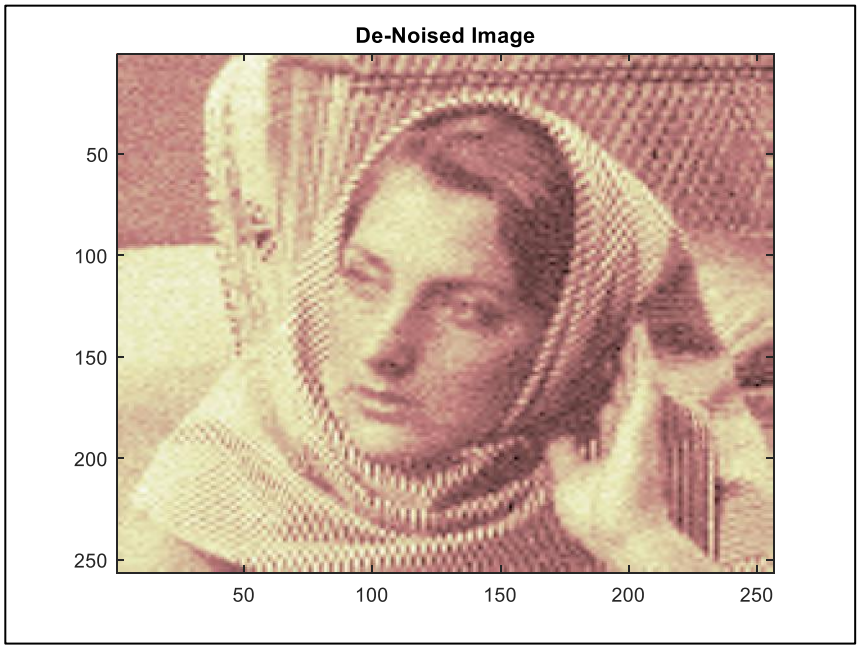

Figure 3: Denoised image using siny_soft for σ = 10 noise level

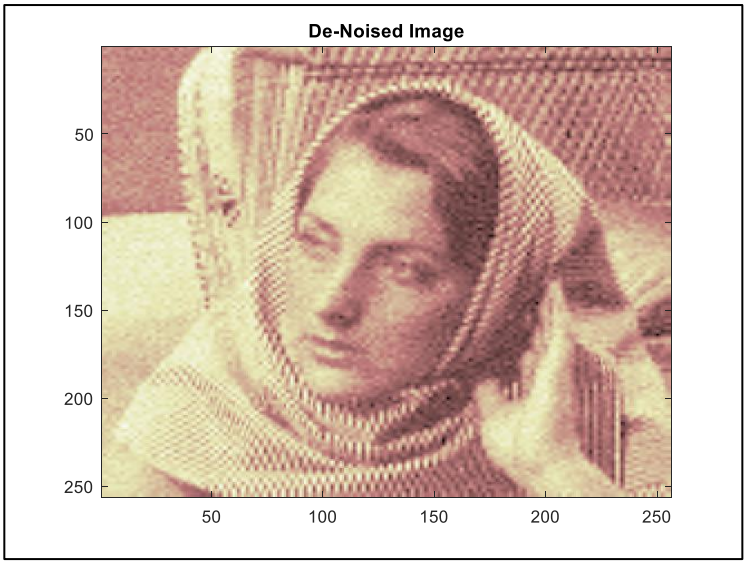

Figure 4: Denoised image using siny_soft for σ = 20 noise level

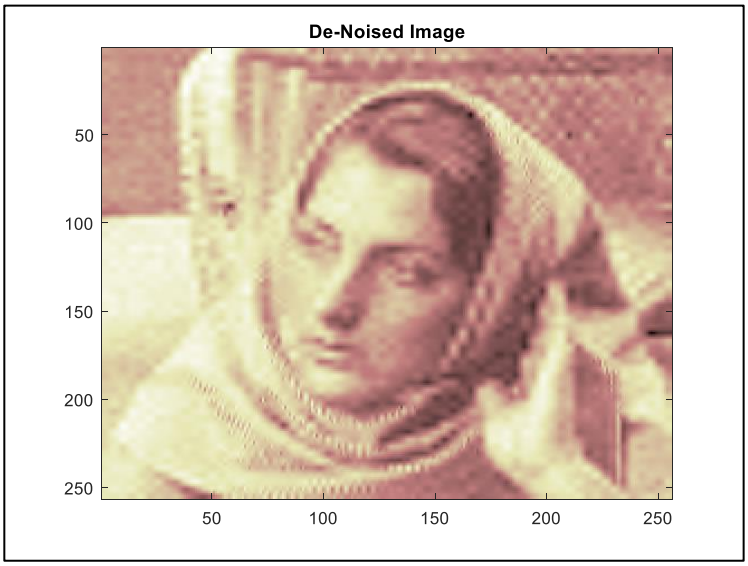

Figure 5: Denoised image using siny_soft for σ = 30 noise level

8. Discussion

Results for denoising methods showed many algorithms with different PSNR values, increasing noise level will degrade the performance of the denoising method as shown in Table 2 when comparing the results for the same used method at the same row , but with increasing noise level from σ =10 to 30.

It is recommended for further studies to examine different types for noise with various wavelet functions and decomposition level, also other performance metric such as MSE can be involved in conjugation with PSNR for further evaluation emphasis.

9. Conclusions

A new proposed wavelet based siny-soft thresholding is proposed in this work. Simulation results of the present method declared that the denoised images resulted from the proposed algorithm have an improved PSNR value when they are compared with other denoising method .so based on these result the proposed thresholding is suited for image denoising when images are corrupted with different types of noise. It is recommended to use the proposed thresholding for further studies of image or signal

processing, especially for signal and image enhancement using wavelet based denoising or compression methods. The scientific novelty for the conducted results is that the method for siny_soft thresholding is firstly proposed. The method shows good results as compared with traditional used methods for image denoising. Acceptable values for PSNR are achieved when using this new proposed method.

The practical significance of the achieved results is that the new proposed method can be adopted deeply in image enhancement problems for further image processing applications. It is recommended to use wavelet based image denoising with siny_soft thresholding for improving PSNR of an image.

Prospects for further research are to study the possibility for extended the implementation of the proposed thresholding for further signal and image applications.

10.Acknowledgements

The work is supported by the computer communication engineering department at Al-Rafidain University College represented by its dean Prof. Dr. Mahmood J. Abu-Alshaeer. So I would like to express my sincere appreciation to Prof. Dr. Mahmood J. Abu-Alshaeer for his help, support, and encouragement during all the periods of my employment.

11.References

[1] Grechaninov, V. (2021). On the Concept of Digital Transformation of the Sphere of National Security and Defense. Technical Sciences and Technology, 3 (25), 179–186. doi: https://doi.org/10.25140/2411-5363-2021-3(25)-179-186

[2] Grechaninov, V. F. (2021). Some issues of improving the network of situational centers of the security and defense sector. Mathematical Machines and Systems, 3, 34–46.

[3] Kharchenko, V. S. (2006). Assurability and Assurable Systems: Elements of the Methodology. Radio Electronic and Computer Systems, 5, 7–19.

[4] Skopik, F. (2019). The limitations of national cyber security sensor networks debunked: Why the human factor matters. Proceedings of the 14th International Conference on Cyber Warfare and Security, 405–412.

[5] Simankov, V. S., Cherkasov, A. N., Buchatskaya, V. V., Teploukhov, S. V. (2021). Situational center as an intelligent decision support system taking into account the uncertainty of the source information. Proceedings of the 4th All-Russian Scientific and Practical Conference with International Participation "Distance Learning Technologies," 2834, 404–414.

[6] Janos, F. D., Dai, N. H. P. (2018). Security concerns towards security operations centers. Proceedings of the IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, Proceedings, 273–278. doi: https://doi.org/10.1109/SACI.2018.8440963

[7] Yandybaeva, N., Rezchikov, A., Gorschkov, E., Bogomolov, A., Kuschnikov, V. (2020). Mathematical models and algorithms for forecasting national security in training situational centers. Proceedings of 2020 13th International Conference Management of Large-Scale System Development, doi: https://doi.org/10.1109/MLSD49919.2020.9247640

[8] Tesler, G. S. (2006). The Concept of Building Guaranteeing Computer Systems. Mathematical Machines and Systems, 1, 134–145.

[9] Fedukhyn, A. V., Sespedes Harsiya, N. V. (2013). Attributes and Metrics of Guaranteed Computer Systems. Mathematical Machines and Systems, 2, 195–201.

[10] Hlukhov, V. S. (2008). Assessing the Security of Cryptographic Computer Systems. Bulletin of the National University "Lviv Polytechnic," 616, 66–72.

[11] Hulak, G. N. (2011). Modeling at the Stage of Assessing the Security of Encryptors of Confidential Information. Modern Special Equipment, 1 (24), 73–81.

[12] Hulak, H. M. (2018). Evaluation of Engineering Cryptographic Qualities during Thematic Research of Cryptosystems. Proceedings of the International Scientific and Practical Conference "Mathematical and Simulation Systems Modeling—MODS'2018," 326–330.

[13] Sespedes Harsiya, N. V. (2014). Assess the Level of Confidentiality of Guaranteed Computer Systems. Mathematical Machines and Systems, 3, 158–164.

[14] Cabinet of Ministers of Ukraine. (June 19, 2019). Resolution “On Approval of the General Requirements for Cyber Protection of Critical Infrastructure,” 518.
[15] Information Technology. Security Techniques. Test and Analysis Methods for Random bit Generators within ISO/IEC 19790 and ISO/IEC 15408. (2019). doi: https://doi.org/10.3403/30356052
[16] Bondaruk, A. V., et al. (2008). Guaranteed Integrated Navigation System for Moving Ground Objects. Bulletin of Lviv Polytechnic. Computer Systems and Networks, 620, 24–30.
[17] Hulak, H. M. (2020). Methodological Ambush and Protection of Guaranteed Information Systems for Remote Learning of Mortgages of Higher Education. Mathematical Machines and Systems, 4, 148–162.
[18] Avizienis, A., et al. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Trans. on Dependable and Secure Computing, 1 (1), 11–33. doi: https://doi.org/10.1109/TDSC.2004.2
[19] TajDini, M., Sokolov V., Buriachok V. (2019). Men-in-the-middle attack simulation on low energy wireless devices using software define radio. Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education": Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 287–296.
[20] Buriachok, V, et al. (2020). Invasion detection model using two-stage criterion of detection of network anomalies. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), vol. 2746, 23–32.
[21] Vladymyrenko, M., et al. (2019). Analysis of Implementation Results of the Distributed Access Control System. 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), doi: https://doi.org/10.1109/picst47496.2019.9061376
[22] Lakhno, V., Plyska, L. (2021). Analysis of Models for Selection of Investment Strategies. Proceedings of the 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, 43–46. doi: https://doi.org/10.1109/PICST51311.2020.9468024
[23] Lavrova, D. S., Solovei, R. S. (2020). Ensuring the Information Security of Wireless Dynamic Networks based on the Game-Theoretic Approach. Automatic Control and Computer Sciences, 54 (8), 937–943. doi: https://doi.org/10.3103/S0146411620080210
[24] Montet, C. D. (2003). Serra Game Theory and Economics. Red Globe Press.
[25] Wang, S., et al. (2021). A Differential Game View of Antagonistic Dynamics for Cybersecurity. Computer Networks, 200. doi: https://doi.org/10.1016/j.comnet.2021.108494
[26] Information technology. Security techniques. Guidelines for cybersecurity. ISO 27032. (2012).
[27] Dibaji, S. M., Hussain, A., Ishii, H. (2022). A Tutorial on Security and Privacy Challenges in CPS. doi: https://doi.org/10.1007/978-3-030-83236-0_5
[28] Ghosh, S., Jaillet, P. (2022). An Iterative Security Game for Computing Robust and Adaptive Network Flows. Computers and Operations Research, 138. doi: https://doi.org/10.1016/j.cor.2021.105558
[29] Yi, N., et al. (2021). A Multi-Stage Game Model for the False Data Injection Attack from Attacker’s Perspective. Sustainable Energy, Grids and Networks, 28. doi: https://doi.org/10.1016/j.segan.2021.100541
[30] Hunt, K., Agarwal, P., Zhuang, J. (2022). On the Adoption of New Technology to Enhance Counterterrorism Measures: An Attacker–Defender Game with Risk Preferences. Reliability Engineering and System Safety, 218. doi: https://doi.org/10.1016/j.ress.2021.108151
[31] Nisioti, A., et al. (2021). Game-Theoretic Decision Support for Cyber Forensic Investigations. Sensors, 21 (16). doi: https://doi.org/10.3390/s21165300
[32] Myshanov, R. O. (2017). Investigation of the Signs, Types, Causes, and Mechanisms of Failures of Microcircuits Made using CMOS Technology. Proceedings of the International Symposium “Reliability and Quality,” 2, 228–234.
[33] Vlasova, A. M., Andreev, P. G., Naumova, I. Y. (2016). Reliability and Quality of Electronic Equipment. Proceedings of the International Symposium “Reliability and Quality,” 1, 313–314.